Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

TRABAJO FINAL DE MAESTRÍA

Supremacía por la información y la dominación cognitiva de las sociedades.

Inteligencia aplicada a operaciones de guerra híbrida.

AUTOR: ESP. ING. ALBIOL PEDRO

DIRECTOR: MBA BRIG. MAYOR(R) MORESI ALEJANDRO

OCTUBRE 2022

REVISIÓN 2023

Documento con fines educativos y académicos. No se autoriza su publicación.

Notas de autor

El capítulo 0 es una sección preliminar que expone los conceptos básicos en seguridad de la información. El objetivo es nivelar los diferentes perfiles y evitar un glosario de términos que solo interrumpirían la lectura. Este capítulo expone los conceptos de forma simple y básica. Sin embargo, al mismo tiempo aporta detalles y ejemplos técnicos, a fin de mantener la atención de los diferentes perfiles de lectores.

El capítulo 1 corresponde a la sección principal del trabajo. La dominación a través de la guerra híbrida y sus operaciones mediante el uso de todos los medios para lograrlo, incluyendo medios no convencionales. El mismo presenta foco en la ciberguerra y particularmente en la guerra psicológica. A su vez, menciona otros aspectos como la guerra económica, entre otros. En dicho capitulo se explica como la inteligencia alimenta algunas operaciones.

El trabajo exhibe hechos históricos relevantes para el trabajo; dado que no es posible determinar la proyección futura de la sociedad, con relación a las TICs, si no comprendemos los orígenes descriptos. Los diferentes sucesos históricos investigados surgen de diversas fuentes, al cual se ha aplicado un esfuerzo a fin de intentar eliminar los sesgos existentes. Vasta tarea dado los mismos, la propaganda, la desinformación y las omisiones encontradas en la actualidad. Dicha investigación ha permitido comprender diversos aspectos históricos, reaprendiendo de los mismos en la labor de abandonar los prejuicios o ideas erróneas.

Aun así, quedo a disposición para realizar correcciones pertinentes ante cualquier error u omisión. Por otra parte, insto a que los investigadores puedan ampliar en el tema estudiado.

A lo largo del trabajo, la idea original ha ido cambiando en base a las evidencias encontradas. Muchas referencias históricas corresponden a EE.UU. como foco principal debido a diferentes motivos aquí detallados. Por una parte, como potencia dominante, presenta una preponderancia histórica en cuanto a la influencia; tanto a nivel regional como internacional. Además, es un precursor en las TICs; incluyendo internet y los gigantes tecnológicos que hoy en día están presentes en nuestra sociedad. Por otra parte, al tratarse de una democracia (con cambio de funcionarios); es más propenso a documentar, transparentar y eventualmente desclasificar información. Si bien veremos que esto no

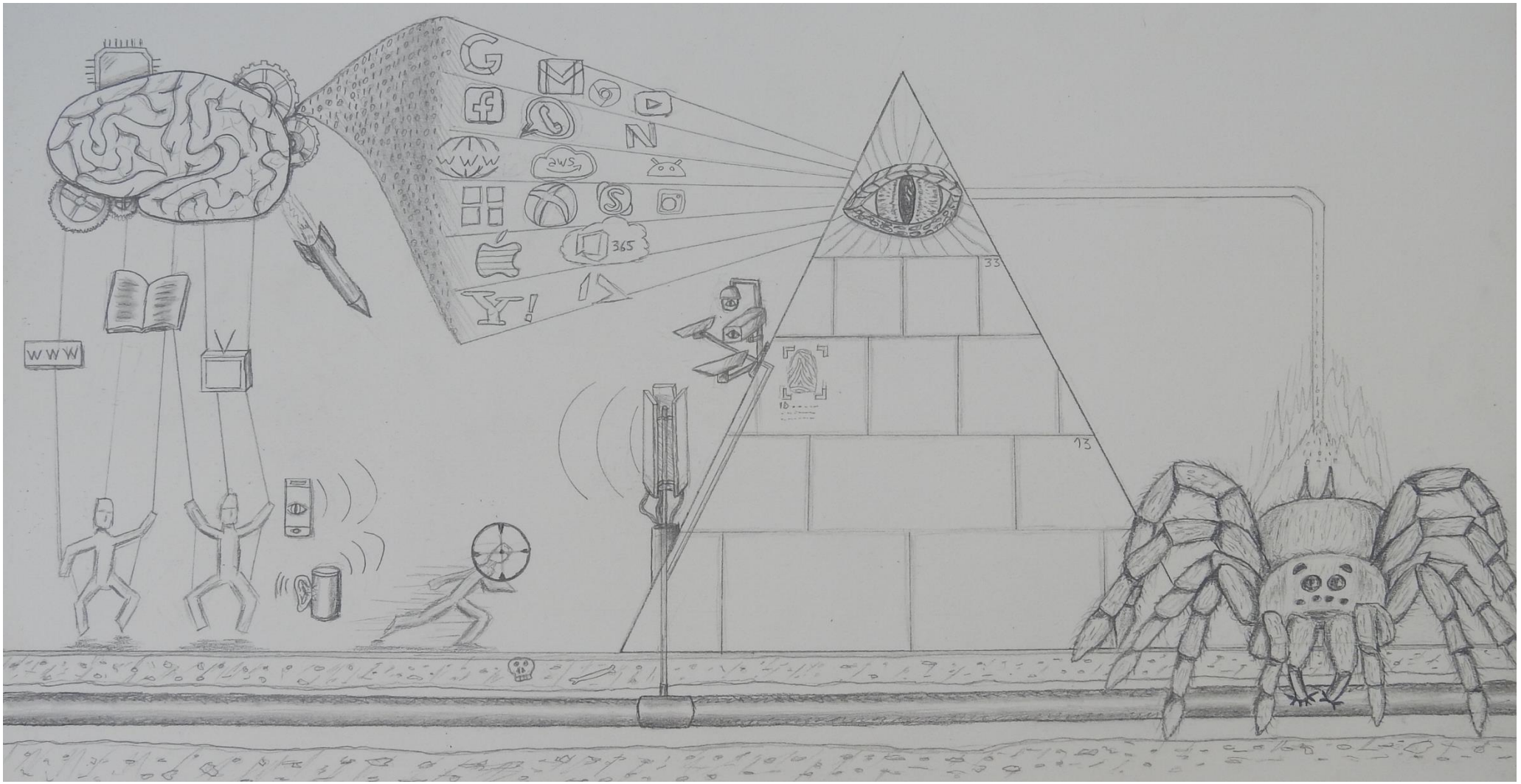
siempre ocurre; en general las investigaciones del senado y la desclasificación son elementos importantes a la hora de comprender la historia.

Desarrollar los mismos aspectos desde la óptica de otros países como Rusia o China sería deseable. Sin embardo, dicha labor escapa los alcances del presente. Por otra parte, las conclusiones difícilmente puedan variar al respecto. Ello se debe a que los países, en mayor o en menor medida, buscan objetivos similares. En el fondo todos los países están conformados por seres humanos. La diferencia reside en sus recursos, estrategias o nivel de agresividad.

El capítulo 2 amplía los diferentes medios de adquisición de información a través de inteligencia sin límites. También menciona las implicancias de ataques sobre la cadena de suministro en equipamiento de cifrado; siendo estos no tan seguros como deberían.

A lo largo del trabajo se intenta exponer algunas aristas de un submundo del que solo conocemos parcialmente. Si bien hay muchos aspectos que pueden ampliarse, es importante el equilibrio entre las evidencias expuestas y una lectura fluida. Los aspectos legales no han sido tratados debido a que implicaría un análisis que se excede de los límites del documento; sumado a las contradicciones entre leyes y jurisdicciones. Sin embargo, insto a que otro maestrando pueda desarrollar el asunto en cuestión.

El capítulo 3 estudia el caso del proyecto Cóndor y su sabotaje: identificando acciones de guerra sin límite. Mientras que el capítulo 4 es un capítulo de soporte que refleja diferentes ciberataques mediante antecedentes históricos. Mientras que el capítulo 4 representa una formalidad del cierre del trabajo. Los dibujos de la tapa y contratapa son de mi autoría.


G
M
N
aws
S
365
Y!
WWW
33
13

Índice:

Resumen ***1***

Metodología ***1***

Introducción (rompiendo el hielo). ***3***

Capítulo ~~(1)~~ Ares – Una guerra invisible por la dominación. ***8***

Consideraciones preliminares. **8**
Arquitectura Von Neumann y la ética en las TICS. 8
Ataques a los sistemas de información. 15

Definiciones iniciales: Kill Chain y evolución. **16**
Marco de referencia Intrusion Kill Chain / Cyber Kill Chain®. 18
Marco de referencia Unified Kill Chain. 21
Marco de referencia Mitre ATT&CK®. 23

Guerra cibernética (Cyberwarfare). **27**
Guerra de información (Information operation / Information warfare) 27
Operaciones en redes de computadoras (Computer network operations - CNO). 28
Operaciones psicológicas (Pyschological Operations - PSYOP). 29
Engaño militar (Military deception - MILDEC). 31
Operaciones de seguridad (Operation security - OPSEC). 32
Guerra electrónica (Electronic Warfare - EW). 32
Operaciones de información y psicológicas de la Central de Inteligencia. 34
Actores en las operaciones de ciberguerra. 36
Individuos solitarios. 36
Grupos no organizados. 37
Grupos organizados (hackers, militares, terroristas, entre otros). 37
Características del teatro de operaciones. 40

Guerra sin limites (Unrestricted warfare). **44**
Rusia / OTAN. 45
Operación Gladio y Cóndor. 50
Un único proceso histórico. 54
¿Guerra cultural y en el deporte? (Cultural / Sports warfare) 55
Corromper pilares (Pillar warfare). 56
Guerra económica (Economic warfare). 56
Deuda. 58
Asesinato económico y de identidad. 60
Guerra biológica / química (Biological / Chemical warfare). 60
Guerra del clima (Weather warfare). 63
Hackear y arrojar (Hack and Dump). 64
Guerra judicial (Lawfare). 65
Asesinatos de objetivos. 67
Caso bomba chocolate (Chocolate bomb). 68
Caso pistola de cianuro (Poison gas gun). 69
Caso píldoras tóxicas. 70
Caso pistoleros y objetivos equivocados (Gunmen / Wrong target). 72
Caso paraguas búlgaro (Bulgarian Umbrella). 72
Caso pistola para asesinatos sigilosos (Nondiscernible microbionoculator / Dart Gun). 73

Caso con explosivos 74
Caso Polonio-210. 74
Caso gas nervioso (Novichok) 75
Caso trampa en embajada (Embassy trap). 75
Caso drones asesinos (Killer drones). 76
Ataques falsa bandera (False flag). 78
Caso Himmler Operation - Gleiwitz Incident (1939). 79
Caso Masacre de Katyn (1940). 79
Caso Operation Embarrass (1946-1949). 79
Caso Operation Susannah - Lavon Affair (1954). 80
Caso COINTELPRO (1961-1971). 80
Caso Siria: complot de asesinato (1957). 82
Caso Operation Northwoods (marzo de 1962) 82
Caso Léonie Duquet y Alice Domon (1977). 84
Golpes blandos 85

Guerra cognitiva (Cognitive Warfare). 87
Asesinato de personaje (Character assassination). 92
Dualidad nosotros vs ellos, buenos vs malos. 96
Ataques de argumento ad hominem (Ad Hominem attack). 97
Ataques de silogismo entimema (Enthymematic attack). 98
Ataque mediante malversación de citas (Misquoting attack). 98
Ataque de culpabilidad por asociación (Guilt by association attack). 98
Asesinato de personaje en el ciberespacio (CA in the cyberspace). 98
Desconexión moral en el ciberespacio (Moral disengagement in cyberspace). 99
Asesinato por intimidación (Intimidation Kill Attack). 100
Medios de comunicación y propaganda. 101
Producción cultural. 107
Autoritarismo psicológico (PsycoAutoritarism). 109
¿Invasión cultural? 110
Crear un evento para promover cambios. 111
¿Disrupción cognitiva emocional? 111
¿Sentimiento de culpa? 112
Redes sociales. 112
Creando realidades. 114
Modificación del comportamiento (Behavior modification). 115

Diagrama de Dominacion y operaciones Kill Chain (Domination – Kill Chain Operations diagram) 122

Marco de dominación (Domination Framework) 124

Algunos conceptos claves del capítulo. 128

Capítulo (~~2~~) Hadēs – Inteligencia y vigilancia masiva 130

Medios para la adquisición de inteligencia (Inteligence gathering). 130
Inteligencia humana (HUMINT). 132
Inteligencia de fuentes abiertas (OSINT). 134
Inteligencia geoespacial (GEOINT). 139
Inteligencia de firma electrónica (MASINT). 141
Inteligencia de señales (SIGINT). 141
Satélites 142
Guerra en el espacio. ..... **¡Error! Marcador no definido.**

Inteligencia sin restricción.....148
Escucha a distancia e implantes. 152
Intercepcion de teléfonos celulares y satelitales. 154
Regalos con sorpresas inesperadas – The Great Seal. 159
Visión remota (Van Eck phreaking). 161
Area 51. 163
Vehículos aéreos no tripulados (UAV: Unmanned Aerial Vehicle). 164
Utilizacion de animales. 167
Rocas espias. 171
Infiltrados. 172
Robos. 174
Caso Project Azorian / Jennifer. 174
Caso Operation Mount Hope III. 176
Abuso judicial. 176
VPN y trackings. 178
DNS, eMail y Browser. 179
Cursos y programas de intercambio. 179
Software, Antivirus y telemetría. 181
Hack. 182
Caso Pegasus Spyware 182
Caso FinFisher / FinSpy / Wingbird Spyware 184
Hack^2 = hack the hacker. 188
Caso Operation ARROW ECLIPSE 188
Cámaras de vigilancia. 189
Intercepción de correspondencias y mensajería. 192
Tarjetas de crédito, consumo de energía y otros servicios. 193

USACORP agreement. 195
El poder dominante de las corporaciones. 196

Filtraciones ANT catalog (leak). 198

Filtraciones Vault 7 (leak).....202
Caso hackeo de automóviles (Car hacking). 204

Caso Shadow Brokers (leak). 206
Caso Fuzzbunch 208
Caso EternalBlue exploit 208
Caso Double pulsar Backdoor 209
Caso PaddleCheap Implant 209
Caso DanderSpritz Framework 210
Caso Operation Telescreen - Bvp47 Backdoor 216

Eavesdrop y Vigilancia. 219
Filtración de datos de Snowden (Snowden leak). 220
Acuerdo originalmente secreto entre Reino Unido y Estados Unidos (UKUSA Agreement) (1946). 222
Programa SHAMROCK (1945-1975). 223
Proyecto MINARET (1969-1973). 223
Programa FROSTING (TRANSIENT + ECHELON) 224
Vigilancia masiva. 225
Caso Operation Ivy Bells 233
Programa WINDSTOP. 234
Caso Programa MUSCULAR (DS-200B). 234
Caso INCENSER (DS-300). 235

Programa RAMPART-A. 238
Caso EIKONAL / GRANAT Operation (2004-2008) 240
Caso Dunhammer Operation 240
Caso Athens Olympic Games 242
Sistema XKEYSCORE 242
Caso Hack Cellphone SIMs 244
Suit QUANTUM - FOXACID 244
Caso Operación Socialist. 247
Programa Downstrem collection (PRISM) 247
Programa Upstream collection 251
Project X (TITANPOINTE) 253
Bumblehive - Centro de datos en Utah (Utah Datacenter). 256
Servicio de recolección especial (Special Collection Service). 258
Caso Olympia. 261
Breve mención de Rusia. 261
La trampa del vigilante. 262
El verdadero poder de las revelaciones sobre la vigilancia. 263

Contramedidas. 264
Paradoja del cifrado. 265
Caso ENIGMA. 265
Caso MINERVA y la vinculación con la guerra de Malvinas (Operación THESAURUS/ RUBICON) 273
Caso BULLRUN 275
Caso SENTRY EAGLE 276
Desinformación y engaño. 277

Algunso conceptos claves del capítulo. 280

Capítulo ~~(3)~~ Fobos y Deimos – Antecedentes en ciber operaciones. 283

Operaciones contra la infraestructura crítica. 289
Caso Operation Olympic Games 290
Vulnerabilidad Aurora. 293
Stuxnet y la caja de pandora en los ICS. 294
Caso Shamoon 294
Caso Steel Mill blow 295
Caso Irongate 296
Caso BlackEnergy 297
Caso Industroyer / Crash Override 298
Caso Havex 300
Caso Triton / Trisis / HatMan 301

Ciberoperaciones de espionaje 302
Caso Moonlight Maze 302
Transferencia de tecnología. 303
Caso Flame / Skywiper. 304
Caso Fanny (2008) 305
Caso DoubleFantasy 306
Caso EquationDrug (2003-2013). 306
Caso GrayFish (2008-2013) 306
Caso Regin 308
Caso Gauss 309
Caso Duqu 310
Caso Operation Cleaver 311

Caso Operation SNOWGLOBE 312

Ciberoperaciones de guerra electrónica en drones.....313
Caso Skygrabber ($25) Vs Predator ($40 Millon). 313
Caso captura de drone (RQ-170 catch and troll). 313

Ciberoperaciones a la cadena de suministro. 314
Caso Juniper Backdoor. 314
Caso Tiny Chip - Big Hack. 315
Breve mención Intel Management Engine. 316
Caso SUNBURST Backdoor. 318

Ciberoperaciones en procesos electorales. 319
Caso Elecciones de Ucrania. 319
Caso Guccifer 2.0 320
Caso Elecciones de Francia. 321

Ciberoperaciones en sistemas financieros. 321
Caso Operation Ababil. 321
Caso robo bancario (Bank Heist). 322
Caso Deep Voice. 323

Ciberoperaciones con Deep Fake (IA). 324

Conceptos claves del capítulo. 325

Capítulo ~~(4)~~ Kairós – Estrategia Argentina.....327

Estrategia Argentina. 328
Sabotaje y robo tecnológico: Caso Proyecto Cóndor. 283

Futuros Peligros.....330

Futuras investigaciones.....332

Apéndices.....334

Capítulo apéndice: ~~(0)~~ Krónos – Conceptos Básicos.....334

Principios de seguridad de la información. 334

Internet: la red de redes. 341

Ataques a los sistemas de información.....344
Vulnerabilidades y exploits. 344
Vulnerabilidades a nivel hardware. 346
Vulnerabilidades a nivel Sistema Operativo. 349
Vulnerabilidades a nivel usuario (Social Engineering). 351
Vishing 353
Phishing 354
Spear Phishing 354
Baiting 354
Typosquatting 356
Comunicación no verbal 357
Vulnerabilidades a nivel comunicaciones. 357
DNS hijacking 357
Sniffing. 357

Man in the middle (MITM). 359
Vulnerabilidades en la cadena de suministro 360
Drive by download / Watering hole attacks. 360
Vulnerabilidades en la disponibilidad 361
Denial of service (DOS) attacks. 361
Distributed denial of service (DDOS) attacks. 364
Jammers 365
Sabotaje 366
Vulnerabilidades a nivel aplicación. 367
Race condition/ TOCTOU attacks 368
Clickjaking. 369
Use after free 369
Directory traversal attack 370
SQL injection 370
Malware attacks. 371
Virus 374
Worm 374
Fileless 375
Macrovirus 375
Tojan Horse 375
Logic bomb 375
Botnet. 376
Rootkit 376
Bootkit 376
Wiper 378
Ransomware 378
Cryopto minners. 378
Backdoor 378
Malware as a service 379
Rogue security malware 379
Spyware 379
Exfiltration 379

Conceptos básicos de cifrado. 380
Esteganografía. 380
Book cipher. 382
Criptografía. 382
Criptografía moderna. 386
Public Key Infrastructure (PKI). 386
Vulnerabilidades a los sistemas criptográficos. 387

Conceptos claves del capítulo. 389

Referencias bibliográficas 392

Resumen

El presente trabajo se encuentra enfocado en la investigación y análisis de los peligros actuales de las operaciones de ciberguerra, guerra de la información y guerra psicológica: cómo son planificadas y ejecutadas en el concepto *kill chain* (inteligencia, toma de decisión y acción). Las mismas van desde ataques a infraestructura crítica de un país, control de las mentes, ataques de falsa bandera, interferencias en procesos electorales, golpes de estado blandos, implantación de gobiernos títeres, asesinato de personajes, asesinatos a objetivos y transferencia de conocimiento tecnológico, entre otros.

La inteligencia alimenta las operaciones dentro de un esquema de guerra invisible enfocada a la supremacía estratégica y la dominación.

Mediante antecedentes empíricos, queda planteada la importancia de la soberanía tecnológica, de datos y del desarrollo de sistemas nacionales propios e independientes: hardware, sistemas criptográficos, sistemas operativos y aplicaciones en el ámbito nacional y de las comunicaciones.

A partir del planteamiento del problema actual y futuro, se presenta un aporte de ideas y conceptos base que conforman una visión necesaria para la elaboración de una planificación estratégica nacional enfocada a la prevención y mitigación de los riesgos expuestos.

Metodología

La metodología utilizada es un enfoque cualitativo de investigación con un alcance inicial exploratorio y una posterior tendencia explicativa a la hora de comprender los sucesos aislados como un todo, dentro del plano geopolítico. A diferencia del método cuantitativo, no se trata de un proceso secuencial, sino más bien circular. Por naturaleza de la metodología, las preguntas de investigación inicialmente no son definidas claramente; sino que toman forma a medida que la investigación avanza. Por lo tanto, las preguntas e hipótesis se desarrollaron durante / después de la recolección de datos.

La estrategia del método implica observar y evaluar fenómenos (en este caso eventos históricos) que sirven como base para establecer suposiciones e ideas junto a su fundamento (Grinnell, como fue citado por Sampieri, 2018). Como indica Sampieri (2014), el método cualitativo busca la expansión de los datos e información. Utiliza la lógica y proceso

inductivo para explorar y describir hechos empíricos para luego generar perspectivas teóricas, desde lo particular a lo general. Como la mayoría de los estudios cualitativos, no se prueban hipótesis, sino que estas son generadas durante el trabajo. Asimismo, los datos cualitativos no resultan estandarizados ni estructurados. La muestra de datos varía según el contexto y las necesidades a fin de comprender el fenómeno. Se fundamenta por una perspectiva interpretativa de la realidad entre el autor y la perspectiva de las fuentes recolectadas; sin dejar de lado la perspectiva analítica de los sucesos. Sin embargo, la posición del investigador puede ser explicita, reconociendo sus valores y creencias. La investigación es flexible y se construye durante el trabajo. Mientas que el análisis de datos permite generar categorías, describir sucesos y desarrollar temas, dando un significado profundo de los resultados.

El incentivo de la presente investigación es explorar y dar visibilidad a la guerra invisible; como así también los peligros para las sociedades modernas respecto al conflicto del siglo XXI. Donde se explotan diversas vulnerabilidades no limitadas únicamente a las TICS sino también estructuras legales, sociales, democráticas, psicológicas, entre otras. Asimismo, aprovechan las capacidades 5to dominio para potenciar las operaciones de guerra sin límite.

El objetivo principal es exponer las operaciones de los conflictos modernos y manifestar la necesidad de una cultura individual y social en contraposición a la ignorancia / indiferencia colectiva frente a semejante exposición. La consecuencia directa de lo expuesto es la necesidad de desarrollar una visión estratégica nacional frente a los desafíos de las guerras modernas en el 5to domino.

Los objetivos secundarios corresponden:

- Exponer las formas de ataques a los sistemas de información que se detallan a lo largo del capítulo 0.
- A lo largo del resto de los posteriores capítulos (1, 2, 3 y 4) permite informar, advertir y generar cultura sobre los peligros a los cuales estamos expuestos los ciudadanos en el conflicto moderno del siglo XXI y la geopolítica mundial.
- Comprender como la inteligencia es el elemento fundamental para alimentar dichas operaciones (principalmente en el capítulo 2).

- Entender como las operaciones no son el fin, sino el medio estratégico para posicionar estados naciones por sobre otros y garantizar la dominación de las sociedades hasta sus cimientos (capítulos 1, 2, 3 y 4).
- Finalmente, el capítulo 4 proponer una propuesta activa para el conflicto futuro.

La hipótesis que emerge a lo largo del desarrollo del trabajo es como los conflictos modernos han dejado de lado las guerras convencionales para migrar a un plano de operaciones estratégicas no visibles, que a su vez son potenciadas mediante las herramientas de la cuarta revolución industrial aplicadas al 5to dominio (ciberespacio).

Introducción (rompiendo el hielo).

Las guerras convencionales parecen ser cosa del pasado y el teatro de operaciones en la actualidad corresponde al mundo entero, el ciberespacio e incluso el espacio exterior. Si bien algunas operaciones son visibles e impactantes, otras no lo son. Sin embargo, eso no las hace menos peligrosas. Detrás del telón del show de caretas, en la oscuridad, se esconden los peores peligros.

Si bien la definición de ciberguerra puede variar según el autor, en términos generales se trata del enfrentamiento entre grupos con diferentes ideas o intereses dentro del plano de las tecnologías de la información. Similarmente a como dijo Carl Von Clausewitz (1780-1831): "La guerra es la continuación de la política por otros medios"; podría afirmarse que la ciberguerra, es la continuidad de la guerra convencional dentro del plano del ciberespacio. El uso de las tecnologías actuales y venideras ha cambiado las sociedades como así también la manera de ver y de actuar en la guerra. Cada vez las tecnologías son más disruptivas y se asemejan a un esquema de *use it or lose it*[1] junto a *the winner takes it all*[2].

Es importante comprender y tener presente que el objetivo final de la guerra es imponer la voluntad propia por sobre la del oponente. Si dicho objetivo puede obtenerse por un medio

[1] Usarlo o perderlo es el dilema que tiene el defensor frente a un ataque superior que pueda desarmarlo (de cierta forma, lo opuesto a la trampa de Tucídides). Sin embargo, en el 5to dominio, desaparecen las distancias y se incrementa la velocidad de ataque. Como apreciación, la conectividad entre sistemas sumado a la automatización/IA; parecerían desdibujar el concepto de superior/inferior. Siendo el primero el golpear potencialmente el primero en ganar.
[2] El ganador se queda con todo, haciendo referencia al punto anterior.

más eficiente/económico que la guerra, como ser el control de las mentes, entonces no hay necesidad de enfrentamiento en absoluto.

En el quinto dominio del ciberespacio existen una variedad de actores que día a día amenazan la seguridad tanto de individuos, empresas como así también estados/naciones. Dichos actores van desde individuos independientes, grupos de crimen organizado, grupos militares o hackers que cuentan con el aval de estados naciones.

Las operaciones comienzan con la adquisición de información a través de inteligencia de las redes de comunicaciones, intromisiones a empresas/individuos objetivos, robo de datos de organismos públicos, datos disponibles de fuentes abiertas/*leaks* o inclusive a través de aplicaciones o plataformas que diariamente utiliza la población civil y militar. Posteriormente, la recolección de información es utilizada para la toma de decisiones en un mejor posicionamiento geopolítico o es utilizada directamente para planificar y lanzar operaciones de ataques con ciber-armas o incluso *kinetic attacks* (ataques cinéticos) sobre infraestructuras críticas, opositores políticos, manipulación de elecciones, promover revueltas sociales, convencer a la población sobre decisiones de interés, etc.

Nuestro país ha sido afectado sistemáticamente desde hace mucho tiempo por diversos tipos de operaciones, como ser sabotaje de la economía o de proyectos estratégicos /tecnológicos. No resulta casual la actual situación económica crítica con una sociedad fragmentada en odio.

Uno de los inconvenientes más graves a la hora de enfrentar esta problemática es la ignorancia o desconocimiento de esta. Ya que no se puede solucionar lo que no se reconoce o no se comprende. Ignorar la cuestión no hace que el peligro desaparezca, sin embargo, comprenderlo en profundidad tampoco es suficiente. Se requieren medidas proactivas en la materia. Es por eso por lo que resulta imperiosa la elaboración de este trabajo de investigación exploratorio, con el correspondiente planteamiento de los ciber-riesgos y las ciber-amenazas presentes en los nuevos paradigmas de las TIC. Una vez adquirido dicho conocimiento es necesario la elaboración de un plan estratégico nacional para la ciberdefensa que contemple una visión holística e interdisciplinaria. Además, la misma debe ser dinámica a los cambios ya que la innovación de las tecnologías y los métodos utilizados por los atacantes varían con una vertiginosidad sin precedentes. El alcance del presente trabajo no pretende la elaboración de un plan propiamente dicho, si no exponer una visión estratégica

sólida con recomendaciones para dicho plan y visibilizar la situación actual para las mentes venideras.

Nuestra sociedad se encuentra expuesta a un peligro y es necesario tomar medidas correctivas inmediatas. El advenimiento del internet de las cosas (IoT), implantes cibernéticos, autos inteligentes, drones, avances sobre el espacio exterior, computación cuántica e Inteligencia Artificial; solo reafirman un crecimiento del problema. Aquellos países que apunten a desarrollar estas tecnologías disruptivas verán como en la prehistoria a los países que no apostaron adecuadamente a las mismas. Por lo tanto, tendrán un control sobre dichas naciones.

Existe una falta de conciencia colectiva sobre los peligros reales de las TIC (tecnología de la información y la comunicación), ya que las tecnologías están diseñadas para operar de forma invisible y clandestina por detrás de un telón de beneficios (lo cual denominaremos "*digital candies*"). Por su parte, se observa que los estados/naciones y las empresas, no solo han demostrado escaso interés en la materia, sino que a su vez han sido "facilitadores" (para sí mismos y para otros estados/naciones) con el mero foco de un beneficio personal en detrimento del beneficio de las sociedades. Afortunadamente esta tendencia pareciera estar cambiando gradualmente y este trabajo pretende ser un humilde aporte en dicho aspecto.

En la contienda mundial no existen buenos o malos, solo intereses. En 1848 ya lo había dicho el primer ministro británico Henry Temple (más conocido como Lord Palmerston), en la House of Commons durante un discurso: "*We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow*"[3] (Ratcliffe, 2016).

La ciberguerra en el fondo se trata de la naturaleza de los seres humanos enfrentados, donde lo que cambian son simplemente los medios. Cada vez más desestabilizadores y potentes. Sin embargo, tal como adelantamos desde un comienzo, todo se resume al dominio de la voluntad del oponente mediante cualquier medio disponible, siendo el control de las mentes, posiblemente uno de los más efectivos y peligrosos dado las bondades del dominio del ciberespacio.

[3] No tenemos aliados eternos ni enemigos perpetuos. Nuestros intereses son eternos y perpetuos, y debemos seguir dichos intereses.

Cada estado nación tiene su propia estrategia: EE.UU.[4] busca el bienestar, desarrollo económico y la supremacía mundial, mediante la vigilancia global (Five eyes y plataformas de comunicaciones como Google/Android, Facebook/WhatsApp, Cloud Amazon/Microsoft, entre otros). En los medios de comunicación masiva la propaganda aplicada busca una aparente victimización en un esfuerzo de mostrarse como el defensor del mundo, sumado a una política de desprestigio a todo aquel que contraponga sus intereses. La inteligencia de información le permite un efectivo killchain (información – toma de decisión – acción) en operaciones de todo tipo desde guerra financiera (FMI), *character assasination*[5] y guerra por las mentes (mediático), asesinatos sigilosos, sabotajes, ataques falsa bandera (terrorismo), compra de vulnerabilidades (desarrollar ciberarmas), lawfare (persecución judicial), financiación de opositores (gobiernos títeres), promover protestas/levantamientos y golpes de estado blandos, entre otros.

Rusia por otra parte busca ampliar su esfera de influencia y contrarrestar los avances de la OTAN, fijando una posición geopolítica más favorable. Los medios de comunicación también han proliferado en la red. Ha conceptos de guerra híbrida[6] en diferentes teatros de operaciones (Georgia, Ucrania, Estonia) combinado con fuerzas armadas sin insignia conocidos como "*Little Green mens*" como también con ciber operaciones (Brose, 2020). Además, experimenta con la influencia en los procesos electorales en EE.UU., tanto con técnicas de hacking como con la influencia de *fakenews*, manipulación mediática, mediante la utilización de la Internet Reseach Agency (IRA). Entre otras características de Rusia podemos mencionar la utilización de veneno para asesinatos a desertores / opositores políticos (ej. neurotóxico Novichok[7]), un potente equipo de hacker para el desarrollo de ciberarmas de espionaje / *DDOS botnets* / *Kill Switch*[8] en *powergrid*[9] e infraestructuras críticas.

China por su parte es una potencia creciente que apunta a denegar la acción militar de EE.UU. y su superación en el plano de las tecnologías avanzadas: Anti-Access área Denial

[4] De aquí en adelante se utiliza el término EE.UU. o USA (United States of America) de forma indistinta.
[5] Asesinato de personaje, desarrollado más adelante.
[6] El concepto de guerra híbrida es mal llamado doctrina Gerasimov (Galeotti, 2013).
[7] Es un agente nervioso (neurotóxica) letal desarrollada por la Unión Soviética.
[8] Implante latente con la capacidad de afectar la disponibilidad del sistema.
[9] Red eléctrica.

(A2/AD), misiles anti-portaaviones (DF-21, DF-26), armamento militar, crecimiento económico, avance en el espacio exterior, desarrollo de tecnologías como inteligencia artificial y el espionaje a EE.UU. con la finalidad del robo de tecnologías. Así mismo, amplía su esfera de influencia económica en diferentes regiones como África y Sudamérica. Todo ello en su estrategia de "*winning without fighting*" [10] basado en el concepto de Sun Wu (SunTzu) de: "En la guerra, evitar lo que es fuerte y golpear lo que es débil" (Sun W., 512 A.C.). China apunta a un continuo proceso de modernización hasta el 2035 y una transformación militar, basado en el concepto de guerras modernas, para mediados de siglo (Nouwens, 2022; Stokes, 2024). Por otra parte, China cuenta con un avanzado control social, de vigilancia y de créditos sociales, que persigue a opositores y castiga todo aquel que no se encuentre alienado a las políticas de estado (Deutsche Welle, 2019).

[10] Ganar sin necesidad de pelar.

Capítulo ~~(1)~~ Ares – Una guerra invisible por la dominación.

El conocimiento es poder y el poder implica un uso sabio y responsable, cosa que usualmente no sucede [11]

"El conocimiento es poder" es una frase correcta pero insuficiente. No explica como la información alimenta operaciones que permiten ejercer el poder y lograr la dominación. Efectivamente, el conocimiento es clave para la libertad, como así también, para su extinción.

En el presente capitulo trataremos la guerra irrestricta, en particular, la ciberguerra y la guerra cognitiva. Las mismas tienen cada vez mayor preponderancia en la actualidad gracias a la conectividad y la integración de las TIC dentro de la sociedad. Por otro lado, la abundancia de datos, su procesamiento masivo y la estratificación psicológica de los individuos; posibilita la elaboración y envío de mensajes a la medida de cada audiencia, enfocados a explotar las vulnerabilidades cognitivas de la población. Todo ello, potenciado por el aparato mediático y amplificado en internet/redes sociales.

Resulta imperioso abordar algunos conceptos iniciales y definiciones básicas como el *kill chain* con su respectiva adecuación al dominio del ciberespacio. Ello permitirá comprender como se llevan a cabo las diferentes operaciones y de qué manera la inteligencia previa es fundamental para lograr los objetivos establecidos.

Previo a ello, algunas reflexiones respecto a la ética y la tecnología.

Consideraciones preliminares.

Arquitectura Von Neumann y la ética en las TICS.

Durante la segunda guerra mundial, en 1941, Reino Unido[12] (UK) comenzó la investigación y desarrollo de energía atómica bajo el Tubes Alloy Directorate[13] (The National Archives, s.f.; Cathcart, 2006) que continuó en 1942 en el Montréal Laboratory en Quebec, Canadá[14] (National Museum of nuclear science & history, s.f.). Por su parte,

[11] Parafraseando a Francis Bacon: "El conocimiento en sí mismo es poder" (1597).
[12] De aquí en adelante se utiliza el término UK (United Kingdom) de forma indistinta.
[13] El nombre de Aleación de tubos es para engañar sobre el verdadero objetivo.
[14] País estratégico por sus minas de uranio.

EE.UU. hizo lo propio con el Proyecto Manhattan. Iniciado en 1942 por el presidente Roosevelt luego de la carta le envió Albert Einstein con ayuda de Leó Szilárd en 1939; remarcando que las investigaciones sobre reacción en cadena de fisión de uranio pudieran producir grandes cantidades de energía y llevar al desarrollo de bombas extremadamente poderosas. Además de la posibilidad de que científicos alemanes pudieran ganar dicha carrera. En 1942 Coronel Leslie Groves se encargó de supervisar el proyecto, siendo el laboratorio de Los Álamos de Nuevo México la ubicación del seleccionada. En 1943, científicos británicos se unieron al laboratorio (U.S. Department of Energy, s.f.). Previamente el intercambio de información entre científicos de Reino Unido y EE.UU. era restringido por razones de secretismo. En 1943, Roosevelt y Churchill firmaron un acuerdo de cooperación conocido como Quebec Agreement. El mismo se formalizó el 19 de agosto de 1943 en La Citadelle de Québec, Canadá (Department of State, s.f.; National Museum of nuclear science & history, s.f.). El acuerdo, entre otros puntos, especificaba que la utilización de armas nucleares debía tener el consentimiento mutuo (The Avalon Project, s.f.).

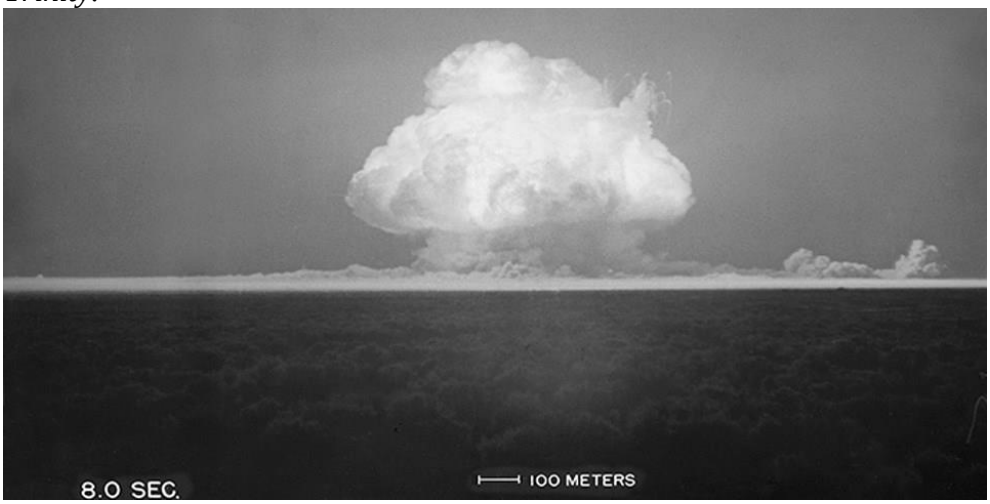
Los alemanes no llegaron a desarrollar la bomba atómica (proyecto Uranverein) debido a diferentes factores. Existen teorías respecto de si el físico alemán Heisenberg no tenía real interés en el desarrollo de la bomba o si habían calculado erróneamente la cantidad de material requerido (National Museum of nuclear science & history, s.f.). Así mismo, los aliados sabotearon el suministro de agua pesada (oxido de deuterio utilizado como moderador de neutrones) de Noruega mediante la operación Grousee (SOE de Noruega para inteligencia), operación Freshman (fallida por clima), operación Gunnerside (implantar explosivos en cámaras de electrólisis) y finalmente el hundimiento del ferry SF Hydro que transportaba el agua pesada en el lago Tinn (Gallagher, 2002; British Embassy Oslo, 2014). EE.UU. envió al espía Moe Berg a la charla de Copenhague durante 1944 con la orden de asesinar a Heisenberg en caso de que demostrara estar cerca de finalizar la bomba para Alemania (Tobey, 2012).

En tanto en el Proyecto Manhattan (EE.UU.) participaron muchos científicos. Entre ellos; Von Neumann, Eugene Wigner y Leó Szilárd (húngaros exiliados). Von Neumann trabajó en el método implosivo para la detonación de la bomba atómica (National Museum of nuclear science & history, s.f.). La primera prueba de explosión nuclear (code name

Trinity) se realizó en Nuevo México[15] durante 1945 (ver figura 1). El periódico se encargó de tapar la noticia indicando una gran explosión de un gran depósito de municiones (U.S. Air Force, s.f.). Posteriormente se realizaron pruebas en diferentes lugares y bajo diferentes condiciones: bajo el agua, bajo tierra y en la atmosfera; por ejemplo, la Operation Starfish Prime o la Operation Hardtack 1 (test YUCCA, ORANGE, TEAK) (Defense Technical Information Center, 1985, 1962). Uno de los lugares más habitúales de pruebas nucleares, es el Nevada Site Test del departamento de energía (exactamente al lado del área 51 de la Fuerza Aérea para tener apoyo aéreo). Debido a las pruebas nucleares, la radiación en la atmosfera llegó a diferentes partes del país mediante lluvia radiactiva causando serios problemas a la salud como ser cáncer de tiroides, de huesos o leucemia, con un pico de casos en 1963 previo al tratado de prohibición de pruebas nucleares, dejando solo habilitadas las pruebas bajo tierra. Un dato curioso es que dichas pruebas fueron detectadas por el Dr. Webb (científico de Kodak), ya que los rollos de película nuevos se vieron afectados por la radiación. Al medir la vida media del isotopo determinó que debía tratarse de Cerio141, la cual solo puede provenir de una fusión nuclear. Finalmente, el gobierno y Kodak tuvieron que ponerse de acuerdo para mantener el secreto de la lluvia radiactiva (Muller, 2020).

Figura 1

Trinity.



Nota. 16 de Julio de 1945, detonación de la primera bomba atómica (fuente imagen: Army White Sands Missile Range photo, s.f.).

[15] El famoso incidente Roswell se trató de un globo meteorológico secreto de gran altitud que contenía micrófonos de ondas de sonido enfocados a detectar detonaciones atómicas de la Unión Soviética (Project Mogul). Esto contribuyó a la propagación de teorías de UFO (Burr, s.f.; National Archives, s.f.; Headquarters United States Air Force, 1997).

En septiembre de 1945, el general Curtis LeMay, bajo órdenes de Harry S. Truman envió el bombardero Boeing B-29 Superfortress (Enola Gay) que arrojó bombas atómicas sobre poblaciones civiles en Hiroshima y Nagasaki (3 días después) (ver figura 2 y 3).

Figura 2

Devastación producida por la bomba atómica en Hiroshima.



Nota. Fuente imagen: U.S. Air Force, 1946.

Figura 3

Atomic bomb damage in Nagasaki, Japan.



Nota. Foto U.S. Air Force Number C58584AC.

Von Neumann calculó la altitud precisa que debía detonar la bomba atómica con el fin de producir el mayor daño posible (National Museum of nuclear science & history, s.f.). Un hecho histórico atroz e innecesario. Recordemos que Alemania ya había firmado la rendición en mayo y que Japón se encontraba bloqueada sin flota[16] (U.S. Navy, s.f.; Richard, 2020). Inclusive el secretario de estado Robert McNamara, de la administración Kennedy, afirmó que atacar a civiles fue inmoral e ilegal (McNamara como fue citado por Cubeddu, 2005; McNamara, 2009). El General Leslie Groves, quien participó del proyecto Manhattan y de la construcción del pentágono, testificó ante el senado:

> La víctima radiactiva puede ser de varias clases. Puede tener suficiente [radiación] para morir instantáneamente. Puede tomar una cantidad menor, lo que le hará morir bastante pronto, y según tengo entendido por los médicos, sin sufrimiento excesivo. De hecho, dicen que es una manera muy placentera de morir. Luego, bajamos hasta el hombre que está levemente herido, y puede que tarde algún tiempo en curarse, pero puede curarse (Atomic Energy, US Senate Special Committee, 1945, p 37).

La referencia no es una crítica a los estados involucrados, los nombres podrían ser diferentes si las circunstancias históricas hubieran sido otras. Lo trascendente es remarcar la naturaleza humana que nos recuerda la importancia en la ética que tenemos como profesionales en el desarrollo y utilización de la tecnología. En particular atención las TIC, que, a modo de apreciación personal, producen un efecto de desconexión emocional. Para el perpetrador no es lo mismo utilizar un arma cara a cara que presionar un botón escondido detrás de un teclado y cuyo poder de daño puede ser desproporcionadamente superior al de una bomba atómica. Las tecnologías exponenciales como la computación cuántica y la singularidad de la IA cambiaran por completo las reglas del juego. En algún lugar en el desierto, podrían estar desarrollando dichas tecnologías, fuera del consenso de la población y con fines armamentísticos.

Lamentablemente, el desarrollo de bombas atómicas continua en la actualidad y quienes poseen las mismas han demostrado irresponsabilidad en la tenencia. Los accidentes con bombas atómicas son denominados *brocen arrow*[17] y el DoD ha reportado 32 casos (U.S. Defense Department, s.f.). Existen innumerables eventos de accidentes e inclusive extravíos. Por ejemplo, en 1966 un bombardeo B-52 colisionó con un KC-135 de abastecimiento de

[16] En abril se produce la invasión a Okinawa y el hundimiento del Yamato.
[17] Flecha rota.

combustible y arrojó 4 bombas atómicas cerca de Palomares, España produciendo una contaminación de plutonio radiactivo. Una de las bombas cayó al mar y tardaron 2 meses y medio en recuperarla. En 1958 un F-86 colisionó con un B-47 que tuvo que arrojar la bomba en Tybee Island (Georgia). Hasta el día de la fecha, la misma continúa extraviada. En 1965, un A-4E Skyhawk, que contenía una bomba B43, rodó fuera de la cubierta del portaviones USS Ticonderoga y jamás fue encontrado (U.S. Defense Department, s.f.; Center for Arms Control and Non Proliferation, 2023). Durante el Damascus accident de 1980, se produjo la explosión dentro de un silo en Arkansas de un misil Titan II (misil balístico intercontinental) con una cabeza nuclear. Afortunadamente no hubo explosión nuclear dado el mecanismo de seguridad (Center for Arms Control and Non Proliferation, 2023).

Según recientes revelaciones de Norton-Taylor (2022), Reino Unido habría enviado 31 armas nucleares durante la guerra de Malvinas. De confirmarse la noticia, demuestra que la humanidad no ha aprendido absolutamente nada de la historia. Bajo el mismo razonamiento, tendríamos indicios que aún siguen existiendo bombas disponibles en Malvinas para ser utilizadas sobre poblaciones civiles en nuestro país.

Otro caso similar es la filtración de la OTAN, indicando que EE.UU. (USA) tiene 150 bombas atómicas B-61 gravity bomb en 5 países de Europa (Bélgica, Holanda, Alemania, Italia y Turquía) (ver figura 4), listas para ser utilizadas. Dichas bombas son entre 10 a 20 veces más poderosas que las arrojadas en Japón (Tweedie, 2019).

Figura 4

Secret locations of US nuclear weapons hidden in Europe.



Nota. 150 bombas atómicas B-61 gravity bomb (Tweedie, 2019)

Es importante recordar dichos sucesos cuando tratemos el tema del proyecto Cóndor de cohetes espaciales argentinos (analizado en capítulos posteriores). Cuyos sucesos, tanto EE.UU. como Reino Unido presionaron para su cancelación, por tratarse de peligroso.

¿Pero qué vinculación tiene con la temática que tratamos? Por un lado, existe un paralelismo interesante respecto al desarrollo de la tecnología disruptiva de la bomba atómica y las TICs en relación con su uso ético. Es relevante para el presente trabajo hacer una mención sobre la ética de la tecnología. Sin embargo, veremos como en las guerras modernas sin restricciones; tanto la ética como las leyes, no son limitantes para los agresores.

Por otra parte, Von Neumann desarrolló en 1945 la arquitectura que lleva su nombre y es utilizada en todas las computadoras hasta el día de la fecha. Su diseño está basado en la máquina Charles Babbage y su predecesor Johann Helfrich von Müller, junto a los aportes de Alan Turing (Turing machine). La arquitectura Neumann consiste en una unidad de procesamiento (*CPU*), una memoria principal (para almacenar tanto datos como instrucciones), almacenamiento masivo externo y mecanismos de entrada y salida (ver figura 5). La *CPU* a su vez contiene una unidad aritmético lógica (*ALU*), registros del procesador, una unidad de control con un registro de instrucciones y un contador de programa.

Figura 5

Esquema arquitectura Von Neumann.



Nota. Izquierda esquema arquitectura (elaboración propia). Derecha, computador digital EDVAC Exhibit catalog 102689071 (Computer History Museum, s.f.).

Un programa consta de instrucciones y de datos (entrada/salida). Las instrucciones son ejecutadas por la *CPU* que se encarga de administrar la memoria principal. Tanto las instrucciones como los datos son almacenados en la misma memoria principal.

Conocer la arquitectura permitirá comprender el concepto detrás de algunos ataques sobre el software. Por ejemplo, podrá notar que si no se controla adecuadamente el tamaño

de los datos de entrada (variables) podría sobrescribirse instrucciones del programa, adulterando el flujo normal del mismo. Esto permite a un potencial atacante tomar el control de la aplicación o incluso del sistema en su totalidad. Lo mencionado es un tipo de vulnerabilidad en el software, como por ejemplo, el *Buffer Overflow*[18].

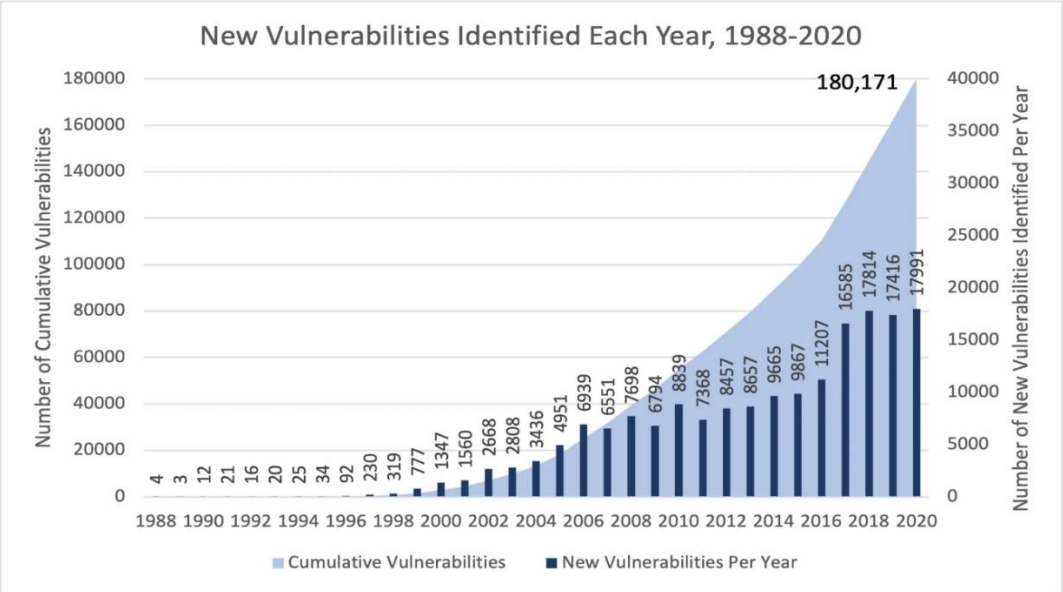
Ataques a los sistemas de información.

Los sistemas informáticos son propensos a tener diferentes tipos de vulnerabilidades. Las mismas están presentes al nivel de hardware, sistema operativo, aplicación y nivel usuario (incluyendo su psicología). Los atacantes pueden aprovechar estas debilidades para lograr sus cometidos mediante la explotación de estas. Las estructuras legales y sociales de organización en las que vivimos también son propensas a tener defectos; y como veremos, serán aprovechadas dentro de la guerra sin límites.

En el siguiente gráfico podrá apreciar el incremento en las vulnerabilidades descubiertas sobres los sistemas de información (ver figura 6).

Figura 6

Vulnerabilidades descubiertas.



Nota. Periodo 1988-2020 (fuente imagen: Singleton, Moore y McMillen, 2021).

[18] Más habituales en los lenguajes de programación de las primeras generaciones, en contraposición a los lenguajes de alto nivel.

En el apéndice del presente trabajo se adjunta un capítulo anexo donde podrá encontrar los principios de seguridad de la información junto al incremento de *leaks* a lo largo de la historia. Además, detalla diferentes vulnerabilidades sobre los sistemas de información y de las comunicaciones. Por lo que su lectura previa es recomendable.

Definiciones iniciales: Kill Chain y evolución.

Kill chain es un concepto militar que involucra un proceso de ataque. El mismo consiste en tres fases: comprensión de la situación, toma de decisión (qué hacer) y ejecución de una acción cuyo efecto logre completar el objetivo deseado (ver figura 7). *Closing the kill* implica completar todas las fases en dicho orden, mientras que frustrar algún paso del *kill chain* enemigo es denominado *breaking the kill chain*. Quien realice estas 2 acciones de la forma más rápida, frecuente y efectiva determina al ganador y al perdedor (Brose, 2020).

Figura 7
Esquema Kill Chain.



Nota. (fuente imagen: elaboración propia a partir del concepto descripto).

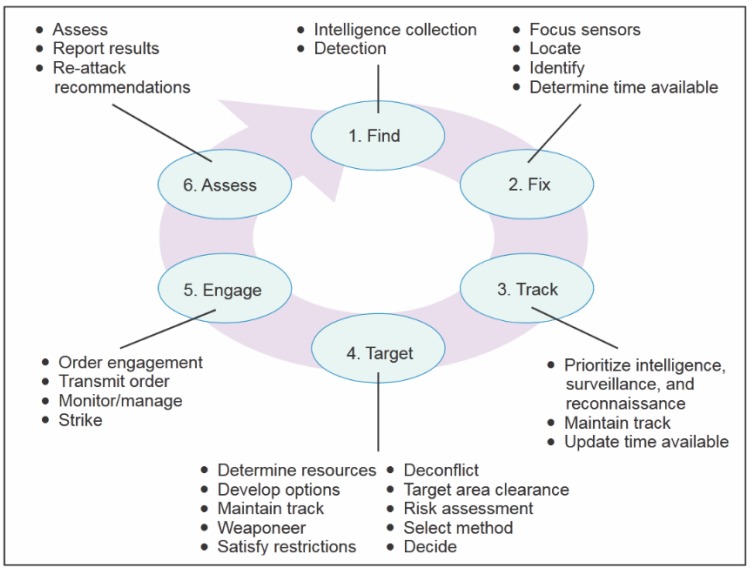
Las TICs potencian un proceso más rápido/preciso e incluso permiten una automatización de este. El incremento de los datos en la nube, las redes de pequeños satélites, los equipos militares cada vez más interconectados, el auge de los sensores y dispositivos (IOT) en todas partes; las tecnologías de vigilancia masiva (*mass surveliance*) y su correspondiente análisis de datos, entre otros, solo auguran un *Kill Chain* más eficiente y letal.

Es una cadena porque una interrupción de una etapa corrompe el proceso completo. En sí mismo, el *kill chain* puede ser utilizado en operaciones contra el *kill chain* enemigo. En el caso de la defensa, mientras más prematuramente pueda romperse/adulterarse la cadena, mejores son las probabilidades de detener/desalentar las agresiones enemigas. El efecto de la desinformación sobre la primera fase de inteligencia implica un acarreo de defectos a las

posteriores fases; conllevando a decisiones/acciones erróneas/equivocadas, consumiendo los recursos del adversario. La denegación a la inteligencia (*Intelligence Gathering*) o la desinformación mediante engaños/*fakes*/*forgeries*, pueden ser potentes herramientas defensivas en caso de ser utilizadas de forma adecuadas.

Vinculado al concepto *Kill Chain*, podemos encontrar modelos como *F2T2EA* (targeting doctrine) cuyas fases son: *Find* (Identificar al objetivo mediante inteligencia), *Fix* (fijar las coordenadas), *Track* (seguir el movimiento del objetivo), *Target* (seleccionar el arma más adecuada a fin de lograr el objetivo deseado), *Engage* (utilizar el arma sobre el objetivo) y *Assess* (evaluación del ataque y una posible retroalimentación del proceso) (Tirpak, 2000) (ver figura 8). Similarmente, el modelo OODA LOOP (observa, orienta, decide, actúa), desarrollado por el Coronel John Boyd de la USAF, busca contextualizar la información disponible y tomar decisiones más rápidas que el enemigo.

Figura 8
F2T2EA: Targeting steps.



Nota. (Fuente: Joint Publication 3-60 Joint Targeting).

Usualmente el *kill chain* se encuentra enfocado a operaciones tácticas en el plano cinético[19]. No obstante, es de menester del presente trabajo comprender su aplicación sobre diferentes dominios y como diseñar/corromper operaciones estratégicas a mediano/largo

[19] *Kinetic* se refiere a medios tradicionales que atacan físicamente al objetivo. En contraposición al plano digital (*cyber*).

plazo. Dentro del plano geopolítico podemos encontrar diferentes operaciones: ciberataques a infraestructuras críticas, transferencia tecnología mediante el robo de información/dispositivos, posicionamiento estratégico de empresas afines, implantación de tecnologías para beneficio propio, intercepción/bloqueo de las comunicaciones, robo de información a fin de retroalimentar un *kill chain*, sabotaje de proyectos estratégicos de otras naciones (usualmente nuclear, energético, militar, espacial o tecnologías exponenciales), romper alianzas/enemistar a otros estados/naciones, fortalecer alianzas de interés, desalentar/desarticular oposiciones/organizaciones en contra de los intereses establecidos, asesinado de objetivos, lobby político, promover revueltas, fomentar golpes de estado, instaurar oposiciones afines (gobiernos títeres) y dentro del plano de las mentes; provocar división ideológica en las personas, implantar ideas favorables, imponer culturalmente a la población, entre otras. El concepto descripto se asemeja a un proceso similar al que podría apreciar a continuación (ver figura 9).

Figura 9
Esquema Strategic Kill Chain propuesto.



Nota. (fuente imagen: elaboración propia).

A fin de apreciar su adecuación en el ciberespacio, mencionaremos a continuación algunas variantes basadas en el *kill chain* original. Sin embargo, cabe aclarar que para el corriente trabajo, es suficiente comprender conceptualmente las tres fases del *kill chain* y el proceso propuesto.

Marco de referencia Intrusion Kill Chain / Cyber Kill Chain®.

En 2011, Investigadores de la firma Lockheed Martin expanden el concepto *kill chain* en un nuevo framework especifico de intrusiones denominado *Intrusion Kill Chain*[20]. El mismo

[20] También conocido como *Cyber Kill Chain*®.

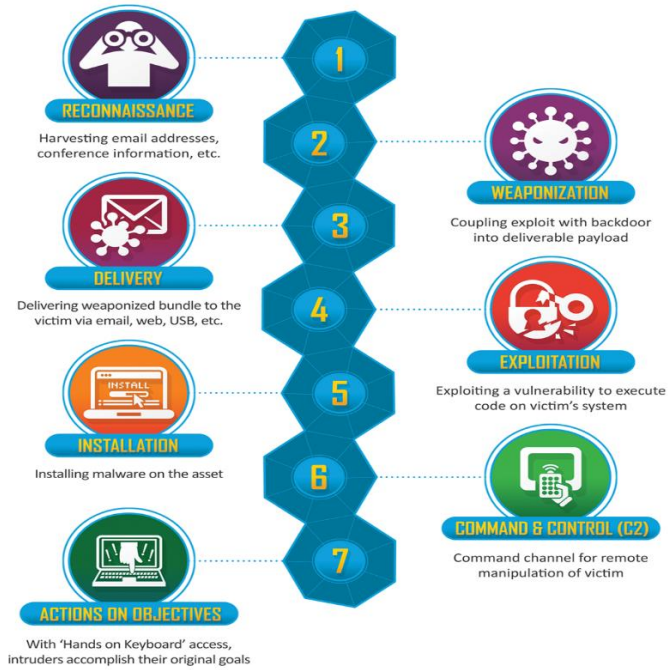
se basa en que las defensas o metodologías de respuesta a incidentes tradicionales[21] no son suficientes para los ataques sofisticados. La propuesta utiliza una estrategia de defensa basada en inteligencia y se enfoca en las intrusiones de amenaza avanzadas (APT). Estas amenazas utilizan herramientas sofisticadas y técnicas diseñadas para eludir los mecanismos de defensa convencionales en las redes informáticas (Hutchins, Cloppert y Amin, 2011).

El Framework permite analizar al adversario, sus capacidades, objetivos, doctrina y limitaciones. El conocimiento del adversario faculta una retroalimentación de información en la defensa, disminuyendo la probabilidad de éxito del adversario (defensa basada en inteligencia). Una sola mitigación rompe la cadena y frustra al adversario (Hutchins et al., 2011).

De forma abreviada, el modelo contempla un proceso sistemático basado en 7 etapas (ver figura 10 y tabla 1), que van desde el reconocimiento/inteligencia previa hasta la última etapa donde el adversario logra su objetivo (usualmente la exfiltración de información). El modelo propuesto apunta a una detección temprana de la amenaza (ver figura 11) (Hutchins et al., 2011).

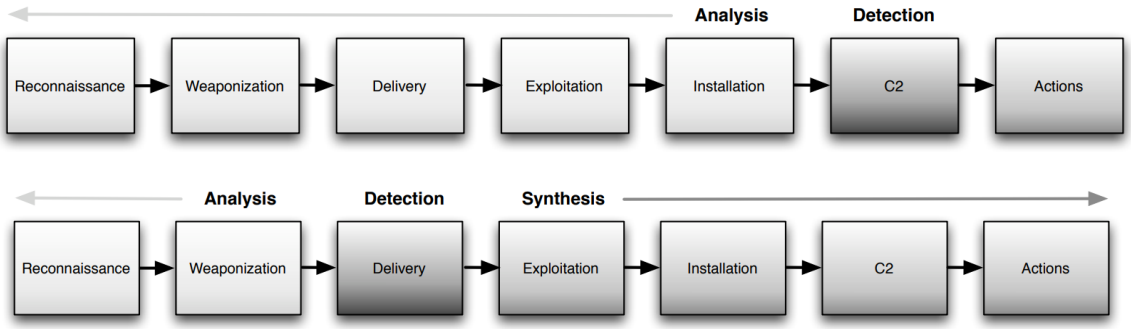
[21] Son erróneas porque se basan en dos premisas incorrectas frente a los APT: que la defensa debe suceder posterior a la intrusión y que el compromiso es el resultado de un defecto corregible (Mitropoulos et al. como fue citado por Hutchins et al., 2011; National Institute of Standards and Technology como fue citado por Hutchins et al., 2011).

Figura 10
Cyber kill chain.



Nota. 7 fases del ataque para lograr el objetivo (Fuente: Lockheed Martin, s.f.).

Figura 11
Cyber kill chain.



Nota. Imagen superior, detección tardía en una metodología de incidentes tradicional. Imagen inferior, detección temprana basada en patrones y comportamientos de los APT; Tácticas, Técnicas y Procedimientos (TTP) (Hutchins et al., 2011).

Tabla 1
Intrusion Kill Chain.

Kill chain phases	Description
Reconnaissance	Investigación, identificación y selección de objetivos, a menudo en sitios web en Internet, listas de correo, relaciones sociales o información sobre tecnologías específicas.
Weaponization	Combinar un troyano de acceso remoto con un *exploit* en un *payload* (normalmente mediante una herramienta automatizada). Algunos ejemplos son los archivos PDF de Adobe o los documentos de Microsoft Office.
Delivery	Transmisión del arma al entorno objetivo. Los tres vectores de entrega más frecuentes de cargas útiles armadas por parte de los actores de APT, según lo observado por el Equipo de Respuesta a Incidentes Informáticos de Lockheed Martin (LM-CIRT) para los años 2004-2010, son los archivos adjuntos en correos electrónicos, sitios web y USB extraíbles.
Exploitation	La explotación activa el código del arma una vez entregada a la víctima. La explotación tiene como objetivo una vulnerabilidad de una aplicación o del sistema operativo, pero también podría explotar más simplemente a los propios usuarios o aprovechar una característica del sistema operativo que ejecuta código automáticamente.
Installation	La instalación de un troyano de acceso remoto o una puerta trasera en el sistema de la víctima permite al adversario mantener la persistencia dentro del entorno.
Command and Control (C2)	Normalmente, los hosts comprometidos deben enviar una señal a un Servidor en Internet (bajo control del atacante) para establecer un canal de comunicación de control. Esto permite una interacción manual en lugar de realizar actividades automáticamente. Los atacantes logran control remoto al entorno objetivo.
Actions on Objectives	Lograr los objetivos deseados por el atacante. Habitualmente la exfiltración de datos, que implica recopilar, cifrar y extraer información del entorno de la víctima. Otros posibles objetivos son afectar la integridad o disponibilidad de los datos. Alternativamente, utilizar el objetivo como punto de salto para comprometer sistemas adicionales y moverse lateralmente dentro de la red.

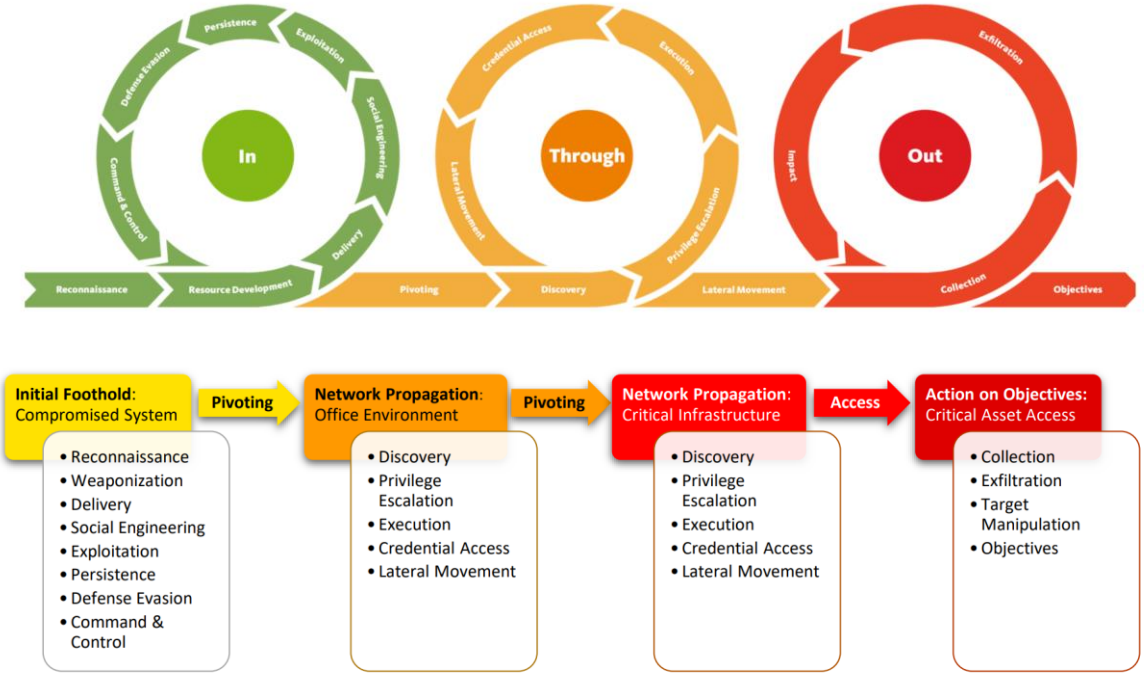
Nota. Fuente (Hutchins et al., 2011).

Marco de referencia Unified Kill Chain.

El modus operandi de los APT no necesariamente coincide con el modelo *Cyber kill Chain*®, dado que estos modelos tradicionales tienen un foco en el malware y el perímetro. Siendo inadecuado frente a ataques internos u otros vectores de ataques. En lugar de centrarse en frustrar los ataques en etapas tempranas, se espera que las estrategias de defensa en capas centren sus esfuerzos en las fases vitales o con mayor frecuencia de éxito. El modelo *Unified Kill Chain* (*UKC*) se enfoca en las tácticas utilizadas en las fases de ataque. Dicho

modelo fue evaluado mediante casos de estudios como el APT28 (Fancy Bear). El *UKC* se basa en una extensión del Cyber Kill Chain® y las técnicas de ataque avanzados de *MITRE ATT&CK*®. Consta en 18 fases y permite el desarrollo de *kill chain* de actores específicos; para su posterior análisis, comparación y defensa (ver figura 12 y 13) (Pols, 2017).

Figura 12
Unified Kill Chain Phases.



Nota. Imagen superior, logros intermedios para obtener los objetivos finales: *in* (ganar acceso a sistemas), *through* (ganar privilegios), *out* (realizar acciones). Imagen inferior, ruta de ataque (Fuente imagen: Pols, 2023 y 2017).

Figura 13
Fases del Unified Kill Chain.

The Unified Kill Chain		
1	**Reconnaissance**	Researching, identifying and selecting targets using active or passive reconnaissance.
2	**Resource Development**	Preparatory activities aimed at setting up the infrastructure required for the attack.
3	**Delivery**	Techniques resulting in the transmission of a weaponized object to the targeted environment.
4	**Social Engineering**	Techniques aimed at the manipulation of people to perform unsafe actions.
5	**Exploitation**	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6	**Persistence**	Any access, action or change to a system that gives an attacker persistent presence on the system.
7	**Defense Evasion**	Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8	**Command & Control**	Techniques that allow attackers to communicate with controlled systems within a target network.
9	**Pivoting**	Tunneling traffic through a controlled system to other systems that are not directly accessible.
10	**Discovery**	Techniques that allow an attacker to gain knowledge about a system and its network environment.
11	**Privilege Escalation**	The result of techniques that provide an attacker with higher permissions on a system or network.
12	**Execution**	Techniques that result in execution of attacker-controlled code on a local or remote system.
13	**Credential Access**	Techniques resulting in the access of, or control over, system, service or domain credentials.
14	**Lateral Movement**	Techniques that enable an adversary to horizontally access and control other remote systems.
15	**Collection**	Techniques used to identify and gather data from a target network prior to exfiltration.
16	**Exfiltration**	Techniques that result or aid in an attacker removing data from a target network.
17	**Impact**	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	**Objectives**	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

Nota. Los nombres *Target manipulation* y *Weponization* cambiaron a *Impact* y *Resource Development* respectivamente; a fin de mantener consistencia con versiones posteriores de ATT&CK® (Fuente imagen: Pols, 2020).

Marco de referencia Mitre ATT&CK®.

Los enfoques contemporáneos de detección no son suficientes ya que las amenazas avanzadas desarrollan herramientas a medida con mecanismos de evasión; las cuales son probadas previamente contra controles de seguridad (ejemplo antivirus). Las acciones realizadas de forma remota son enmascaradas en el funcionamiento legítimo del sistema como así también se camuflan con el tráfico habitual de la red, evitando sospechas. El análisis de trafico de red suele ser inútil dado que es usualmente cifrado. El comportamiento basado en *threat intelligence* también es insuficiente dado la velocidad en que el adversario cambia y se adapta.

El Framework ATT&CK (ver figura 14) es un modelo que describe las acciones que realiza un adversario avanzado mientras opera dentro de una red empresarial luego del compromiso inicial. El modelo admite una mayor comprensión del comportamiento de un adversario, posterior a su intrusión. El objetivo es obtener patrones de comportamientos basados en las acciones que realiza para lograr su objetivo. Sirve tanto para emulación del

adversario como también descubrir analítica y brechas de defensa dentro de una red objetivo (Strom, Battaglia, Kemmerer, Kupersanin, Miller, Wampler, Whitley, Wolf, 2017). El objetivo es mejorar la detección post compromiso a través de sensores de telemetría y analítica de comportamiento. Fue desarrollado en 2013 y publicado en 2015 con 96 técnicas dentro de 9 tácticas. Originalmente categoriza tácticas, técnicas y procedimientos (TTP) utilizados por adversarios en entornos *Windows*. Posteriormente fue ampliado a entornos *Mac*, *Linux*, *Mobile*, *Cloud* e *ICS* (*Industrial Control Systems*) (Strom, Applebaum, Miller, Nickels, Pennington y Thomas, 2020).

Los adversarios usualmente dedican meses en las redes corporativas, realizando inteligencia, escalando privilegios y efectuando movimientos laterales, entre otros. Los objetivos que pretende lograr un adversario en una intrusión son denominados *Tactics*. Acorde a (Strom et al., 2017), dichas tácticas[22] se clasifican en:

- *Persistence*: Las acciones necesarias para mantener acceso persistente a los sistemas indistintamente de reinicios, actualizaciones, cambio de credenciales, etc.
- *Privilege Escalation*: Obtener el mayor nivel de permisos a nivel sistema o de red. Ejemplo: Mimikatz (Cute cats) es una herramienta desarrollada por Benjkamin Delphy que obtiene credenciales[23] en memoria, como ser una cuenta administrator autenticada en el mismo servidor. La escucha del tráfico no cifrado de red (*sniffer*) es otra técnica que permite lograr similares objetivos.
- *Defense Evasión*: Técnicas de evasión a fin de no ser detectado.
- *Credential Access*: Control sobre las credenciales corporativas.
- *Discovery*: Obtener conocimiento sobre la red interna y sus sistemas.
- *Lateral Movement*: Acceder a otros sistemas de la red. Se refiere a obtener accesos que no conducen a mayores privilegios, pero si a garantizar la persistencia. Este movimiento lateral, a su vez, podría facilitar un segundo paso de escalamiento de privilegios.

[22] Ampliado posteriormente a: *Reconnaissance*, *Resource Development*, *Initial Access*, *Execution*, *Persistence*, *Privilege Escalation*, *Defense Evasion*, *Credential Access*, *Discovery*, *Lateral Movement*, *Collection*, *Command and Control*, *Exfiltration* e *Impact* (https://attack.mitre.org/tactics/enterprise/).
[23] Ticket de Kerberos en entornos Windows/Active Directory.

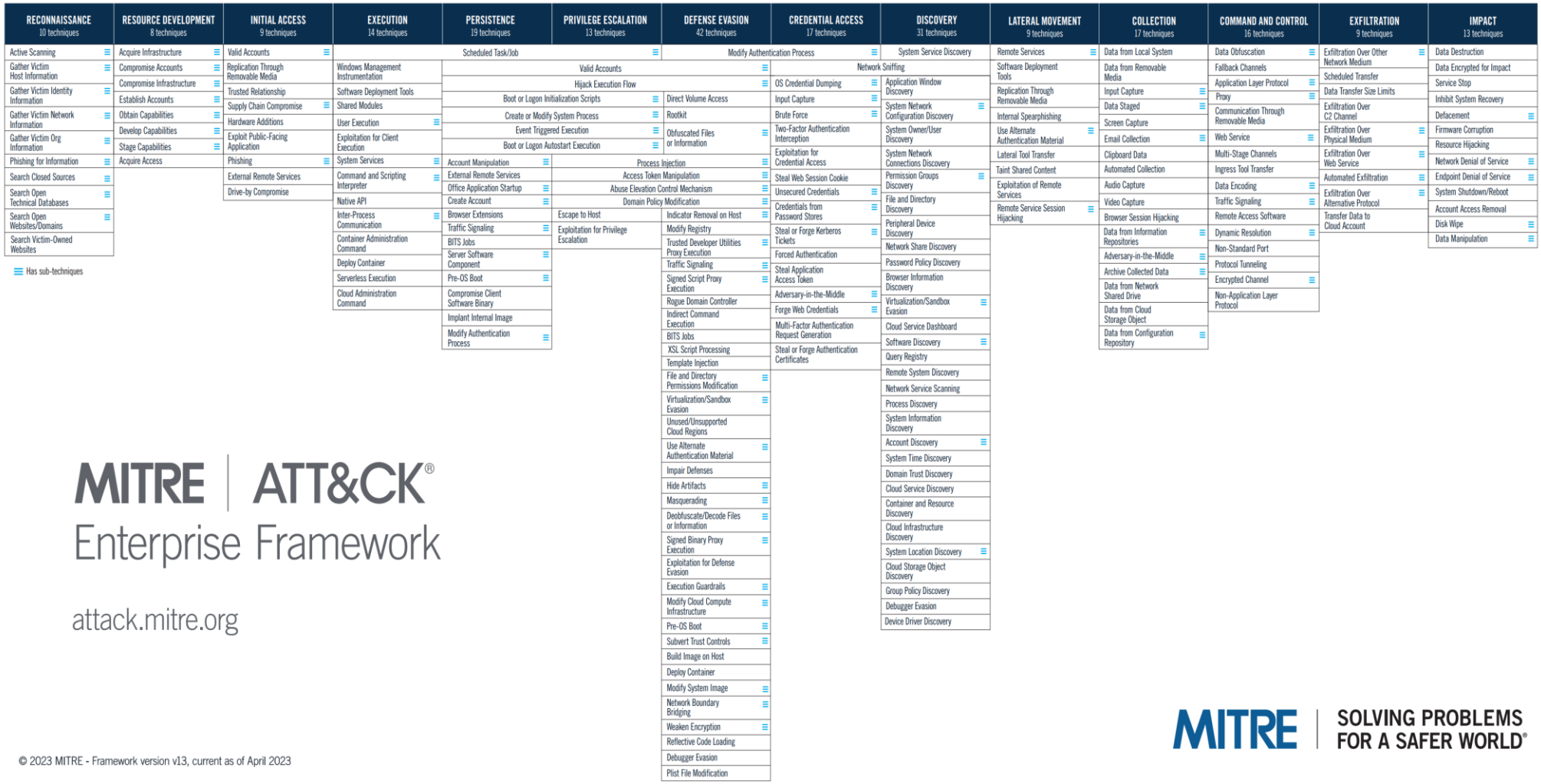
- *Execution*: Lograr la ejecución local o remota de un código.
- *Collection*: Recopilar información de documentos/archivos de valor.
- *Exfiltration*: Extraer archivos o información de la red interna.
- *Command and control*: Técnicas de como el atacante se comunica con la red interna.

Las acciones que debe realizar el adversario a la hora de lograr su objetivo (*tactics*) se denominan *techniques.* Estas técnicas describen a que sistemas afecta (plataforma), métodos de detección y mitigación. Existen diferentes técnicas detalladas para lograr cada una de las diferentes tácticas. Mitre permite desarrollar *analytics* enfocadas a detectas las técnicas utilizadas (Strom et al., 2017).

A continuación, definiremos la ciberguerra, sus actores las características que presenta el plano del ciberespacio.

Figura 14

MITRE ATT&CK Matrix.



Nota. (Fuente imagen: MITRE ATT&CK Matrix Poster, 2023).

Guerra cibernética – 5to dominio (Cyberwarfare).

Si bien el termino es ampliamente utilizado en la actualidad, no existe una definición consensuada. Sin embargo, diferentes autores apuntan a que se trata de ataques a los sistemas de información por parte de estados/naciones.

Cada país puede tener una visión propia respecto al tópico y su tratamiento. No obstante, a fin de tener un marco de referencia, mencionamos la doctrina de Estados Unidos[24]. En la misma tampoco existe una definición oficial de *information warfare.* Pese a ello, se encuentra vinculado estrechamente con las operaciones de información (*Information operation*) que veremos a continuación. Cabe anticipar que la ciberguerra es un elemento de la guerra híbrida que trataremos más adelante.

Guerra de información (Information operation / Information warfare)

Según el Joint Publicacion 3-13 - Information operations (2005), la finalidad de las operaciones de información son ganar una ventaja en las capacidades de toma de decisiones, mientras apunta interrumpir la habilidad del enemigo a tomar decisiones. Busca crear un efecto en el adversario para lograr un objetivo propio.

Básicamente, el entorno de la información se compone por una *Physical dimension* (*C2 systems, key decision makers, newspapers, Smart phones*, etc.), *Informational dimension* (donde se almacena y procesa la información) y una *Cognitive Dimension* (las mentes de quienes transmiten reciben y toman decisiones en base a la información). Ver figura 15.

Las técnicas de *Information Related Capabilities* (IRC) buscan influenciar el comportamiento del *target audience* (objetivo) mediante diferentes medios, afectando la capacidad de procesar, percibir, difundir y actuar sobre la información. Nuevamente, la inteligencia es una capacidad vital para lograr el objetivo de las *Information Operations*.

Acorde al Departamento de Defensa (DoD):

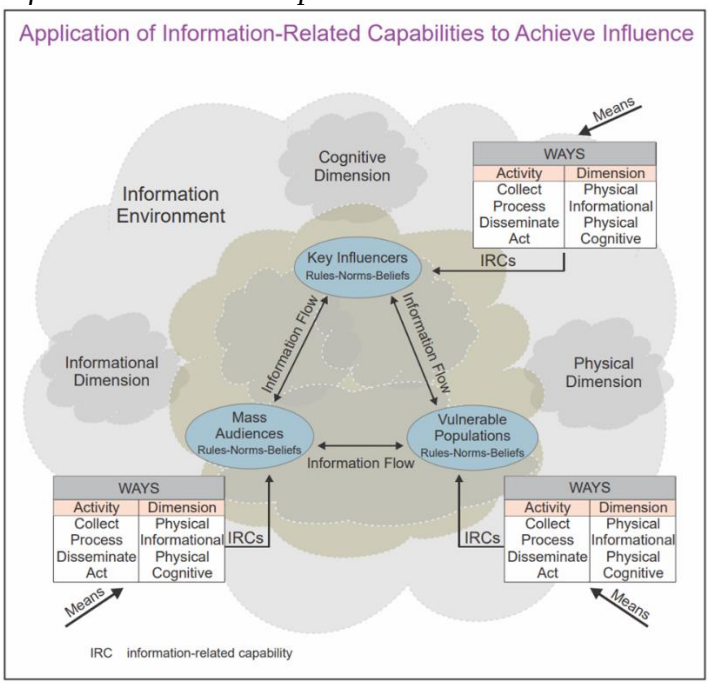
> La información es siempre importante en la guerra, crítico para el éxito militar y cada vez más en el futuro previsible […] el DoD está construyendo una fuerza centrada en la información. Las redes son cada vez más el centro de gravedad operacional y el Departamento de Defensa debe estar preparado para pelear en la red […] potente

[24] Basado en algunos documentos públicos. Tener presente que por razones de seguridad nacional o por su naturaleza de operaciones clandestinas, existen documentos a los cuales no tenemos acceso.

contribución de las operaciones basadas en efectos en toda la gama de operaciones militares durante tiempos de paz, crisis y guerra […] requieren una amplia preparación en tiempo de paz […] a través de inteligencia, vigilancia, reconocimiento y amplias actividades de planificación. Las funciones principales son disuadir, desalentar, disuadir y dirigir al adversario, rompiendo así su unidad de mando […] proteger nuestros planes y desviar los enemigos […] controlar las comunicaciones y redes enemigas mientras se protegen las propias. (Information Operations Roadmap[25], 2003).

Figura 15

Information related Capabilities.



Nota. Como influenciar a un objetivo basado en las 3 dimensiones (fuente imagen: Joint Chiefs of Staff, 2014).

Las Information Operation (IO) se compone de 5 pilares: Computer network operations (CNO), Psychological Operations (PSYOP), Military deception (MILDEC), Operation security (OPSEC) y Electronic Warfare (EW) (Information Operations Roadmap, 2003).

Operaciones en redes de computadoras (Computer network operations - CNO).

Las operaciones en el *cyberspace* basado en la doctrina JP 3-12 (2018).

- Computer network Defense (CND): Proteger, monitorear, analizar, detectar y responder a ataques de red, intrusiones, interrupciones u otras acciones no

[25] Desclasificado solo parcialmente mediante FOIA request.

autorizadas que comprometerían o paralizarían los sistemas y redes de información de defensa.

- Computer network attack (CNA). Interrumpir, negar, degradar, destruir o manipular la información dentro de las computadoras y redes informáticas enemigas, apuntando a efectos en el plano físico.
- Computer network exploitation (CNE). Descubrir vulnerabilidades y recopilación de inteligencia a través de redes informáticas para futuras operaciones militares (ej. ganar y mantener accesos a ciertas redes/sistemas).

Operaciones psicológicas (Pyschological Operations - PSYOP).

> *"No se puede hacer la guerra en las condiciones actuales sin el apoyo de la opinión pública, que está tremendamente moldeada por la prensa y otras formas de propaganda." (General MacArthur durante la WWII).*
>
> *"El objetivo real en la guerra es la mente del comando enemigo, no los cuerpos de sus tropas. Si operamos contra sus tropas es fundamentalmente por el efecto que la acción producirá en la mente y voluntad del comandante" (Capital Sir Vasil Liddel Hard, 1944)*

Las operaciones psicológicas son también mencionadas en algunos documentos como Military information Support Operation (MISO). Acorde a la Doctrine for Joint Psychological Operations - JP 3-53 (Joint Chiefs of Staff, 2003), se trata de operaciones planeadas que buscan influir, de forma favorable; las emociones, motivos, razonamiento y el comportamiento de gobiernos, organizaciones, grupos e individuos extranjeros. Son elementos vitales en el ámbito diplomático, informativo, militar y económico durante tiempos de paz o conflicto. En combate refuerza la moral aliada y reduce la voluntad del adversario a combatir.

El apoyo del DoD a la diplomacia y los asuntos públicos mejorará la capacidad del DoD para llevar a cabo operaciones de información de manera agresiva y hacerlo de manera totalmente consistente con los objetivos más amplios de seguridad de la nación (Information Operations Roadmap, 2003).

PSYOP se integra en los otros pilares de la information operation.

Ejemplos de PSYOP: Durante la operación Allied Force, en la guerra de Kosovo, arrojaron 104,5 millones de panfletos sobre Kosovo. También emitieron programas de radio/televisión desde aviones *Lockheed EC-130E Command Solo* para contrarrestar la propaganda Serbia. Las operaciones demostraron un desempeño clave para la victoria. Durante la operación Shield y Desert Storm en la guerra del Golfo; arrojando panfletos a las fuerzas de Irak, llamando a rendirse y mantenerse lejos de los equipamientos que eran objetivos de los ataques aéreos. Como ejemplos de PSYOP durante tiempos de paz, el comando sur arrojó panfletos en Colombia para disuadir a la población de que el Glifosato no era nocivo al medio ambiente (durante la lucha contra el narcotráfico) (Joint Chiefs of Staff, 2003).

El uso efectivo de las operaciones psicológicas se sustenta en el conocimiento de las condiciones políticas, militares, económicas, culturales religiosa, sociales y psicológicas del adversario. Por lo cual es fundamental la inteligencia previa[26] y un proceso de retroalimentación para una mayor eficiencia en los efectos deseados (Joint Chiefs of Staff, 2003).

Acorde al manual FM 3-05.30 - Psychological Operations (Department of the Army, 2005), la propaganda y la desinformación forman parte de las *Information Operations*. PSYOP se utilizan en apoyo de operaciones especiales, en tiempos de paz, antiterrorismo, guerra no convencional, operaciones de contrainsurgencia, etc. Las operaciones abiertamente reconocidas por EE.UU. son denominadas White PSYOP, mientras que las Black PSYOP son encubiertas; quedando las Grey PSYOP como un punto intermedio (Department of the Army, 2005).

Durante la guerra de Corea (1950-1953), Corea del sur y las Naciones Unidas realizaron una intensa guerra psicológica para debilitar a los adversarios comunistas. Los medios utilizados incluyeron: radio, altoparlantes y panfletos (la mayoría arrojados desde aviones). El contenido estaba basado en información sobre vulnerabilidades/preocupaciones obtenidas de prisioneros coreanos/chinos en interrogatorios. Los tópicos incluían: ventajas/métodos de rendición, los riesgos de continuar pelando (bajas/superioridad de poder), los objetivos de las Naciones Unidas (Corea pacifica/unificada) y la ilegitimidad de los objetivos comunistas.

[26] Inclusive interrogatorios

Sobre este último, cambiaba según el destinatario: a los coreanos/chinos los mensajes indicaban que estaban siendo usados por la URSS; a los coreanos que China quería colonizarlos; y a los chinos dudas sobre pelear una guerra extranjera de la cual no tenían interés. En 1953 se aprueba la *Operation Moolah*, que buscaba la deserción de pilotos enemigos ofreciendo $100 mil USD al primer piloto comunista que volara un MIG a Corea del Sur (los subsiguientes recibirían $50 mil USD). La operación no tuvo el efecto esperado, pero persuadió a la URSS de retirar sus pilotos de la guerra de Corea por miedo de que aceptaran la oferta quedando expuesta su participación encubierta en la guerra (Hosmer, 1996). Finalmente, un piloto coreano desertor entregó un avión en Kimpo Air Base de Corea del Sur en 1953. El avión proporcionó importantes datos de inteligencia, sobre todo porque era la versión avanzada del MiG-15(bis). Hoy se exhibe en el museo (National Museum of the United States Air Force, s.f.). Sin embargo, este piloto nunca había escuchado sobre la recompensa, por lo que no puede considerarse un caso de éxito. Aun así, recibió el pago y asilo en Estados Unidos (Jones, 2007).

Engaño militar (Military deception - MILDEC).

Acorde al Joint Publication 3-13.4 (2017), son acciones que se ejecutan para engañar deliberadamente a los tomadores de decisiones de las organizaciones militares, paramilitares o extremistas violentos; lo que provoca que el adversario tome medidas específicas que contribuirán al cumplimiento de la misión deseada. La metodología "ver, pensar, hacer" manipula el proceso cognitivo engañando la mente objetivo, conduciendo a decisiones ventajosas (los esfuerzos deben ser coordinados para que el objetivo observe, crea y piense que el engaño es real y que no existan elementos incongruentes/contradictorios). Una operación de engaño requiere una sincronización cuidadosa para que la inteligencia adversaria pueda recopilar, analizar y reportar; y que el adversario tome una decisión basada en dicho engaño (Joint Chiefs of Staff, 2017).

El engaño militar se integra en los otros pilares de la *Information Operation*.

Un ejemplo de MILDEC es la operación Bodyguard durante el desembarco de Normandía en la WWII, donde los aliados amenazaron con una invasión paralela por Noruega y los Balcanes (aumentando la ambigüedad crea confusión y conflicto en la mente del adversario) mientras que convencían a los alemanes de una invasión a través de Francia

en Pas-de-Calais (disminuyendo la ambigüedad hace que la mente del adversario crea estar muy seguro de sus decisiones cuando en realidad se encuentra muy equivocado) (Joint Chiefs of Staff, 2017). La Operación Fortitude (1944), como parte de Bodyguard, utilizó el Double-Cross System de John Masterman[27], donde dobles agentes daban desinformación a los alemanes, ayudando al engaño del desembarco del día D (Operación Overload) (Lintott, 2015; Joint Chiefs of Staff, 1996).

Operaciones de seguridad (Operation security - OPSEC).

Según el Joint Publication 3-13.3 (2006), busca reducir las vulnerabilidades frente a la explotación exitosa de información crítica por parte del adversario (ej. utilizar modelos analíticos basado en indicadores que predicen operaciones gracias a los patrones de comportamiento característicos, como por ejemplo el movimiento de tropas). El proceso OPSEC identifica información crítica para posteriormente analizar las acciones asociadas a operaciones militares y tomar medidas para reducir la visibilidad de estas. Consisten en 5 acciones: identificación de información crítica, análisis de amenazas, análisis de vulnerabilidades, evaluación de riesgos y aplicación de medidas OPSEC apropiadas. OPSEC también incluye información de fuentes abiertas (internet) y además complementa las operaciones de decepción (MILDEC) (Joint Chiefs of Staff, 2006).

Guerra electrónica (Electronic Warfare - EW).

Respecto al Joint Publication 3-13-1 (Joint Chiefs of Staff, 2012), busca proteger las operaciones dentro del espectro electromagnético propio mientas que niega las del adversario dentro del *operational enviroment* (inteligencia, comunicaciones, posicionamiento, procesamiento de información, *ranging*, etc.). Se encuentra ampliamente

[27] Masterman ya había utilizado el engaño a favor de los aliados en el plan Nunton para ayudar a romper la línea Gustav al sur de Roma en 1944, la operación Toch en 1942 (desembarco al norte de África), Huscky en 1943 (invasión de Sicilia) y Dragoon en 1944 (sur de Francia) (Lintott, 2015).
En la operación Mincemeat forzaron a los alemanes a enviar refuerzos a la península de Balcanes cuando en realidad los aliados invadieron Sicilia. Para lograr el engaño, plantaron documentos falsos en el cuerpo de un vagabundo muerto, vestido de royal marine en una supuesta misión de mensajería. El avión aparentemente se había estrellado en las costas de España (el cuerpo en realidad fue plantado desde un submarino británico). La carta que contenía el cuerpo indicaba la intención de invadir Grecia. Esta operación fue en apoyo a la invasión de Sicilia (Operación Husky) (Lintott, 2015). Para mayor credibilidad incorporaron fotos y cartas personales de una falsa novia, que en realidad era una agente del MI5 (s.n., 2012).

vinculado además al dominio del espacio (segmento tierra, espacio, link) en capacidades como ser posicionamiento, navegación y timing (PNT) y el dominio del ciberespacio (redes *wired* y *wireless* vulnerables a ataques electromagnéticos). Acorde a (Joint Chiefs of Staff, 2012), las tres divisiones de guerra electrónica son:

- *Electronic attack (EA):* Uso de energía electromagnética, energía directa o armas anti-radiación (como ser Laser, electroóptico, infrarrojo, radio frecuencias, microondas de alta potencia, armas EMP). Utilizadas para atacar personal, instalaciones o equipamientos (Ver figura 16).

  Figura 16
  Active Denial System.

  Nota. Ejemplo de energía directa no letal (fuente imagen: Schloeffel, 2007).

- *Electronic protection (EP):* Sistemas de protección contra los *electronic attack (EA)* enemigos.
- *Electronic warfare Support (ES):* Buscar, interceptar, identificar y localizar fuentes de energía electromagnética radiada intencional y no intencional con el propósito de reconocimiento inmediato de amenazas, focalización, planificación y realización de futuras operaciones. Producir inteligencia de señales (SIGINT[28]), proporcionar objetivos y producir inteligencia de firma electrónica.

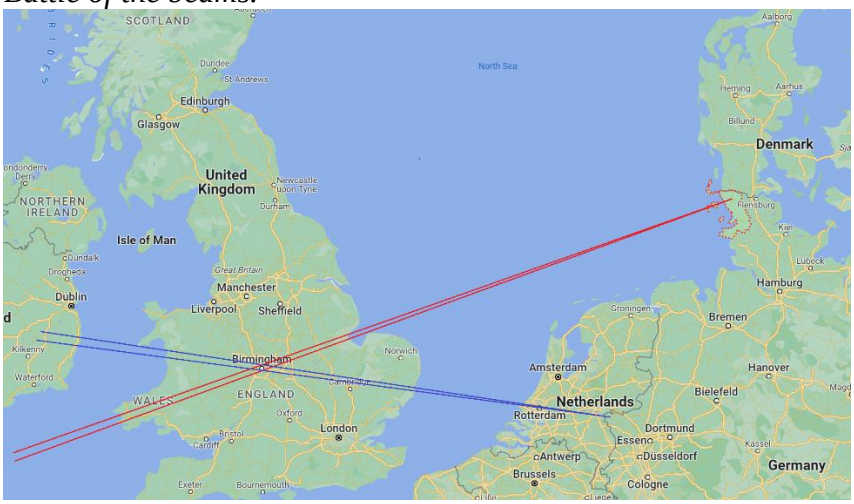
Un ejemplo de guerra electrónica es el caso de *Battle of the Beams* durante la WWII. Los alemanes tenían 2 grandes antenas direccionales de señales de radio (Knickebein y X-Gerät)

[28] Lo que cambia respecto a la inteligencia de señales del National Security Agency (NSA) / Central Security Services (CSS) es el alcance, propósito y contexto. La información electromagnética recopilada sin procesar es utilizada operativamente por *Electronic warfare Support* (ES) para mantener conciencia situacional. Es utilizada como SIGINT cuando es retenida y procesada por inteligencia, dando respuesta a requisitos específicos de inteligencia. En caso de conflicto entre ES e inteligencia, el comandante decide quien tiene prioridad (Joint Chiefs of Staff, 2012).

que utilizaban como sistema de navegación para guiarse durante la noche y bombardear los objetivos ingleses (Lorenz beam). Los alemanes conocían el punto donde debían atacar gracias a la señal de la segunda antena (Ver figura 17). Los británicos desarrollaron contramedidas de engaño imitando las señales de radio, indicando la posición incorrecta. Además, los engaños británicos hacían imposible el regreso a casa de los alemanes o inclusive terminaban aterrizando equivocadamente en pistas británicas (Manners, 2016).

Figura 17

Battle of the beams.



Nota. Las contramedidas de engaño británicas previnieron ataques (fuente imagen: elaboración propia a partir de Google maps).

Operaciones de información y psicológicas de la Central de Inteligencia.

La Central de Inteligencia (CIA) también tiene su injerencia en la guerra de la información y guerra psicológica, pero no se limitan únicamente a ello. Acorde al NSC 4-A (1947), NSC 10/2 (1948, amplía operaciones encubiertas) y NSC 59 (1950), entre otros; autoriza a la Office of Policy Coordination (posteriormente llamada Directorate of Plan, Directorate of Operations y finalmente National Clandestine Service - NCS) de la CIA, a realizar information operations y psychological operations abiertas/encubiertas en el extranjero, tanto en tiempo de paz como de guerra. Luego ampliado a operaciones de "propaganda, guerra económica; acción directa preventiva, incluidas las medidas de sabotaje, anti-sabotaje, demolición y evacuación; subversión contra estados hostiles, incluida la asistencia a movimientos clandestinos de resistencia, guerrillas y grupos de liberación de refugiados, y apoyo a elementos indígenas anticomunistas en países

amenazados del mundo libre" (Keane, Warner y Keefer, 2007). El NCS cuenta, entre otras divisiones, con una específica para Latinoamérica (revelado por Jeffrey Richelson en 2015 mediante FOIA[29] request).

Un ejemplo son los esfuerzos de guerra psicológica de la CIA contra Alemania oriental, donde se publicaba propaganda anticomunista durante 1950-1959. El nombre el código del proyecto era LCCASSOCK y el principal agente llamado Marbach (ex oficial de la marina nazi). Durante 1957, la CIA también interfirió con las elecciones de Alemania del Este enviando 15 mil globos por mes, con panfletos que atravesaban la cortina de hierro (Rid, 2020). Otro ejemplo es el escándalo Irán-Contra de los 80' que fue investigado por el Tower Commission (1986): donde EE.UU. vendió armas a Irán, que tenía un embargo armamentístico impuesto por el mismo país que le vendía armas. El dinero era utilizado para financiar a los Contra en Nicaragua que peleaban en oposición al gobierno de Nicaragua (movimiento de revolución sandinista que desplazó a los gobiernos dictatoriales en el 79 y tenía tendencias comunistas). El gobierno de facto argentino también colaboró a modo proxy dentro de la operación Charlie (Chomsky, 1986; Seoane, 2006; Balerini Casal, 2018).

La CIA cuenta con una división llamada Special Activities Center (SAC), como tercera opción para realizar *black operations* (operaciones clandestinas no reconocidas por ninguna agencia/estado), cuando la diplomacia y la acción militar no son posibles. Conformado por unidades especiales como SEAL Team Six (Naval Special Warfare Development Group) y Delta Force (1st Special Forces Operational Detachment–Delta), entre otras fuerzas especiales con conocimiento en *covert channels*, *cyber warfare*, explosivos, armas, combate, evasión de la aprensión, buceo, supervivencia, comunicaciones tácticas. El SAC se divide en dos grupos: el Special Operation Group (SOG), encargado de operaciones tácticas paramilitares; y el Political Action Group (PAG) encargado de operaciones políticas encubiertas, operaciones psicológicas, guerra económica y ciberguerra. Las misiones incluyen *humint*, raid, emboscadas, sabotaje, asesinatos y guerra no convencional (ej. entrenamiento de guerrillas, apoyo a medios de comunicación a fin, apoyo técnico para relaciones públicas, campañas publicitarias, apoyo a candidatos políticos que tomen decisiones que favorezcan la política de USA, etc.) (Rojas, 2022; Jacobsen, 2019). Dado que

[29] Freedom of Information Act.

las operaciones son secretas, poco se conoce de sus antecedentes, aunque algunas se han filtrado y como ejemplos podemos mencionar: El SOG participó de la lucha antiterrorista en Afganistán/Pakistán/Siria; el PAG impidió que el partido comunista italiano ganara las elecciones entre 1948 y finales de 1960, derrocó al gobierno de Irán en 1953 para hacerse del control del petróleo (Operación TPAJAX para EE.UU. y Operación Boot - Reino Unido[30]) y al gobierno de Guatemala en 1954, armó rebeldes en Indonesia durante 1957 y apoyó económicamente la federación sindical solidaridad luego de la ley marcial en Polonia en 1981 (Daugherty, 2004).

Actores en las operaciones de ciberguerra.

Es importante conocer los actores que intervienen en las ciber agresiones, dado que los mismos poseen diferentes motivaciones y capacidades técnicas. En relación, existen diferentes clasificaciones acordes a cada autor. Pese a ello, no resulta preponderante la clasificación por sí misma, sino la comprensión conceptual de los mismos. Los profesionales cuya tarea sea diseñar en una estrategia disuasiva/defensiva, previamente deben comprender los actores a los que se enfrentan. A modo pedagógico, clasificaremos los de actores como:

Individuos solitarios.

Habitualmente, estudiantes o personas curiosas que utilizan herramientas desarrolladas por otros (*script kiddies*). Aunque también los hay con intereses económicos personales. No cuentan con tanto conocimiento técnico y son fácil de disuadir. Sin embargo, no debe subestimarlos ya que la suerte y la perseverancia suele estar de su lado. Los ataques suelen ser más del tipo masivo en contraposición a los ataques focalizados que realizan los actores más avanzados que veremos a continuación. Como analogía, podría pensar en un pescador que arroja una red a la espera de cualquier presa.

[30] Según un documento clasificado filtrado al NYT, aparentemente habría incluido un ataque bomba simulando atribución al partido comunista que buscaba la nacionalización del crudo. Además de la utilización de propaganda (Risen, 2000). Posteriormente la CIA reconoció que participó del golpe de estado con sobornos a políticos/militares y con propaganda a favor del golpe, aunque alega que algunos documentos se perdieron (Byrne, 2013).

Grupos no organizados.

Usualmente con intereses ideológicos y capacidades mixtas. Al no estar organizados son un poco más fácil de desarticular. Nuevamente no debe subestimarse sus capacidades. Los foros y redes sociales pueden ser un medio para una posible coordinación. Pueden conseguir seguidores para una causa (similar a como opera una botnet, pero desde el plano psicológico). Realizar ataques al azar o a objetivos específicos (usualmente sus objetivos suelen ser organizaciones o gobiernos).

Una operación habitual es el *deface* o el *hack and dump*. En el primer caso modifican el *homepage* (sitio web principal) con algún tipo de mensaje. En el segundo caso realizan el robo[31] de información para su posterior publicación (leak). El efecto puede ser un impacto negativo por la información en si misma (si reflejan acciones no éticas o ilegales) o simplemente una pérdida de confianza de la institución para el cuidado y resguardo de la información de sus clientes/ciudadanos.

Grupos organizados (hackers, militares, terroristas, entre otros).

Son los más peligrosos porque poseen gran conocimiento técnico, recursos innumerables y una motivación inquebrantable. Pueden contar con financiación externa, herramientas propias/a medida (*cyberarms*), poseer vulnerabilidades *0 days*[32] (propias o de terceros), afectar la cadena de suministro, contar con implantes físicos en el hardware, poseen capacidades SIGINT (*Signal Intelligence*), tener espías infiltrados en la organización (*insiders*), entre otros.

Los intereses pueden ser tanto económicos, ideológicos, militares o estratégicos. Trabajan para un beneficio personal (*cybercrime*), por razones ideológicas (hacktivistas), razones religiosas/ideológicas (grupos terroristas), son contratados por corporaciones para sabotaje de la competencia / espionaje industrial, o simplemente trabajan para estados/naciones de forma directa (*cyberarmy*) o indirecta (*cybermercenary*). Es importante remarcar que no siempre es tan clara la clasificación. Por ejemplo, un ciber soldado que

[31] En términos legales no es correcto decir "robo", pero es adecuado para la comprensión del lector.
[32] Los *0 day* son vulnerabilidades no conocidas a la fecha y que por lo tanto no existe un parche o mitigación para la misma. Muchas veces los gobiernos utilizan empresas fantasmas dedicadas a comprar dichas vulnerabilidades en el mercado. Los profesionales acceden a participar en esos programas ya que las pagas suelen ser sustanciosas y además no conocen la finalidad para la cual va a ser utilizada dicha debilidad.

trabaja durante la semana para un estado nación puede realizar trabajos por su propia cuenta durante los fines de semana. En el caso de los grupos terroristas tampoco son fácil de estudiar ya que en el fondo suelen existir intereses y estados involucrados. Los servicios de inteligencia pueden alimentar/fomentar dichos grupos en beneficio propio y en contra de otras naciones. Utilizar técnicas de guerra cognitiva para captar adeptos les resulta sencillo y de muy bajo costo. Los ataques de falsa bandera o de desprestigio son su especialidad a la hora de justificar acciones posteriores en la población.

En el caso de los mercenarios/hackers contratados en la *Dark Net*[33], pueden trabajar en una porción especifica de un código (rutina) o tarea específica. Por lo tanto, desconocen para quien trabajan o la finalidad de lo que hacen (sesgo). Cuando son contratados por un tercero nos referimos que trabajan a modo de proxy[34], evitando la atribución directa del atacante (ideólogo).

Como se indica a lo largo del trabajo, los objetivos de los estados/naciones son diversos y van desde inteligencia, robo tecnológico, sabotajes financieros, sabotaje a proyectos estratégicos (ej. nucleares), implantación de *kill switch*[35] en tiempos de paz para tener disponibles en tiempos de guerra, actos de ciberguerra, entre otros.

Dentro de la última clasificación de actores avanzados, cabe la mención de los grupos denominados *Advanced Persistent Threats* (APT). Estos son *Advanced* por los conocimientos técnicos, las herramientas que utilizan y la información de inteligencia para coordinar las operaciones (*Computer Network Operations*). Son *Persistent* porque tienen un objetivo específico y toman todo el tiempo que se requiera para completarlo. Buscan

[33] Término habitualmente confundido con *Deep Web*. Acorde a (Bergman, 2001), la *Deep Web*, en contraposición a la *Surface Web*, es la que no puede ser encontrada por los buscadores tradicionales. Por otra parte, según (Biddle, England, Peinado y Willman, 2003), la *Dark Net*, es una colección de redes y tecnologías utilizadas para compartir contenido digital. La *Dark Net* no es una red física separada, sino una capa de aplicación y protocolo que se encuentra en las redes existentes. Ejemplos de redes oscuras son el intercambio de archivos entre pares, la copia de CD y DVD y el intercambio de claves o contraseñas en correos electrónicos y grupos de noticias (Biddle et al., 2003). Algunos ejemplos de *Dark Net* son la *Freenet* de (Clarke, Sandberg, Wiley y Hong, 2001) o la red *TOR* de (Syverson, Tsudik, Reed y Landwehr, 2001) cuyos inicios datan de 1995 en el U.S. Naval Research Laboratory (Tor Project, s.f.). Estas redes son utilizadas por amantes de la privacidad, periodistas, intercambio de información, hackers, criminales, entre otras.

[34] Cuando actúa en nombre de otra persona. Similar a como trabaja un *Proxy Server*, donde la dirección de origen (*IP*) queda enmascarada por la dirección del proxy server.

[35] Funcionalidad para apagar/deshabilitar un dispositivo o software. En el contexto citado, una funcionalidad latente implantada en un sistema que, una vez activada mediante una señal o evento, puede desencadenar una acción especifica como destrucción (bomba lógica) o deshabilitar sistemas (afectar disponibilidad).

disponer de accesos redundantes de los sistemas para no perder el control de estos y poseen mucha paciencia y perseverancia. Pasan muchos meses de forma sigilosa dentro de las organizaciones obteniendo información para sus operaciones, efectuando movimientos laterales y escalando privilegios[36]. Usualmente se menciona que operan *low-and-slow* en referencia a movimientos sigilosos para no llamar la atención de los "radares" o defensores. Finalmente, se dice *Threats* debido a sus intenciones y capacidades malintencionadas de alto impacto.

Los investigadores clasifican a los APT basado en *fingerprint*[37] que encuentran en los códigos fuentes de los *malware*, similitud con otros ataques (modus operandi), objetivos logrados, analizando contextos geopolíticos (quien se beneficia), entro otros. Algunos investigadores los clasifican por nombres, mientras que otros utilizan números. Es por ello por lo que un mismo APT contiene un numero identificador y puede tener más de un nombre a la vez. Por ejemplo: el APT28 es también llamado Fancy Bear según la firma CrowdStrike, Sofacy Group según Kaspersky, Tsar Team según FireEye[38]. Es importante notar que los informes en las investigaciones a veces pueden contener sesgos debido al país donde residen o la historia de sus integrantes (vinculados al gobierno, contratistas, exfuncionarios), por lo cual siempre resulta importante disponer de múltiples fuentes y un análisis crítico.

Existe un punto importante a remarcar sobre el origen de los ataques. Usualmente, la atribución de los ataques suele ser más una presunción que una evidencia sólida contundente. Ello se debe en parte a la naturaleza del ciberespacio. Los APT pueden utilizar herramientas robadas de otros estados/naciones, compartir/vender código fuente en foros o simplemente imitar el comportamiento de otro estado/grupo con la finalidad de desviar el foco de la investigación. Por ejemplo, acorde a una filtración de WIKILEAKS, la CIA (Central Intelligence of Agency) cuenta con un grupo de trabajo remoto denominado UMBRAGE destinado al robo de técnicas de otros estados/naciones, incluyendo Rusia, con la finalidad especifica de engañar a los investigadores forenses a que falsamente atribuyan ciertos

[36] Una analogía de los movimientos laterales y escalamiento de privilegios podría ser el juego de arcade Donkey Kong. Para escalar cada piso Mario debe previamente moverse lateralmente hasta las escaleras, con diferentes movimientos laterales y de escalamiento finalmente logra su objetivo de llegar donde se encuentra la princesa.
[37] Al igual que una huella dactilar, es un elemento digital utilizado para identificar al autor de una acción dentro del dominio de las TICS.
[38] Los estados también identifican a los *Threat Actors*. Ejemplo: MAKERSMARK para el grupo TURLA.

ataques a otras naciones (Madhani, Heath y Kelly, 2017). Es por eso por lo que no deben descartarse los ataques de falsa bandera con la finalidad de desprestigio de ciertos estados dentro de un plan superior de operación psicológica; o de obtener cuantiosos contratos de defensa.

Características del teatro de operaciones.

La guerra ha evolucionado a lo largo de la historia en función de los nuevos descubrimientos/conocimientos y del desarrollo de técnicas que permitieron un aprovechamiento más eficiente de los medios y de los recursos. Tanto la tecnología como la estrategia suscitan una ventaja competitiva frente al adversario.

El dominio tradicional por excelencia es el terrestre (1ro). Podemos observar su evolución con la incorporación del forjado de armas en metales, la utilización de caballería, el descubrimiento de la pólvora, el desarrollo del tanque en la guerra de trincheras, etc. Las técnicas también forman parte de la evolución. Por ejemplo, Alejandro Magno utilizaba la infantería firme como un yunque y la veloz/aplastante caballería como un martillo. En el caso de la batalla de Gaugamela, derrotó al ejército del rey persa Darío que lo superaba ampliamente en número. La inusual estrategia consistió atacar directamente al rey persa, causando la retirada y desorganización del ejercito enemigo.

Con la invención de los barcos surgió el dominio marítimo (2do) y muchos años después aparece el dominio aéreo (3do) con el descubrimiento de los aviones. A partir de la carrera espacial nace el dominio del espacio exterior (4to) y con las TICS el dominio del ciberespacio (5to). En un futuro es posible que veamos dominios como: biotecnología, logística, cognitivo, etc.

A modo de referencia, la doctrina militar de Estados Unidos plantea estos cinco dominios principales de operaciones que operan de forma independiente. Su visión futura es el desarrollo de una integración multidominio con una coordinación e intercambio de información entre los diferentes dominios. Con lo cual la adquisición de información, las comunicaciones/coordinación y la denegación del enemigo, resultaran un punto crítico.

El plano del ciberespacio presenta características específicas que resultan de vital importancia su conocimiento y comprensión.

Podríamos afirmar que las TIC tienen su propia lógica e incluso su propia tribu/cultura. Fuera del ciberespacio, ya sea por curiosidad o simplemente alegando que se trata de una vulnerabilidad de diseño que debe ser mejorada, usualmente no observamos individuos cortando el freno en los vehículos o rompiendo columnas en edificios. Algunos factores que conformaron la cultura actual en el ciberespacio podrían ser: la cultura hacker, el anonimato, el subgénero ciberpunk de ciencia ficción y la poca transcendencia que podían significar modificar algunos bits, entre otros factores. Lo que antiguamente podía ser una picardía, hoy en día tiene implicancias preponderantes e inclusive puede tener un impacto directo sobre la sociedad, la economía o la seguridad de las vidas humanas (*safety*).

Por empezar, en el ciberespacio las distancias digitales son reducidas y tanto la comunicación como los ataques son prácticamente instantáneos desde un lado al otro del mundo. Las fronteras entre países desaparecen, la jurisdicción suele no ser clara y las legislaciones pueden no estar adecuadas a la actualidad.

La evidencia digital puede perdurar cuasi eterna en el tiempo en una imagen forense, solo limitada por la vida útil del medio; sin embargo, los sistemas en su estado dinámico cambian permanentemente y no siempre cuentan con las capacidades de registros (logs).

La información discretizada en bits puede ser copiada de forma perfecta y de manera cuasi instantánea (tanto el duplicado de información, como ciberarmas propias / ajenas). Los costos de ciber operaciones/ciberarmas son reducidos en comparación con los otros dominios (ej. fabricar tanques). Además, hablamos de asimetría dado que los países en subdesarrollo quedan equiparados las potencias en capacidades[39].

Las ciber armas tienen una peculiaridad. Por un lado, son sumamente poderosas. Sin embargo, basta con un parche de seguridad para transformar meses o años de investigación y desarrollo en obsoletos.

En los dominios tradicionales un atacante requería una relación de 3 a 1 respecto de un defensor, sin embargo, en el ciberespacio el atacante se encuentra en igualdad o inclusive con una ventaja sobre el defensor.

[39] A futuro, con el desarrollo de ciberarmas, la creciente información de la vigilancia masiva, la inteligencia artificial y las tecnologías exponenciales es posible que algunos países ganen la carrera del ciberespacio y rompan con dicha asimetría.

Todas estas características incentivan al ciberespacio a un estado de guerra permanente en tiempos de paz, usualmente por debajo de cierto umbral para prevenir una escalada.

El teatro de operaciones descripto además presenta un problema de atribución, dado que no es simple identificar el origen de los ataques. Los posibles escenarios son diversos. Un atacante "A", puede comprometer servidores en un país "B" para posteriormente atacar la infraestructura de un país "C"; quedando "B" como origen del ataque (Ver figura 18). Además, "A" puede lanzar un *wiper*[40] en su retirada con la finalidad de destruir la evidencia del primer compromiso. Asimismo, "A" podría plantar una falsa evidencia, comprometiendo aún más a "B". Otro posible escenario es que "A" podría querer enemistar a "C" con "B"; o inclusive, realizar un ataque falso de bandera contra sí mismo con la finalidad de justificar un posterior contrataque contra su víctima original (Ver figura 19). Es por ello por lo que las propuestas de contrataque (*retaliation*), en concepto de una legítima defensa, son insuficientes para abordar la problemática. Así mismo, resultan irresponsables y peligrosas. Según el Australian Strategic Policy Institute, en 2019 surge el primer antecedente de un contrataque cinético en respuesta a un supuesto ciberataque. La fuerza aérea de Israel, luego de eliminar un supuesto *malware* (HamasCyberHQ.exe) del cual no dieron mayores explicaciones, bombardeó un edificio en la franja de gaza, alegando que se trataba de un edificio de cyber operaciones de Hamas (Thomas, 2019). ¿Contrataque o excusa perfecta?[41]

Por otra parte, las noticias sobre ciberataques deben ser tomadas con cautela. En ocasiones, presentan una componente propagandista para difamar otros estados. Además de causar cierto ánimo en la población, para luego justificar cuantiosos contratos de inversión de en defensa.

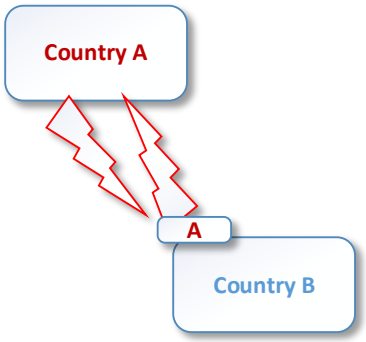
[40] Borrado seguro / no recuperable.
[41] Como se ha remarcado en varias oportunidades, no es menester del presente trabajo responder o investigar situaciones puntuales, ni tomar posturas. Si no plantear conceptualmente la problemática a la cual nos enfrentamos, abrir un espacio de debate y fomentar al intercambio de ideas. Incentivando el pensamiento crítico del lector a que pueda profundizar en la temática y sacar sus propias conclusiones.

Figura 18
Atribution problems.



Nota. A ataca a B para luego atacar a C, dejando a B como atacante (fuente: elaboración propia).

Figura 19
Atribution problems.



Nota. A realiza un ataque de falsa bandera, justificando una supuesta legítima defensa contra B (fuente: elaboración propia basado en los conceptos tratados).

El ciberespacio tiene su complejidad. Dentro del actual conflicto entre Rusia y Ucrania (2022), los rusos han lanzado varios ciberataques del tipo w*iper* al mismo tiempo que iniciaron una ofensiva terrestre y aérea dentro de un esquema de guerra híbrida. Por otra parte, una cuenta de Twitter no oficial de "Anonymous" llamó a los hackers del mundo a atacar a Rusia (Milmo, 2022). Desde entonces se realizaron gran cantidad de ataques a diferentes sitios web, incluyendo el leak de 28GB de información del banco central de Rusia (Scott, 2022). ¿Quién está detrás de esta cuenta? ¿Son los ataques de ciudadanos auto convocados o es una pantalla de algunos países para realizar ciber operaciones dentro de un plano no tangible? Estas son algunos aspectos típicos que reflejan la complejidad del teatro de operaciones de las guerras modernas, dentro del ciberespacio.

Como se ha identificado, las características del ciberespacio potencian las capacidades de la guerra híbrida, la cual detallaremos adelante.

Guerra sin límites (Unrestricted warfare).

Más de 70 años bajo una guerra invisible…

La guerra híbrida es también conocida como guerra no convencional, guerra de las sombras, o como fue publicado en 1999 por China People Liberation Army (PLA): guerra sin restricción. La misma, definida:

> Utilizando todos los medios, incluyendo las fuerzas armadas o no armadas, militar o no militar, letal o no letal para obligar al enemigo a aceptar los intereses propios […] Guerra que trasciende las fronteras y limites, en pocas palabras, *unrestricted warfare* […] El nuevo concepto de armas es diferente y trasciende el dominio tradicional […] No hay nada que no pueda ser un arma […] producir un *crash* del mercado de acciones, una invasión de un virus de computación, un simple rumor/escándalo que afecte la moneda o exponga a los líderes, son todos ejemplos de las nuevas armas […] en las guerras contemporáneas existe una diferencia entre los objetivos manifiestos [ante la población] y los objetivos encubiertos [ej. decir que van a ayudar cuando en realidad van en busca del petróleo] […] La mejor manera de obtener la victoria no es mediante la muerte si no mediante el control […] El espacio tecnológico permite penetrar y controlar espacio convencional sin necesidad de ocupación […] tanto la tecnología militar y civil como los soldados profesionales y guerreros no profesionales se solapan y la línea divisoria es cada vez menos clara […] el campo de batalla es en todas partes. Otros medios incluyen *psychological warfare* (esparcir rumores para intimidar al enemigo o quebrar su voluntad), *smuggling warfare* (arrojar los mercados en confusión y atacar el orden económico), *media warfare* (manipular que ve y escucha la gente para dirigir la opinión pública), *drug warfare* (obtener un repentino y enorme beneficio ilegal al esparcir desastre en otros países), *network warfare* (aventurarse en secretos y ocultar la propia identidad en un tipo de guerra contra la que es prácticamente imposible protegerse), *technological warfare* (crear monopolios mediante el establecimiento de normas), *fabrication warfare* (presentar una falsa apariencia de fuerza real ante los ojos del enemigo), *resources warfare* (acaparamiento de riquezas saqueando reservas de recursos), *economic aid warfare* (otorgando favor abiertamente e idear el control de los asuntos en secreto), *cultural warware* (liderando las tendencias culturales para asimilar a aquellos con una visión diferente), *international law warfare* (aprovechar la oportunidad más temprana para establecer regulaciones), etc […] el objetivo es utilizar todos los medios (medios que impliquen la fuerza de las armas y medios que no impliquen la fuerza de las armas, medios que impliquen poder militar y medios y que no impliquen poder militar, medios que impliquen bajas y medios que no impliquen bajas) para forzar el enemigo al servicio de los intereses propios […] Con la asistencia de la prensa mediática, los comandantes influyen los ojos y oídos del mundo entero, haciendo que la gente vea todo lo que los militares quieran que vean, mientras que nadie puede ver absolutamente nada de lo que no quieran mostrar […] la fuerza de los reporteros tiene un efecto dramático en la dirección estratégica y alcance de las operaciones militares [ej. utilización del manual *FM100-6 Information Operation* durante la guerra del golfo] […] La fuerza de los

> medios de comunicación será cada vez más un jugador importante en promover el curso de la guerra con un rol comparable a un ataque militar […] ya no será posible depender únicamente de la fuerza militar sin la participación de los medios de comunicación para lograr la victoria en la guerra. (Qiao y Wang, 1999).

Como veremos más adelante, en algunas operaciones dentro de la guerra híbrida invisibilizan al enemigo. Se trata de una guerra invisible que utiliza medios de aniquilación/dominación mientras que por otra parte puede valerse de la propaganda para mostrarse como aliado.

Rusia / OTAN.

Rusia ha sacado provecho de la guerra híbrida en diferentes teatros de operaciones de forma estratégica. Esta guerra híbrida/no lineal, es mal llamada doctrina Gerasimov (Galeotti, 2013). Rusia parece intentar de recuperar la influencia de poder que tenía antiguamente la Unión Soviética[42] y de contrarrestar los avances de la OTAN[43] sobre los países del este de Europa (Ver figura 20).

Como indica Morris (2015): "Los medios no militares han superado el poder de la fuerza para lograr objetivos estratégicos y políticos". Los ciberataques a la infraestructura de Estonia en 2007 como represalia a la relocalización del monumento del soldado de bronce son evidencia directa de ello. Tales ataques no fueron reconocidos por el gobierno ruso, alegando un movimiento de ciudadanos indignados. La denegación de servicios obligó a Estonia a desconectar al país durante algunos días de internet y Alemania acudió en su ayuda con la ciberdefensa. Como consecuencia del incidente se crea el Cooperative Cyber Defence Centre of Excellence (CCDCOE) en Tallin.

Durante 2008, Rusia apoyó a los separatistas de Osetia del Sur en Georgia, mientras que Georgia solo reconoce dicho territorio como propio, dando así un nuevo conflicto. Como

[42] De aquí en adelante, indistintamente como URSS.
[43] La OTAN, en ingles NATO (North Atlantic Treaty Organization), se formó en 1949 como disuasión a la amenaza soviética después de la WWII. Utilizado por USA como herramienta política en el continente europeo. Su origen se remonta a 1947 con el tratado Dunkerque entre Francia y Reino unido contra la eventualidad de un ataque alemán. La OTAN, entre otras cosas, especifica en su artículo 5, que un ataque armado contra uno de sus miembros se considera como un ataque contra todos ellos (defensa colectiva). La URSS, en respuesta a la OTAN, crea el Warsaw Pact en 1955. Para Rusia, la posibilidad de que el país satélite soviético de Ucrania ingrese a la OTAN es una línea roja (Kiebler, 2022).

paralelismo, algunos autores (Rankin, 2017; Wilson, 2020; s.n., 2021) indican el apoyo de Rusia al movimiento separatista catalán en España durante 2017.

Figura 20

NATO Expansion by year.



Nota. (fuente imagen: OTAN como fue citado por Kiebler, 2022).

En 2014 se producen ciberataques[44] y envío de soldados sin bandera (conocidos como "little green mens") a Ucrania. Dicha operación finaliza con la anexión de la península de Crimea a Rusia (Greenberg, 2019). Durante 2022 (actualidad), resurge nuevamente el conflicto con Ucrania con una intervención que combina ciberataques[45]. Rusia no reconoce una "invasión", sino como una "operación especial" para desmilitarizar la región, remover supuestos grupos "nazis" del poder y garantizar la seguridad de Rusia (Russian Defense Ministry como fue citado por el U.S. Department of State, s.f.). Por su parte la OTAN

[44] Mencionaremos algunos en el capítulo 3.

[45] Los sitios web del ministerio de defensa y de las fuerzas armadas, junto con 2 bancos del estado; fueron atacados por un ataque de DDOS (Denegación de servicio distribuido) (Centre for Strategic Communications and Information Security, 2022). También reportados 70 sitios afectados con la leyenda "prepárense para lo peor" (*defacement attack* buscando con un efecto psicológico) (Tidy, 2022).

denuncia una invasión ilegitima, entrega armamento[46]/información de inteligencia a Ucrania, incentiva sumarse en la defensa como voluntarios[47], envía fuerzas especiales encubiertas[48], aplica sanciones[49] (incautación de bienes, denegar el uso de la red SWIFT[50], restricciones tecnológicas[51]), fomenta la propaganda en los medios de comunicación al mismo tiempo que censura los medios rusos[52], promueve la ruptura de lazos económicos con Rusia mientras que refuerza sus intereses económicos (en particular los relacionados con la energía[53]). En el plano del ciberespacio, el IT Army of Ukraine convoca voluntarios para atacar sitios web rusos (Pearson, 2022) mientras que una supuesta cuenta del grupo Anonymous llama a la ciberguerra contra Rusia (Milmo, 2022).

Durante el presente conflicto se han observado diferentes estrategias en el plano militar y psicológico. Ucrania ha denunciado reiteradas oportunidades ataques sobre las centrales nucleares y la necesidad de una respuesta militar internacional. Afirmación falaz en el contexto tratado, dado que dicho ataque no resulta beneficioso para el agresor[54]. Rusia aprovecha este hecho resguardando tropas y provisiones en dichas centrales. Desde un principio, Rusia intentó dominar la capital ucraniana en un esquema del tipo guerra

[46] Entre otros, Mi-17 helicopters, Javelin anti-armor systems, Switchblade unmanned aerial vehicles, arms/munitions, body armor, High Mobility Artillery Rocket Systems, grenade launchers, patrol boats, Advanced Surface-to-Air Missile Systems, counter-artillery radars, Phoenix Ghost Tactical Unmanned Aerial Systems, C-4 explosives, demolition munitions, and demolition equipment, Claymore anti-personnel munitions, VAMPIRE Counter-Unmanned Aerial Systems, Laser-guided rocket systems, Puma Unmanned Aerial Systems (UAS) and support equipment for Scan Eagle UAS systems, Night vision devices, Howitzers, T-72B Tanks, Tactical secure communications systems and surveillance systems (U.S. Department of Defense, s.f.) y Tranques Abrams (Pruchnicka, 2023).
[47] Ucrania llama a voluntarios de otras naciones (McKernan, 2022) lo cual tuvo mucha repercusión mediática como el caso del francotirador Wali (nickname) (Woodward, 2022; Brewster, Burke, 2022).
[48] Documentos filtrados indican la participación encubierta de fuerzas especiales (Davies, Ganguly, 2023; Averre, 2023).
[49] (The White House, 2022; U.S. Department of State, 2023; European Council, 2023; EUR-Lex, 2022).
[50] Estados Unidos, Reino Unido, Canadá y la Union Europea tomaron la decisión de quitar a los bancos rusos del sistema Swift (Proveedor de servicios seguros de mensajería financiera) (European Commision, 2022; Swift 2022). Visa y MasterCard bloquearon su uso en redes rusas (TELAM, 2022).
[51] La Casa Blanca anunció restricciones a los procesadores/chip de Intel, Nvidia y Qualcomm (TELAM, 2022).
[52] Como ejemplos: Youtube bloqueo RT news (Paresh, 2022) y Facebook a RT News como Sputnik (Culliford, 2022).
[53] Estados Unidos obtuvo enormes ganancias vendiendo gas natural a Europa a medida que los precios se disparaban (Robertson, 2022). Las importaciones de GNL se incrementaron en 148% (US Department of Energy como fue citado por Donnelly, 2023), Europa es el principal destinatario de exportaciones de Estados Unidos (U.S. Energy Information Administration, 2023).
[54] No resulta beneficioso dada la proximidad como la intención de una posible anexión de territorios. Los ataques buscan evitar cualquier intervención internacional que complique la avanzada.

relámpago y de presiones psicológicas a las cuales la voluntad ucraniana no ha claudicado. Las tropas ucranianas evitaron las batallas en terrenos abiertos y utilizaron las ciudades civiles como escudo, causando emboscadas a las avanzadas rusas. Cualquier bombardeo ruso es condenado como un ataque contra la población civil. La utilización de los misiles Javelin provistos por la OTAN junto con los drones turcos Bayraktar han sido decisivos para causar grandes daños al ejército invasor.

Pero sin lugar a duda, la estrategia suprema la ha planteado EE.UU., ganando sin necesidad de pelear. El aprovisionamiento de armamento impulsa su deteriorada economía (golpeada por el COVID). Por un lado, causas grandes bajas a su enemigo ruso, mientas que, por otra parte, endeuda a Ucrania. La cual deberá hacer frente económicamente privando su futuro o entregando recursos a cambio. La propaganda se utiliza para socavar la imagen de Rusia y favorecer la figura de EE.UU. Finalmente, el lobby político, ha logrado cortar los lazos económicos en Europa respecto al suministro de gas ruso y otros negocios. Como consecuencia, Europa ha caído en una crisis conveniente para EE.UU., quien les vende gas licuado a precios elevados. El contexto resulta un adecuado pretexto para justificar la inflación norteamericana causada por la emisión monetaria[55] más grande de la que se tenga recuerdo.

Próximo a la entrega del presente trabajo, se produce el sabotaje al gasoducto Nord Stream 1 y Nord Stream 2 con la utilización de explosivos[56] (Ver figura 21). El precio del gas incrementó su valor, pero luego decreció al bajar la incertidumbre vinculada al suministro del gas ruso (DW News, 2023). Durante el atentado, se inauguró un gasoducto que une Noruega con Polonia a través de Dinamarca que busca reducir la dependencia de Rusia (Scislowska, Olsen y Keyton, 2022). Las hipótesis de sabotaje son diversas: una falta bandera rusa para evitar sanciones por el corte del suministro de gas, una operación de Ucrania contra Rusia o un ataque de EE.UU. que obtiene ventajas económicas por la venta de gas licuado, entre otras posibilidades (DW News, 2023). El presidente norteamericano había prometido poner fin al gasoducto. En palabras del presidente Joe Biden (Daily Mail, 2022): “Pondremos fin a esto […] te prometo que seremos capaces de hacerlo”. Las

[55] (Orgaz, 2020).
[56] Si bien la noticia es reciente, resulta de interés para la investigación.

investigaciones alemanas apuntan a un velero ("Andrómeda") que se encontraba en el lugar del hecho, donde posteriormente encontraron rastros de los mismos explosivos utilizados. Esta pista apunta a sus tripulantes ucranianos bajo órdenes de un general ucraniano (von Hein, 2023). Sin embargo, hasta el momento no existen confirmaciones ni es prudente realizar afirmaciones. En términos legales, "el gasoducto es un proyecto de infraestructura civil, y de acuerdo con los estatutos de Roma, del Tribunal Penal Internacional, la destrucción de infraestructura civil es incluso un crimen de guerra", en caso de un tercer país involucrado: "el asunto no podría ser evaluado en el marco del derecho de guerra, sino que sería en último término un ataque terrorista" (Talmon como fue citado por von Hein, 2023). Ello nos lleva a comprender que el perpetuador de esta operación clandestina no confirmará su autoría. Demostrando la dificultad de determinar las atribuciones en las operaciones de guerra híbrida. No siempre tan claras o directas como se podría llegar a pensar. De aquí en más, solo quedan tres posibilidades respecto de la verdad: se puede encontrar, extraviar o fraguar.

Figura 21

Sabotaje con explosiones.



Nota. Provee gas desde Rusia hacia Alemania (fuente video: DW News, 2022).

En relación con el conflicto con Ucrania. La información de inteligencia entregada es un elemento crítico y decisivo para cualquier conflicto. La misma habría sido provista por inteligencia norteamericana para localizar y asesinar a generales de alto rango rusos (Barnes, Cooper y Schmitt, 2022). Similarmente, un P-8A Poseidón de vigilancia marítima norteamericano localizó al buque insignia ruso (Moskva) (Boyle, 2022; Dilanian, Kube y Lee, 2022) que fue posteriormente hundido a causa del impacto de 2 misiles ucranianos R-360 Neptune, mientas los sistemas defensivos del buque podrían haber sido engañados por

un drone TB2 Bayraktar (Trevithick y Togoway, 2022); por otro lado, la administración de Biden negó brindar información a Ucrania y transmitió que las filtraciones deben detenerse (Lee, Kube y Dilanian, 2022). Estos ataques apuntan no solo a causar daños económicos sino también un golpe psicológico a la moral. Resulta inevitable citar el paralelismo con el hundimiento[57] del ARA General Belgrano en el conflicto por Malvinas. En aquella oportunidad, EE.UU. se declaraba públicamente como neutral en el conflicto, mientras que la CIA encubiertamente brindaba a Reino Unido información de apoyo logístico e inteligencia detallada (satelital) sobre las fuerzas argentinas, tal como es revelado en la desclasificación de documentos (Osorio, Christiano y Maskell, 2012).

Operación Gladio y Cóndor.

En los últimos años la propaganda ha puesto de moda el concepto de guerra híbrida, como una cuestión poco ética, remarcando el peligro de China sobre occidente. Sin embargo, el concepto de guerra híbrida no es nuevo. Desde la creación de la CIA en 1947 (cuando Harry S. Truman firma the National Security Act) y la NSA en 1952 (Burns, 1990); EE.UU. ha realizado todo tipo de operaciones encubiertas a lo largo del mundo, con la finalidad de garantizar su influencia de poder y sus intereses. Tal es el caso del plan Gladio de la CIA junto al MI6 de Reino Unido. A través de la OTAN, durante la guerra fría, crearon y entrenaron ejércitos secretos llamados *stay behind* con la finalidad de realizar operaciones tras las líneas enemigas en caso de una invasión soviética sobre territorio europeo (Ganser, 2005, 2007). Dado que la supuesta invasión soviética nunca llegó y las ideas comunistas empezaron a ganar poder a través de la democracia y el voto popular, dichos ejércitos tomaron un rol diferente. En combinación con diferentes grupos de ultraderecha de cada país, llevaron a cabo diferentes tipos de ataques falsa bandera, golpes de estado y atentados a lo largo de Europa[58]. Posteriormente fue extendido a América latina durante los 70’ bajo

[57] Autores como (Pellicer como fue citado por Natalizio, s.f.), plantean el debate de que el hundimiento se trató de un crimen. El Belgrano no fue hundido en momentos en que se dirigía a atacar a las unidades inglesas, sino cuando se hallaba navegando en dirección al continente desde hacía varias horas y que no fue atacado al ser sorprendido en una incursión, sino después de un prolongado seguimiento por el submarino (Parlamento inglés relatado por Pellicer como fue citado por Natalizio, 2013).

[58] Uno de los ejemplos citados es el atentado a la Piazza Fontana en Italia durante 1969. Según el testimonio del ex jefe de la contrainteligencia italiana General Giandelio Maletti, el servicio de inteligencia italiano colocó evidencias falsas (piezas de bombas) para culpar a los comunistas y a la extrema izquierda (Comisión parlamentaria del Senado de la República como fue citado por Ganser, 2007).

la operación Cóndor (Ganser, 2005). La idea de los ejércitos *stay behind* nació en Inglaterra durante 1940 ante el temor de una invasión Nazi a las islas británicas. El Estado Mayor propuso la organización de grupos armados tras las líneas enemigas, llevando acciones de guerrilla contra las fuerzas de ocupación (Cacciatore, 2021; Avilés, 2019).

La teoría de Ganser vinculada con al terrorismo suele ser criticada. Por citar algún autor, Avilés (2019) sostiene que las actividades terroristas son teorías conspirativas infundadas, dado que las investigaciones parlamentarias en Italia no encontraron pruebas concretas de que Gladio hubiera estado implicado de alguna manera en la supuesta estrategia de la tensión. Sin embargo; menciona documentos que fueron destruidos, dificultando la investigación. Según (informe del Comité Parlamentario para los Servicios de Información y Seguridad de 1992 como fue citado por Avilés, 2019) no había pruebas ni indicios concretos, aunque ello no implicara llegar a conclusiones definitivas. Por otra parte, uno de los documentos (US Army Field Manual 30-31B) mencionados por Ganser es cuestionado por Peer Henrik Hasen. Thomas Rid, opina que se trata de una falsificación de la oficina "A" de la KGB para desprestigiar a EE.UU. (Rid, 2020). Por otro lado, Licio Gelli reafirma que la CIA le entregó dicho documento y es genuino (Francovich, 1992).

Ello evidencia la difícil tarea de encontrar la verdad en el mundo del engaño y la desinformación. El debate académico en relación con el tema continua vigente[59]. El solo hecho de plantar una duda es en sí un elemento relevante dentro del esquema de guerra híbrida. En relación, cuando no es factible encontrar la verdad, los hechos puntuales pasan a ser secundarios y resulta más indicativo para un investigador apreciar la historia a lo largo de patrones reiterativos que marcan un modus operandi. El caso Gladio resulta de interés con paralelismos históricos inquietante; cuyas investigaciones debieran profundizarse más allá de la breve mención en el presente apartado.

Con relación a nuestro país, durante el periodo de la operación Cóndor, el ex secretario de estado Henry Kissinger (Ver figura 22) con colaboración del FBI, es mencionado como autor intelectual de diferentes crímenes de guerra (Hitchen, 2001). Indicamos el paralelismo en las fotos con la invasión de Indonesia a Timor oriental en el 75' (Ver figura 23). Acorde

[59] El National Security Archive de George Washington University intentó solicitar información vía Freedom of Information Act (FOIA), a lo cual la CIA respondió que "no puede confirmar ni negar la existencia o no existencia de registros que respondan a su solicitud" (como fue citado por Ganser, 2007).

a documentos desclasificados, EE.UU. y Reino Unido dieron apoyó a la invasión de Timor incluyendo la provisión de armas[60]. Lo que llevó a una serie de atrocidades en la región, estimando 200 mil muertes (Burr y Evans, 2001; Simpson y Venkatasubramanian, 2019; Downson, s.f.); incluyendo 5 periodistas conocidos como Balibo Five[61]. Posteriormente, la administración de Carter aumentó la venta de armas, incluyendo a otros países como Canadá, Inglaterra, Holanda. La cobertura mediática de las atrocidades fue prácticamente nula (Chomsky, como fue citado por Achbar y Wintonick, 1992).

Figura 22

Secretario de estado de EE.UU. en Argentina y Chile.



Nota. A la izquierda junto con Videla, lo felicitó por su trabajo durante su visita en el mundial de futbol del 78' (fuente imagen: Sagaian, s.f.). A la derecha junto a Pinochet en el 76' (fuente imagen: galería Bettmann como fue citado por Laborde, 2023).

[60] El contexto: Timor era una colonia de Portugal y grupos de izquierda lograron la independencia. En el contexto de la guerra fría lo consideraban una tendencia peligrosa para la región. Otros antecedentes en la región fueron los bombardeos encubiertos en Laos, Cambodia y Vietnam (Operation Menu y Operation Freedom Deal) (guerra de Vietnam y guerra Civil en Cambodia).

[61] Dos australianos, dos británicos y un zelandés asesinados en la ciudad de Balibo.

Figura 23

Secretario de estado de EE.UU. en Indonesia.



Nota. Henry Kissinger y el presidente Gerald Ford dando su apoyo al presidente Suharto días previos a la invasión del 75' (fuente imagen: Kennerly, s.f.).

Documentos desclasificados reafirman que el secretario de estado conocía sobre los planes de golpe de estado en Argentina. Sin embargo, dieron su asistencia y apoyo. En una transcripción de Kornbluh del National Security sobre una reunión desclasificada (The Secretary's Staff Meeting – Friday, 3/26/76):

> William Rogers informa a Kissinger que para que el gobierno militar tenga éxito, los generales harán "un esfuerzo considerable para involucrar a Estados Unidos, particularmente en el campo financiero". Kissinger responde: "Sí, pero eso nos interesa". Rogers advierte que "no debemos apresurarnos en este momento y abrazar este nuevo régimen" porque espera una represión significativa después del golpe. "Creo que también debemos esperar una buena cantidad de represión, probablemente mucha sangre, en Argentina en poco tiempo. Creo que van a tener que ser muy duros no solo con los terroristas sino también con los disidentes de los sindicatos y de sus partidos". Pero Kissinger deja claras sus preferencias: "Sea cual sea la oportunidad que tengan, necesitarán un poco de aliento... porque yo sí quiero alentarlos. No quiero dar la sensación de que están hostigados por Estados Unidos". El 27 de marzo de 1976, el FMI liberó $127 millones en crédito para la junta militar, y poco después de que el gobierno de Videla llegara al poder, la administración de Ford aprobó silenciosamente $49 millones en asistencia de seguridad. Esto marcó el comienzo de una serie de decisiones políticas que brindaron un apoyo esencialmente irrestricto a los generales argentinos.

Según Osorio (2004), en la reunión desclasificada de Chile del 1976, el secretario Kissinger le indica a Guzzetti:

> Si hay cosas que deben hacerse, debe hacerlo rápidamente. Pero debe volver rápidamente a los procedimientos normales […] Nuestro principal problema en Argentina es el terrorismo. Es la primera prioridad del actual gobierno que asumió el 24 de marzo. La solución tiene dos aspectos. El primero es velar por la seguridad interna del país; el segundo es resolver los problemas económicos más urgentes en los próximos 6 a 12 meses. Argentina necesita la comprensión y el apoyo de Estados Unidos […] Hemos seguido de cerca los acontecimientos en Argentina. Le deseamos lo mejor al nuevo gobierno. Deseamos que tenga éxito. Haremos lo que podamos para ayudar a que tenga éxito (Kissinger como fue citado por Osorio, 2004).

Estos son solo algunos de los tantos documentos desclasificados. Sin embargo, aún quedan otros por desclasificar. Con relación al golpe de estado en Chile, a partir de documentos desclasificados, remarcan la estrategia Nixon-Kissinger para desestabilizar el gobierno:

> [Nixon] le pide al director de la CIA, Richard Helms, que informe a los asistentes sobre la evaluación de la CIA de un gobierno de Allende en Chile. Siguiendo a Helms, el asesor de seguridad nacional Henry Kissinger presenta las ventajas y desventajas de varias opciones que los funcionarios estadounidenses han considerado para responder a Allende. Los participantes están de acuerdo con la declaración del Secretario de Estado William Rogers: "Si tenemos que ser hostiles, queremos hacerlo bien y derribarlo. Una postura de hostilidad pública nos traería problemas en América Latina. Podemos apretar económicamente. Él ha solicitado una reprogramación de la deuda pronto: podemos ser duros. Podemos traer su caída tal vez sin ser contraproducente ". Durante la reunión, el NSC analiza la manipulación del precio del cobre en el mercado mundial para socavar los ingresos de exportación de Chile bajo Allende, una opción que Nixon respalda como "muy importante". Da instrucciones a su equipo de seguridad nacional para que adopte una postura hostil, pero de bajo perfil, hacia el nuevo gobierno chileno, diseñada para socavar a Allende sin permitirle culpar a Estados Unidos. "Nuestra principal preocupación en Chile es la perspectiva de que [Allende] pueda consolidarse y la imagen proyectada al mundo será su éxito", explica con franqueza Nixon. "Seremos muy buenos y correctos, pero haciendo esas cosas que serán un mensaje real para Allende y otros" (Kornbluh y Bock, 2020).

Un único proceso histórico.

El proceso histórico no corresponde a hechos aislados sino a un único proceso continuo. En el siglo pasado podemos apreciar que segunda guerra mundial fue la continuidad de la primera guerra, como consecuencia de las sanciones económicas asfixiantes impuestas por Francia a Alemania. El fin de la segunda guerra enfrenta a dos modelos diferentes de

sociedad (EE.UU. y La Unión Soviética), dando lugar a la guerra fría y diferentes hostilidades en teatros de operaciones secundarios hasta la disolución de la URSS en 1991. Posteriormente, EE.UU. (a través de la OTAN) buscó avanzar en su esfera de influencia hacia el este, mientas que el rápido crecimiento de China plantea lo que se conoce como trampa de Tucídides[62]. Rusia por su parte intenta recuperar su posición previa. Todo ello manifiesta una historia con conflictos de intereses, la búsqueda del poder y la dominación, sin importar los medios empleados.

Seguidamente, continuamos estudiando diferentes elementos que conforman la guerra híbrida extendiendo la definición planteada en un comienzo.

¿Guerra cultural y en el deporte? (Cultural / Sports warfare)

En el actual conflicto Rusia – Ucrania, se aprecia un nuevo e impensable medio de guerra que afecta al deporte y a la cultura. Esto es, excluir a los deportistas rusos de diferencias competencias internacionales, como ser el mundial de futbol de Qatar 2022, el gran premio de Rusia de F1, el consejo mundial de boxeo, atletismo, tenis, rugby, básquet, entre otros (Grez, 2022; Ruiz, 2022; ESPN, 2022).

En el ámbito cultural, Orquesta Filarmónica de Zagreb canceló conciertos que incluían piezas del compositor ruso Piotr Ilich Tchaikovsky, la Filarmónica de Múnich junto a la Orquesta Filarmónica de Viena prescindieron del director Valeri Gergiev por no querer pronunciarse en contra de la guerra, Royal Opera House de Londres canceló el ballet de Bolshoi (el director Vladimir Urin respaldó la anexión de Crimea en 2014) (Pintos, 2022). También la Universidad Bicocca de Milán, quiso cancelar conferencias del escritor ruso Fiódor Dostoievski, aunque tuvo que retractarse dado la polémica de la censura (Télam, 2022).

Por citar otros casos similares en la historia, el *International Olympic Committee* excluyó a Sudáfrica a los juegos olímpicos de 1962 condenando el apartheid (sistema de segregación racial de dicho país) (International Olympic Committee, 2023). Otro es el caso del boicot a los juegos olímpicos de 1980. EE.UU. no permitió que sus atletas participaran de los juegos realizados en Moscú, en el contexto político de la guerra fría. Como represalia, la URSS no

[62] Termino popularizado por Graham Allison en 2012, inspirado en el historiador Tucídides de Atenas cuando dijo: “fue el ascenso de Atenas y el temor que infundio a Esparta lo que hizo inevitable la guerra”.

participó de los juegos de 1984 realizados en Los Ángeles (U.S. Department of State, s.f.; Bauso, 2020).

Corromper pilares (Pillar warfare).

> *Las decisiones son tomadas por personas cuyos intereses pueden no ser los de la sociedad (reflexión de elaboración propia).*

Los mensajes de odio y discriminación buscan corromper los valores de la sociedad como así también dividir a los ciudadanos de una nación. Elementos como las drogas, la pornografía infantil, la discriminación, el odio, la corrupción, la falta de empatía; solo deterioran la nación. Las drogas, a su vez, favorecen económicamente al quienes las distribuyen. Estos elementos, entre otros, impactan en los valores de la población y deben ser contemplados dentro del esquema de guerra híbrida. La pérdida de valores fomenta a que los gobernantes del pueblo sean más propensos a aceptar sobornos y a tomar decisiones/acciones en favor de intereses extranjeros; contra de los intereses de los ciudadanos. Cuyo efecto deteriora aún más a la sociedad, retroalimentando un proceso en espiral descendente. Otros pilares primordiales para el desarrollo de una nación son: la salud, la educación y la cultura. A su vez; las infraestructuras críticas, los activos de una sociedad o incluso sus ciudadanos pueden ser blanco de diferentes ataques. Simplemente a modo identificatorio, podemos referir el concepto como *pillar warfare*.

Guerra económica (Economic warfare).

> *Las operaciones económicas sumergen a la población en miseria y sus efectos son más devastadores y crueles que una bomba (reflexión de elaboración propia).*

La guerra económica puede tomar diferentes aspectos a fin de debilitar la economía de otra nación. Opera en el plano abierto, encubierto o inclusive en el ciberespacio. A continuación, algunos ejemplos.

Durante la segunda guerra mundial la marina de Reino Unido bloqueó los suministros a Alemania y viceversa; de forma similar, los submarinos de EE.UU. bloquearon a Japón.

En la operación Ranch Hand (1961-1971), EE.UU. arrojó diferentes químicos (Pink, Green, Dinoxol, Trinoxol, Purple, Blue, Orange, Orange II, White) en Vietnam/Laos con la finalidad de privar al Viet Cong de alimentos y a su vez quitar la cobertura. Estuvo inspirado en la emergencia de Malasia (1948-1960) a lo largo de su independencia a Reino Unido, donde los británicos arrojaron herbicidas (National Museum of USA Air Force, s.f.; Buckingham, 1982).

Es bien conocido el embargo económico que aplicó Estados Unidos (presidente Kennedy en 1962) a Cuba, que ha afectado seriamente su economía durante décadas.

En la guerra árabe-israelí del 1974, los miembros árabes de la *Petroleum Exporting Countries* (OPEC) impusieron un embargo contra EEUU, Países Bajos, Portugal y Sudáfrica; debido a la decisión de EEUU de reabastecer al ejército israelí y ganar influencia en las negociaciones de paz. El embargo afectó gravemente a una economía estadounidense dependiente del petróleo importado. Así mismo, incremento los precios a nivel global, llegando a cuadriplicar su valor. Dentro de las negociaciones de paz, se incluyó la retirada israelí del Sinaí y los Altos del Golán (Department of State, s.f.).

En 2020, el presidente de EE.UU. (Donal Trump) amenazó a la plataforma china Tiktok con un bloqueo si no era vendida a Microsoft. Tiktok se negó y el presidente firmó 2 órdenes ejecutivas que prohibían la transacción económica con Tiktok/Wechat por razones de seguridad nacional (la ley china de 2017, similar a la norteamericana, obliga a las empresas a colaborar con inteligencia nacional) (Singh, 2020). Es un caso de guerra económica / tecnológica. Finalmente, la justicia federal terminó evitando el bloqueo.

En el actual conflicto de Ucrania – Rusia; países de la OTAN, entre otros, han impuesto embargo a la importación de gas ruso. Tratándose de una imposición compleja debido a la dependencia de Europa de dicho recurso. Por otra parte, se impone la prohibición de negocios con Rusia, operaciones en el sistema Swift, bloqueos de VISA y Mastercard a ciudadanos rusos, cierre del espacio aéreo a aviones rusos, sanciones económicas sobre activos, confiscación de bienes de empresarios/miembros de parlamento, restricciones a la venta de recursos tecnológicos (procesadores, chips tecnológicos, sistemas operativos, etc.) (Télam, 2022). A su vez, medios rusos indican que la guerra no deja de ser un negocio. Rusia tardó 61 años pagar la ayuda militar que recibieron durante la WWII y las futuras generaciones ucranianas tendrán que hacer frente a los costos en ayuda militar (RT, 2022).

Si bien el concepto de explotación en momentos de conflictos para proveer armas y endeudar dichas naciones podría tratarse de propaganda rusa, la ley firmada por el congreso de EE.UU. indica: "cualquier préstamo o arrendamiento de artículos de defensa al Gobierno de Ucrania estará sujeto a todas las leyes aplicables relativas a la devolución, reembolso y pago de artículos de defensa prestados o arrendados a gobiernos extranjeros" (US Congress, S.3522 de 2022).

Otro suceso vinculante a la guerra económica y al contexto mundial actual, es el caso del buque petrolero iraní Lana (previamente Pegas ruso). El mismo fue confiscado en Grecia, cuyo petróleo incautado fue enviado a EE.UU. a causa de las sanciones impuestas (Agence France-Presse, 2022). A modo represalia, Irán capturó en una operación a dos buques petroleros griegos (Delta Poseidon y Prudent Warrior) en el Golfo Pérsico (Gambrell y Paphitis, 2022). Sucesos ocurridos en un contexto de una nueva escalada de tensiones, días posteriores al asesinato del coronel iraní de la fuerza Quds[63], Sayad Khodayee (The Guardian, 2022).

Deuda.

Autores como el Dr. Eric Toussaint del CADTM (*Committee for the Cancellation of the Third World Debt*), afirman que organismos de deuda (como ser el FMI y el Banco Mundial) son utilizados como arma de dominación y expolio (Toussaint, 2018). Indica que se trata de un instrumento de dominación de los acreedores sobre los deudores y que dichos países quedan sumidos a las condiciones que imponen, reduciendo la soberanía a decidir sus propias políticas. Por otro lado, indica que es un instrumento para quitar riqueza del país, como causa de los intereses impuestos. Una vez que los deudores no pueden pagar, deben pedir más deuda y la deuda externa se transforma en deuda eterna. Remarca como las elites están a favor del endeudamiento externo porque evaden sus capitales y compran títulos de deuda (sumado a menor necesidad del cobro de impuestos). Además, señala como en América Latina el FMI ha apoyado económicamente a las dictaduras de la región o a gobiernos afines, siendo más riguroso con gobiernos opositores (Toussaint, 2010, 2018, 2020). Los prestamos constituyen el medio más seguro de los viejos países capitalistas para

[63] Especializado en guerra no convencional y operaciones de inteligencia militar. Apoya a actores no estatales como Hezbollah (Líbano), Hamas (Palestina) o Houthis (Yemen).

mantener bajo su tutela a los países jóvenes, de controlar sus finanzas y de ejercer una presión sobre su política exterior, aduanera y comercial (Rosa Luxemburgo 1913, como fue citada por Toussaint, 2018). Con las presiones del FMI y del Banco mundial; EE.UU. logró desmantelar el proyecto Cóndor de cohetes argentinos (De León, 2017).

Posterior a que Francia y España fomentaran la revolución norteamericana para independizarlo de Inglaterra. Londres apoyaba la independencia de las colonias en Latinoamérica en pos de debilitar a España y así lograr un control mediante mecanismos de endeudamiento. Recordemos que las invasiones previas mediante la fuerza habían fracasado y requería de otro enfoque. El plan de Thomas Maitland de 1800 para la liberación fue posteriormente materializado por San Martin. Acorde a Terragno (1998), es posible que San Martin haya conocido el plan gracias a la logia Lautaro[64] (fundada por Miranda y MacDuff). Inglaterra proveía a las recientes naciones independientes prestamos con condiciones leoninas. Esos préstamos volvían nuevamente a Inglaterra mediante la compra de insumos y armamento (comercio). Además, fomentaban la industrialización de dicho país en detrimento del desarrollo local. En palabras de Simón Bolívar (1823):

> Inglaterra es la primera interesada en el éxito de esta transacción[65], ya que desea formar una liga con todos los pueblos libres de América y de Europa contra la Santa Alianza, para ponerse a la cabeza de los pueblos y dirigir el mundo. No es interesante para Inglaterra que una nación europea como España mantenga una posición como Perú en América. Prefiere que sea independiente con un poder débil y un gobierno frágil. Es por eso por lo que, bajo un pretexto cualquiera, Inglaterra apoya la independencia de Perú (Simón Bolívar como fue citado por Toussaint, 2018, p 30).

En resumen, las deudas muchas veces son contraídas con la utilización de influencias, dictaduras o gobiernos afines a los cuales ayudan a llegar al poder con los medios de comunicación y con el financiamiento de las campañas políticas. Son contraídas en contra de los intereses del pueblo. Utilizan vulnerabilidades democráticas para legitimar deudas que en realidad son ilegitimas por encontrarse bajo un esquema del tipo fraudulento por la naturaleza explicada. Deudas que en caso de no ser pagadas activa mecanismos de

[64] Organización política con el fin de separase de la metrópoli y acceder al poder. La misma no tuvo un carácter masónico, sino que se sirvió de las formas y usos de la masonería para constituirse en una sociedad secreta (Castro Olivas, 2009).

[65] A modo aclaratorio, aquí estamos realizando una simplificación histórica dado que el contexto del plan Maintland (la amenaza de Napoleón) no era el mismo que el de las palabras de Bolívar (la amenaza de la Santa Alianza). Sin embargo, a los fines prácticos las conclusiones para Inglaterra eran las mismas.

expropiación de bienes y/o recursos naturales, que en cuyo caso son el fin ulterior (un ejemplo estratégico fue la apropiación de Reino Unido de una parte del Canal de Suez en 1875). Las exigencias suelen ser el libre comercio y la reducción de gastos: sociales, salud, educación, entre otros pilares primordiales para el desarrollo de cualquier nación. Además, es habitual que surja la falacia de las inversiones, que desembarcan para captar mercados / empresas devaluadas y ofrecer empleos de baja calidad para luego exportar las ganancias en regalías. Los inversores locales no tienen posibilidad alguna de competir contra las grandes corporaciones / inversiones extranjeras.

Los medios de comunicación también cumplen un rol en la confianza de los ciudadanos sobre los mercados y pueden llevar a cabo operaciones para afectar los mismos.

Asesinato económico y de identidad.

En las sociedades modernas, prolifera la utilización de dinero digital como así también el uso de la identidad digital para los ciudadanos. El bloqueo a los activos de un ciudadano o la restricción / supresión de identidad de un objetivo resulta plausible dentro del dominio de las TIC. Configurando de esta manera el asesinato económico y el asesinato de identidad como armas dentro de un esquema de guerra invisible.

Guerra biológica / química (Biological / Chemical warfare).

Durante la guerra entre Japón y China, la unidad japonesa Unit 731 (*biological warfare unit*) arrojó pulgas infectadas con peste bubónica, ántrax, cólera, viruela y botulismo. También utilizó gas mostaza y el agente Lweisite. La operación Cherry Blossoms at Night (WWII) incluía arrojar pulgas infectadas con peste al sur de California utilizando aviones lanzados desde submarinos (I-400-class). La operación no llegó a completarse debido a la rendición de Japón, días previos al operativo. Al finalizar la guerra contra EE.UU., los japoneses negociaron brindar información sobre la guerra biológica a cambio de evitar cargos por crímenes de guerra (Cox, 2021).

Durante la Operation Bluebird (posteriormente MKULTRA) de la CIA, al investigador de armas biológicas del ejército de EE. UU., Dr. Frank Olson, se le administró la droga LSD sin su conocimiento, lo que provocó su muerte al saltar desde un edificio (Jacobsen, 2014).

Por otra parte, el ejército alemán (Wehrmacht) proveía a sus soldados de Pervitin (anfetaminas). Una droga que aumentaba la confianza, la concentración y la disposición a correr riesgos. También reducía el cansancio, la sensibilidad al dolor, el hambre y la sed. Otra droga probada con la tripulación de submarinos fue la D-IX, que contenía cocaína, Pervitin y Eukodal (basado en morfina) (Ulrich, 2005). De forma similar a como sucedió con los japoneses; los científicos/expertos alemanes de diversas ramas, fueron absorbidos por el gobierno de EE.UU. (Paperclip Operation). Por ejemplo, el biólogo Kurt Blome desarrollo capacidades ofensivas y defensivas para contrarrestar las actividades de guerra biológica soviéticas. En otras áreas, científicos alemanes desarrollaron el Saturn V y el equipo de Wernher von Braun desarrolló la tecnología de cohetes que terminó por llevar a la luna al Apolo 11 (Jacobsen, 2014).

El Departamento de Defensa de EE.UU. continuó las investigaciones japonesas y alemanas en el uso de armas biológicas. Reino Unido, Canadá y Australia también participaron en colaboración (Cole, 2016; Coulthart, 2008). Desde 1962 hasta 1973, el Departamento de Defensa llevó a cabo una serie de pruebas[66] operativas para evaluar ciertos agentes biológicos y químicos. El Project 112 consistió en pruebas tanto terrestres como marítimas. Las pruebas marítimas (Project SHAD[67]) buscaban identificar la vulnerabilidad de los buques de guerra estadounidenses a ataques químicos, nucleares y biológicos. El proyecto incluyó la utilización de agentes y biológicos/químicos[68] (como ser el Sarín o el agente nervioso VX) e incluyó más de 5800 militares que participaron de las pruebas, aunque solo unos pocos estaban informados (Committee on Veterans' Affairs, 2002; Military Health System, s.f.; William, Heather y Harriet, 2007). Un ejemplo vinculado es la misión Red Hat de 1962, donde enviaron y almacenaron diferentes agentes químicos en Okinawa.

[66] 134 pruebas de guerra biológica (de las cuales se ejecutaron 50). Se realizaron en mar abierto en el Atlántico Norte, en lugares de aguas abiertas del Océano Pacífico y cerca de las Islas Marshall, Hawái, Puerto Rico y la costa de California. Las pruebas terrestres se llevaron a cabo en Alaska, Hawái, Maryland, Florida, Utah, Georgia y Panamá, Canadá y el Reino Unido (Military Health System, s.f.)
[67] Shipboard Hazard and Defense.
[68] Bacillus globigii (BG), Betapropiolactone (beta-propiolactone; BPL), Bis Hydrogen Phosphite (BHP), Calcofluor, Coxiella burnetii (CB; Q fever), Diethylphthalate (DEP or D), Escherichia coli [E. coli], Methyl Acetoacetate (MAA), Phosphorus-32 [32P], Sarin, Serratia marcescens (SM), Staphylococcal, Enterotoxin Type B (SEB), Sulfur Dioxide (SO2), Trioctyl Phosphate (TEHP or TOF), Pasteurella tularensis (Francisella tularensis), Uranine, VX Nerve Agent (VX) y Zinc Cadmium Sulfide (ZnCdS) (William, Heather y Harriet, 2007).

Descubiertos en 1969 y retirados en 1971 a Johnston Atoll (Hawaii) en la operación Red Hat (National Archives and Records Administration, 1971).

Otras investigaciones son los experimentos en humanos del US Army Chemical Corps en la base Edgewood Arsenal entre 1948 y 1975. Que involucró agentes nerviosos (como el Sarín), agentes mostaza y agentes psicotrópicos (LSD, cannaboides), entre otros (U.S. Department of Veterans Affairs, s.f.).

Desde 1952 hasta 1969, MKNAOMI (CIA/DoD) incluyó el desarrollo, pruebas y sistemas de entrega de armas biológicas contra humanos, animales y cultivos (Church Commitee Report, 1973). Otros proyectos son el MKULTRA citado previamente y que desarrollaremos más adelante en la guerra psicológica.

En 1950, Operation Sea-Spray, US Navy arrojó bacterias (Bacilo atrophaeus y Serratia marcescens[69]) en la bahía de San Francisco (CA) para estudiar el impacto de bioarmas. Similarmente en 1966, US Army arrojó una bacteria (Bacilo atrophaeus) en el subte de NY y Chicago para investigar la vulnerabilidad de los pasajeros ante un arma biológica, ambos experimentos fuera del consentimiento de los ciudadanos afectados (Moreno, 2001).

Durante los 50, el United States Army Chemical Corps realizó operaciones[70] para estudiar la utilización de insectos como vector de ataque (*entomological warfare)*. Uno de los insectos elegidos fue el mosquito, arrojado desde aviones/helicópteros para propagar agentes como la fiebre amarilla (U.S. Army Chemical Corps Historical Office, 1960; U.S. ARMY, 1960; Rose, 1981). En la operación Large Area Coverage (LAC) de 1957, el Chemical Corps investigó la viabilidad de contaminar una gran área del continente con organismos biológicos, arrojando una miríada de partículas microscópicas fluorescentes de sulfuro de zinc y cadmio a lo largo de un camino desde Dakota del Sur hasta Minnesota (Sidell, Takafushi y Franz, 1997).

Muchos proyectos fueron descontinuados por prohibición del uso de armas biológicas del presidente Nixon (1969). A pesar de ello, la investigación del senado de 1977 reveló 2 venenos tóxicos (Cobra venon y shellfish toxin) en poder de la CIA que no fueron destruidos

[69] Usualmente inofensivos para el ser humano, excepto para quienes tengan el sistema inmunodeficiente deprimido. Algunos de esos casos terminaron hospitalizados, incluyendo una persona que falleció.
[70] Operation Big Itch (1954) utilizando insectos en municiones E-14 arrojados desde altura, Operation Big Buzz (1955) para desarrollo de municiones con mosquitos, Operation DROP KICK/May Day (1956) dispersión de mosquitos en zonas urbanas de Savannah, Georgia, y QUICKHENRY (1960).

y violaron la directiva de Nixon (Select Committee on Intelligence and Committee on Human Resources, 1977). Dichos antecedentes son un fiel reflejo del interés en la materia.

Próximo a nuestros días, hallamos un contexto de sobrepoblación mundial en crecimiento sobre un planeta de recursos finitos en merma. Sumado una fuerte disputa de poderes en un mundo multipolar. Por lo que las armas biológicas podrían tener un papel trascendente en sucesos futuros. Con especial interés, en un esquema de guerra sin límites y sin atribución.

Vinculado a la materia, existen únicamente dos laboratorios con muestras de Viruela en el mundo con fines de investigación: el laboratorio ruso Vector Reseach Center en Kosovo y el US Center for Desease Controls and Prevention en Atlanta (Gretchen, 2004; Kaise, 2014; World Health Organization, s.f.). El laboratorio ruso Vector sufrió una inesperada explosión de gas durante una reparación en septiembre de 2019. Algunos días posteriores al evento aflora el virus del Covid-19 (SARS-CoV-2) próximo al laboratorio Wuhan Institute of Virology en Wuhan China. Lo que dio lugar a la pandemia del COVID. ¿Se trata de un arma biológica? ¿salió del laboratorio chino? ¿pudo ser plantado convenientemente en dicho lugar? ¿se trató de un sabotaje o ataque de otro país? o simplemente ¿han sido casualidades caprichosas de la naturaleza? Si bien estas no son preguntas de la presente investigación, evidencian, una vez más, la complejidad que enfrentan los estados ante un esquema de guerra invisible y los posibles peligros sobre la sociedad.

Guerra del clima (Weather warfare).

Modificar el clima es otro instrumento de control y poder. Como ejemplo, Project Popeye durante la guerra de Vietnam (1967–1972), la USAF sembraba las nubes a fin de prolongar la temporada de lluvias (*monsoon*) y reducir la movilidad en las rutas de abastecimiento de suministros del Norte Vietnam. Así mismo, también es posible utilizar las nubes como defensa de *direct energy weapons* (Boges, 2009).

En 1965, el Joint Chiefs of Staff, solicitó al Forest Service of the Department of Agriculture una investigación para determinar las características de inflamabilidad de los bosques y selvas (la utilización de incendios como arma militar). Modificando la inflamabilidad de la vegetación y determinando las condiciones climáticas óptimas para favorecer la combustión. Desarrollando medidas para la destrucción de grandes áreas de

bosques con incendios. Algunos ejemplos son la operación Hot Tip o Pink Rose realizadas en Vietnam[71] (Chandler y Bentley, 1970).

En 1977 se firma el tratado para prohibir el uso militar de estas tecnologías (*Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*).

En otros contextos, el fuego como arma también es utilizada por el terrorismo. Por lo que comprender sus implicaciones son esenciales para dar respuesta dentro del marco de la seguridad nacional (Pfeifer, 2013).

Resulta de interés el seguimiento de dichas tecnologías por sus peligros implícitos, dentro del ámbito de estudio.

Hackear y arrojar (Hack and Dump).

Cada vez más usuales las operaciones encubiertas que sacan a la luz actos de corrupción, evasión impositiva o actos inmorales (ya sean reales o no). Los efectos buscados son diversos; desde afectación emocional en la población, indignación, manchar la imagen de candidatos / políticos opositores, interferir procesos electorales, dañar la imagen de un estado, causar depresión de los mercados, retrasar / sabotear proyectos estratégicos de una nación, destrucción de imagen corporativa con la intención de comprar / instaurar empresas afines a la nación atacante, entre otros.

Dichas operaciones son habitualmente apoyadas por la propaganda mediática, la guerra psicológica o la guerra judicial. En este último caso, cuando los funcionarios judiciales o las fuerzas de seguridad están vinculados / comprometidos con otras naciones, los intereses sesgan el debido proceso y amplifican la operación.

Dentro del mundo del ciberespacio, las ciber operaciones enfocadas al punto en cuestión, penetran los sistemas como explicamos con el concepto cyber kill chain o con las técnicas en la matriz de Mitre ATT&CK. La información exfiltrada es posteriormente disponibilizada (*leak*), en lo que se conoce como *Hack and Dump*.

[71] La Operación Ranch Hand, previamente citada, secaba la vegetación con agentes químicos para que posteriormente fuese más inflamable a las bombas incendiarias.

Guerra judicial (Lawfare).

> *Cuando el poder es amenazado hasta un cordero puede ser ejecutado por la ley. Pero cuando el poder está en el ojo de la tormenta, la ley es tan visible como el aire. En cualquier caso, es la prensa quien convierte inocentes en demonios y demonios en corderos antes los ojos de la sociedad (reflexión de elaboración propia).*
>
> *Escriben con la mano y borran con el codo (como ilustra Orwell en la rebelión de la granja)*[72].

La utilización de las leyes como arma de guerra es otro elemento de ejercer poder en la guerra no convencional. Es un término que tiene varios significados. Según Tiefenbrun (2011): "es un arma diseñada para destruir al enemigo mediante el uso, mal uso y abuso del sistema legal y los medios de comunicación con el fin de levantar una protesta pública contra ese enemigo". En Latinoamérica se refiere a la judicialización de la política (armado de causas contra los políticos). Hay que tener presente que también es funcional para los corruptos alegar que sufren persecuciones judiciales. Con lo cual la justicia debe ser objetiva a la hora de investigar los casos.

Este tipo de ataques explota la vulnerabilidad del sistema judicial. Por un lado, los tiempos de investigación son lentos y el acusado ve deteriorado su imagen; por ejemplo, durante un proceso electoral. Perder una elección implica que el atacante logra su cometido, sin importar que luego el juicio demuestre la inocencia del objetivo. Por otra parte, la justicia que debiera ser objetiva, imparcial y justa; es completamente subjetiva, corrupta y deficiente. En nuestro país, es de amplio conocimiento su vinculación con la política, la embajada norteamericana y los servicios secretos.

En los últimos años se ha evidenciado una persecución judicial a políticos y empresarios en Latinoamérica que ha deteriorado las instituciones democráticas cambiando el destino de

[72] El contexto del libro en realidad es la corrupción del régimen de Stalin en la Unión Soviética. Paradójicamente igualmente valido para nuestros días en diferente régimen. Por qué se comprende que no se trata de estructuras, si no de la naturaleza del ser humano.

elecciones y ha afectado proyectos económicos / estratégicos en la región. ¿Podría tratarse de un plan Cóndor 2.0 con una modalidad más amable pero igualmente brutal?[73]

Según O'Donnell (2011, 2014), Julian Assange le entregó un pendrive con filtraciones de cables diplomáticos[74]. En su investigación expone las vinculaciones de la embajada norteamericana con la política (de diferentes partidos/candidatos), los medios de comunicación/periodistas, fuerzas de seguridad e inclusive jueces. Los interesados concurren a informar o solicitar ayuda, aunque la embajada es prudente a la hora de intervenir (solo cuando sus intereses competen). Dentro de las revelaciones figura el interés en la no proliferación nuclear, pedidos del candidato a presidente Macri para que critiquen al gobierno (solicitud no efectuada), el lobby para sus empresas (ej. utilización del glifosato de Monsanto), vinculaciones con editores/periodistas (ej. Anthony Wayne: "Clarín tiene poderes de marcar la agenda política y es usualmente descripto como tener la capacidad de derribar gobiernos" [75]; como fue citado O'Donnell, 2011), esfuerzos conjuntos en el narcotráfico (acceso del FBI y DEA a dependencias de gobierno), un acuerdo para dejar de lado el caso de la valija de dinero[76] (en pos de fortalecer la cooperación bilateral), el presidente del Banco Central como informante (Redrado), entre otros. En lo que respecta al presente apartado, se menciona múltiples encuentros con el presidente de la corte suprema de justicia (Lorenzetti) financiando viajes y congresos. Además, el presidente de la corte otorgó accesos a especialistas de la embajada al sistema informático de la corte suprema, supuestamente para asistencia en la modernización[77]. Por otra parte, O'Donnell (2011) menciona como el fiscal Nissman anticipaba fallos y pedidos de disculpas por no haber notificado previamente del pedido de captura del expresidente (Menem). También revela

[73] Cabe aclarar que pueden existir igualmente individuos corruptos que no deben ser confundidos con este esquema explicado de persecución de inocentes con fines políticos.
[74] Si bien el periodista puede tener una tendencia política; los extractos aquí mencionados son objetivos y pueden verificarse en los cables de publicados en el sitio WikiLeaks. Ejemplo: https://wikileaks.org/plusd/cables/08BUENOSAIRES702_a.html
[75] https://wikileaks.org/plusd/cables/07BUENOSAIRES976_a.html
[76] El caso Antonini Wilson tuvo un impacto en las relaciones entre ambos gobiernos.
[77] Ganar accesos a sistemas de información. Tema desarrollado en el capítulo próximo de inteligencia.

como la embajada alentaba al fiscal a seguir la pista iraní[78] y se preocupaban respecto de la pista siria que involucraba al expresidente (O'Donnell, 2011).

Los aspectos mencionados son ejemplos que generan cierta preocupación desde el punto de vista de la soberanía, la independencia de poderes y la imparcialidad de la justicia.

Dado la mención realizada sobre el periodista Assange, vale la pena recordar la persecución judicial que sufre a pesar de estar protegido por la primera enmienda de la constitución (libertad de prensa y de expresión). La misma es una represalia por haber publicado en Wikileaks documentos secretos que le fueron entregados. Tal es el caso del video que muestra un ataque aéreo (invasión de Irak) el 12 de julio de 2007, donde un helicóptero Apache AH-64 asesinó a civiles y periodistas de la agencia Reuters (dos niños heridos pudieron salvarse)[79]. Hecho que generó gran controversia. Además, la persecución judicial resulta un mensaje de adoctrinamiento hacia otros periodistas que publiquen documentos secretos. El caso de Assange es tan serio que la CIA evaluó planes[80] para su secuestro o asesinato mientras se encontraba bajo resguardo en la embajada de Ecuador en Londres (Dorfman, Naylor y Isikoff, 2021).

Asesinatos de objetivos.

Los asesinatos se llevan a cabo para eliminar personas que representan un peligro para los intereses de la nación atacante, personas clave en el desarrollo de otro país (nuclear,

[78] Un reciente informe del Mossad publicado en NY Times indica que el atentado se llevó a cabo por una célula de Hezbolá libanesa (unidad 910) y rechazó sospechas sobre iraníes o argentinos (Bergman, 2022). El mismo reporte, presentado en Infobae, indica que si existió algún tipo de decisión de Irán (Lejtman, 2022). El informe en Infobae es detallado; pero contiene faltas ortográficas, errores tipográficos y no presenta evidencias a las afirmaciones. Menciona el contenido de un llamado telefónico libanes que no se comprende cómo se obtuvo y porque se presenta 28 años después del hecho. La vinculación con Irán responde al financiamiento histórico al grupo Hezbolá que a indicios puntuales. La información del Mossad contradice a la embajada norteamericana; exponiendo a posible encubrimiento y desvío de causa. Ello remarca el delicado equilibrio de la diplomacia internacional, inclusive entre países aliados.
En 2020, la interventora de la AFI envió datos a la justicia, donde filtró información que incluía un agente encubierto en el Líbano (Lavieri, 2020; s.n., 2020). Por lo cual es de suponer que la AFI estaba siguiendo dicha pista. Según la justicia argentina (UFI-AMIA, 2022), el ataque fue ideado/preparado por quienes ejercían el gobierno en Irán y fue ejecutado por la organización terrorista libanesa Hezbollah. Siendo la causa más compleja de la historia judicial argentina (UFI-AMIA, 2022).

[79] Namir Noor Eldeen (camarógrafo) y Saeed Chmagh (conductor). Video: https://es.wikipedia.org/wiki/Archivo:CollateralMurder.ogv

[80] También pensaban que agentes de inteligencia rusos planeaban ayudarlo a escapar a Rusia. Por lo que propusieron planes adicionales como tiroteos contra agentes rusos, chocar un vehículo contra el auto diplomático ruso o disparar a los neumáticos de un avión ruso (Dorfman, Naylor y Isikoff, 2021).

tecnológico, etc.), estrategas militares, líderes políticos opositores, personas influyentes o simplemente para enviar una señal (ej. desertores de una nación). Durante tiempos de guerra, tales actos afectan negativamente la moral enemiga mientras que sube la moral de las tropas aliadas.

Los ataques falsa bandera son fructíferos para desprestigiar una nación involucrada en una situación de sospecha (ampliaremos este punto en el próximo ítem). En caso de querer ocultar la atribución, usualmente se llevan a cabo de forma clandestina, contratando mercenarios o enmascarado en accidentes (ej. tránsito). Cuando la intención es enviar una señal disuasiva (*deterrance signals*), se lleva a cabo de forma abierta o manifiesta.

Para efectuar dichos ataques, es necesario inteligencia previa a fin de elaborar un plan y fijar (*lock*) al objetivo en espacio/tiempo durante la fase de ataque. Como veremos, la sociedad actual es más vulnerable a tales ataques dado que estos requerimientos necesarios son más simples de obtener debido a la conectividad, intercambio abundante de información, sistemas de vigilancia, entre otros; características presentes en el ciberespacio.

Cuando ampliemos la guerra cognitiva, presentaremos como dichos ataques pueden realizarse en la mente de las personas; lo que implica menos costos / riesgos / responsabilidad sobre el hecho. Previo a ello, algunos ejemplos de operaciones de asesinato[81].

Caso bomba chocolate (Chocolate bomb).

En 1943, durante la WWII, espías encubiertos nazis (trabajando en Reino Unido) habrían intentado colocar un explosivo simulando ser un chocolate (Peter's) en el comedor del gabinete de guerra británico. El explosivo, con forma de chocolate, era de acero y estaba recubierto con verdadero chocolate (Ver figura 24). La intención sería asesinar a Winston Churchill, aunque el plan fue frustrado por inteligencia británica (MI5) (The Rothschild Archive, s.f.; Higham, 2015).

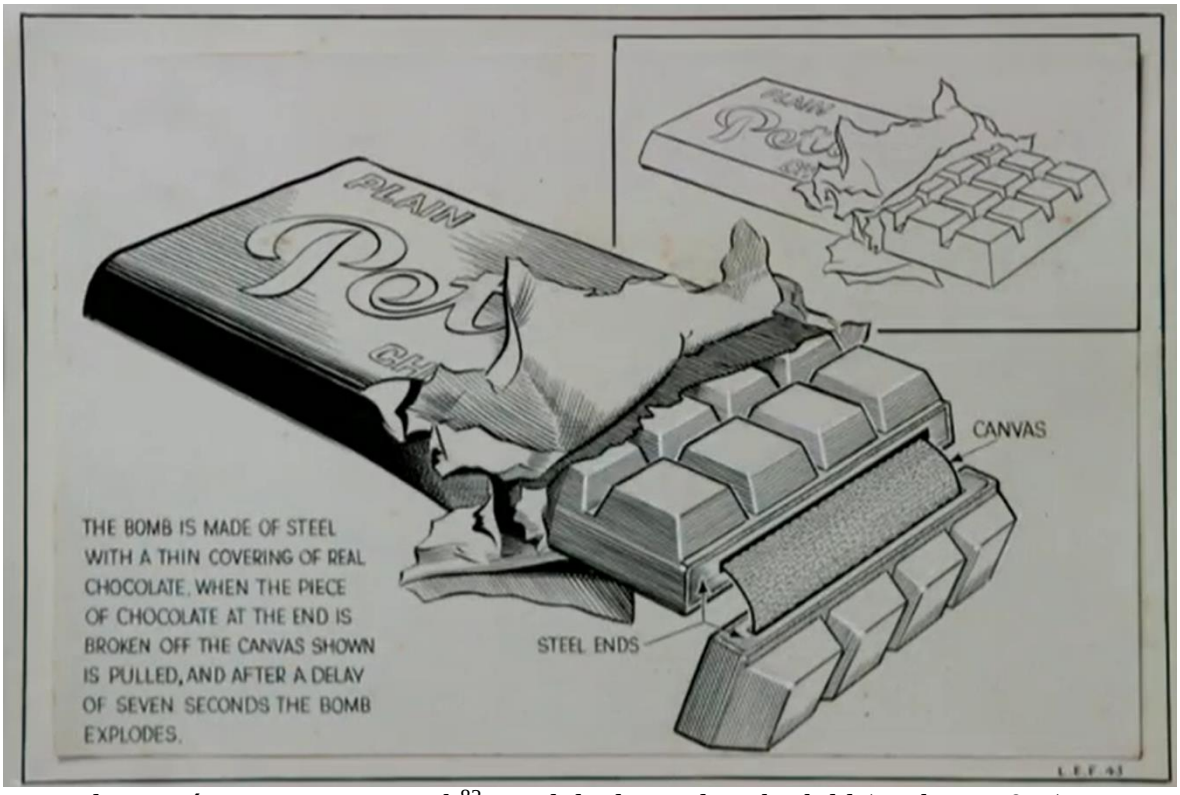
La *Operation Weitsprung* (Long Jump) fue otro intento en donde los alemanes interceptaron / rompieron un código del US Navy que indicaba que Stalin, Churchill y Roosevelt iban a estar presentes en una conferencia en Teherán. Contrainteligencia soviética

[81] Mencionamos algunos casos dado que historia es amplia para contar en su totalidad. Tener presente que existe desinformación y no es una tarea simple separar / obtener de forma objetiva datos concretos.

descubrió el plan y los alemanes, que se encontraban bajo seguimiento, tuvieron que cancelarlo (Enoch, 2012).

Figura 24

Chocolate Bomb.



Nota. Ilustración por Laurence Fish[82] a pedido de Lord Rothschild (Higham, 2015).

Caso pistola de cianuro (Poison gas gun).

El oficial de la KGB (Bogdan Stashinsky) utilizó una pistola de gas de cianuro para asesinar a dos disidentes ucranianos en Alemania; Lev Rebet (1957) y Stepan Bandera (1959). Rebet era un líder político anticomunista que participó de la independencia de Ucrania de 1941. Bandera era activista político del movimiento nacionalista ucraniano (Plokhy, 2017).

La pistola contenía una capsula de cianuro que se aplastaba con el mecanismo (Ver figura 25). Stashynsky utilizaba un periódico para envolver y disimular el arma (Andrew y Mitrokhin, 1999).

[82] La historia salió a la luz en 2009 por una carta que encontró la esposa del fallecido Fish. Existen otras 25 ilustraciones de explosivos ocultos en latas de aceite, cacerolas, entre otros.

Figura 25
Gas Assassination Weapon, KGB, 1950's.



Nota. Escondida en un periódico enrollado (International Spy Museum, 2018).

Caso píldoras tóxicas.

En 2007, CIA desclasificó un documento llamado "Family Jewels" que indican intentos de asesinato, espionaje doméstico, infiltración de grupos de izquierda y secuestros durante 1950 y 1970. En el mismo documento, se revela un memo que indica el asesinato con veneno de Patrice Lumumba (premier de república del Congo) (Blanton, 2007). Sin embargo, Lumumba fue asesinado en diferentes circunstancias[83]. Otro caso mencionado es el de Rafael Trujillo de República Dominicana donde se apoyó a los disidentes con armas. Si bien algunos funcionarios del Gobierno tenían conocimiento de que los disidentes pretendían matar a Trujillo, hay pruebas contradictorias sobre si las armas fueron suministradas a sabiendas para su uso en el asesinato (United States Senate, 1975).

En relación con Fidel Castro, en 1960, la CIA ofreció (a través de Robert A. Maheu) $150 mil a Johnny Roselli (mafia italiana) para matar a Fidel Castro. Roselli rechazó el pago, aunque puso en contacto a miembros de la mafia Cosa Nostra (Sam Giancana/Santo

[83] Para quien quiera profundizar el caso, el Church Committee del senado de USA investigó el asunto y confirmó el complot de asesinato, pero no encontró pruebas sólidas para vincularlo a su asesinato.

Trafficante, Jr), vinculados a Florida/Cuba. Sam propuso utilizar una píldora potente en la bebida / comida de castro, en vez de un disparo (United States Senate, 1975). El TSD[84] (Technical Services Division de la CIA) creó 6 píldoras[85] (CIA Memorandum, 1966). El primer intento fue a través de un oficial cubano (Juan Orta) que recibía sobornos de los intereses de las apuestas. Orta devolvió las pastillas dado que perdió su cargo cercano a Castro. En el segundo intento, contactaron con Dr. Anthony Verona (Junta de cubanos en exilio) quien decía tener un contacto en el restaurante frecuentado por Castro. No queda claro si el plan falló porque Castro dejó de concurrir al restaurant o porque nunca recibieron la señal de confirmación para proceder. El proyecto se canceló con la fallida invasión a Bay of Pigs. Posteriormente, bajo el acrónimo ZR/RIFLE y con colaboración con la estación de la CIA en Miami (JM/WN7AVE), se enviaron nuevamente 4 pastillas destinadas al Che Guevara, Fidel y Raúl Castro. Harvey canceló el plan en 1963 por razones no indicadas (United States Senate, 1975).

Según una investigación del Church Committee del senado de EE.UU., se encontró evidencia concreta de al menos 8 complot de la CIA para asesinar a Fidel Castro entre 1960 y 1965, aunque solo el caso mencionado de las píldoras tuvo progresos. El resto quedaron en etapas de planeamiento y preparación (United States Senate, 1975).

Intentos previos fueron destinado a destruir la imagen pública de Castro. Según el reporte del inspector general de la CIA de 1967, TSD discutió el uso de un spray (similar al LCD) en el estudio de transmisión o impregnar una caja de cigarros con un químico que produzca desorientación, con la finalidad de afectar sus discursos. Se planteó sacudir sus zapatos con sales de Talio a fin de que perdiera su barba (que se pensaba que estaba vinculado a su carisma popular). El plan no se llevó a cabo por una cancelación del viaje de Castro (United States Senate, 1975).

Entre los complots no llevados a cabo se incluían el pago de 10 mil dólares[86] a un cubano para producir un accidente (que no tuvo la oportunidad de realizarlo); colocar un veneno letal (toxina botulínica) en los cigarrillos favoritos de Castro (no hay registro si se llegaron

[84] Encargado de del soporte a las operaciones clandestinas (drogas, gadgets, disfraces, falsificaciones, escritos secretos, armas, entre otros).
[85] Probadas en monos dado que la primera versión no se disolvía.
[86] Incluyendo el pago universitario a sus hijos en caso de muerte.

a enviar); un crustáceo explosivo / traje de buceo con un hongo que produciría una enfermedad en la piel / una bacteria (bacilo tuberculoso) en el respirador (quedaron en etapa de laboratorio); AM/LASH (Rolando Cubela Secades con cargo en las fuerzas cubanas) incluía utilizar un potente rifle a distancia / un bolígrafo con una aguja hipodérmica que contenía Blackleaf-40 (Nicotine sulfate) (cancelado debido al asesinato del presidente Kennedy); nuevamente AM/LASH reinició en 1965 con una pistola / FAL con silenciador junto a explosivos (cancelado por razones de seguridad) (United States Senate, 1975).

Reciente revelaciones indican el intento de asesinato del hermano Raúl Castro. El plan consistía en el pago de USD $10000 al piloto de avión José Raúl Martínez, para arreglar un accidente fatal, pero no se llevó a cabo por no encontrar oportunidad (Kornbluh, 2021).

Caso pistoleros y objetivos equivocados (Gunmen / Wrong target).

En 1972, durante los juegos olímpicos de Alemania occidental, el grupo terrorista Black September[87] tomó de rehenes a 9 atletas israelitas que terminaron asesinando. El hecho se conoce como la masacre de Múnich. Como represalia, Israel realizó varias operaciones de asesinato contra los autores intelectuales (Gómez, 2014).

El servicio secreto (Mossad) tiene una larga lista de asesinatos de científicos nucleares, militares y terroristas, entre otros. Utiliza francotiradores, explosivos o más habitualmente motos con armas de fuego, (Fassihi y Bergman, 2022; Beaumont, 2021; The Guardian, 2022). En una de las operaciones (1973), los agentes del Mossad cometieron una equivocación. Identificaron erróneamente al objetivo y terminaron asesinando un mesero inocente en Noruega. Esto causó repercusiones internacionales en lo que se conoce como Lillehammer affair (Gómez, 2014; s.n., 2001; Mellgren, 2000).

Caso paraguas búlgaro (Bulgarian Umbrella).

Georgi Markov fue un disidente que desertó de Bulgaria (comunista) en 1969. Trabajó criticando el gobierno de Bulgaria en varias emisoras en occidente como ser la radio Free Europe (radio de propaganda occidental anticomunista financiada por la CIA). En 1978, el mismo día del cumpleaños del presidente búlgaro (Todor Zhivkov), Georgi fue asesinado en

[87] Cinco terminaron muertos y tres encarcelados.

el puente de Londres con un diminuto perdigón que contenía 2 orificios con una toxina dentro (ricina con un revestimiento que se derretía a los 37°C). Aparentemente, el atacante habría utilizado un arma disimulada en forma de paraguas (Ver figura 26). El hecho se atribuye a los servicios secretos de Bulgaria presuntamente con asistencia de la KGB (Nelsson, 2020; Wheelis, Rózsa y Dando, 2006; Jones 2010).

Figura 26
Bulgarian Umbrella replica.



Nota. foto izquierda réplica del paraguas (Spy Museum, s.f.), foto derecha perdigón (PBS como fue citada por Jones, 2010).

Caso pistola para asesinatos sigilosos (Nondiscernible microbionoculator / Dart Gun).

En 1975, William Colby (Director of Central Intelligenge - DCI), testificó ante el comité del senado (Senate Select Committee) y presentó un curioso prototipo denominado Nondiscernible microbionoculator. El mismo consistía en una pistola (Colt M1911) modificada con disparo electrónico cuasi silencioso (Ver figura 27). La munición era un dardo tóxico[88]. Dentro de los diferentes sistemas de armamento, uno estaba diseñado para potencialmente impactar al objetivo sin su percepción. Pensado para que no pudiera ser detectado en una autopsia (C-Span, 1975).

[88] Según testimonio de Mary Embree en la película “Secrets of the CIA” de 1998, una toxina congelada ingresaba en la victima a alta velocidad, simulando un ataque cardíaco. Al descongelarse, no dejaba rastros más que un diminuto punto rojo en el cuerpo (The Indegraph Times, 2016). Sin embargo, no se encontró confirmación oficial sobre este testimonio documental, que podría resultar dudoso.

Figura 27
Nondiscernible microbionoculator.



Nota. Captura Church Committee Hearings CIA William Colby (C-SPAN, 1975).

Caso con explosivos

Karl Heinz Beckurts fue un físico responsable de la Oficina Corporativa de Investigación y Tecnología de Siemens, enfocado en la ingeniería eléctrica. Previamente trabajó en el centro de investigación nuclear de Jülich (Illinger, 2010; Siemens AG, 2011). Beckurts se había reunido con representantes de la U.S. Strategic Defense Initiative (SDI) (sistema de defensa contra misiles conocido como Star Wars) (Westwick, 2010; Tagliabue, 1986).

Fue asesinado en 1986[89] cuando su BMW blindado transitaba una carretera al sur de Múnich. Una bomba al lado del camino arrojó al auto (McCartney, 1986).

Una carta a máquina dejada en el lugar atribuye el hecho al *Red Army Faction* (Tagliabue, 1986). Sin embargo, funcionarios del gobierno indicaron que el *Red Army*, nunca había utilizado dispositivos de control remoto de ese tipo (McCartney, 1986). Hasta el día de la fecha, tanto la investigación como las muestras de ADN, no llegaron a ninguna conclusión (Siemens AG, 2011). Los atacantes conocían exactamente el recorrido, por lo que el ataque contó con inteligencia previa.

Caso Polonio-210.

Alexander Litvinenko, desertor del FSB (Federal Security Service de Rusia), denunció que le habían pedido asesinar al empresario Borís Berezovski. Ambos, opositores al gobierno de Rusia, tuvieron asilo en Reino Unido. Litvinenko fue crítico del gobierno ruso

[89] Fecha posterior al accidente de Chernóbil.

y trabajó como periodista, escritor y asesor de los servicios secretos británicos. Se encontraba investigando el reciente asesinato de la activista de derechos humanos, Anna Politkóvskaya; crítica del conflicto con Chechenia, a quien le dispararon en su casa en Rusia.

En 2006 Alexander enfermó abruptamente y murió a causa de envenenamiento por un elemento radiactivo (polonio-210). Antes de morir, contó que el mismo día que enfermó se había encontrado con 2 ex agentes del KGB y luego almorzó con un experto italiano en desechos nucleares. Según un cable filtrado en Wikileaks, uno de los exagentes (Kovtun) habría dejado rastros de polonio en la casa y auto que utilizó en Hamburgo (Wikileaks, 2010).

Caso gas nervioso (Novichok)

Sergei Skripal, ex oficial de inteligencia militar rusa (GRU), trabajó como doble agente para el MI6 (Reino Unido) durante 1990 y 2000. Fue condenado a 13 años de prisión en Rusia y en 2010 fue a vivir a Reino Unido gracias a un programa de intercambio de prisioneros. En 2018, Sergei y su hija fueron encontrados inconscientes en una plaza. Dos oficiales (Alexander Petrov y Ruslan Boshirov[90]) del servicio de inteligencia militar ruso (GRU), habían llevado una muestra de un perfume a su casa. El perfume en realidad contenía un agente nervioso (Novichok). Los oficiales quedaron registrados en todo su recorrido por las cámaras de la ciudad. Luego de varias semanas en el hospital y bajo estado crítico, Sergei Skripal y su hija lograron recuperarse (De Miguel, 2018).

Como efecto colateral, Policías e investigadores que fueron a su casa también tuvieron problemas de salud. Un hombre (Charlie Rowley) encontró el perfume en la calle se lo obsequio a su novia (Dawn Sturgess), quien murió días después (Ma, 2018).

Caso trampa en embajada (Embassy trap).

En 2018, el periodista del Washington Post, Jamal Khashoggi, recibió una llamada de la embajada saudí en Turquía. Jamal era crítico del gobierno saudita y se encontraba exiliado por dicha razón. La llamada de la embajada se debía a que necesitaba unos papeles de divorcio. El día anterior, un equipo de inteligencia saudí (Tiger Squadron) viajó a Turquía y

[90] Se sospecha que los nombres podrían ser identidades falsas.

preparó una trampa en la embajada. Dieron el día libre a todo el personal y cubrieron el piso con láminas de plástico. Jamal ingresó a la embajada para nunca más salir. El hecho salió a la luz por la denuncia de la novia y gracias a la intervención de la inteligencia de Turquía que investigó el crimen. Los aterradores audios y videos que consiguió inteligencia turca permitieron reconstruir el hecho. El periodista fue asesinado y cortado en pedazos. Se cree que fue colocado en maletas y trasladado en vehículos diplomáticos para ser descartado en un bosque. La CIA indicó al príncipe heredero saudita como autor intelectual[91]. Dado el escándalo internacional, solo los autores materiales fueron puestos en prisión en Arabia Saudita (Corbin, 2019). Como veremos en el próximo capítulo, para la inteligencia previa, se habría utilizado el *malware* israelí Pegasus (Priest, 2021).

Caso drones asesinos (Killer drones).

En un contexto de crecientes tensiones entre EE.UU. e Irán, en 2019, rebeldes Huthi de Yemen atacaron a la petrolera saudí Aramco con drones provocando incendios. En aquel entonces EE.UU. señaló a Irán como responsable (Espinosa, 2019).

En 2020, el general iraní Qasem Soleimani fue asesinado durante la noche junto a 9 personas cuando se retiraban del aeropuerto de Baghdad (Irak) en vehículos.

La operación contó con apoyo de inteligencia israelita, quienes proporcionaron los números de teléfonos utilizados para el seguimiento. En el ataque, EE.UU. envió 3 drones no tripulados (MQ-9 Reaper) lanzados desde la base Al Udeid Air Base (Qatar). Los drones eran controlados remotamente desde Creech Air Force Base (Nevada, cerca del área de pruebas nucleares). Los drones estaban equipados con misiles Hellfire R9X de 45kg con 6 *sharp blades* laterales (energía cinética en vez de carga explosiva). Se Utilizaron al menos 3 misiles contra los vehículos que salían del aeropuerto (Chandran, 2020) (Ver figura 28).

El U.S. Department of Defense, emitió una declaración de que llevo a cabo el ataque bajo la dirección del presidente y con la finalidad de disuadir futuros ataques (U.S. Department of Defense, 2020).

Existe una controversia legal por el hecho. Naciones Unidas investiga la legalidad del accionar, teniendo en cuenta la falta de peligro inminente, las muertes colaterales y la falta

[91] En la geopolítica los países aliados dejan pasar por alto todo tipo de atrocidades. Cuando se trata de países rivales, hasta un saludo es mal visto.

de consentimiento de Irak. Según Agnes Callamard (Naciones Unidas), las acciones no se pueden justificar bajo la legislación internacional como respuesta de una amenaza inminente y fijan un peligroso precedente (Dilanian, 2020; Cumming-Bruce 2020).

En 2021 nuevamente utilizaron un misil Hellfire desde un drone Reaper durante la retirada de tropas norteamericanas en Kabul, Afganistán. El contexto fue que días atrás un ataque suicida del Estado Islámico había asesinado soldados y civiles. El objetivo del drone (Zemari Ahmadi), aparentemente un facilitador del Estado Islámico con un auto cargado de explosivos resultó ser en realidad un ingeniero eléctrico que trabajaba para Nutrition and Education Internacional (enfocada en la desnutrición) y llevaba bidones de agua para su familia, como hacia a diario. El ataque norteamericano asesinó a 10 personas inocentes incluyendo 7 niños. El pentágono intentó ocultar el hecho indicando explosiones secundarias luego del impacto del misil, remarcando la presencia de explosivos; lo que la investigación demostró ser una afirmación falsa. Luego de la publicación de la investigación, el pentágono finalmente reconoció el hecho como un error trágico (New York Times visual investigation, 2022).

Figura 28

Killer drones.



Nota. Vehículo impactado, drone Reaper y misil Hellfire con cuchillas laterales (fuente imágenes: Chandran, 2020).

Ataques de falsa bandera (False flag).

Los ataques falsa bandera son ataques que buscan atribuir el origen a un tercero (individuo/estado/organización). Pueden ser utilizados para enemistar naciones. En caso de auto atentados cumplen el designio de justificar acciones contra un supuesto agresor (quien no tiene ninguna vinculación con el hecho) o inclusive contra la población. Dichos ataques suelen sustentarse con una fuerte utilización mediática (operación psicológica) para convencer a las masas de la culpabilidad del supuesto agresor, demonizar su imagen, justificar el desvío de fondos a un organismo / empresa específica o tomar acciones que restrinjan los derechos / libertados de la población (que de otra forma no hubieran aceptado).

La retórica opuesta también es útil. Cuando se realiza una operación encubierta y la misma sale a la luz, es usual negar los hechos alegando un ataque de falsa bandera cuyo objeto es el desprestigio de la reputación del noble agresor.

Una variante consiste en provocar de diversas formas a los contrincantes, forzando su respuesta violenta. Ello justificaba el *casus belli*[92] y aprobación del senado / pueblo al enfrentamiento bélico.

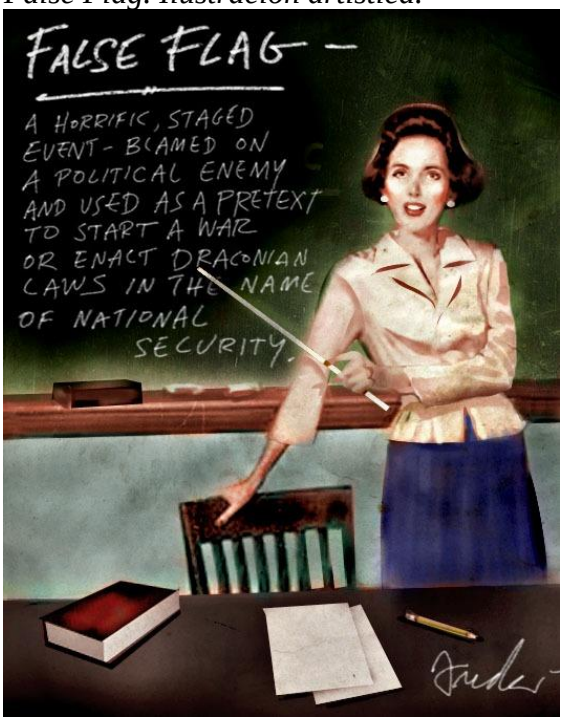
Los ataques falsa bandera son difíciles de identificar dada su naturaleza intrínseca. En caso de auto atentado a nivel estado, resulta inclusive más difícil de probar el hecho, dado que el propio estado perpetuador encargado de llevar a cabo la investigación (escondiendo / fraguando pruebas).

Los ataques falsa bandera son una estrategia militar que, natural e indefectiblemente, pasan al plano del ciberespacio; cuyas características del teatro de operación lo hacen puntualmente propenso. Dichos aspectos, deben ser tenidos en cuenta a la hora de estudiar los ciberataques.

Dado que no podemos saber hacia dónde nos dirigimos, si no conocemos de dónde venimos; a continuación, veremos algunos ejemplos de falsa bandera, como referencia una publicación en Washington's blog (2020) (Ver figura 29):

[92] Término latín que hace referencia al motivo o justificación para la guerra.

Figura 29
False Flag. Ilustración artística.



Nota. Autor - Anthony Freda.

Caso Himmler Operation - Gleiwitz Incident (1939).

Testimonios del juicio a Nuremberg revela que los alemanes crearon una serie de ataques en la que utilizaron presos con uniformes polacos (con la intención de posteriormente justificar la invasión a dicho país) (The Avalon Project, s.f.).

Caso Masacre de Katyn (1940).

En la masacre de Katyn, Stalin ordenó a policía secreta soviética (NKVD) el asesinato de 22 mil polacos con la finalidad de culpar a los alemanes (Parfitt, 2010).

Caso Operation Embarrass (1946-1949).

Según el libro “MI6: The History of the Secret Intelligence Service 1909-1949” de Keith Jeffery, inteligencia británica utilizó desinformación, propaganda y explosivos en barcos; para prevenir que refugiados judíos del holocausto pudieran llegar a Palestina. Crearon una organización falsa llamada “Defenders of Arab Palestine” a fin de asumir la atribución del hecho (Roberts, 2010).

Caso Operation Susannah - Lavon Affair (1954).

Israeli Military Intelligence del Israel Defense Forces, reclutó y entrenó egipcios judíos a modo de celda terrorista. La finalidad era colocar explosivos en el Cairo y Alejandría (cines, librerías, estaciones de trenes y centros de educación perteneciente a egipcios, norteamericanos y británicos). La atribución del hecho señalaría a organización "Muslim Brotherhood", a comunistas egipcios, nacionalistas locales, entre otros. La idea era generar inestabilidad y convencer a los británicos de que no se retiraran del canal de Suez, dado que ello le otorgaba cierta protección a Israel. El nombre de la operación viene dado porque la celda debía actuar cuando escuchara la canción "Oh Susannah" en la radio israelí, mientras que el otro nombre viene del ministro de defensa, Pinhas Lavon, quien dimitió posterior al incidente. El hecho salió a la luz puesto que una bomba detonó antes de tiempo y la policía capturó a los terroristas. No hubo víctimas en el hecho salvo los 4 espías capturados (2 se suicidaron debido a las torturas de los interrogatorios mientras que los otros 2 fueron sentenciados a muerte). Recién en 2005, Israel admitió el hecho, condecorando a los 9 espías sobrevivientes (Beinin, 1996; The Library, s.f.).

Caso COINTELPRO (1961-1971).

El FBI contaba con un programa de acción encubierta llamado COINTELPRO[93] (counterintelligence program) que fue investigado por el senado en 1976. El mismo salió a la luz con el robo de documentos del FBI con la finalidad de exponer dicha operación (Bertram y Magratten, 2014). La justificación de COINTELPRO era proteger la seguridad nacional, prevenir la violencia y mantener el orden social/político. Estaba dirigido contra grupos "subversivos" (Communist Party, Socialist Workers Party, Black Power movement, grupos de izquierda, derechos civiles, movimientos antiguerra de Vietnam e inclusive Ku

[93] Resulta de interés comprender la mentalidad de dicha época. Además, el lector podrá apreciar ciertos paralelismos con la guerra híbrida, el plan cóndor y otros puntos que trataremos. Muchos mecanismos siguen presentes en la actualidad. Las técnicas recuerdan al testigo plantado por el FBI para la persecución contra Julián Assange. Según Fürstenau de DW (2021), el testigo Sigurdur Siggi Thordarson que había dicho que Assange le pagó para espiar/hackear políticos se ha retractado de esas declaraciones. Implicado en actividades delictivas, dijo que eran ficticias y las había hecho a cambio de garantías de inmunidad judicial por parte del Departamento de Justicia de EE.UU. y la Oficina Federal de Investigación (FBI). Acorde a (Poulsen, 2013), Thordarson trabajó infiltrado en WikiLeaks durante 2011 como mole del FBI para espiar la organización y robar documentos a cambio de $5000.

Klux Klan) (United States Senate, 1976). Utilizaba técnicas típicas de tiempos de guerra. Incluía operaciones de vigilancia ilegal (intercepción telefónica, implante de micrófonos, violación de correspondencia) y de guerra psicológica. Las técnicas utilizadas causaban daños emocionales, económicos e inclusive físicos como ser: llamadas telefónicas anónimas con amenazas, envío de falsas cartas sobre infidelidad para romper matrimonios, reimpresión de periódicos para convencer a los objetivos de que estaban equivocados, contactar al empleador para su despido, desparramar rumores para desacreditar, arreglar reporteros con preguntas plantadas, falsificar pruebas para encarcelar (con intimidación de testigos), espías infiltrados en reuniones para alienar/sembrar disidencia con temas controversiales (lo que llevó al asesinato de Malcolm X), arengar guerra de pandillas etiquetando falsamente a miembros de grupos violentos como informantes de policía, avisar a la policía local sobre falsos delitos (allanamientos ilegales que terminaban con enfrentamientos a tiros y miembros del partido Pantera Negra muertos) (United States Senate, 1976). Un caso controversial es el de Fred Hampton que un infiltrado le dio Secobarbital para incapacitarlo y posteriormente fue asesinado por la policía) (Dolak, 2021). Como indica el Senado en su investigación, el FBI le envió a Luther King Jr., dos días antes de recibir el premio nobel, un kit suicida que incluía una carta y grabaciones de infidelidades, indicando que debía cometer suicidio para que las grabaciones no salieran a la luz (United States Senate, 1976). La CIA también tenía su propio programa llamado Operation CHAOS (1967 al 1974) para espionaje doméstico contra grupos antiguerra, protestas y disidentes políticos. El Project HT/LINGUAL se encargaba de interceptar y espiar correspondencia proveniente de URSS y China (Prados y Nichter, 2020).

Según documentos descalificados, la vigilancia del FBI y la CIA; también incluyó a John Lennon y sus cercanos (por su apoyo a movimientos pacifistas) (Federal Bureau of Investigation, s.f.). Otros documentos desclasificados indican la vigilancia a periodistas: Michael Getler del Washington Post (CELOTEX I); columnista Jack Anderson, comentarista Britt Hume, periodista Leslie Whitten (CELOTEX II); escritor Víctor Marchetti que publicó sobre la agencia (BUTANE) (National Security Archive, 2007). La NSA por su parte también investigó a líderes de derechos civiles (Martin Luther King y Whitney Young); al boxeador Muhammad Ali; al periodista Tom Wicker, al humorista Art Buchwald; e inclusive a los senadores Frank Church y Howard Baker (Matthew y Burr,

2013). Los programas de vigilancia MINARET y SHAMROCK son mencionados en el siguiente capítulo.

Caso Siria: complot de asesinato (1957).

En 1957, el primer ministro británico (Harold Macmillan) y el presidente de EE.UU. (Dwight Eisenhower), temían que Siria pudiera propagar el comunismo a los países vecinos de Oriente medio (en aquel entonces, prooccidentales), sumado a que la tubería que enviaba el petróleo desde Irak a Turquía pasaba por Siria. En dicho contexto histórico, aprobaron un plan en el que la CIA y el MI6 debían orquestar falsos incidentes violentos en la frontera de Siria. El gobierno sirio debía parecer patrocinador de los complots, sabotajes y la violencia contra los gobiernos vecinos. Ello daría el pretexto para una intervención militar de Irak y Jordania. Se planteó la posibilidad de reemplazar el régimen Ba'ath/Comunista por uno antisoviético, aunque esto fue descartado dado que la medida sería impopular. El plan debía financiar un "Free Syria Committee" y armar a facciones políticas con capacidades paramilitares, sumando a levantamientos internos. Dicho plan, incluía el asesinato del jefe de inteligencia militar siria, jefe del estado mayor sirio y el líder del partido comunista sirio. Además, la CIA y el MI6 debían utilizar sus capacidades tanto en el campo de la acción como en el plano psicológico a fin de aumentar la tensión. Dicho plan nunca se llevó a cabo dado que no pudieron persuadir a los vecinos árabes de Siria (Fenton, 2003). Otros intentos fueron la Operación Wakefull / Straggleel (1956) para llevar a cabo un golpe de estado, cancelado por la Crisis de Suez; y Operación Wappen (1957) también golpe de estado mediante soborno a los militares, que salió a la luz y fue negado como propaganda soviética (Prados, 2006).

Caso Operation Northwoods (marzo de 1962)

Como parte del Cuban Project / Operation Monsoose (este último con la finalidad de remover a los comunistas del poder en Cuba, incluyendo asesinatos de líderes clave y planes de ataques falsa bandera). La preocupación[94] de que Cuba pudiera ingresar al Pacto de

[94] Preocupación genuina si recordamos el fallido intento de invasión de EE.UU./CIA (cubanos exiliados) a Cuba en la Bahía de Cochinillos (1961), sumado a la instalación de misiles nucleares PGM-19 Jupiter en Italia y Turquía por parte de USA (1961). Posiblemente, presuponían que la URSS podría hacer lo mismo en

Varsovia (*Warsaw Pact*) o que la URSS instalase bases en Cuba propiciaron la idea de que debían tomarse medidas urgentes, lo que dio lugar a la Operación Northwoods. El mismo consistía en un complejo plan de falsa bandera para justificar, ante la opinión pública internacional, el ataque de EE.UU. a Cuba. El plan debía engañar a los cubanos y hacerles creer una inminente invasión. Así mismo, incluía que US Navy realizara acciones de falsa bandera cerca del área de Guantánamo a fin que los ataques parecieran de origen cubano (desparramar rumores, colocar uniformados cubanos, capturar un falso saboteador cubano, iniciar disturbios cerca de la base, explotar municiones en la base, quemar aviones en la base, arrojar morteros desde afuera de la base dañando instalaciones, capturar la milicia atacante, capturar equipos de asalto en el mar, sabotear con incendios el puerto, hundir barcos, etc.). Además, se proponía hundir un buque no tripulado cerca de aguas cubanas (simulando ataque cubano), campañas de terror comunista en Florida o Washington (fomentar atentados contra refugiados cubanos, detonar algunos explosivos plásticos en lugares específicos, arrestar agentes cubanos y exponer documentos falsificados sustentando la participación cubana). Particular atención al manejo de la opinión mundial favorable, mostrando al gobierno de Cuba como imprudente e irresponsable y una amenaza para la paz de los países occidentales (los periódicos norteamericanos deben causar una ola de indignación nacional). Otras acciones eran simular piratas cubanos atacando a sus vecinos del Caribe, simular un B-26 / C-46 "cubano" atacando campos de caña en República Dominicana durante la noche (incluir rastros de bombas incendiarias soviéticas) y encontrar en la playa mensajes cubanos enviados a supuestos comunistas "*underground*" en República Dominicana. Dado que conocían que castro apoyaba clandestinamente a movimientos subversivos en los países de la región se proponía exponer magnificando los mismos. Igualmente plateaba el secuestro de aviones civiles / transportes terrestres y derribo de un avión civil transitando Cuba con estudiantes de vacaciones. El complejo plan implicaba clonar un avión de la CIA en la base Eglin AFB, intercambiar los aviones evacuando los pasajeros, continuar el vuelo remotamente para luego derribarlo con un falso Mig cubano (F-86 pintado) que debía simular un posterior derribo (cuando en realidad regresaba a la base de EE.UU. a muy baja

Cuba y efectivamente eso fue lo que sucedió posterior al rechazo a la Operación Nothwoods, con la famosa Crisis de los misiles en octubre de 1962.

altitud) y un submarino debía dejar restos del avión / paracaídas. La Operación Northwood fue rechazada por el presidente Kennedy, sin embargo, resulta un relevante antecedente de estudio (Ruppe, 2006; Joint Chiefs Of Staff, 1962).

Caso Léonie Duquet y Alice Domon (1977).

Según testimonios (Horacio Domingo Maggio / Lisandro Raúl Cubas) del informe "Nunca Más" de la comisión nacional sobre la desaparición de personas (CONADEP), en 1977, la dictadura cívico militar en Argentina secuestró e hizo desaparecer a 2 monjas francesas (Léonie Duquet[95] y Alice Domon), simulando que las mismas fueron secuestradas por la organización guerrillera montoneros. La declaración por escrito de una de las monjas se obtuvo bajo tortura, y la foto con la bandera de montoneros detrás fue tomada en la ESMA (CONADEP, 1984). En un memo desclasificado en 2017, el oficial de derechos humanos (Tex Harris) de la embajada de EE.UU. reafirma todo lo sucedido mientras reclamaba que la embajada norteamericana bloqueaba el envío a EE.UU. de informes sobre las violaciones de derechos ocurridos[96]. Comenta a detalle como la policía fue a detener a las monjas y

[95] En 2005, el Equipo Argentino de Antropología Forense, confirmó mediante una verificación de ADN el hallazgo del cuerpo de Duquet en un cementerio de General Lavalle. Hasta la fecha no se pudo encontrar a Domon (DW, 2005; Cámara Federal de Casación Penal, s.f.; Poder Judicial de la Nación, 2008).
[96] Como mencionamos anteriormente, el gobierno de EE.UU. quería ocultar las violaciones de derechos humanos para no afectar la tramitación de créditos en apoyo a las dictaduras militares.

además agrega el dato de que las fotos no correspondían a los tipos de cámaras utilizadas por montoneros[97] (U.S. Department of State, 2017; Osorio y Blanton, 2002).

Golpes blandos.

"El que así os domina tiene sólo dos ojos, sólo dos manos, sólo un cuerpo, no más que el que posee el más pequeño de los hombres entre los infinitos que habitan en vuestras ciudades; en verdad no tiene nada más que el poder que le conferís para destruiros".

(Etienne de la Boétie en 1576)

"La clave para la obediencia habitual es llegar a la mente" (Bertrand de Jouvenel, 1952).

Acorde a Gene Sharp (1973), los gobiernos dependen de la sociedad que gobiernan, pero los mismos pueden ser debilitados / destruidos, si socava su fuente de poder político. Siendo la obediencia y la aceptación de la autoridad, el corazón del poder político. La obediencia viene dada por los hábitos, miedo a sanciones, interés propio (económico / posición / prestigio), identificación emocional con el líder (creencias / propósito en común),

[97] Contexto histórico: El golpe militar del 66, conocido como Revolución Argentina, derroca al presidente Arturo Illia (con el apoyo de EE.UU. dentro del marco de la guerra fría, conocido como Ideología/Doctrina de Seguridad Nacional en temor a las ideas comunistas que atraían a jóvenes y trabajadores). El gobierno de facto, que comienza con Onganía; asesinas manifestantes, prohíbe los partidos políticos, bares nocturnos, pelo largo, polleras cortas, centros de estudiantes y se produce la famosa represión universitaria (noche de los bastones largos) seguida de una fuga de científicos del país, entre otros. Todo ello provoca una escalada y el nacimiento de los grupos guerrilleros (Montoneros, ERP, FAP, FAR). Grupos que buscaban contrarrestar (también con violencia) al gobierno de facto y llamar a elecciones. Estos grupos también recurrían a robos y secuestros para poder financiar sus actividades. Con un clima tenso, surgen puebladas como el Cordobazo. Perón, quien estaba exiliado en España, aguardaba regresar al poder y alentaba a los grupos guerrilleros, como así también a la derecha sindical. Perón designa a Cámpora para ganar las elecciones del 73 quien quita su proscripción. Durante el regreso de Perón, la derecha sindical embosca a la izquierda peronista (la masacre de Ezeiza). Hecho que genera una nueva escalada de violencia y venganzas. Durante el mandato democrático de Perón (en realidad el gobierno interino previo que duro 2 meses) se crea la Alianza Anticomunista Argentina (AAA o Triple A); grupo parapolicial con el objetivo de asesinar a los mismos grupos revolucionarios que previamente había apoyado (estos grupos esperarían de Perón algún tipo de revolución similar a la cubana, cosa que nunca sucedería). La Triple A no se limitaba a esos grupos violentos, también colocó una bomba en el auto de un senador de la nación de izquierda, Hipólito Solari Yrigoyen (quien sobrevivió). La Triple A operaba como célula y fue originalmente organizada por el ministro de Bienestar Social (José López Rega) y el jefe de la PFA (Alberto Villar); luego incluyó personal policial, militar y agentes de inteligencia. Ocho meses después de asumir la presidencia, Perón muere a los 78 años. Asume María Estela Martínez de Perón, quien firma los decretos para "neutralizar y/o aniquilar el accionar de elementos subversivos" (Operativo independencia). Al llegar el golpe de estado del 76 (Plan Condor ya mencionado), el manual del ejército de operaciones contra elementos subversivos (RC-9-1) indica: "Aplicar el poder de combate actuando con la máxima violencia para aniquilar a los delincuentes subversivos donde se encuentren."

indiferencia (aceptación sin cuestionamientos consientes), falta de autoestima (no confían en su propio criterio / prefieren que les digan que hacer, desligando su responsabilidad a decidir) u obligaciones morales (legitimidad del líder / bienestar de la sociedad / principios religiosos). Tales obligaciones están arraigadas en la conciencia propia del individuo y es por tal motivo que la propaganda está dirigida a la mente de las personas. El líder requiere un sistema jerárquico de funcionarios y agentes subordinados que ayudan a someter a la sociedad a su dominación. El consentimiento de los individuos no es constante y puede ir variando (por cambios en la percepción), debilitando o fortaleciendo al régimen (según sea el caso). En especial cuando se afecta la opinión de los agentes que sustentan la estructura de poder.

Sharp estudió como atacar el centro de gravedad (vulnerabilidades) del poder político para resolver conflictos por medios no violentos[98] con el fin de lograr reformas, objetivos puntuales o incluso defender o destruir al gobierno. De aquí viene el termino de golpe blando, golpe encubierto o golpe no tradicional. El modelo de Sharp utiliza armas psicológicas, sociales, económicas y políticas (protestas, huelgas, no cooperación, boicots, descontento popular). En caso de una represión como respuesta del poder, la misma puede redirigirse para debilitar aún más la posición de poder (política Jiu-Jitsu). Esto último se logran exponiendo la represión a la luz de la opinión pública, que usualmente quedará favorable a los grupos no violentos (Sharp, 1978).

Como indica Sharp, su marco contiene 198 métodos y los mismos se agrupan en 3 categorías: protesta / persuasión no violenta, no cooperación e intervención no violenta. Existen 4 mecanismos de cambios: conversión (cuando el poder acepta las peticiones de la resistencia), acomodación (acuerdo de las partes dado que ambos han logrado algún objetivo parcial), coerción no violenta (las fuerzas ya no obedecen las ordenes de reprimir) y desintegración (el líder pierde toda su estructura de poder y el sistema cae a pedazos). A fin de tener mayores probabilidades de éxito, los métodos se aplican a través de campañas estratégicas dentro de un plan general, enfocadas a fortalecer a la oposición y debilitar al gobierno (autoritario). Dicho plan debe desarrollarse con un profundo entendimiento del

[98] En realidad, su propuesta incluye cierto grado de violencia. Cuando dice “No violento”, hace referencia a una contraposición con lo que son los golpes de estado tradicionales mediante el uso de la fuerza (explícitamente violenta).

conflicto particular y de los diferentes factores socioculturales, psicológicos, económicos, militares, políticos, etc. Además, es fundamental que la población asimile las ideas de la no cooperación (Sharp, 1978).

La idea de Sharp se enfoca en las libertades de los individuos en contra de los gobiernos totalitarios y ha inspirado diferentes revoluciones a lo largo del mundo (Estonia, Lituania, Letonia, Polonia, Europa del este, Checoslovaquia, Eslovenia, Madagascar, Mali, Bolivia y Filipinas). Sin embargo, existen algunos usos alternativos para tener en cuenta. Para un gobierno que se perpetua en el tiempo resulta útil desacreditar una manifestación genuina alegando que están intentando un golpe blando contra dicho gobierno (fomentado desde un estado externo). Además, el mismo modelo puede ser utilizado de forma maliciosa para socavar el poder político de un gobierno genuino, opositor al atacante; a fin de reemplazarlo por otro con mayor afinidad. Por lo tanto, tener en cuenta que dichos métodos pueden ser una carta adicional en el mazo de la guerra irrestricta. Adicionalmente, dichas técnicas no necesariamente deban ser aplicadas de forma rigurosa, pudiendo ser combinado con otros elementos (inclusive violentos).

El lector podrá sentirse identificado con algunos métodos aplicados en la historia reciente de su país. Donde la población actúa acorde a lineamientos infundidos por los medios de comunicación, redes sociales, personas influyentes; creado así un ejército de títeres cuyo combustible principal son las emociones. Títeres que actúan sin siquiera entender la operación a la cual están participando. A continuación, intentamos desentrañar dichos conceptos dentro del plano de la guerra cognitiva.

Guerra cognitiva (Cognitive Warfare).

Antes hacían desaparecer a quienes pensaban diferente. Hoy es suficiente con reprogramar sus mentes (reflexión de elaboración propia)

Al igual que la ciberguerra, la guerra cognitiva forma parte de la guerra híbrida y le hemos dedicado un apartado independiente debido a su preponderancia en el presente trabajo.

En la guerra cognitiva, el cerebro humano se transforma en el nuevo campo de batalla y sus implicancias quizás sean las más poderosas de todas.

Acorde a Claverie, Prebot, Bouchler y Du Cruzel (2021), el objetivo de la guerra cognitiva es influir no sólo en lo que piensan los objetivos, sino también en su forma de pensar y, en definitiva, en su forma de actuar. Según aportes de Du Cruzel:

> La sobrecarga de información no permite garantizar una toma de decisiones informadas y oportunas... La guerra cognitiva se alimenta de la desinformación y la propaganda dirigida a agotar psicológicamente al receptor… Tiene como objetivo controlar el flujo de información... Las ciencias cognitivas abarcan todas las ciencias que conciernen al conocimiento y sus procesos (psicología, lingüística, neurobiología, lógica y más) … La Guerra Cognitiva degrada la capacidad de conocer, producir o frustrar el conocimiento ...Cualquier usuario de las modernas tecnologías de la información es un objetivo potencial… dirigida a la totalidad del capital humano de una nación… Similar a la propaganda, donde se busca provocar la participación o pasiva mediante acciones psicológicas… Las campañas utilizan información real y distorsionada (*misinformation*), hechos exagerados y noticias falsas (*disinformation*). La desinformación se presenta sobre las vulnerabilidades cognitivas de sus objetivos aprovechando las ansiedades o creencias preexistentes que predisponen a que acepten información falsa. Esto requiere que el agresor tenga una comprensión aguda de la dinámica sociopolítica en juego y para saber cuándo y cómo penetrar para explotar mejor estas vulnerabilidades. La guerra cognitiva explota las vulnerabilidades innatas de la mente humana (Du Cruzel, 2020).

China ha definido el dominio cognitivo de las operaciones como campo de batalla para llevar a cabo la penetración ideológica con el objetivo de destruir la moral y la cohesión de la tropa, así como formar o deconstruir capacidades operativas. Abarca seis tecnologías, divididas en dos categorías. *Cognition* incluye tecnologías que afectan la capacidad de pensamiento y actuar. *Subliminal cognition* cubre las tecnologías que se dirigen a las emociones, el conocimiento, la fuerza de voluntad y las creencias de una persona que se dirigen a las emociones subyacentes de una persona. El objetivo de las operaciones cognitivas es lograr un *mind superiority* mediante el uso de información para influir en las funciones cognitivas de un adversario, que abarca de la opinión pública en tiempos de paz hasta la toma de decisiones en tiempos de guerra (Beauchamp Mustafaga, 2019)

Estas definiciones corresponden al plano militar. Sin embargo, la guerra cognitiva se extiende más allá de dichas definiciones y tiene una preponderancia trascendental en cada aspecto de nuestra sociedad.

En la actual guerra entre Rusia y Ucrania percibimos una la utilización de redes sociales en el plano cognitivo. Tanto de Rusia para justificar sus acciones como de Ucrania / OTAN para demonizar y condenar las acciones de Rusia. En las imágenes y videos transmitidas se

han encontrado imágenes correspondientes a otras guerras, fotos adulteradas o inclusive escenas de videojuegos retransmitidas por noticieros como fidedignas. Ucrania utiliza ampliamente la difusión de redes sociales para resaltar las atrocidades de la guerra, apelando a la emocionalidad para demonizar a su agresor (ej. incluir niños o rescate de mascotas). Cada vez que destruyen / capturan una unidad enemiga graban videos para su difusión, con la finalidad de mostrarse triunfante / subir la moral de los defensores (sin importar si en realidad la unidad fue derrotada o abandonada por razones mecánicas). A nivel de operaciones psicológicas (*PSYOPS*), capturan fotos muy crudas de soldados rusos muertos y envían mensajes por las redes sociales, apelando a que los agresores deben retirase y regresar a su país para no sufrir el mismo destino. Rusia por su parte se muestra ante sus ciudadanos como triunfante, remarca el objetivo de una causa justa y captura en video a ucranianos rendidos obligados a enviar diferentes tipos de mensajes desalentadores para sus compañeros (alentando a la rendición). La comunicación no verbal apreciada (tema tratado en el apéndice) deja en claro que dichos mensajes no son genuinos.

Por otra parte, se viralizó un video denominado *Ghost of Kiev*, en referencia a un héroe de la aviación que derribó 6 aviones rusos. El video resultó ser una escena de un videojuego de simulación de combate (Digital Combat Simulator World). El ex presidente de Ucrania subió a Twitter una foto del piloto héroe. El supuesto piloto indicado en redes como Vladimir Abdonov no existe, las fotos son de vieja data y están adulteradas. Detectado mediante un *noise analysis*[99](ver figura 30) (Eisele, 2022).

[99] Técnica basada en la variación de brillos y colores que detecta imágenes adulteradas.

Figura 30
Ghost of Kyiv.



Nota. Fotos adulteradas y piloto falso (Eisele, 2022).

Como dijo alguna vez un autor desconocido[100]: “En la guerra, la verdad es la primer víctima”. Similarmente en 1758, Samuel Johnson identifica las cualidades necesarias de un periodista como "desprecio por la vergüenza e indiferencia por la verdad", y dice que la guerra ofrece la oportunidad perfecta para ejercerlas: “Entre las calamidades de la guerra pueden enumerarse conjuntamente la disminución del amor a la verdad por las falsedades que dicta el interés y alienta la credulidad” (Johnson, 2004).

Otro elemento apreciable en dicho conflicto, son los intentos de difamación de sus líderes. Rusia presenta en sus medios de comunicación al presidente de Ucrania como payaso en referencia a sus antecedentes como comediante. De igual forma, al presidente de Estados Unidos como viejo senil que se pierde en los discursos, cae de las escaleras del avión presidencial / bicicleta y se desorienta en las conferencias de prensa. Como contraparte, los medios afines a la OTAN muestran al presidente de Rusia con temblores, enfermo y hablan

[100] Esta frase se atribuye a el dramaturgo griego Esquilo (525 AC – 456 BC). Sin embargo, no hay referencias objetivas del mismo. También se atribuye falsamente a Warren Johnson en 1917 pero no existen registros de sus discursos, sumado a que previamente en 1915 la frase fue citada por Ethel Annakin haciendo referencia a un autor anónimo (quoteinvestigator, 2020).

de un cáncer terminal. Mencionan la enfermedad de Parkinson, demencia y lo presentan como peligro dado su falta de racionalidad y el armamento nuclear.

Estos elementos no son nuevos. El presidente Franklin Roosevelt sufría parálisis debido a una enfermedad tipo poliomielitis o síndrome Guillain–Barré (Berish, 2019). El público conocía que estaba cojo por su enfermedad, pero se ocultó el avance de esta. Nunca se lo mostró en silla de ruedas en la prensa y los servicios secretos cuidaron su imagen (Gallagher, 1985). Su auto fue modificado al igual que el Jeep a fin de que pueda sostenerse firme y erguido (ver figura 31 y 32).

Figura 31

US President Franklin D. Roosevelt.



Nota. Teniente coronel Clayton Stiles (extremo derecho), comandante del grupo de transporte de tropas 314, escolta al presidente Franklin Roosevelt y al jefe de las Fuerzas Aéreas, general Henry Arnold, en diciembre de 1943 durante la visita del presidente al 314 en Castelvetrano, Sicilia, después de la Conferencia de Teherán (314th Airlift-Wing, s.f.).

Figura 32

Jeep modificado.



Nota. Jeep modificado con asiento en altura y barras para sujetarse (Mondt y 62nd AHL como fue citado por Vlahos, 2019).

Este tipo de ataques responden a un pensamiento conservador. Antiguamente los líderes tenían que ser fuertes, sanos e imponer sus ideas y órdenes. Hoy en día, la imagen de líder político es completamente diferente. El líder es, por sobre todas las cosas, carismático. Se espera que sea comprensivo, mediador y respete la diversidad de opiniones e ideas. Por lo cual, estos tipos de ataques en realidad solo hablan mal del locutor. Sin embargo, es comprensible que dichos mensajes logren influenciar algún publico minoritario.

Estos ataques psicológicos son un tipo de *character assassination*. Como veremos, para ser efectivos deben estar adecuados a las características socio culturales de la época.

Asesinato de personaje (Character assassination[101]).

Hoy en día el asesinato se produce en la mente de las personas
(reflexión de elaboración propia)

Las imágenes y las palabras son armas psicológicas. Ya lo dijo el hermano de Marcus Tullius Cicero (106-43 AC): "tampoco estaría de más recordarles lo sinvergüenzas que son tus oponentes y difamar a estos hombres en cada oportunidad con los crímenes, escándalos sexuales y corrupción de su forma de vida" (Cicero, How to win an election). La propaganda británica acusó a Napoleón de todo tipo de atrocidades y crearon una caricatura diminuta con un sombrero gigante, tratándolo como un soldado de juguete en vez de una amenaza (Burrows, 2005).

El asesinato del personaje (*Character assassination*, de ahora en más CA) es el esfuerzo deliberado y sostenido de destruir la reputación o credibilidad de un individuo (Samoilenko, 2016). Se basa en la utilización de estigmas, estereotipos, tabúes, apelaciones directas / indirectas sobre moralidad, mezcla de verdades y mentiras, insultos, entre otros. Por ejemplo, estereotipos negativos sobre religión, orientación política, regímenes adversarios (comunista, fascista) pueden ser utilizados para socavar un personaje. Es bueno aclarar que lo que es "bueno" o "malo" en la sociedad varía según la cultura y la época temporal. El personaje (*Character*) es el conjunto relativamente estable de rasgos de una persona enraizados en los estándares morales, cognitivos, conductuales y emocionales de una cultura (es algo que la persona tiene) (Samoilenko, Icks, Shiraev y Keohane, 2020). Mientras que la

[101] Apartado basado en el libro: Routledge handbook of character assassination and reputation Management.

reputación es la percepción, en los ojos de los demás, de lo que es respetable. Por lo que no necesariamente refleje las características de la persona. Es por ello por lo que el ataque en realidad no se dirige directamente al objetivo, si no que se produce en la mente de los demás (como lo perciben y lo juzgan) (Schreiber, 2011). Sin embargo, es bueno aclarar que pueden existir posteriores consecuencias psicológicas / cambios de actitud o forma de actuar del objetivo, como resultado de la difamación social sufrida.

Las campañas de CA están destinadas a una audiencia, a fin de que la misma pueda cambiar negativamente su opinión sobre el objetivo, independientemente si las acusaciones son verdaderas o falsas.

Los objetivos de un CA puede ser una persona (ej. presidente), empresa, organización o inclusive un país/nación. En el caso de naciones:

> Los estados buscan deconstruir o incluso destruir la imagen de sus oponentes, quienes intentan amenazar su legitimidad o confiabilidad y desestabilizar su posición en el sistema internacional [...] Los ataques retóricos de líderes políticos, gobiernos y élites, cuando se utilizan contra otros gobiernos o países, pueden dañar la imagen de un país, afectar sus relaciones diplomáticas, económicas y comerciales con otros países […] la comunicación estratégica y el manejo de la imagen de nación se convierte en un arma que forma alianzas o aísla y sataniza a los adversarios […] Los ataques retóricos se instrumentalizan en las relaciones internacionales. Los líderes políticos los emplean para manipular a la opinión pública internacional y a otros líderes en la búsqueda de objetivos políticos y diplomáticos, así como para desmovilizar a los gobiernos a favor o en contra de otros estados [...] Los ataques retóricos en el discurso entre estados apuntan a deslegitimar o deconstruir la imagen del otro, generalmente a través de la demonización, la dicotomía nosotros vs ellos y la imagen del enemigo […] la satanización del otro puede ayudar a unir a los ciudadanos, legitimar la autoridad política, proporcionar una justificación moral para la violencia y movilizar a los militares y a la población […] un ataque constante, internacional y público a la imagen o reputación de un país puede destruir completamente la imagen de ese país y resultar en su exclusión moral. Este proceso se emplea para justificar cualquier tipo de intervención militar o aislamiento económico (embargo). La destrucción total de las relaciones diplomáticas, internacionales o económicas que se produzca paralelamente o resulte de estos constantes ataques se define como *country assassination.* (Aspriadis, Takas y Samaras, 2019).

Los 5 pilares de un CA son: el **atacante**, el **objetivo**, el **medio**, la **audiencia** y el **contexto**. El **atacante** es quien ataca deliberadamente la reputación del objetivo con la finalidad de disparar una reacción en el público (respuesta emocional, juicio, indignación) y consecuentemente socavar la posición social del objetivo. Mientras más creíble sea la fuente

atacante, mayor es la probabilidad de lograr un resultado estratégico (McCroskey y Teven, 1999). Como indica (Samoilenko et al, 2020), el **objetivo** es el individuo con una reputación o fama (capital social) y los ataques se enfocan a un aspecto del objetivo; como ser: la personalidad, lo que hace (actual, pasado o futuro) o afiliación única de identidad (hombre/mujer, joven/viejo, blanco/negro, nativo/extranjero). El **medio** de comunicación utilizado tiene su complejidad. Su velocidad y direccionalidad afecta como nuestra sociedad entiende el mundo, da forma a nuestra percepción y comportamiento; siendo una extensión de nosotros mismos a medida que los consumimos. En dicho aspecto, internet amplifica los CA mediante rumores y mentiras, comentarios negativos, *fake news*, anonimato (desinhibición sin consecuencias / normas sociales), falta de sustento, entre otros. La **audiencia** es el grupo de personas que se busca influenciar a fin de cambiar su percepción sobre el objetivo y está involucrada en la construcción compartida de realidades, dado que puede aceptar o rechazar la acusación de la fuente. El **contexto** político, cultural social varía según el caso. El contexto viene de los códigos morales inherentes a las normas sociales y culturales. Lo que es moralmente aceptado en un lugar podría no serlo en otro lado del mundo, así mismo el periodo de tiempo puede ir variando dichos aspectos (Samoilenko et al, 2020, pp. 11-22).

Existen siete métodos de CA que vale la pena detenerse un instante a describir. Es altamente probable que se sienta identificado al leerlos, ya que están presentes de forma sistemática en los medios de comunicación que consumimos (ver tabla 2).

Tabla 2
Métodos de Character assassination.

Método	Efecto deseado	Ejemplos
Name Calling: Etiquetar con un término despectivo.	Reducir al objetivo a un rasgo que dispare una asociación negativa.	"chorro", "incompetente", "zurdo", "borracho", "populismo", "facho" "nazi" (reductio Ad Hitlerum).
Making allegations: Acusar de un defecto personal o comportamiento de forma directa o indirecta (independientemente de su veracidad).	Poner en duda la integridad, moral, capacidades mentales u otras características personales.	Acusaciones de corrupción o incompetencia para gobernar. "El presidente esta mentalmente desequilibrado".
Ridiculing: Poner en ridículo con bromas o caricaturas en relación con la personalidad, apariencia, defectos físicos, etc. (Argumentum Ad Carricare)	Ya no se toma en serio al objetivo y pasar a ser fuente de bromas.	Fotos de políticos en momentos inoportunos (con gestos tontos). Caricaturas grotescas en los periódicos. Imitadores en programas de TV.
Fearmongering: Presentarlo como una amenaza o peligro. Deshumanización.	El objetivo se convierte en fuente de miedo, odio, disgusto.	Presentar a un candidato como un peligro para nuestro estilo de vida / condiciones laborales. "Si gana tal candidato vamos a pagar más impuestos".
Exposing: Publicar evidencias (falsas o verdaderas) de defectos de personalidad o fechorías.	Exponer al objetivo como inmoral, criminal u otro defecto.	"Es un traidor a la patria". "Impone reglas que no cumple".
Disgracing: Deshonrar al objetivo. Poner bajo humillación pública. Expulsarlo de la comunidad.	Quitar los honores y status.	Vandalismo de estatuas. Tildar a una mujer de prostituta en internet.
Erasing: Destruir completamente la presencia pública. Quitar de los libros de historia.	El objetivo es removido de la memoria colectiva.	Destrucción de las imágenes de Calígula o Nero en Roma. Políticos removidos de los libros de fotos en la URSS de Stalin.

Nota. Fuente (Samoilenko et al, 2020, p. 21). Con adaptación de los ejemplos.

A modo de ejemplo se muestran algunas caricaturas en el conflicto Rusia – Ucrania/OTAN (ver figura 33). Tener presente que mucha gente ha sufrido pérdidas irrecuperables, tanto de seres queridos, como por lo que trabajaron durante toda su vida. Por lo que se apela el mayor respeto y responsabilidad por parte del lector, enfocándose al ámbito de estudio que nos compete.

Figura 33

Caricaturas dentro del conflicto Rusia-Ucrania/OTAN.



Nota. Muestra de caricaturas críticas presentes en Internet. Autores de izquierda a derecha y de arriba abajo (Ukraine / Україна, 2022; Vagué, 2022; Mulder como fue citado por The New Voice of Ukraine, 2022; Lui, 2022; Latuff como fue citado por Designers for Palestine, 2022; Tan cómo fue citado por Zhu, 2022; Zach, 2022).

Seguidamente, continuamos brevemente con algunos elementos de interés vinculados a los *Character Assassination*.

Dualidad nosotros vs ellos, buenos vs malos.

La retórica de crear una imagen del enemigo, la creación del "ellos", se encuentra vinculado a CA. La diferencia es que es un ataque dirigido a un grupo. Es la creación de la

percepción sobre personas/grupos hostiles outsiders/extranjeros donde se proyectan características indeseadas (débil, barbaros, irracionales, etc.) en una simplificación estereotípica. Se construye y cultiva una percepción imaginaria del enemigo en el público. Esto permite tratar al enemigo de formas que normalmente serian consideradas inhumanas, pero que se reconstruye cognitivamente como digna y moral porque ELLOS merecen dicho trato (Bandura, 1999). Por ejemplo, cuando en medios occidentales hablan de "Enemigos" o "Terroristas" a otras naciones o líderes/presidentes de otros países. También es utilizado por la política como medio de polarización (demonizando a los otros). Las personas asimilan de forma cómoda la abstracción de buenos vs malos, dado que resulta conveniente para la mente humana la simplificación de la complejidad variable del mundo real (la cual involucra múltiples actores con intereses variantes en el tiempo).

Dentro del plan Cóndor de los 70, los militares en Latinoamérica fueron entrenados con métodos de tortura en Panamá en la Escuela de las Américas (*USARSA: United States Army School of the Americas* - renombrado a Instituto del Hemisferio Occidental para la Cooperación en Seguridad). Ejemplo, el manual KUBARK indica métodos de tortura (amenazas, miedo, dolor, privación sensorial, uso de narcóticos, descargas eléctricas, entre otros) (National Security Archive, s.f.). Resulta comprensible pensar que dicho entrenamiento incluyó elementos de guerra psicológica sobre los militares, apelar al odio, la dualidad nosotros / ellos, desconexión emocional y una radicalización, con el fin de influenciar a que puedan llevar a cabo actos inhumanos contra sus propios ciudadanos.

Ataques de argumento ad hominem (Ad Hominem attack).

Busca sacar el foco de atención del debate. Al no poder refutar el discurso, se ataca al emisor de este. Es una falacia que intenta desacreditar al locutor y, por ende, deja sentado que todo lo que diga el locutor, es cuestionable. Es un ataque eficiente para convencer a las audiencias más emocionales que racionales.

Como A es una persona con una mala personalidad, entonces el argumento de A debe rechazarse (Walton, 1998). Es falaz porque la veracidad del mensaje no depende del emisor.

Ataques de silogismo entimema (Enthymematic attack).

Según Aristóteles, la lógica entimema es un tipo de silogismo en el que se ha suprimido alguna de las premisas o la conclusión, quedando la misma implícita. La audiencia del mensaje completa la parte del argumento ausente.

Ataque mediante malversación de citas (Misquoting attack).

Tomar fragmentos del discurso de un objetivo y exponerlo fuera de contexto, con la finalidad de hacer creer a la audiencia una realidad parcial o completamente equivocada. De dicha forma, el locutor queda desacreditado.

Ataque de culpabilidad por asociación (Guilt by association attack).

Es un tipo de CA que también utiliza una lógica falaz. Nuevamente, en vez de refutar el discurso, busca vincular al locutor a una persona con mala reputación y de esa forma desacreditar su discurso. Como A es amigo de B y B es corrupto, entonces A también es corrupto y lo que diga debe ser rechazado.

Reductio Ad Hitlerum es CA basado en *guilt by association*. El atacante invalida el discurso de un objetivo, basado en la premisa de que Hitler/Nazis/fascismo tenía/n la misma postura, negando así el derecho moral a expresarse.

Asesinato de personaje en el ciberespacio (CA in the cyberspace).

El CA es efectivo, fácil y económico de realizar (en particular con la utilización del ciberespacio). El atacante asume un menor riesgo que un asesinato convencional. La implicancia de exponer una operación de este tipo suele ser poco trascendentes, difícil de atribuir y/o revertir. Resulta complejo desenredar una mentira en la sociedad una vez que la misma ha causado su efecto. Las consecuencias para el atacante son prácticamente nulas.

Las TICS cambiaron la dinámica de la propaganda, donde los consumidores dejan de ser pasivos y pasan a ser activos. La utilización de Internet puede causar que los ataques se vuelvan virales rápidamente, en especial si logran afectar a un influencer a fin de que replique y amplifique el ataque. Las campañas pueden ser lanzadas desde cualquier lugar del mundo y a diferencia de los medios convencionales, los ataques en internet permanecen por tiempo indeterminado.

Los mensajes de ataque en internet suelen presentarse a modo multimedia con descripciones reducidas. Las imágenes, con fuerte contenido, apuntan a cultivar la emocionalidad cegando el pensamiento crítico y lógico. Las emociones (como la ira, bronca, frustración, indignación) son movilizantes y el atacante logra canalizar la energía de la audiencia en contra del objetivo (presente como responsable de algún hecho injusto, indigno, impopular, ilícito, entre otros). Como indica Stuckless y Goranson (1992), la venganza es el impulso humano básico de infligir castigo a cambio de alguna acción mala, y puede ser un fuerte motivador del comportamiento social, inclusive más allá de una agresión verbal.

Los memes también son un mecanismo interesante de CA, que por su naturaleza se propagan rápidamente.

Desconexión moral en el ciberespacio (Moral disengagement in cyberspace).

La desconexión moral es un tema que merece la pena mencionar brevemente, dado su vinculación no solo a los CA, sino también a las operaciones en el ciberespacio y los temas abordados en el presente trabajo.

Acorde a Bogolyubova (2019), se trata de una característica psicológica de los CA. Las particularidades del ciberespacio (distancias, anonimato, virtualidad) facilitan la desconexión moral (distorsionan las consecuencias de un ataque y deshumaniza a las víctimas).

Según Moore (2015), la desconexión moral es un mecanismo cognitivo que facilita a personas ordinarias perpetrar actos dañinos. Dichos actos se disocian mentalmente de los valores/normas del individuo y se reformulan como justificados/nobles. Banduna (1996) explica 8 estrategias de desconexión.

1. *Moral justification*: Justifica los hechos en busca de un propósito moralmente superior. Ej. la tortura es aceptable si obtiene información que permita proteger a los ciudadanos de ataques terroristas.
2. *Euphemistic language*: Moldea el lenguaje a fin de remover connotaciones negativas. Ej. “dispatch targets” en vez de “matar personas”.
3. *Advantageus comparison*: Justificar una acción comparándola con otra peor.
4. *Displacement of responsibility*: Justificar el accionar bajo el pretexto de estar siguiendo órdenes de un superior.

5. *Diffusion of responsibility*: Distribuir la responsabilidad en un grupo, así nadie siente culpabilidad.
6. *Disregarding or Distoring the consequences*: Cuando las consecuencias / impacto sobre la víctima no es visible por el atacante.
7. *Dehumanization*: Los objetivos son rotulados de forma inferior al humano, justificando un trato inhumano.
8. *Attribution of blame*: Cuando se culpa a la víctima por el hecho. Ej. el asalto sexual es consecuencia de cómo se vestía.

Asesinato por intimidación (Intimidation Kill Attack).

Un cuerpo sin mente es un cuerpo muerto (reflexión de elaboración propia)

Las operaciones intimidatorias y de persecución, buscan disuadir al objetivo de su accionar o en caso más extremos llevarlos a una situación de stress y paranoia. Esto lleva al objetivo a una sobrecarga cognitiva y emocional. Aquí entra en juego la fortaleza mental del objetivo respecto al ataque. También intervienen los miedos internos del objetivo en cuanto su vida, la de sus seres queridos, o que pueda darse a conocer información que destruya su imagen. Información no necesariamente ilegal o inmoral; recordemos que se trata de la percepción mental del objetivo. Lo que para una persona puede ser de suma importancia para otra puede ser intrascendente. Es por eso por lo que la información de inteligencia es primordial para conocer la personalidad de sus objetivos, sus miedos y sus puntos débiles.

Estos ataques además impulsan al objetivo a actuar de forma desorientada de su entorno, siendo altamente propenso de accidentes. En algunos casos limite, puede incitar al suicidio. En dichos casos estamos en presencia de un *intimidation kill*.

Medios de comunicación y propaganda.

"Ordenaba a sus secuaces que sembraran confiadamente la calumnia, que mordieran con ella, diciéndoles que cuando la gente hubiera curado su llaga, siempre quedaría la cicatriz" Medio de Larisa (alrededor de 300 A.C. según Plutarco, capítulo 4º del libro I de sus Obras Morales).

"Como suele decirse de la calumnia: calumnien con audacia, siempre algo queda" Roger Bacon (1214-1294).

"Mientras más increíble es una calumnia, más memoria tienen los tontos para recordarla" Jean-Jacques Rousseau (1712-1778).

Paradójicamente la frase fue falsamente atribuida a Goebbels (1941), lo que en realidad dijo fue *"Una vez proferida una mentira, sigue repitiéndola [refiriéndose a Churchill] sin que nada ni nadie se lo pueda impedir, hasta que al final acaba él mismo creyéndola" en la obra "De la fábrica de mentiras de Churchill".*

El solo hecho de plantear la duda ya es en sí un ataque efectivo.

La verdad la tiene quien posea una mejor propaganda (reflexión de elaboración propia).

En Internet, existe una amplia variedad de medios de comunicación y cualquier persona con una Webcam o Smartphone puede transmitir sus contenidos por *streaming*. Internet ha puesto en disputa la hegemonía de los medios tradicionales atentando contra sus intereses. No es raro observar campañas difamatorias sobre la veracidad del contenido de internet o inclusive ataques contra voces alternativas. Internet no es impoluto, sin embargo, cuando se trata de subjetividad, omisión, manipulación o engaño; los medios tradicionales están a la vanguardia. Por otra parte, los reiterativos mensajes de odio son efectivos a la hora de penetrar la psiquis de la población; manipulando los pensamientos a partir de las emociones[102]. A pesar de todo, los medios tradicionales terminan poco a poco integrándose al ciberespacio (si no puedes contra ello, únete).

[102] El concepto está relacionado con la dualidad nosotros vs ellos. El odio se sustenta de un grupo de pertenencia contra otro grupo/individuo diferente. El odio es una emoción movilizante que a lo largo de la historia fue aprovechada inclusive en el plano bélico. Por ejemplo, Acorde a (Marxists Internet Archive, s.f.),

Los medios de comunicación pueden ser privados o estar en manos de estados. Cualquiera sea el caso, siempre responden a intereses que sesgan e influyen en el contenido de la información provista al público.

En los medios tradicionales, los periodistas se dedican cada vez menos a informar objetivamente a la población y cada vez más a formar la opinión de la gente[103]. Los medios radicalizan a la población con emociones negativas, como odio e indignación; que luego reflejan acciones violentas en la vida cotidiana. En vez de fomentar un pensamiento crítico, indican a la población "que" y "como" deben pensar sobre diferentes tópicos que imponen. Son los que fijan agenda de los temas relevantes y realizan preguntas en las cuales inducen la respuesta en el receptor. También preparan el clima social previo a un suceso relevante. Cuando se trata de *carácter assassination*, tienen un repertorio cuasi ilimitado y no es necesario ampliar en dicho aspecto dado que el lector podrá apreciar con su experiencia propia. Como apreciación personal, los periodistas se han transformado en lo que podemos denominar *asesinos mediáticos seriales*.

Los medios de comunicación son expertos en el sesgo de la información y la manipulación de datos estadísticos. Las estadísticas son interpretadas acorde a la necesidad del locutor y lo que se pretende comunicar.

Los medios de comunicación también poseen un papel en la confianza de los ciudadanos sobre los mercados. En nuestro país es habitual observar la manipulación psico mediática operando sobre las masas en sucesos específicos de la política / mercado en coordinación a sectores empresariales y políticos. Dichos eventos terminan causando un impacto en los mercados (ej. acciones o divisas) que justamente están basados, por naturaleza, en la confianza. Remarcamos, a modo aclaración, que tales ataques no serían tan efectivos si el mercado tuviese suficiente fortaleza. Dicha mención es un ejemplo de combinación de guerra económica y psicológica.

Los medios también cumplen un rol en el control social. Operan como cortina de humo quitando el foco de atención de los temas relevantes. El espectáculo (futbol, cine, series,

Che Guevara mencionó en un discurso al odio como factor de lucha necesario para triunfar sobre un enemigo brutal (en relación con la invasión de EEUU en Vietnam, entre otros conflictos).

[103] Resaltamos los aspectos negativos de los medios de comunicación a fin de abordar el tema planteado. Sin embargo, gracias al trabajo de algunos periodistas, se han revelado abusos del poder que de otra forma no podríamos conocer. Estos periodistas se arriesgan al informar y luego pueden ser perseguidos.

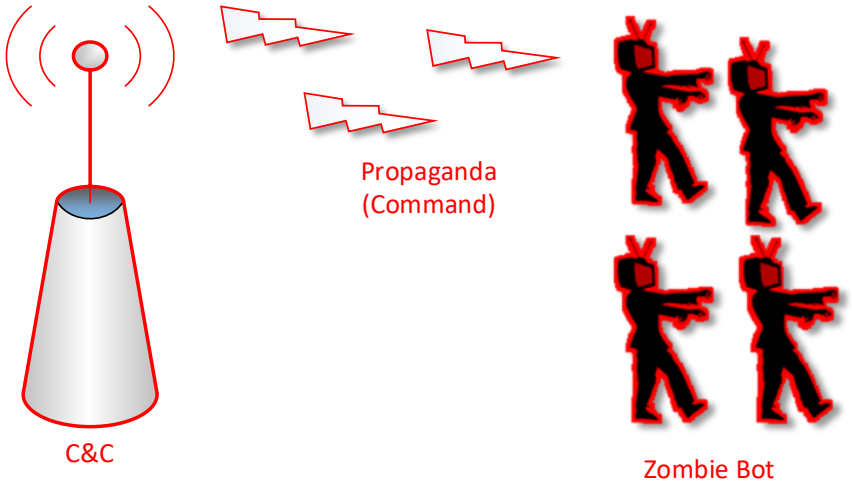
shows, entre otros) mantiene a la población ocupada y contenta (panem et circenses); sin tiempo de pensar, reflexionar o cuestionar al poder. El control, que antiguamente era ejercido por la iglesia, hoy es suplantado en gran parte por la industria del entretenimiento. Como indica Han, el poder maneja o guía la comunicación en una dirección determinada suprimiendo la posible discrepancia que existe entre el soberano y el súbdito a la hora de seleccionar la acción (Han, 2005).

Además, los medios de comunicación son un mecanismo imprescindible de control y manipulación mediante la amplificación de propaganda.

Según Pratkanis y Aroson (2001): “La palabra propaganda ha evolucionado para significar sugerencia o influencia masiva a través de la manipulación de símbolos y la psicología del individuo. La propaganda implica el uso diestro de imágenes, consignas y símbolos que juegan con nuestros prejuicios y emociones; es la comunicación de un punto de vista con el fin último de que el destinatario del llamamiento llegue a aceptar voluntariamente esa posición como si fuera la suya propia”.

Acorde a Noam Chomky (1997): "La propaganda es a la democracia lo que el garrote es al estado totalitario". Refiere a que el poder totalitario utilizar la violencia mientas que la democracia tiene que recurrir a controlar a las mentes de las masas mediante la propaganda (fabricación del consentimiento). Crear ilusiones necesarias para distraer, confundir y generar apatía/ecuanimidad (ver figura 34). Los medios tienen una agenda y eligen los temas a tratar, distribuyen las preocupaciones, filtran la información, delimitan los límites de los debates, amoldan, restringen y sirven a los intereses de los grupos dominantes (Wintonick y Achbar, 1992). A continuación, se aprecia los conglomerados mediáticos en Argentina y en EE.UU. (ver figura 35 y 36).

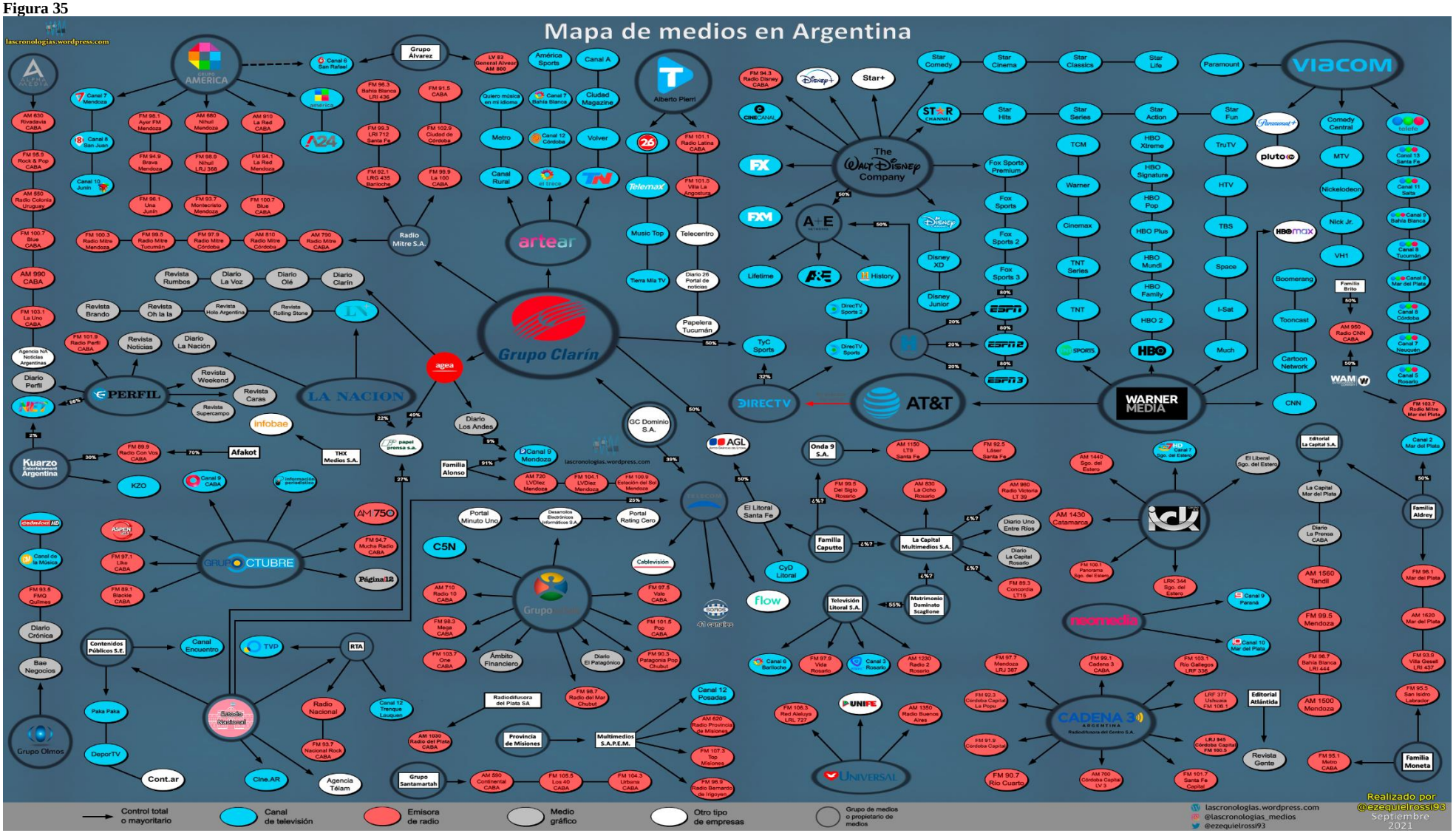
Figura 34
Propaganda ZombieBot.



Nota. Analogía con una botnet (fuente: elaboración propia basada en OpenClipart-Vector[104]).

[104] Autor OpenClipart-Vectors from https://pixabay.com/vectors/zombie-tv-man-stagger-156746/

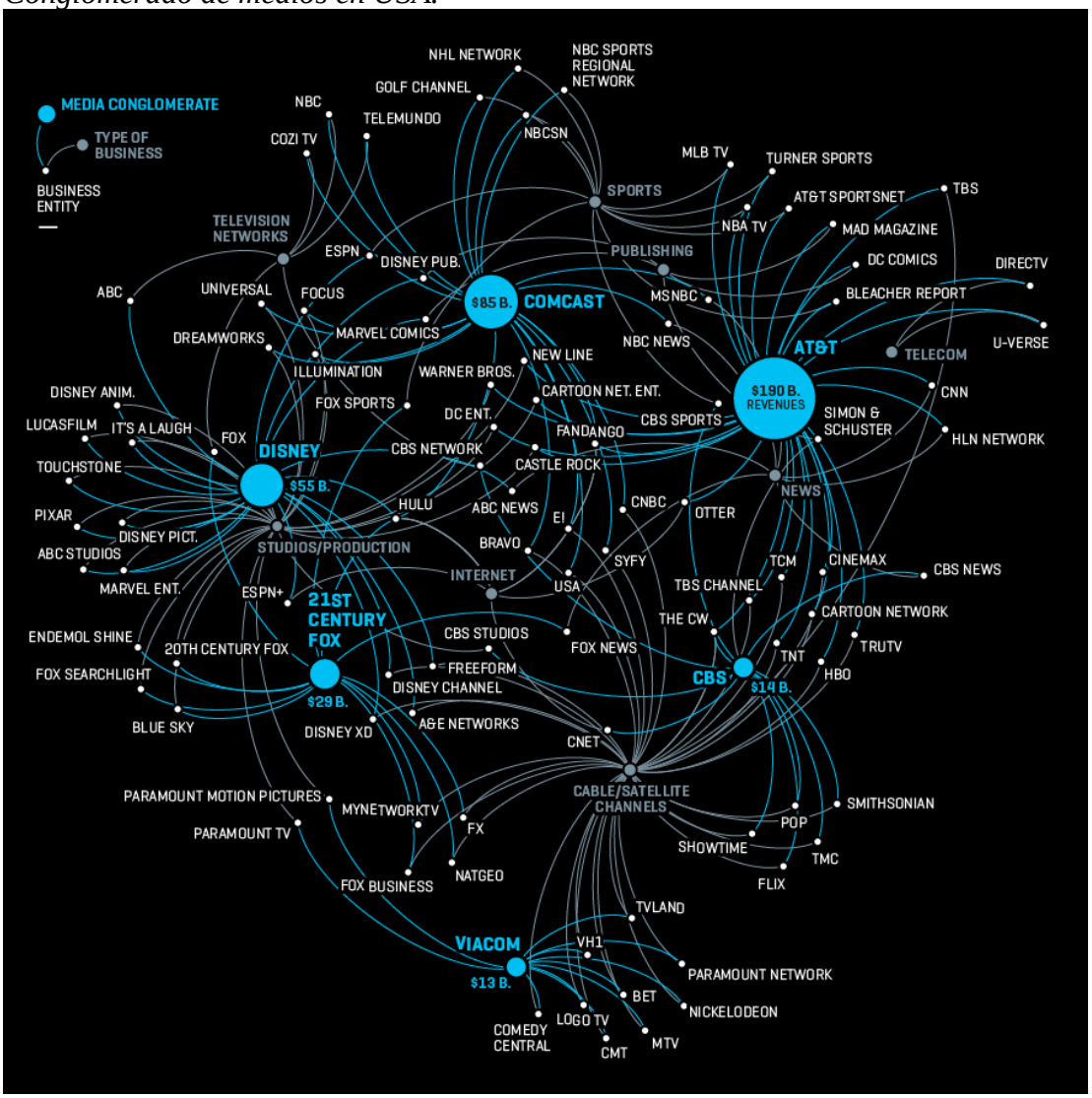
Figura 35



Nota. Conglomerado mediático en Argentina (Rossi, 2021).

Figura 36

Conglomerado de medios en USA.



Nota. Centrado en 6 corporaciones (Rapp y Jenkins, 2018).

Durante la última dictadura argentina, a fin de manejar la propaganda, el control de los canales pasó a las FFAA. El canal 13 (ls85) a la Marina, canal 11 (ls84) a la Fuerza Aérea, canal 9 (ls83) al Ejército (Rossi, 2021).

En lo que respecta a la actualidad, ¿Cómo es posible que al escuchar un medio de comunicación resulte tan convincente como un medio con una visión antagónica? Los mensajes que se transmiten están altamente sesgados. Cada uno da su visión de los hechos acorde a sus intereses, omitiendo lo que no conviene y resaltando lo que sí. Pero ¿quién tiene razón? ¿dónde está la verdad? La mente hace de la realidad objetiva una subjetividad

psicológica y existen al menos tantas realidades como observadores. Si a ello sumamos un intermediario en la comunicación la entropía se incrementa. La verdad y la razón la tiene quien controle más medios de comunicación para imponer la misma. La realidad es un menú a la carta, hecha a la medida de cada consumidor acorde al canal que quiera consumir. Buscar la realidad es como buscar una zapatilla en una tienda, donde el cliente puede elegir[105] el producto que más se adapte a su pie. Los medios de comunicación cumplen un rol importante en una agenda de control sobre la población[106].

Producción cultural.

En las películas y series también existen mensajes de diferente índole que apuntan a la mente del espectador. Para mayor eficacia del emisor, se apela a situaciones de extrema tensión o emocionalidad, donde el receptor absorbe el mensaje a modo de aprendizaje.

Mientras que algunos mensajes tienen una funcionalidad más benigna (fomentar sentimientos patrióticos, incentivar el ingreso a las fuerzas armadas, luchar en defensa del país, etc.), otros no lo son (desprestigio u odio de otras naciones, dualidad nosotros vs ellos, justificar actos inhumanos, etc.). En algunos casos, notará que incluso algunos mensajes preparan a la población a una agenda de acciones futuras.

Gran parte de las historias transcurren con la perspectiva de los personajes principales, que defienden a sus seres queridos y pelean por causas justas (una visión humanizada). Por otra parte, los enemigos presentan características negativas (maldad, codicia, corrupción, amoralidad, etc.) y no conoceremos sus sentimientos ni de sus seres queridos (des humanizados). En ocasiones aparecen como NPC[107] de un juego.

La película Unthinkable (2010) justifica la utilización de la tortura para conseguir información y prevenir la detonación de una explosión nuclear en una ciudad civil. Propone el debate de la tortura, aunque finaliza con una explosión de una bomba como consecuencia de no haber torturado suficiente al enemigo. El mensaje de la película es tan atroz como falaz. Hemos reiterado como la tortura es infructuosa como mecanismo de obtención de

[105] Elegir es en realidad la falsa sensación de libertad de seleccionar dentro de las opciones que ofrece el vendedor. Esto surge porque se ha desvirtuado el concepto de libertad como preferencia reflexiva de lo mejor.
[106] Constatación de 1984 de George Orwell.
[107] Bot (*Non Player Character*).

información. Las víctimas no proveen información de valor o simplemente terminan afirmando (inclusive a veces creyendo) lo que el torturador quiere escuchar[108].

Respecto a la propaganda en la industria del cine, Vega Durán (2020) realiza un estudio donde indica que el pentágono (Departamento de Defensa) colabora en producciones con equipamiento, ubicaciones y personal a cambio de poder sugerir cambios en los guiones. La intención es transportar valores que beneficien los intereses del gobierno de Estados Unidos. La propaganda implica un control del flujo informativo como la creación, refuerzo o modificación de una respuesta ante un mensaje. Pretende influir en las conductas y opiniones de los receptores. Acorde a Follow (2018, citado por Vega, 2020), el encargado del departamento de relaciones con las industrias del entretenimiento del Pentágono (Philip Strub) es la persona que más aparece en los agradecimientos del top 200 de películas entre 1997 y 2016. Teun van Dijk (1999, como cito en Vega, 2020) menciona que el discurso tiene el potencial de influenciar las creencias de los individuos y según Habermas (1992, como cito Vega, 2020) el discurso es un medio más de dominación que sirve para legitimar las relaciones de poder. Finalmente, la propaganda, la ideología y el discurso terminan funcionando dentro de las estructuras de poder con intención de legitimarlas, modificarlas o derribarlas. El poder, en definitiva, consiste en la influencia en la actuación de terceros a conducir conductas en base a un interés. Acorde a Nye (2004, citado por vega, 2020), *soft power* es el poder que obtiene por atracción (en vez de coerción o recompensas). El atractivo de la cultura de una nación transmitido mediante la comunicación es una de las estrategias utilizadas. Vega (2020) concluye que el cine de EE.UU. tiene una vocación persuasiva / manipulativa, donde se utiliza el engaño (omisión / distorsión de información) o la incentivación (recompensa a quien respeta los valores estadounidenses). Algunas representaciones recurrentes que observa son:

- Instituciones estadounidenses decididos e implacables, aunque humildes en reconocer errores.
- El ejército, siempre presente, se muestra más como una familia en busca del bien del país y sus ciudadanos (empático). Los protagonistas que logran un

[108] En los regímenes autocráticos, la tortura es inmanente al lavado cerebral. El libro de 1984 de Orwell es específico sobre este punto.

beneficio para EE.UU. se convierten en héroes. Los valores son valentía, solidaridad, libertad y justicia.

- En el caso de países enemigos son representados como inflexibles, corruptos, subdesarrollados, incomprensibles y alejados del bien común. Mientras que sus militares son representados como cueles, amorales y violentos; que quieren destronar a EE.UU. y crear un mundo oscuro y pobre.

Un último elemento por mencionar sobre la propaganda en el cine es la imposición de marcas norteamericanas. Utilizan varios elementos psicológicos (como el sentido de pertenencia) para reforzar la invasión económica / cultural. Marcas que en realidad son solo una imagen psicológica y no poseen un valor especial; dado que la mayoría envían a producir sus productos a fábricas en China / Asia. Lo que se vende no es un producto si no una imagen psicológica que fomenta el consumo.

Autoritarismo psicológico (PsycoAutoritarism).

El ser humano ha infectado a la tecnología con su sed de poder y el afán por el control (reflexión de elaboración propia)

Cuando tenemos la situación de gobiernos democráticos que realizan un esfuerzo deliberado en moldear la forma de pensar de su población, como así también la de otras naciones, mediante la utilización de propaganda u otras acciones psicológicas, podríamos estar hablando de gobiernos *psicoautoritarios*. Decimos autoritarismo, a pesar de estar enmascaradas en una democracia, debido a que los ciudadanos no tienen un real discernimiento y sus decisiones no resultan verdaderamente genuinas.

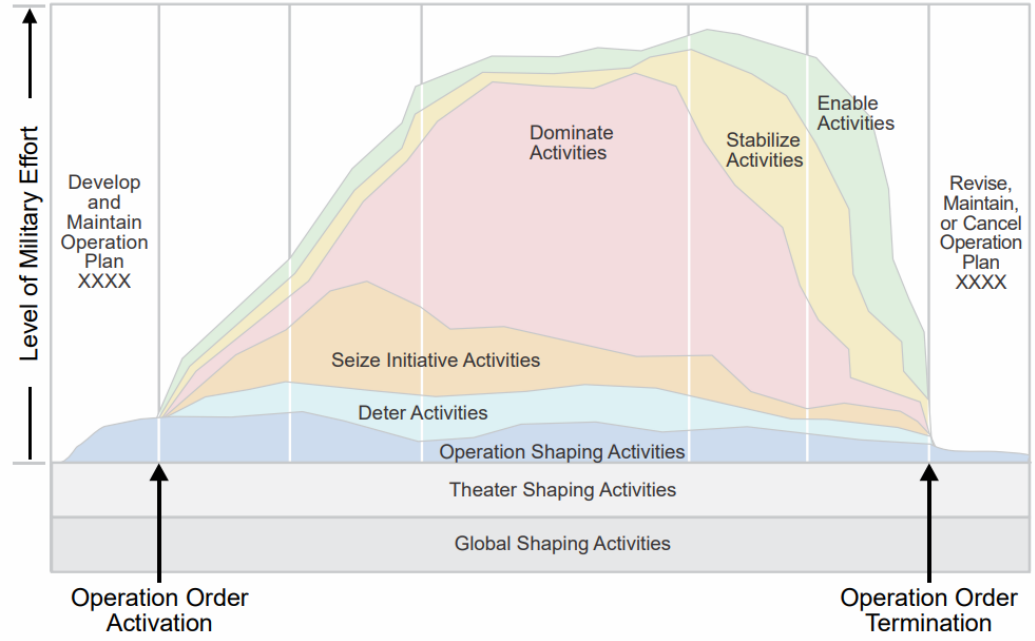
¿Invasión cultural?

En las invasiones convencionales, por ejemplo, el modelo Joint Combat Operation de 6 fases (ver figura 37), primero opera la intervención militar y luego somete a la población (sumado al restablecimiento de las infraestructuras críticas y la estructura gubernamental) (Joint Publication 3-0) (Joint Chiefs of Staff, 2018). Tal esquema resulta ineficiente y arduo dado que la población invadida no se siente identificada con el invasor y rechaza dicho poder mediante insurrección, sabotaje, guerrilla y diferentes actos en contra.

Convencer / ablandar a la población previo a la invasión física resulta menos problemático. La invasión cultural ocurre desde diferentes ámbitos como la música, el idioma, ideales / valores, la forma de vivir y vestir, etc. Esquemas de guerra psicológica son utilizados y amplificados con medios de comunicación. El lobby, el soborno y la corrupción de gobernantes también pueden ser potentes armas contra un pueblo con escasos valores o sin fuertes leyes que castiguen dichas conductas. Cuando se logra someter psicológicamente a los ciudadanos y a sus dirigentes, las invasiones físicas dejan de ser necesarias.

Figura 37

Joint Combat Operation Model.



Nota. Shape, Deter, Seize Initiative, Dominate, Stabilize y *Enable Civil Authority (Joint Chiefs of Staff, 2018).*

Crear un evento para promover cambios.

El poder puede utilizar un evento de alto impacto emocional para luego promover leyes o quitar derechos. Estos no son impuestos, sino que son los mismos ciudadanos que exigen el cambio que, de otra forma, jamás hubieran tolerado aceptar. Un ejemplo es restringir las libertades o derechos de privacidad apelando a luchas contra el "terrorismo". Palabras como "terrorismo" funcionan similar a las *power word* en neuromarketing. Un evento dantesco capta la atención, el miedo detona la parte emocional y ayuda a fijar la impronta en la mente para no olvidar el suceso.

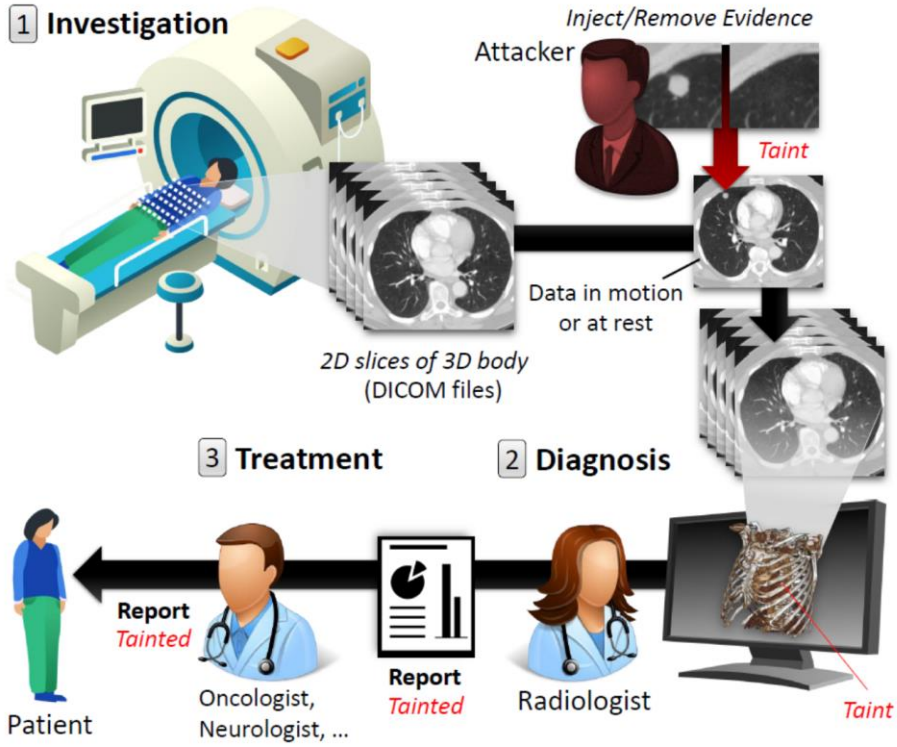
¿Disrupción cognitiva emocional?

En 2019, un grupo de investigadores realizó una prueba de concepto sobre la adulteración de estudios médicos. Con un *malware* lanzaron un ataque *man in the middle* con *tampering* en imágenes de resonancias magnéticas. Mediante técnicas de *Deep learning* evidenciaron dos escenarios previos al diagnóstico del profesional: remover un tumor existente o incorporar un tumor ficticio a los resultados médicos (ver figura 38). Además, indicaron que el ataque es factible para diversas enfermedades, incluidos aneurismas, enfermedades cardíacas, coágulos de sangre, infecciones, artritis, problemas de cartílago, ligamentos desgarrados y tumores en el cerebro, el corazón o la columna vertebral (Mirsky, Mahler, Shelef y Elovici, 2019).

En primer escenario estaría privando a la víctima de un tratamiento médico y por lo tanto hablamos de un acto de asesinato. En el segundo escenario, apunta a preocupar / estresar / impactar a la víctima en un plano emocional, afectando su capacidad cognitiva para enfocarse o tomar decisiones en otros planos (ej. estrategia militar). Este último caso, es un claro ejemplo donde *cyber warfare* se combina con *cognitive warfare*.

A fin de lograr el mismo fin, no debe descartarse la utilización de ataques reales o encubiertos como accidentes, sobre un objetivo o familiares.

Figura 38
Ataque de tampering sobre resonancias magnéticas.



Nota. Autores (Mirsky, Mahler, Shelef y Elovici, 2019).

¿Sentimiento de culpa?

Cuando el estado ejerce una excesiva presión impositiva o en leyes, los ciudadanos se ven obligados al incumplimiento en pos de la subsistencia. Este sentido psicológico de culpabilidad / complicidad causa que los ciudadanos sean menos propensos a cuestionamientos y más proclives a aceptar actos de corrupción y otros abusos del poder. El sentido de culpa y complicidad es un elemento más del ejercicio del poder.

Redes sociales.

Las redes sociales captan a sus usuarios explotando vulnerabilidades sociales como ser el sentido de pertenencia. Ofrecen beneficios a fin de captar a sus víctimas (*digital Candy*), como la utilización de las diferentes características de la plataforma, juegos, comunicaciones, conocer que hacen tus contactos, etc. A cambio y bajo engaño, obtienen una inmensa cantidad de información de sus usuarios, usualmente fuera de su *awareness*. Para sustentar dichas operaciones utilizan términos y condiciones ambiguos, confusos,

infinitamente largos y que a su vez cambian en el tiempo. Toda la información recolectada es luego puesta a disposición del mejor postor, quien la utiliza en diferentes operaciones. Algunas operaciones son un poco más inocentes como el uso publicitario, pero otras no tanto, como influir en elecciones democráticas. En dichas redes, el usuario cree ser el cliente, cuando en realidad es el producto a la venta y quien adquiere los datos es el verdadero cliente. Desde el punto de vista del modus operandi, actúan de igual forma que una red de trata de personas.

Más adelante ampliaremos este concepto de la falsa creencia de que la persona debe obligatoriamente aceptar todas las imposiciones para obtener el *digital Candy* (beneficio señuelo). La falacia se sustenta en que de otra manera la tecnología no podría funcionar.

¿Cómo funcionan las operaciones citadas? Antiguamente había que lanzar cientos de misiles para impactar en un blanco. De a poco la tecnología logró crear misiles inteligentes capaces de alcanzar sus objetivos con alta precisión y velocidad. Al igual que los misiles evolucionaron en eficiencia y precisión, lo ha hecho la manipulación psicológica. Los ataques psicológicos son amplificados con las TICs. En vez de bombardear a la población con mensajes masivos de baja efectividad, se utiliza la IA para micro segmentar a la población y se envía un único mensaje de alta precisión / efectividad. El mensaje se encuentra hecho a medida del perfil psicológico del objetivo.

Según el documental “The great hack” (Amer and Noujaim & White, Dreyfous, Korin and Kos, 2019), Cambridge Analytica Ltd. ha influenciado elecciones democráticas en diferentes partes del mundo mediante la manipulación selectiva de personas (objetivos) utilizando modelos matemáticos de clasificación entrenados a partir de 5000 datapoints obtenidos de Facebook. La indagatoria del parlamento británico a Alexander Nix, CEO de Cambridge Analytica Ltd., permite apreciar que la empresa operó en las elecciones presidenciales de argentina en 2015 (Channel 4 News, 2018), lo que resulta una severa intromisión a la soberanía nacional. Una reciente investigación de Channel 4, revela como los datapoints de Facebook fueron utilizados para clasificar personas a partir de ciertos rasgos característicos (ej. gustos sobre mascotas, armas, planes de casamiento, o inclusive datos más sensibles como ser apertura de conciencia, extraversión, amabilidad, neuroticismo, etc.). Mediante la utilización de modelos matemáticos, determinaron la respuesta de los individuos a ciertos estímulos (publicidad de campaña selectiva) que fueron

utilizadas durante las elecciones de EE.UU. en 2016. El objetivo no apuntaba a obtener votos, sino más bien, convencer a ciertos grupos opositores (targets), que se quedarán en sus casas el día de las votaciones presidenciales, influenciados por publicidades difamatorias sobre su candidato (Rabkin, Basnett, Howker, Eastham, and Pett, 2020).

Otras operaciones se sustentan en que los mismos usuarios retransmitan el mensaje de forma viral. Para ello es usual apelar a la emocionalidad en vez de la racionalidad. Cuando un mensaje logra llegar a un famoso o influencer y el mismo lo retransmite, se produce una amplificación del ataque.

Los estados explotan las redes sociales para afectar e influenciar a otras naciones. Por otra parte, es cierto que la tecnología también permite a los ciudadanos organizarse y reclamar derechos que antiguamente resultaban difícil de exponer. Por ello, el poder recurre a deslegitimar y desarticular los reclamos genuinos de los ciudadanos alegando una organización externa o de opositores.

Creando realidades.

Mientras les hagas creer que están comiendo algo rico, no importara lo que les des (reflexión de elaboración propia).

Resulta evidente que el imperio[109] de Google forma resultados diferenciales acorde a cada país e inclusive censura contenido. Últimamente han censurado todas las visiones divergentes a la explicación oficial del atentado del 11 de septiembre de 2001. La plataforma YouTube resalta los medios de comunicación rusos (ejemplo Sputnik o RT news) con carteles. En los mismos indica que están financiados por el estado, deslizando en el publico la noción cognitiva de que el contenido se encuentra sesgado (busca influir mediante la duda). Sin embargo, no hace lo mismo con los medios de comunicación norteamericanos. En el reciente conflicto Rusia-Ucrania han censurado completamente todos los medios afines a Rusia. Desde el punto de vista militar, es comprensible denegar cualquier posible propaganda a favor de Rusia y en contra de las acciones de la OTAN. No obstante, desde el punto de vista civil, resulta un grave atropello a la libertad de expresión y los valores de las democracias occidentales; lo que es un punto de debate en la actualidad. El Golden Shield

[109] En referencia al colonialismo tecnológico en todo el mundo y en cada nivel: Harware, OS, aplicación y SaaS.

de China que censura las TICs (Walton, 2001), es también un reflejo de la tendencia a controlar la información en el ciberespacio.

¿Qué sucederá el día que los resultados sean completamente a medida de cada usuario? la visión distópica del ministerio de la verdad de la novela de 1984[110] de Orwell nos alerta de los peligros existentes de crear realidades a medida de la conveniencia o necesidades. La capacidad de recomendar contenido, formar o sesgar resultados diseñados acorde a cada usuario; facilita el poder de influir cognitivamente en los actores clave de tomas de decisiones, afecta las investigaciones universitarias o influencia a la población en relación con ciertos tópicos. Nuevamente resaltamos la importancia de la ética profesional en los desarrollos de software y en sus arquitecturas. Ignorar los peligros no hace que los mismos desaparezcan, solo les da rienda suelta. Un profesional ya no puede seguir ignorando tales peligros. Las pirámides siempre se construyen desde sus cimientos. Los ciudadanos son esclavos de sus propias cárceles.

Modificación del comportamiento (Behavior modification).

Controlar la forma en cómo actúan y se comportan las personas es quizás el arma definitiva.

El interés por controlar la mente y el comportamiento de las personas es de vieja data. En 1957, James Vicary realizó un experimento sobre mensajes subliminales en un cine de New Jersey. Un mensaje subliminal es un mensaje oculto que aparece por una fracción muy corta de tiempo y pasa por debajo del umbral de percepción consiente del espectador. El mensaje subliminal es percibido por el inconsciente de la mente. Vicary afirmó que el experimento aumentó la venta de pochoclos en 57.5% y Coca Cola en 18.1%, lo que llevó a interesar a la CIA (Robin, 2015). La desclasificación de la CIA de la publicación “The operational potential of subliminal perception” concluyó que los mensajes subliminales con la finalidad de no alertar las defensas conscientes no tienen la confiabilidad para ser utilizados en operaciones (Gafford, 1957). Finalmente se descubrió que Vicary falsificó los resultados de forma fraudulenta (Robin, 2015). A pesar de ello, en 1978 el FBI intentó

[110] Inspirado en la novela “nosotros” de Zamiantin Yevgueni.

atrapar al asesino serial BTK con un mensaje subliminal en Kake-TV, el cual tampoco funcionó (True Crime Magazine, 2016), aunque resalta los intereses en la materia.

Otros antecedentes son el Proyecto MKUltra de la CIA, donde investigaron experimentos en humanos en el ámbito del behavioral modification. Se estudió la utilización de drogas e hipnosis, tanto voluntarios como personas sin consentimiento.

Según (Select Committee on Intelligence and Committee on Human Resources, 1977), el proyecto ARTICHOKE (posteriormente BLUEBIRD) de 1951, incluyó drogas e hipnosis para convencer a personas de cometer asesinatos fuera de su voluntad. Esto empujó la creación de proyecto MKULTRA mencionado (posteriormente MKSearch). MKULTRA (1953-1964) financió trabajos en conjunto de la CIA/DoD. Poco se conoce dado que el director de la CIA, Richard Helms, envió a destruir todos los documentos en 1973. Posteriormente encontraron documentación sin destruir en archivos de la sección de presupuestos (parcial dado que se trata de información financiera). MKULTRA incluyó 149 proyectos en behavior modification (con drogas e hipnosis), adquisición de nuevas drogas y pruebas en humanos (sumado a colaboración de Fort Detrick, utilización de electroshock, técnicas de hostigamiento, asesinatos con aerosol, percepción extrasensorial, sabotaje de cultivos, almacenamiento de energía en sistemas orgánicos, utilización de técnicas de magia en operaciones, entre otros) (Select Committee on Intelligence and Committee on Human Resources, 1977). MKULTRA involucró experimentos sin consentimiento con ciudadanos norteamericanos en bares, colegios, universidades, cárceles, safehouse en San Francisco / Nueva York, entre otros. También la utilización de instituciones a modo pantalla. Continua que el proyecto QKHILLTOP estudiaba técnicas chinas de lavado de cerebro y formas efectivas de interrogatorios mediante la utilización de drogas. La Operación Midnight Climax incluyó la contratación de prostitutas para atraer clientes a los safehouse, donde le administraban drogas (como ser LCD) y eran monitoreados detrás de vidrio espejo a la espera que la combinación droga / sexo pudiera revelar secretos bajo interrogatorio (Select Committee on Intelligence and Committee on Human Resources, 1977). El instituto de Canadá Allan Memorial Institute, estudió bajo financiación de la CIA, como borrar la mente de personas, retrocediendo al nivel de un bebe para luego reprogramar la personalidad a medida; utilizando técnicas de choques eléctricos, coma inducido, privación sensorial y mensajes reiterativos, entre otros (Otterman, 2007). El programa OFTEN incluía pruebas de

componentes en animales y CHCKWIT buscaba nuevas drogas en Europa/Asia (Statement of director of CIA before Subcommittee on health and scientific research senate committee on human resources, 1977). El Project CHATTER del U.S. Navy también incluyó la utilización de drogas para interrogatorios. Entre 1961 y 1962, de forma operacional, el Army Special Purpose Team (SPT) utilizó el LCD en interrogatorios en Europa (Project Third Chance / Derby Hat) (Select Committee on Intelligence and Committee on Human Resources, 1977).

El concepto de modificación del comportamiento se remonta mucho antes de los experimentos de la CIA. El psicólogo Ivan Pavlov formuló en 1901 la ley de reflejo condicional al observar que los perros salivaban como un reflejo psicológico. El experimento consistía en emitir un sonido previo a cada comida. Una vez reforzada dicha asociación (estimulo / respuesta) mediante repetición, observó cómo los animales empezaban a salivar con tan solo escuchar el sonido (Schultz, Schultz; 2011). Pavlov es considerado el padre del condicionamiento clásico. El psicólogo Edward Thorndike estudió en 1898 como los gatos podían resolver una serie de cerraduras para escapar de una caja y recibir alimento a modo de recompensa. El aprendizaje en el tiempo les permitía escapar cada vez más rápido. Esto llevó a formular la ley del efecto. Las respuestas que se refuerzan y asocian a un estímulo tienen mayor probabilidad de ocurrencia en el futuro (Thorndike, 1898). Thorndike es considerado el padre del condicionamiento operante, método de aprendizaje donde una acción es seguida de un estímulo deseable o indeseable. John Watson (1913) continuó los estudios y fundó la escuela conductivista basada en la observación. El análisis de la conducta con relación a los estímulos y respuestas del ambiente. Posteriormente, B.F. Skinner experimentó con palomas y amplió los estudios en relación con la modificación de la conducta. Un experimento consistió en alimentar a una paloma cada vez que empieza a girar contra reloj, reforzando sucesivamente cada vez que hace un movimiento más pronunciando, para finalmente lograr que realice un giro completo; el refuerzo de pequeñas conductas termina condicionando una conducta compleja (Schultz, Schultz; 2011). Las técnicas son *reinforcement* (positivo y negativo), *punishment* (positive y negativo), *extinction*, *shaping*, *fading* y *chaining.* De forma resumida:

- *Positive reinforcement*: Inmediatamente después de realizar de la conducta esperada se refuerza con un estímulo deseable.

- Negative *reinforcement*: Inmediatamente después de realizar de la conducta esperada se elimina un estímulo indeseable.
- Positive *punishment*: Cada vez que se realiza una acción que se busca disminuir, se genera un estímulo desagradable.
- Negative *punishment*: Cada vez que se realiza una acción que se busca disminuir, se elimina un estímulo deseable.
- *Extintion*: Omisión del refuerzo al observar la conducta que se pretende que desaparezca.
- *Shaping*: Reforzar aproximaciones sucesivas para lograr una conducta meta más compleja (el ejemplo de la paloma con el giro completo).
- *Fading*: A medida que el individuo va aprendiendo se reducen las indicaciones.
- *Chaining*: El comportamiento a aprender se divide en una secuencia de pasos más pequeños. La enseñanza no avanza hasta no aprender el paso previo de la cadena.

Como indica Zuboff (2019)[111], la modificación del comportamiento se realiza a gran escala con la utilización de las TICs, incluyendo dispositivos utilizables (*wearables*) y las redes sociales. Internet se transformó en un gran laboratorio de experimentación. Un ejemplo citado es el estudio del contagio emocional en las redes sociales a partir de la alimentación de mensajes positivos o negativos. Otro es el caso del juego Pokemon Go, donde las recompensas surgen a partir del comportamiento deseable de los jugadores en el mundo real (*gamification* / *exploitationware*). Esto es, llevar los jugadores a ciertos lugares físicos para capturar/entrenar Pokemones; cuando en realidad están incrementando el consumo de productos en diferentes comercios de la zona. Otro ejemplo que hemos anticipado es el caso de cómo la empresa Cambridge Analityca que ha influenciado el comportamiento de los votantes. Afectando procesos electorales y dando una puñalada al corazón de la democracia.

Según un documental de la DW[112] "China La vigilancia absoluta" (2019), el sistema de créditos sociales de China es quizás uno de los usos más perversos en la modificación de las conductas individuales para formar la sociedad a la medida del poder. El sistema se sustenta

[111] Una visión escueta y parcial del amplio trabajo de Zuboff.
[112] Deutsche Welle.

en una red de vigilancia de cámaras con reconocimiento facial. El crédito social sirve para clasificar a los ciudadanos en función de su comportamiento. Los comportamientos no deseables son castigados, mientras que los deseables son reforzados con recompensas. Algunos comportamientos para recibir castigos son: conducir mal, fumar en zonas para no fumadores, pagar tarde los impuestos, comprar demasiados videojuegos, publicar noticias falsas en línea, no tener pareja ni hijos, entre otros. Los castigos incluyen restricción a la compra de ticket (tren, vuelos), privar a los hijos el acceso a ciertas escuelas, prohibición para trabajar en el estado o bancos, prohibición de vacaciones y hoteles para los que rechazan el servicio militar, publicación en listas negras para que no puedan ser contratados por empresas, entre otros. El sistema es también utilizado para perseguir periodistas que revelan actos de corrupción u opinan diferente al gobierno; como para marcar las etnias minoritarias islámicas. El sistema está orientado a formar y adoctrinar a que las personas no tengan libertad de acción o elecciones genuina y actúen como estipula el poder (DW, 2019).

Como indicamos, la guerra psicológica es un elemento más de la guerra híbrida y el fin último es la dominación a partir del ejercicio del poder mediante diferentes medios. La modificación del comportamiento es una potente arma psicológica independiente del medio y cumple una función del ejercicio del poder en el marco de la dominación de la población.

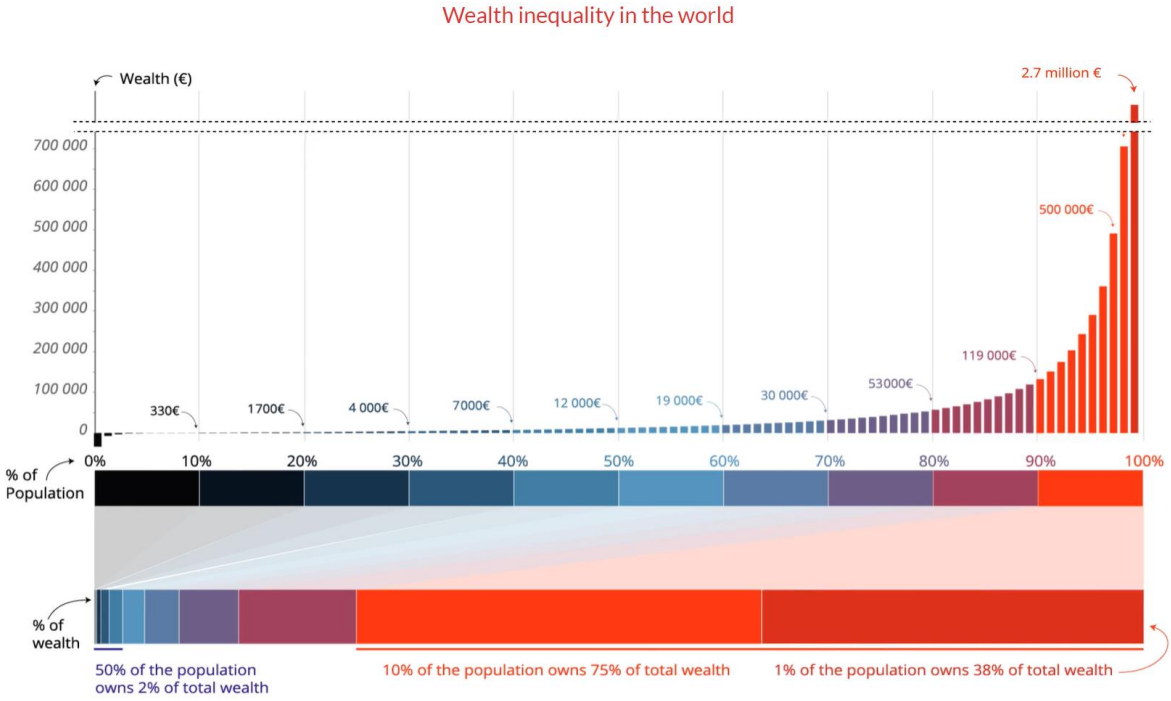
Ejercer poder mediante la modificación del comportamiento también está presente en micro aspectos de la sociedad. Las personas al nacer en la sociedad encuentran un mundo que ha sido dividido con reglas impuestas por sus dueños. Dicha división fue históricamente realizada mediante el uso de la fuerza, la violencia y el derramamiento de sangre. Enmarcando de dicha forma un nuevo estándar base que debe ser aceptado y respetado. A partir de ello, se impone un contrato social que no puede ser rechazado (inclusive teniendo minoría de edad). La persona recibe la ley bajo un brazo y la biblia bajo el otro. El comportamiento es amoldado a respetar las reglas impuestas (castigo o refuerzo). Enseñan a seguir órdenes y cumplir horarios en institutos educativos (reforzado mediante calificaciones / perdida de vacaciones). Cualquier desvío de adultos implica enfrentar al monopolio del uso "legitimo" de la violencia (ley, encarcelamiento o incluso la muerte). La estructura de la sociedad se sustenta en la modificación del comportamiento desde niños. El concepto de identidad, nación y patria son estructuras psicológicas de poder. El poder cuenta con ello y se sustenta en su estructura piramidal donde una minoría ostenta la riqueza de todo el planeta

mientras que el resto queda sumido en la pobreza (ver figura 39). El poder teme que la mayoría sea consiente de ostentar el verdadero poder y revierta el contrato impuesto, dejando caer las estructuras de poder como castillos de naipes. Todos los sistemas son defectuosos, trituradores de sueños para la realización de unos pocos. ¿Cómo han logrado eso? ¿Por qué está sobrevalorado el capital, cuando son los trabajadores quieres materializan las ideas y producen la riqueza? el poder avanza paso a paso sobre los derechos y naturaliza nuevos estándares a los nadie cuestiona ni racionaliza. Originalmente mediante la violencia, posteriormente con técnicas como dividir, confundir, cambiar el foco y mantener ocupada a la población (arduo trabajo durante la semana / pan y circo los días libres). La guerra psicológica cumple un rol fundamental para el ejercicio del poder. El mismo avanza en su sed de codicia hasta encontrar puntos de fricción y resistencia. Los modelos totalitarios / distópicos continúan avanzando mediante el ejercicio de la violencia, mientras que los modelos más benignos permiten ciertos márgenes para fomentar la falsa sensación de libertad, ya que termina siendo funcional al sistema (mayor productividad, menos desacato / cuestionamientos). La explotación más eficiente es la voluntaria, que apunta al objetivo del rendimiento. Como reflexiona Byung Chul Han (2014), el poder se vuelve inteligente frente al sujeto transparente. Anular la libertad es signo de debilidad del poder; por ello recurre a valerse de la libertar para dominar (fase positiva del poder). El dominado es más eficiente cuando no se siente dominado. El poder busca seducir y motivar. Así actúa el poder neoliberal. El poder no opera con coerción externa sino desde adentro, haciendo que libertad y sometimiento coincidan. Las personas se transforman en sus propios verdugos (Han, 2005). “Un déspota imbécil puede obligar a unos esclavos con unas cadenas de hierro; pero un verdadero político ata mucho más fuertemente por la cadena de sus propias ideas” (Servan, como fue citado por Foucalt, 1989). Según Michael Foucault, la *biopolítica* es la forma de ejercer poder sobre las personas, la administración de los cuerpos para que sean productivos y no para castigarlos (dócil es útil). Para alcanzar la mente y no solo el cuerpo, hay que recurrir a la información y a la TICs, como la IA.

El ejercicio del poder en una sociedad no es diferente al ejercicio del poder entre naciones. Inclusive pueden alimentarse mutuamente mientas que los intereses de los actores concuerden. Ello auspicia la creación de actores insiders en la sociedad que operan para los intereses de estados extranjeros.

Figura 39

Distribución de la riqueza en el mundo.



Nota. Fuente Chancel, Piketty, Saez y Zucman, World Inequality Report 2022.

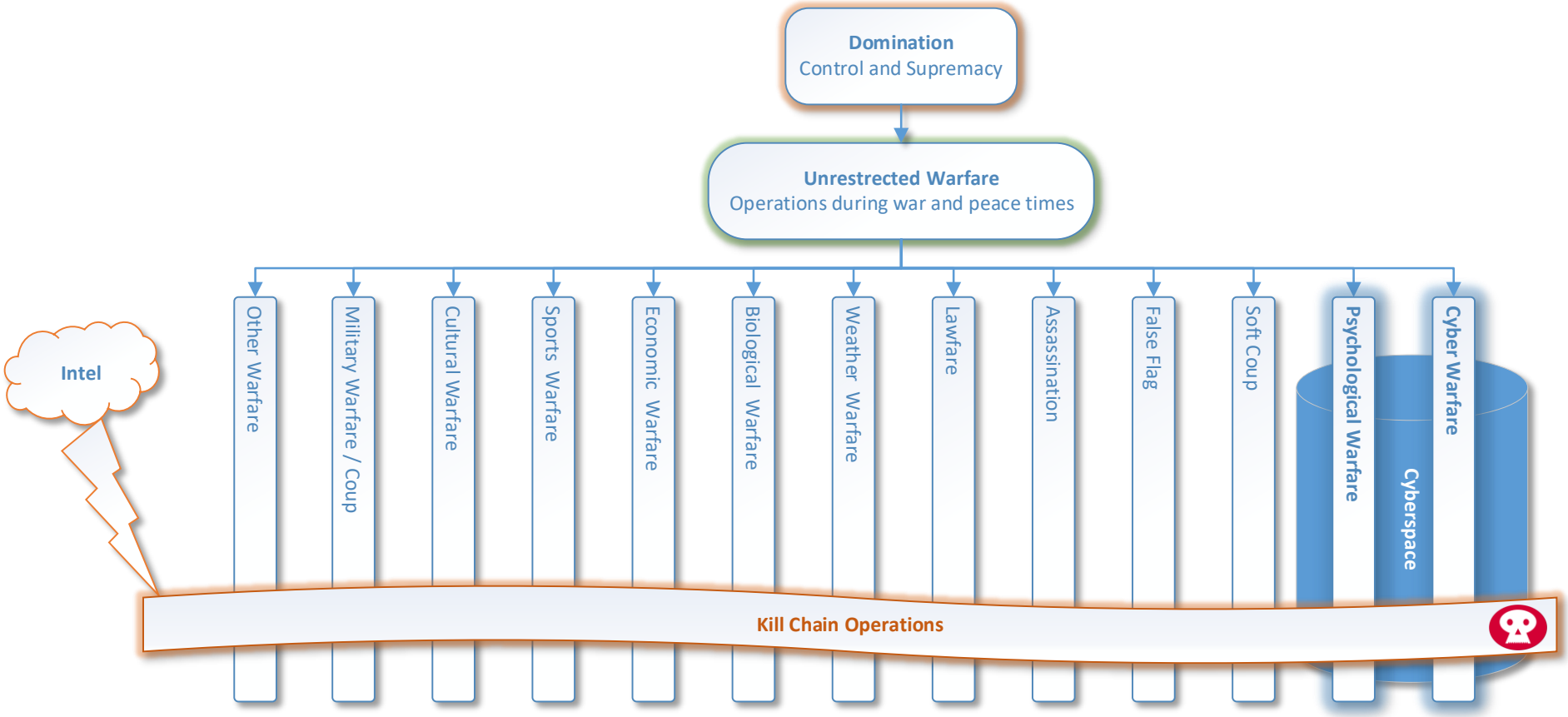
Para finalizar, la tecnología ha incrementado la desigualdad en la sociedad y sus capacidades han potenciado todos los elementos de la guerra híbrida, en particular, la guerra psicológica. En el capítulo exploramos la guerra sin límites más allá de sus definiciones conocidas y su relación con las TICs. Dicha exploración no buscó focalizar, sino más bien expandir el conocimiento en dicha materia. Particularmente en el último tramo, hemos intentado desentrañar y describir desde diferentes ópticas. Así mismo, queda planteada la vinculación con la información y el poder. Aclarando que la información no es el fin, solo el medio para el ejercicio del poder.

Diagrama de Dominación y operaciones Kill Chain (Domination – Kill Chain Operations diagram).

Mantener a las personas inteligentes ocupadas con tecnologías cambiantes e irrelevantes, en vez de enfocarse en los verdaderos problemas de la humanidad (reflexión de elaboración propia)

A lo largo del capítulo hemos expuesto diferentes elementos de guerra irrestricta, en particular atención a la guerra psicológica y la ciberguerra; con sustentación en las capacidades del ciberespacio. La información obtenida a partir de inteligencia alimenta operaciones en un esquema *kill chain*. Tales operaciones son transversales a las diferentes formas de la guerra irrestricta. Dicha guerra busca alcanzar, como fin último; el control y la dominación de las sociedades. A modo ilustrativo se propone un diagrama conceptual (ver figura 40).

Figura 40
Domination – Kill Chain Operations Diagram.



Nota. (Fuente: elaboración propia basada en conceptos tratados).

Marco de dominación (Domination Framework).

Una vez los hombres entregaron su pensamiento a las máquinas con la esperanza de que esto los liberaría. Pero eso solo permitió que otros hombres los esclavizaran.
(Frank Herbert, 'Dune', 1965).

Estamos próximos a alcanzar el fin del juego, pero todo dependerá de las decisiones de las personas respecto a la tecnología (reflexión de elaboración propia).

En la antigüedad, las invasiones consistían en el sometimiento mediante el uso de armas de fuego contra lanzas, junto al saqueando oro y riquezas. Luego, los medios cambiaron a la utilización de gobiernos títeres y el abuso del sistema deuda como arma. Podríamos afirmar que en la actualidad la invasión mutó a una forma de colonialismo tecnológico (ver figura 41); con la imposición de tecnologías y la dominación total de las comunicaciones en la búsqueda de datos. Sin embargo, la imposición no es mediante el uso de la fuerza sino más bien con medios cognitivos y mediante formas amables.

Antiguamente se creía que no iba a ser posible marcar a las personas o colocar rastreadores y micrófonos para su control. En la actualidad, los medios psicológicos no solo han logrado eso, sino que también han superado las expectativas; al hacer que el costo de la esclavitud sea pagado por sus víctimas. Por demás, los Smartphone han transformado a los ciudadanos una vasta red de zombies espías que al mismo tiempo son víctimas del espionaje y verdugos de su propio futuro.

Hoy en día, la dominación llega a las mentes de las personas. Justamente es el ciberespacio donde las fronteras desaparecen. La dominación penetra y opera desde adentro; directamente sobre la mente de los individuos de otras naciones. Explotando las vulnerabilidades tanto de la democracia como las propias del ser humano.

Se propone como aporte el presente framework de Dominación[113] para futuras investigaciones en la materia (ver figura 42):

[113] El mismo corresponde a una elaboración propia. Surge de pensar lo expuesto en el presente capítulo mediante un diagrama temporal a lo largo de la historia; en vez de un diagrama por clasificación.

- Colonización 1.0 - *Military slavement*: Opera sobre el plano terrenal mediante el control y la coerción física. Es uso convencional de la fuerza (*Military Warfare*).
- Colonización 2.0 – *Pupet slavement*: Opera en mismo plano pero diferente método. Control a través de un líder que opera fuera de los intereses del pueblo.
- Colonización 3.0 - *Economic slavement*: Opera en el plano económico y del endeudamiento. Control mediante definición de políticas y expropiación de riquezas (pérdida de soberanía).
- Colonización 4.0 – *Cyber slavement*: Implantación de plataformas y tecnologías. Control mediante el uso y explotación de la información de forma estratégica (*a step forward*). Comienza la supremacía por la información.
- Colonización 5.0 – *Total Domination*: Explotación eficiente y automática de los datos mediante técnicas de IA. Control psicológico micro segmentado y masivo de la población. Moldeamiento de las conductas individuales (crear sociedades a medida). Sus modelos se sustentan en la supremacía de la información.

Respecto a los actores: La dominación se efectúa a diferentes niveles (corporativo, social en el ámbito local o internacional entre estados). Los actores por lo tanto difieren para cada situación. A pesar de ello, en cada caso abusan de su posición dominante. En el caso de los estados podemos pensar en el ámbito de la política, militar, religión, corporación o financiero. En donde sus intereses pueden estar alineados o ser divergentes generando conflictos de intereses.

Figura 41

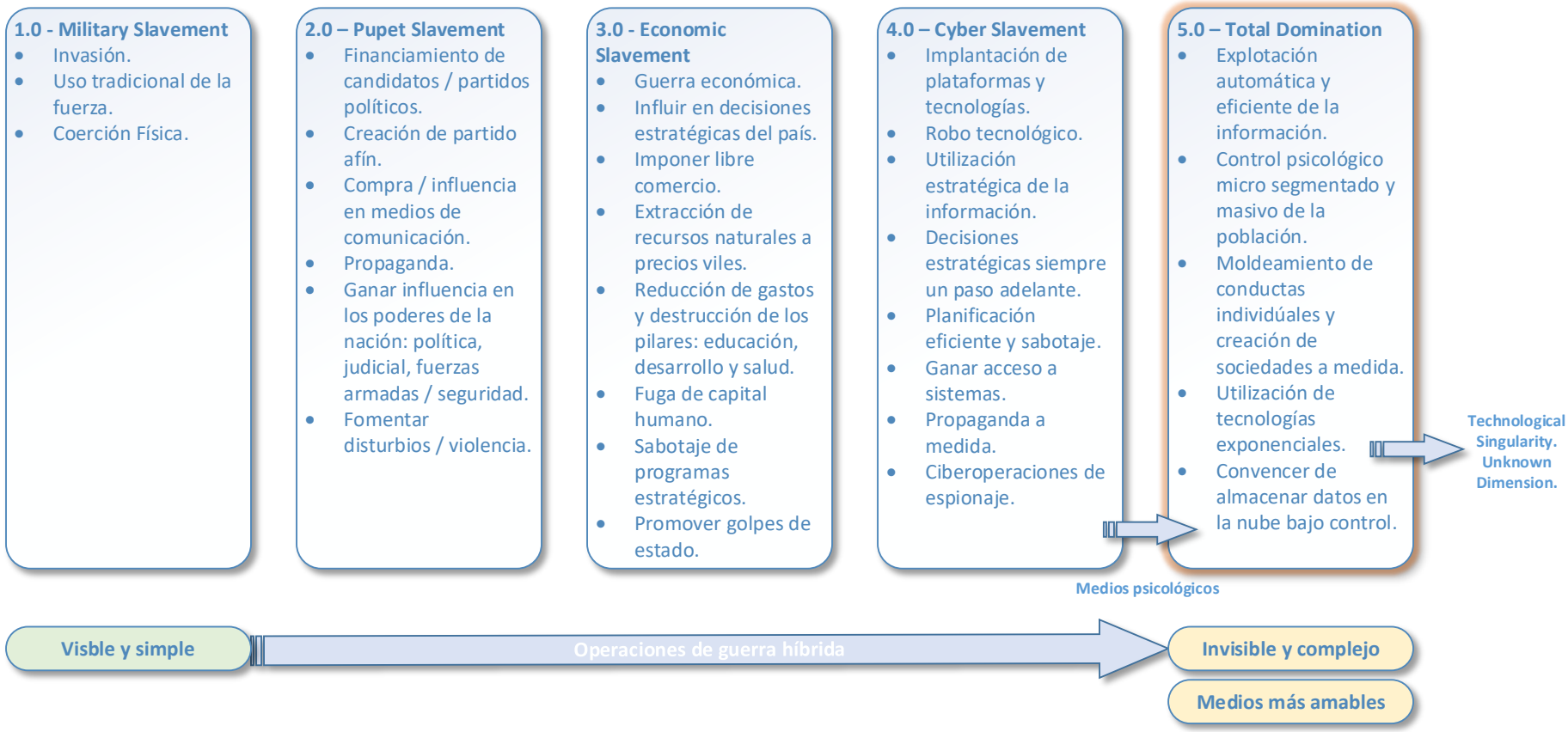
"Segundo Homenaje a Colón" - Colonialismo tecnológico.



Nota. Edición propia basada del óleo "Primer Homenaje a Colón" de José Garmelo (1892)[114].

[114] Presente en el Museo Naval de Madrid.

Figura 42
Domination framework.



Nota. (Fuente: elaboración propia basada en conceptos tratados).

Algunos conceptos claves del capítulo.

A continuación, repasaremos brevemente algunos conceptos relevantes del presente capitulo:

- La guerra irrestricta es la guerra empleando todos los medios disponibles, es la guerra continua en tiempos de paz (por debajo de los límites tolerables), como también en tiempos bélicos. Algunos elementos son la guerra: económica, judicial, cultural, biológica, química, asesinatos, ataques falsa bandera, golpes de estado, ciberguerra y la guerra cognitiva.
- La información no es el fin, solo el medio para el ejercicio del poder.
- *Kill chain* es un proceso conceptual de ataque de 3 etapas: entender la situación (inteligencia), decidir qué hacer (planificar) y realizar la acción (ataque). *Closing the kill* implica completar las fases mientras que *breaking the kill* implica frustrarlo. Las TIC potencian la velocidad y precisión del proceso. El proceso puede ser entendido para operaciones estratégicas y tácticas dentro del ámbito de la guerra irrestricta.
- El proceso fue ampliado al ciberespacio como *Cyberkill Chain* e incluye, entre otros, *weponization* y explotación de una vulnerabilidad. *Cyberkill Chain* conceptualmente mantiene sus principios originales.
- La adquisición de la información es una etapa necesaria y fundamental para llevar a cabo un ataque. La inteligencia previa podría considerarse en si un acto ofensivo, aunque también puede ser utilizada con fines defensivos.
- La definición de ciberguerra no está consensuada, aunque muchos actores convergen a que se trata de ataques a sistemas de información auspiciados por estados.
- El ciberespacio tiene sus propias características y actores, desde individuos solitarios hasta los temidos APT. Mitre Attack es un framework que permite comprender las acciones ofensivas en el ciberespacio por actores avanzados (persistencia, movimientos laterales, escalamiento de privilegios, técnicas de evasión de detección, etc.).

- La guerra cognitiva implica varios elementos explorados: propaganda, producción cultural, asesinato de personajes y la modificación del comportamiento. Las TICS han amplificado el poder de la guerra de las mentes en precisión y capacidad. La mente de las personas es el nuevo plano de batalla.
- Argentina podría tener un derecho en relación con las deudas ilegitimas contraídas en gobiernos defectos (apoyados) o democráticos, pero influenciados bajo un esquema de guerra híbrida.
- El poder explota vulnerabilidades de la democracia y de las sociedades humanas. La sociedad puede recurrir a las TICs para organizar manifestaciones genuinas. Pero a su vez, los atacantes explotan las vulnerabilidades de redes sociales para influir a los ciudadanos. Para los estados también resulta funcional poder desarticular una manifestación genuina alegando una injerencia extranjera. Cada vez resulta más confusa la diferenciación de los casos, dado que indefectiblemente son polos atrayentes.
- La dominación es ejercida por el poder en diferentes ámbitos, incluyendo la supremacía por la información a través del colonialismo tecnológico. A su vez, el poder recurre a las operaciones de guerra sin límites basado en inteligencia previa. Los medios han pasado de operaciones visibles y violentas; a medios invisibles y más amables. La guerra por las mentes y la modificación del comportamiento son la última frontera.

Capítulo (~~2~~) Hades – Inteligencia y vigilancia masiva.

Si decides jugar mi juego, yo impondré las reglas. De lo contrario, te convenceré para que decidas jugarlo (reflexión de elaboración propia).

En el presente capitulo se amplían los aspectos de obtención de información a partir de la inteligencia y la vigilancia masiva. La inteligencia es un elemento fundamental para las operaciones ofensivas de todo tipo. Por lo tanto, pueden entenderse en sí mismo como un ataque ofensivo. Por otra parte, debemos indicar que la inteligencia es a su vez, un medio para contrarrestar operaciones enemigas (contrainteligencia). Sin embargo, la guerra sin límites busca explotar la información para potenciar sus capacidades ofensivas.

El capítulo también menciona mecanismos para contrarrestar la inteligencia enemiga: evitar, cifrar y/o desinformar. Los mismos no son perfectos y tienen sus limitantes para tener en cuenta.

Cabe aclarar que en este capítulo no desarrollaremos las técnicas básicas de reconocimiento, escaneo y enumeración típicas de un ciberataque que podrá encontrar en bibliografía sobre *ethical hacker*[115].

Medios para la adquisición de inteligencia (Inteligence gathering).

A lo largo del capítulo veremos diferentes medios de recolección de información. En términos generales, *passive collection* corresponde a la escucha de las comunicaciones en el aire, cables (ver figura 43), *hub* (centros concentradores como empresas proveedoras), etc. Mientas que *active collection* implica acciones de hacking, utilización de *malware*, implantes, espías o informantes infiltrados (ver figura 44), entre otros.

[115] Como adelantamos en el capítulo anterior, el reconocimiento utiliza técnicas para descubrimiento de los sistemas, servicios disponibles, puertos abiertos, potenciales vulnerabilidades, etc. Información que luego alimentara las fases posteriores de un ciber ataque.

Figura 43

British campaign Anti-rumour and careless talk (WWII)



Nota. Fuente The National Archives (Reino Unido).

Figura 44

Careless talk (WWII)



Nota. Fuente U.S. National Archives and Records Administration (USA).

En cuanto al alcance, puede ser masivo o dirigido a objetivos específicos (incluyendo contactos de hasta 3 saltos). Los objetivos pueden ser desde simples personas[116] hasta las más diversas: organizaciones, proyectos, instalaciones estratégicas, edificios, agencias de inteligencia, geografía, entre otros.

La información recolectada usualmente proviene de sistemas de comunicaciones y sistemas informáticos por excelencia, pero no son los únicos. La recolección de información puede provenir desde otros medios como el seguimiento de personas, patrones de comportamiento, movimientos de tropas, SIGINT, ELINT, COMINT, OSINT, HUMINT, RUMINT[117] y otras.

Inteligencia humana (HUMINT).

Human Intelligence. Recolección de información de fuentes humanas con el fin de responder a requerimientos de información de inteligencia, ya sea de forma cooperativa, con espías o de manera forzada. A modo referencia, según el manual FM 2-22.3 el proceso consiste en 5 fases: *planning and preparation*, *approach*, *questioning*, *termination* y *reporting.* Las actividades incluyen las siguientes categorías: *tactical questioning* (primeras preguntas con valor táctico), *screening* (identificar y evaluar las áreas de conocimiento, nivel de cooperación y posibles técnicas de acercamiento a un individuo), *interrogation* (mediante técnicas de preguntas directas e indirectas), *debriefing* (cuestionar fuentes humanas colaborativas como refugiados o fuerzas aliadas), *liaison* (intercambiar información con el país anfitrión, agencias militares, civiles y ONG), *human source contact operations* (fuentes humanas que han acordado reunirse), *document exploitation-DOCEX* (recopilar información de documentos de fuentes abiertas / cerradas / publicadas, tanto físicos o digitales, incluyendo dispositivos) y *captured enemy equipment (CEE) Operations* (Department of the Army, 2006).

[116] Pueden ser personas importantes/influyentes como políticos, líderes, periodistas, activistas, terroristas, empresarios, jueces, peritos, militares, hackers, etc; como también simples personas si así es requerido por los intereses. Nadie esta excepto.

[117] SIGINT (Signal Intelligence) - inteligencia de señales, ELINT (Electronic Intelligence) - inteligencia de señales electrónicas, COMINT (Communications Intelligence) - inteligencia de comunicaciones, OSINT (Open Source Intelligence) – inteligencia de fuentes abiertas, HUMINT (Human Intelligence) – inteligencia de fuentes humanas y RUMINT (Rumour Intelligente) – Inteligencia basado en rumores.

En el caso de operaciones clandestinas, los *Black Sites* son centros clandestinos de detención utilizados por la CIA. *Extraordinary rendition* es cuando se realiza un secuestro forzado (generalmente con la utilización de agentes incapacitantes) por fuera de la ley. La víctima es enviada a un tercer país para su tortura (tortura proxy) (The Guardian, 2011; Ganser, 2007). Es una técnica utilizada por la CIA y el MI6. Según el agente de la CIA Bob Baer: "Si quiere una interrogación seria, envía el prisionero a Jordania; si quiere que sea torturado lo envía a Siria; y si usted quiere que desaparezca y no volverlo a ver, lo envía a Egipto" (The Guardian, 2011). Usualmente utilizado para sospechosos de terrorismos. Sin embargo, han existido desaciertos. Tal es el caso del alemán Khaled Masri que fue secuestrado por equivocación, trasladado clandestinamente a Afganistán; interrogado, golpeado, desnudado, sodomizado y torturado (European Court of Human Rights, 2012). Se estiman 3000 detenidos secuestrados entre 2001 y 2005 (Priest, 2005). Los casos de tortura fueron investigados por el Comité Selecto del Senado sobre Inteligencia quien publicó parcialmente un informe ejecutivo de 525 páginas en 2014 (el informe completo de 6000 páginas es clasificado). La conclusión resuelve que la tortura fue brutal y más dura de lo que la CIA mostraba. Las victimas que se negaban a comer o tomar eran forzados vía oral[118] o rectal. Algunos tenían signos de violación. Hubo asesinato de una víctima por hipotermia. Eran torturados psicológicamente con simulacros de ejecución o con armas de fuego. Ahogados con la técnica *Waterboarding*, privados del sueño y de sus sentidos. A una víctima le quitaron el ojo y a otro lo colocaron en un ataúd durante 11 días, entre otros métodos (Bradner, 2014; Matthews, 2014; Senate Intelligence Committee's, 2014).

La CIA otorgó información inexacta al departamento de justicia respecto a la investigación. El comité tuvo inconvenientes durante la investigación dado que la CIA (Robert Eatinger) solicitó al FBI realizar una investigación criminal sobre los miembros del comité a modo intimidatorio. Asimismo, la CIA hackeo la red informática del comité para ver cómo habían obtenido información (Mazzetti y Weisman, 2014). El senado no levantó cargos por el hackeo. La conclusión fue que la tortura no ayudo a obtener información fiable y que solo deterioró la imagen de Estados Unidos.

[118] La técnica que recuerda a la utilizada en la prisión de Guantánamo contra las huelgas de hambre. Alimentación forzada con sonda a través de la nariz (Fisher, 2013; Joint Task Force Guantánamo 2003).

Por otro lado, la actividad de HUMINT también presenta sus riesgos. En 2009, siete agentes de la CIA murieron cuando un informante se inmoló con explosivos en Khost, Afganistán (Lowenthal y Clark, 2015).

Como ejemplo puntual de HUMINT, podemos mencionar a Victor Belenko. Quien desertó de la URSS en 1976 piloteando un MiG-25/Foxbat fighter que aterrizó en Japón. Donde EE.UU. desmanteló el avión para obtener información sobre su tecnología. Belenko proporcionó a EE.UU. información valiosa sobre los sistemas de armas de los aviones soviéticos, las tácticas y la doctrina de la Fuerza Aérea Soviética (Lowenthal y Clark, 2015).

Inteligencia de fuentes abiertas (OSINT).

La información confiere poder. Quien sea mejor obteniendo y explotando información relevante, tiende a ganar (Lowenthal y Clark, 2015).

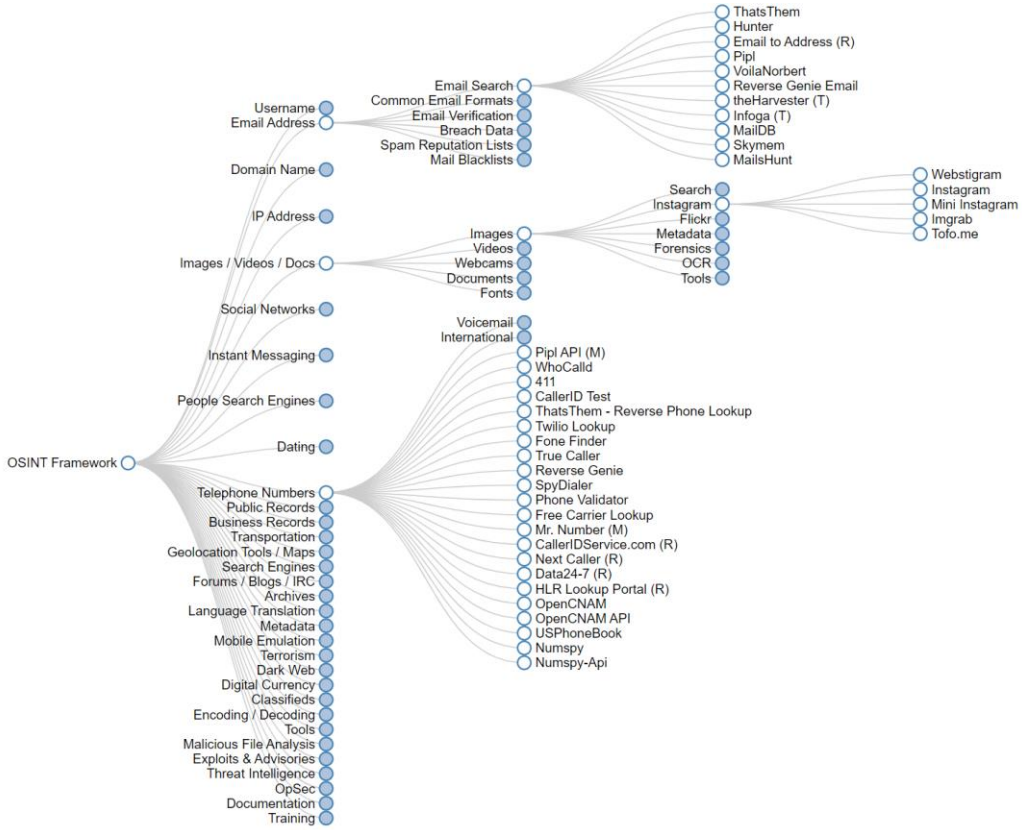
Open-source intelligence. Es una técnica popular en las fuerzas de seguridad. Consiste en inteligencia producida a partir de información disponible públicamente que se recopila, explota y difunde de manera oportuna a una audiencia adecuada con el fin de abordar un requisito de inteligencia específico (DoD[119], 2006). El proceso puede realizarse de forma manual o con herramientas automáticas (Maltego, Harvester, Recon-ng, etc). Utiliza técnicas de *web scraping*, bases de datos, registros gubernamentales, aprovechamiento de API en redes sociales / registros de datos, fuentes publicadas (*leak* en la *Deep web*), *Google Dorks*, entre otros. También puede utilizar la extracción de metadatos / geolocalización en archivos publicados. El Framework de OSINT es una fuente útil de consulta (ver figura 45). Como cuenta (Lowenthal y Clark, 2015); el análisis de las redes sociales; busca representar, medir y comprender la estructura evidente en un grupo de individuos conectados por una o más interacciones o relaciones. Identificando la estructura de la red y cómo opera; a su vez, predecir futuras interacciones.

Cada dato obtenido es un nuevo elemento utilizado para retroalimentar el proceso de investigación. La información puede graficarse en árboles / grafos. El conocimiento obtenido del objetivo puede ser utilizado para revelar contactos (futuras búsquedas laterales / infiltrar),

[119] https://www.govinfo.gov/content/pkg/PLAW-109publ163/html/PLAW-109publ163.htm

tatuajes, gustos / preferencias (infiltrar agentes u obtener posibles contraseñas), lugares habituales (futuras operaciones de seguimiento[120] o *lock and kill*), revelar vulnerabilidades (ciberataques / cibercrimen). Usos más benévolos pueden ser el esclarecimiento de un crimen, desarticular el crimen organizado o contrainteligencia.

Figura 45
OSINT Framework



Nota. Desplegando el dato de búsqueda indica las posibles herramientas (Fuente imagen: https://osintframework.com/).

Como ejemplo en el ámbito de inteligencia podemos mencionar el Directorate of Digital Innovation/Open Source Enterprise (absorbió al Director of National Intelligence/Open Source Center, previamente Foreign Broadcast Information Service) que recolectaba información de "Internet, bases de datos, prensa, radio, televisión, video, datos geoespaciales, fotografías e imágenes comerciales". Según CIA's Deputy Director David Cohen (como fue citado por Cooney, 2015): "Será el centro de los esfuerzos de la Agencia

[120] En la jerga local: "Caminando". Además del seguimiento para saber su destino y con quien interactuar, implica capturas fotográficas, aproximarse para escuchar, sentarse de espalda en un bar, etc.

para inyectar soluciones digitales en cada aspecto de nuestro trabajo. Será responsable de acelerar la integración de nuestras capacidades digitales y cibernéticas en todas nuestras áreas de misión: recopilación de inteligencia humana, análisis de todas las fuentes, inteligencia de fuente abierta y acción encubierta."

Por citar otros ejemplos: en el caso de Reino Unido, las actividades OSINT son guiadas por el *U.K. Joint Intelligence Committee* bajo la órbita del *Deputy Chief of Defence Intelligence* del Ministerio de Defensa. En el caso de Israel, depende de la unidad *Hatzav* perteneciente a la unidad 8200. Rusia sustenta sus actividades OSINT en el *Russian Foreign Intelligence Service* (SVR) (Lowenthal y Clark, 2015).

Como cuenta (Lowenthal y Clark, 2015); los datos recolectados en bruto (*raw*) por las diferentes fuentes de inteligencia, deben atravesar un proceso denominado TPED o TCPED (asignación de tarea, recolección, procesamiento, explotación y difusión[121]) a fin de que puedan tener un valor para los analistas y responsables políticos. Todas las agencias de EE.UU., explotan OSINT. En relación con las otras fuentes de inteligencia, OSINT suele ser la menos confiable. Es por ello que el Department of Homeland Security creo el siguiente criterio de evaluación (ver tabla 3, 4 y 5):

[121] DNI-U es la red interna que comparte información dentro de las agencias. Aunque también existe la International Open Source Working Group (IOSWG) que intercambia información entre diferentes países miembros.

Tabla 3
Intelligence Evaluation Criteria.

Evaluación de la información	Descripción
Confirmada.	Confirmado por otras fuentes respetables; lógica; consistente con otra información referida al tema.
Probablemente verdadera.	No confirmada; lógica; consistente con otra información referida al tema.
Posiblemente verdadera.	No confirmada; razonable; concuerda con otra información referida al tema.
Dudosamente cierta.	No confirmada; posiblemente verdadera pero no lógica; concuerda con otra información referida al tema.
Improbable.	No confirmada; no lógica; contradictoria con otra información referida al tema.
No puede ser juzgada.	No existe una base para evaluar la validez de la información.

Nota. Department of Homeland Security (Lowenthal y Clark, 2015).

Tabla 4
Intelligence Evaluation Criteria.

Evaluación de la fuente en credibilidad.	Descripción
Confiable.	Sin dudas de la autenticidad, confiabilidad y competencia; tiene una historia de completa credibilidad.
Usualmente confiable.	Dudas menores de la autenticidad, confiabilidad o competencia; la mayoría de las veces provee información valida.
Bastante confiable.	Dudas de la autenticidad, confiabilidad o competencia; ha brindado información valida en el pasado.
Usualmente no confiable	Dudas significativas de la autenticidad, confiabilidad, competencia; ha brindado información valida en el pasado.
No confiable.	Falta de autenticidad, confiabilidad, competencia; históricamente ha brindado información invalida.
No puede ser juzgada.	No existe una base para evaluar la validez de la información.

Nota. Department of Homeland Security (Lowenthal y Clark, 2015).

Tabla 5
Intelligence Evaluation Criteria.

Evaluación de la fuente en frecuencia.	Descripción
Proveedor constante.	El propósito principal de la fuente es proporcionar información sobre el objetivo o el tema.
Proveedor frecuente.	La fuente habitualmente provee información sobre el objetivo o el tema.
Proveedor limitado.	Ocasionalmente proveed información sobre el objetivo, tema o vinculantes.
Proveedor nuevo o desconocido.	Primera vez que provee información sobre el objetivo o asunto.

Nota. Department of Homeland Security (Lowenthal y Clark, 2015).

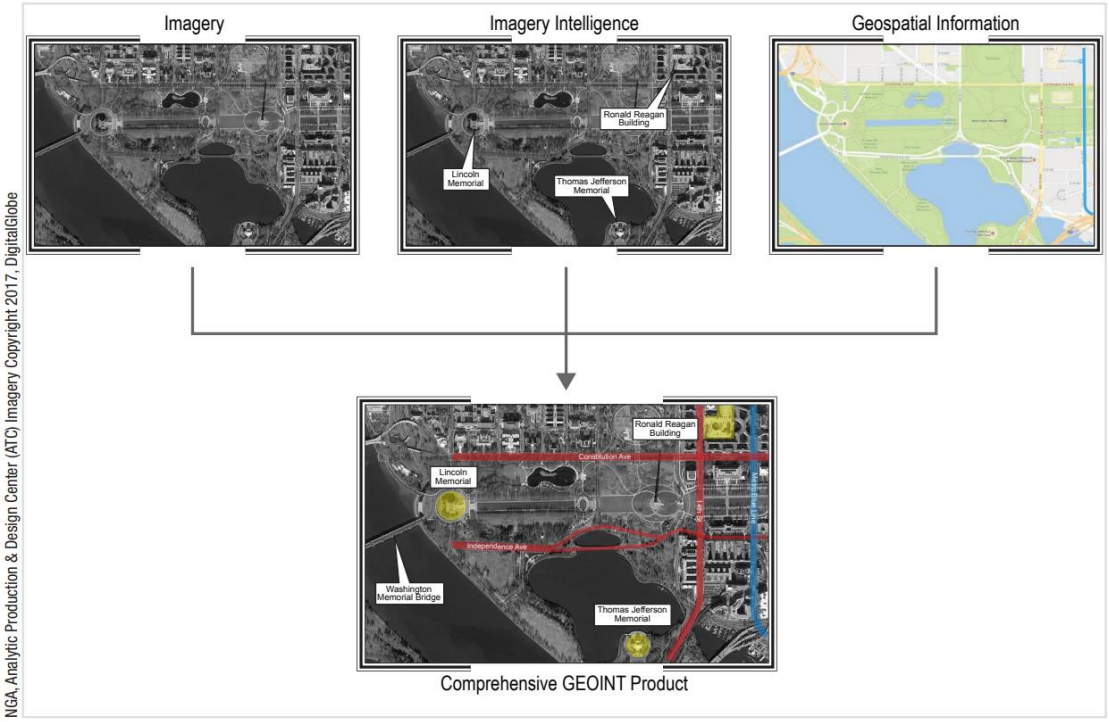
Finalmente, (Lowenthal y Clark, 2015) remarcan que el Intelligence Community Open Source Program (COSPO) estableció el Internacional Open Source Working Group (OISWG) a mediados de los 90 como un framework colaborativo de OSINT para el intercambio de información entre sus miembros: Australia, Canadá, Dinamarca, Francia, Alemania, Reino Unido, Israel, Italia, Países Bajos, Noruega, Suecia y EE.UU.

Inteligencia geoespacial (GEOINT).

Eyes in the sky…

Geospatial intelligence: "significa la explotación y el análisis de imágenes [IMINT] e información geoespacial para describir, evaluar y representar visualmente características físicas y actividades geográficamente referenciadas en la tierra. La inteligencia geoespacial consiste en imágenes, inteligencia de imágenes e información geoespacial" (Title 10 of the U.S. Code, Section 467 como fue citado por el National System For Geospatial Intelligence, 2018). El sistema desarrollado facilita el análisis, difusión e incorporación de videos y presentaciones producidas por plataformas terrestres, incluidas fotografías de mano o clandestinas (HUMINT) o disponibles como información de fuente abierta (OSINT). (Ver figura 46).

Figura 46
GEOINT



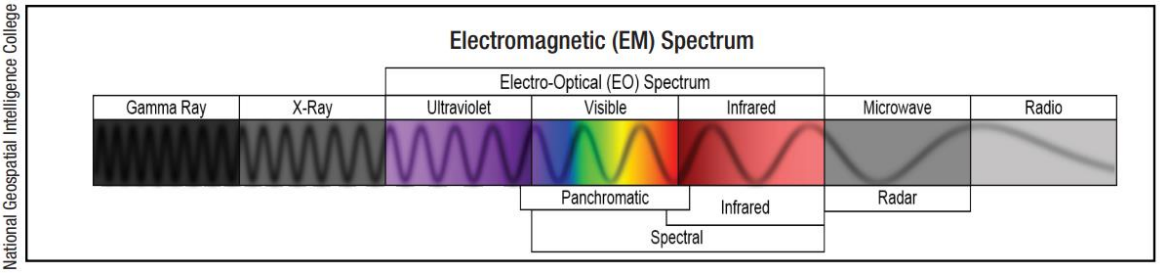
Nota. La imagen satelital es analizada y complementada con las características del terreno.

La información se obtiene desde satélites (militares o comerciales), vehículos aéreos (tripulados o no), plataformas terrestres o marítimas. Los sensores utilizados para recolectar

información tienen un rango específico dentro del espectro electromagnético y obtienen diferentes representaciones de un objetivo (Ver figura 47).

Figura 47

Espectro electromagnético.



Nota. Fuente: National System for Geospatial Intelligence.

Según la doctrina GEOINT, los sensores EO-Electroópticos (captan la energía emitida por el objeto) incluyen: PAN-Panchromatic imaging (detalles y sombras), IR-Infrared (calor emitido/seres vivos). TIR-Thermal Infrared (temperatura), MSI-Multispectral Imaging (características del terreno basado en el color del rango de frecuencia), HSI- Hyperspectral Imaging (detección de materiales), LIDAR-Light Detection And Raging (mediciones de distancia basado en un láser emitido). La combinación de los sensores descriptos crea lo que se conoce como Overhead Persistant Infrared (OPIR), (National System For Geospatial Intelligence, 2018)

Los sensores en el rango electromagnético del radar pueden utilizarse de día/noche y son indiferentes respecto al clima. Sin embargo, no genera una foto precisa, sino más bien, reflejan las características del objetivo. El radar emite energía y crea una imagen de las características del objeto basado en la respuesta a dicha energía sobre el objetivo iluminado: SAR-Synthetic Aperture Radar (utiliza pulsos microondas), IFSAR-Inferomatic SAR (observa al objetivo desde dos orígenes, dando lugar a datos de elevación del terreno), (National System For Geospatial Intelligence, 2018).

Tanto las características del radar como las Electroópticas permiten el seguimiento de objetivos móviles (Motion GEOINT): FMV-Full motion video (video a partir de varias imágenes), MTI-Moving Target Indication (dirección/velocidad de objetos en movimiento) y WAMI-Wide Area Motion Imagery (Mantiene vigilancia persistente sobre objetivo), (National System For Geospatial Intelligence, 2018).

Inteligencia de firma electrónica (MASINT).

Corresponde a la firma características distintivas de un objetivo que facilitan la medida e identificación (como ser la firma del radar o el sonido característico). Como explica Sislin (2019), consiste en medir las características de un objetivo (radiación, vibración, etc.) para luego compararlas contra una biblioteca de características conocidas; permitiendo su descripción e identificación. Los sensores típicamente utilizados son radar, geofísicos, muestreo de material, radiación nuclear, electroóptica y radiofrecuencias. Como indica:

> Inteligencia derivada técnicamente (excluida la inteligencia de señales y la inteligencia de imágenes tradicionales) que, cuando se recopila, procesa y analiza, da como resultado una inteligencia que ubica, rastrea, identifica o describe las firmas (características distintivas) de fuentes objetivo-fijas o dinámicas. Incluye el procesamiento avanzado de datos y la explotación de datos de sistemas de recopilación de imágenes aéreas. MASINT se puede adquirir desde una variedad de plataformas satelitales, aerotransportadas o aéreas; vehículos piloteados a distancia; o desde sitios de recolección móviles o fijos en tierra. Sus sensores incluyen, entre otros, sistemas de radar, láser, ópticos, infrarrojos, acústicos, nucleares, de radiación, de detección, espectro radiométricos y sísmicos, así como sistemas de muestreo de gases, líquidos y materiales sólidos (U.S. Department Of Defense, 1993).

Inteligencia de señales (SIGINT).

Corresponde a la inteligencia de señales derivadas de la recopilación y procesamiento de datos de información transmitidos electrónicamente. Formas como la comunicación de lenguaje humano (COMINT o inteligencia de comunicaciones) y emisión electrónica de dispositivos, principalmente radar (ELINT o inteligencia electrónica). También se incluye la intercepción de telemetría y otras señales de instrumentación (FISINT o inteligencia de señales de instrumentación extranjera) (Lowenthal y Clark, 2015).

Durante la WWII, 20 mil norteamericanos estuvieron trabajando en la intercepción y decodificado de señales japonesas y alemanas. Inteligencia que ayudo en la defensa de los bombardeos en Reino Unido y los ataques de submarinos en el Pacífico; el desembarco del día D, neutralizado de la superioridad de la flota japonesa, etc. Tanto US Navy como Army descifraron la máquina japonesa Type 97 – Purple. Luego de la guerra, los esfuerzos se enfocaron en la URSS, dado que se requería un *strategic warning* en caso de ataque nuclear (utilizando bombarderes TU-4 o jet TU-16). Por ejemplo, en la operación Gold (CIA) / Stopwatch (MI6) (1954-1955), cavó un túnel (ver figura 48) desde Berlín occidental para

interceptar (*wiretap*) las comunicaciones de 3 cables, que incluía comunicaciones soviéticas y alemanas (oriental) (CIA Historical Stuff, 1971). Los soviéticos ya conocían la operación por la infiltración de un *mole* en el MI6 (George Blake), pero permitieron que la operación prosiguiera para no exponer a su informante y aprovecharon la ocasión para brindar desinformación en las comunicaciones pinchadas (Roberts, 2019).

Más adelante veremos el caso de la máquina enigma alemán y ampliaremos el concepto de inteligencia de señales cuando tratemos la vigilancia masiva en las comunicaciones.

Figura 48
Gold / Stopwatch Operation.



Nota. Túnel subterráneo para wiretap de cables (comunicaciones telefónicas) (Kreusch como fue citado por Roberts).

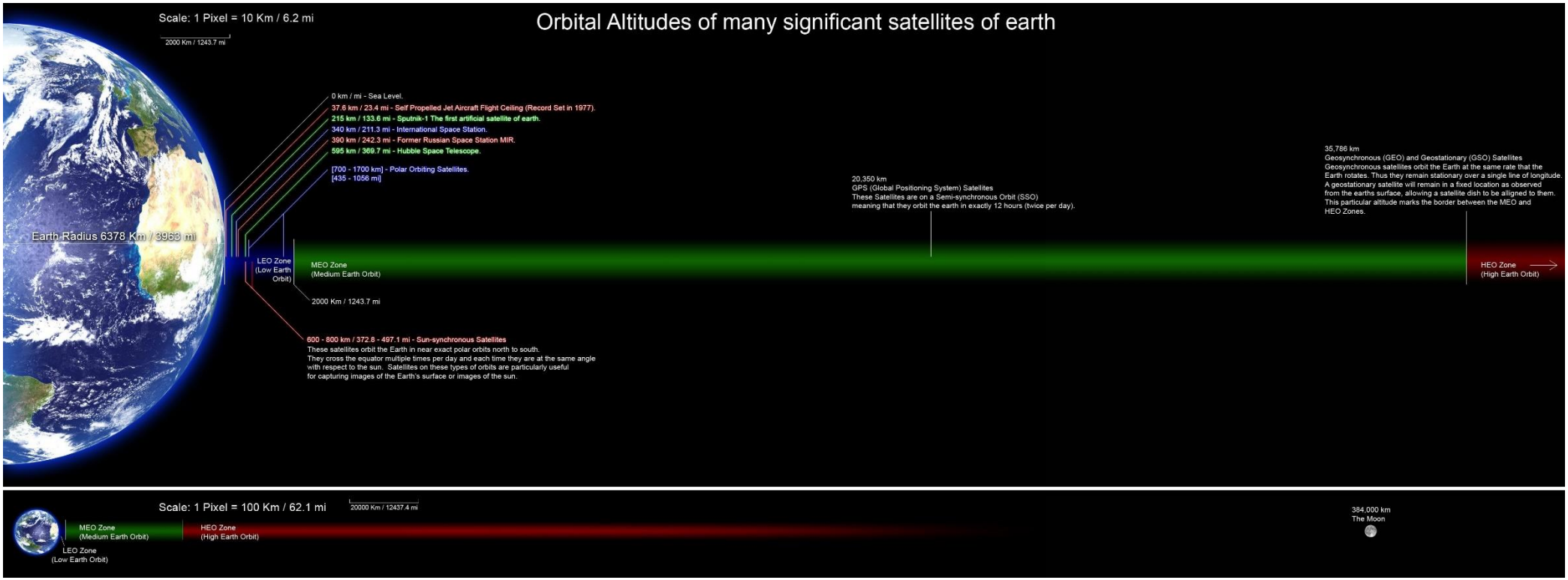
Satélites.

Las orbitas[122] de los satélites pueden ser diversas: Low Earth Orbit (LEO), Medium Earth Orbit (MEO), GEO (Geoestacionaria), High Earth Orbit (HEO), entre otros (ver figura 49).

[122] Los GEO giran a la misma velocidad que la tierra lo que hace que parezcan estacionarios (aproximadamente 3 km por segundo a una altitud de 35 786 km), orbitan el ecuador y un uso habitual son las telecomunicaciones. Los LEO (menos de 1000km) tiene mayor velocidad mientas lo que hace difícil su seguimiento, un uso habitual es la captura de imágenes (para comunicaciones pueden formar redes de satélites). Los MEO, al igual que los LEO, no requieren una órbita específica y son habitualmente utilizado para navegación (European Space Agency, 2020).

Figura 49

Orbitas satelitales.



Nota. (fuente imagen: Reinemann, s.f.).

Como breve mención sobre el inicio de la historia de los satélites de reconocimiento: En 1946 la USAF encarga al proyecto RAND la investigación de satélites (Project Feedback que incluía reconocimiento fotográfico sobre la URSS). Esto llevó al desarrollo conceptual del primer satélite (Weapon System 117L). Posteriormente separado en tres: Discoverer Program, SAMOS (Satellite and Missile Observation System) para reconocimiento y en MIDAS (Missile Defense Alarm System) para alertas de misiles. Discoverer estaba pensado para fotografiar a URSS y China, descender en paracaídas y ser recuperado por un avión C-119J. Discoverer inicio bajo el Code Name Corona en 1959 y finalizó en 1962 (continuó clandestino hasta 1972). En 1961 Corona pasa a la órbita del nuevo organismo National Reconnaissance Office (NRO[123]) (ver figura 50). SAMOS utilizaba reconocimiento fotográfico, electromagnético y transmitía los datos electrónicamente (lanzamientos del 60 al 62). Más adelante vinculado al Defense Dissemination System (DDS) para uso estratégico y táctico. MIDAS enfocado en detectar lanzamientos de misiles con sensores infrarrojos (1960-1961). Renombrado a proyecto 461 luego de varias fallas continuo hasta 1968. Similar es el Defense Support Program (DSP) iniciado en 1963 con bases en tierra (Overseas Ground Station - OGS) en Australia, Europa y EE.UU. (con lanzamiento en 1970). Posteriormente, Space-Based Infrared System (SBIRS) (USAF, s.f.).

[123] NRO es una de las 5 agencias más importantes de inteligencia junto a la CIA, NSA, DIA y NGA.

Figura 50
USA-247 reconnaissance satellite patch.



Nota. Curioso logo que refleja el espíritu de la agencia. Fuente imagen (Graham, 2013; Szoldra, 2013; Mullin, 2013), derecha Atlas V NROL-39 Launch (United Launch Alliance vía ODNI como fue citado por Mullin, 2013).

Recordemos el contexto de la época donde la URSS lanzaba el primer satélite al espacio (Sputnik) en 1957, el incidente del U2 en 1960 y la crisis de los misiles en 1962, entre otros eventos de la guerra fría.

Algunos satélites que mencionar. Vela Hotel fue una serie de satélites para detectar explosiones nucleares. GEOINT: Corona (KH-4), Argon (KH-5), Lanyard (KH-6), Gambit (KH-7), Hexagon (KH-9) (ver figura 51 y 52), Kennen (KH-11), Quill (radar imaging, 60), Topaz, Lacrosse (radar imaging), Misty/ Zirconic (IMINT). ELINT: Galactic Radiation and Background (Grab, 60-62 escucha radares soviéticos), Poppy (71-71). SIGINT: Rhyolite, Intruder, Sharp, Nemesis, Magnum/Orion (85), Canyon/Runway (68-77 operado desde Alemania en Bad Aibling station para intercepción de comunicaciones rusas), Chalet (78' renombrado a Vortex y luego a Mercury - controlado desde Menwith Hill Reino Unido, cubre las Comunicaciones de Europa, Oriente Medio y Asia; también fue utilizado en la guerra de las Malvinas), Advanced Vortex (94 – microwave y cellphones), Jumpseat (71-83 ELINT de radares ABM - Soviet antiballistic missile, posteriormente COMINT y FISINT), Samos, Advanced Orion / Mentor (95), Trumpet (97), Project 8300 (2004 reemplazo Orion / Vortex), Nemesis (2009 - principalmente comunicaciones chinas, posteriormente Latinoamérica, Oriente Medio y norte de África), CLIO 2014 (ver figura 53) (Richelson,

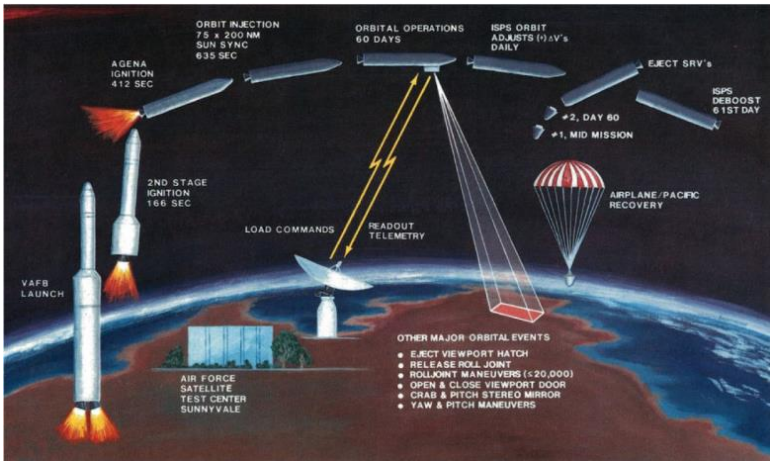
2006, 2012, 2015; Sciaroni, 2016; Day, 2013; Gunter, S.F.; The intercept, 2016; U.S. Department of Defense, 2019).

Figura 51
KH-9 Hexagon.



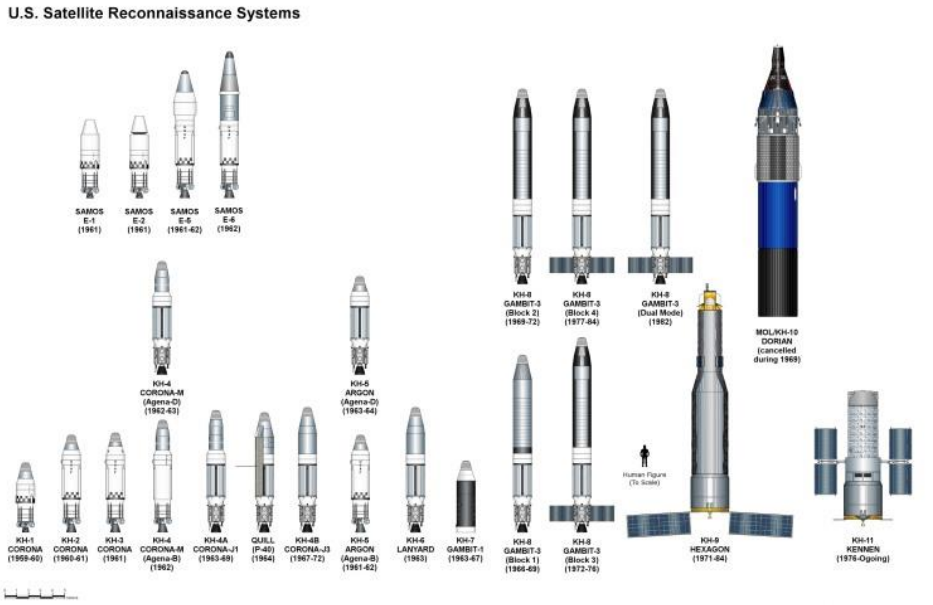
National Museum of U.S. Air Force (Foto Copes Jim, s.f.).

Figura 52
Gambit 3.



Gambit, Corona y Haxagon recuperaban el film al regreso a la tierra (National Museum of United States Air Force).

Figura 53
Satélites.



Fuente: Giuseppe De Chiara 1968.

Por describir algunos de los mencionados, el programa RHYOLITE (renombrado a AQUACADE) de los 60’ consistía en satélites (SYNCOM) geos sincrónicos para cubrir la telemetría (lanzamiento de misiles) en Europa/Asia (NRO National reconnaissance Office / CIA), Pine Gap Australia (codename Rainfall) es una de las estaciones terrestres. Posteriormente la NSA adicionó capacidades COMINT/ELINT (70’). Algunas estaciones terrestres son: Aerospace Data Facility (ADF) en Colorado (Buckley AFB, Co - High-altitude SIGINT), ADF Southwest (White Sands, New Mexico - Radar imagery), ADF-E (Fort Belvoir, Virginia – Electro optical imagery), RAF Menwith Hill en Reino Unido (Geosynchronous SIGINT) y Joint Defense Facility Pine Gap Australia (Geosynchronous SIGINT)[124] (Richelson, 2012, 2015).

Otros países hacen lo propio, por ejemplo, Rusia tiene en Lourdes Cuba una base SIGINT que operaba en la guerra fría y fue reabierta en 2014 (Adwar y Kelley, 2014).

La historia de los satélites es tan apasionante como amplia y excede los límites del presente trabajo. A modo resumen conceptual, más allá de los complejos nombres de los proyectos, existen satélites en diferentes orbitas, permanentes o satélites que son lanzados

[124] Veremos más adelante que estos países no casualmente forman parte de la alianza del Five Eyes.

para operaciones particulares que luego deben ser recuperados. Los mismos tienen una serie diversa de sensores dentro del amplio espectro electromagnético para captar imágenes / comunicaciones / señales. Además, pueden comunicarse con estaciones terrestres para control o bajada de datos adquiridos.

En lo que respecta a la guerra híbrida, es factible la utilización militar de satélites civiles (uso mixto), lo cual reduce la posibilidad de ser interceptado / atacados en situaciones de conflictos. Las armas anti satélites con conocidas como ASAT (*Anti-satellite weapons*), hasta el momento solo han sido utilizadas en pruebas contra satélites propios, aunque es de esperar un uso ofensivo en tiempos de conflictos futuros. Anticipando dicho escenario y a fin de garantizar la disponibilidad, la tendencia apunta a esquemas de enjambres de pequeños satélites. Por lo mencionado, proyectos como Starlink o Cubesat (ver figura 54), parecen mostrar una tendencia.

Figura 54
Cubesat.



Nota: 10cm de lado. Desarrollado en el 99 por el profesor Jordi Puig-Suari (California Polytechnic State University) y Bob Twiggs (Stanford University).

Guerra en el espacio.

En 2014, el Lieutenant general David Buck (Comandante del Joint Force Space Component en la base Vandenberg Air Force) (ver figura 55), comenta que mientras monitoreaban el lanzamiento de un satélite ruso, observó algo nunca visto. Una pieza de escombros comenzó a maniobrar en las proximidades del propulsor del cohete. Especulaciones indican que el satélite (Kosmos 2499 alias Kamikaze) podría tener la

funcionalidad de impactar y destruir satélites. Al poco tiempo Rusia lanza otro satélite espía con iguales capacidades llamado Luch. Fue observado acercándose a satélites norteamericanos de uso comercial como ser el Intelsat, posiblemente para recolectar información en tránsito (Sciutto y Rizzo, 2016). Intelsat paradójicamente también es espiado por la NSA con la red Echelon que veremos más adelante (Bamford J. como fue citado por Richelson, 2005).

Otro acontecimiento observado fue el satélite chino Shiyan lanzado en 2013. El mismo desapareció al aproximarse a un satélite más pequeño para luego reaparecer al alejarse. El gobierno chino afirmó que el satélite posee un brazo robótico para observar desechos en el espacio. Mientras que los norteamericanos piensan que podría tener una capacidad para secuestrar otros satélites (*kidnap*). Por su parte EE.UU. prueba drones para el espacio (X-37B - ver figura 56) y armas laser (Laser Weapons System - LaWS) en el Golfo pérsico. Piensan que otros países podrían utilizar similares armas para cegar o inclusive destruir satélites (Sciutto y Rizzo, 2016).

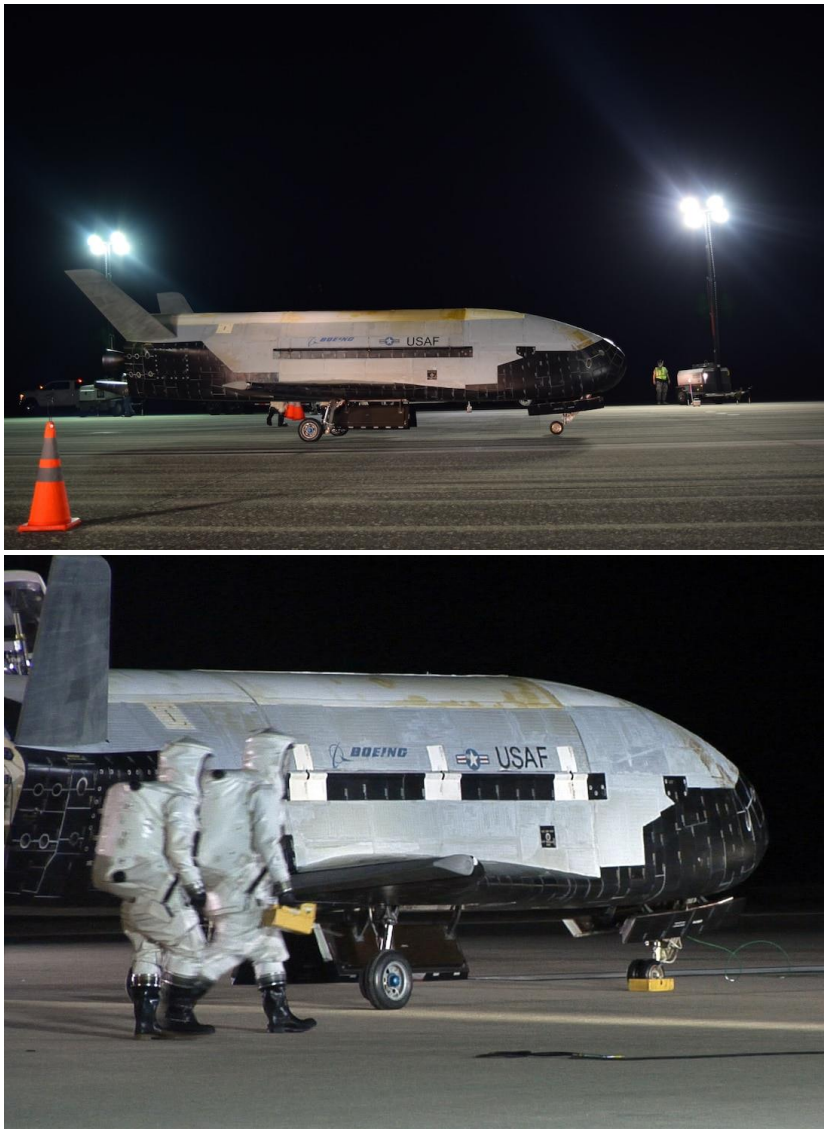
Figura 55

Operators at the Joint Space Operations Center (JSpOC) at Vandenberg Air Force.



Nota: sistemas informáticos diseñados para detectar, rastrear e identificar todos los objetos hechos por el hombre en la órbita de la Tierra para mantener el Awareness espacial (JFCC Space photo).

Figura 56
X-37B.



Nota: drone para operaciones en el espacio. Fotografía (Stonecypher, 2010, 2019).

En lo que respecta a ciberataques, el reporte de U.S.-China Economic and Security Review Commission (2011) remarca:

> Los actores maliciosos pueden usar actividades cibernéticas para comprometer, interrumpir, negar, degradar, engañar o destruir sistemas espaciales. Las explotaciones o los ataques podrían tener como objetivo la infraestructura terrestre, los sistemas espaciales o los enlaces de comunicación entre ambos. Como se señaló anteriormente, los escritos militares chinos autorizados abogan por tales actividades, particularmente en lo que se relaciona con la infraestructura espacial terrestre, como el control de satélites. Los satélites de varios programas espaciales del gobierno de los EE. UU. utilizan estaciones terrestres satelitales operadas comercialmente fuera de los Estados

Unidos, algunas de las cuales dependen de la Internet pública para "acceso a datos y transferencias de archivos", según un informe trimestral de la Administración Nacional de Aeronáutica y del Espacio de 2008. El uso de Internet para realizar ciertas funciones de comunicación presenta oportunidades potenciales para que los actores malintencionados obtengan acceso a redes restringidas. En particular, al menos dos satélites del gobierno de EE. UU. han experimentado al menos dos instancias separadas de interferencia aparentemente consistentes con actividades cibernéticas contra sus sistemas de comando y control:

El 20 de octubre de 2007, Landsat-7, un satélite de observación terrestre de EE.UU. administrado conjuntamente por la Administración Nacional de Aeronáutica y del Espacio y el Servicio Geológico de EE. UU., experimentó 12 minutos o más de interferencia. Esta interferencia solo se descubrió después de un evento similar en julio de 2008.

El 20 de junio de 2008, Terra EOS [sistema de observación de la Tierra] AM–1, un programa administrado por la Administración Nacional de Aeronáutica y del Espacio para la observación de la Tierra, experimentó dos o más minutos de interferencia. La parte responsable logró todos los pasos requeridos para comandar el satélite, pero no emitió comandos.

El 23 de julio de 2008, Landsat-7 experimentó 12 o más minutos de interferencia. El responsable no logró todos los pasos requeridos para comandar el satélite.

El 22 de octubre de 2008, Terra EOS AM–1 experimentó nueve o más minutos de interferencia. El responsable realizó todos los pasos necesarios para comandar el satélite, pero no emitió comandos. La Administración Nacional de Aeronáutica y del Espacio confirmó dos eventos sospechosos relacionados con el satélite Terra EOS en 2008 y el Servicio Geológico de EE. UU. confirmó dos eventos anómalos relacionados con el satélite Landsat-7 en 2007 y 2008.

Si se ejecuta con éxito, dicha interferencia tiene el potencial de plantean numerosas amenazas, en particular si se logra contra satélites con funciones más sensibles. Por ejemplo, el acceso a los controles de un satélite podría permitir que un atacante dañe o destruya el satélite. El atacante también podría negar o degradar, así como falsificar o manipular la transmisión del satélite. Un alto nivel de acceso podría revelar las capacidades o la información del satélite, como imágenes, obtenidas a través de sus sensores. También pueden existir oportunidades para reconocer o comprometer otras redes terrestres o basadas en el espacio utilizadas por el satélite (p215-216).

Inteligencia sin restricción.

Mencionamos la adquisición de información por medios convencionales. Así como la guerra sin límites busca sus objetivos a través de todos los medios disponibles; proponemos el termino de inteligencia sin estricción enfocada en la adquisición de información a través de todos los medios posibles. Resultado un elemento estratégico para

potenciar las diferentes operaciones. A continuación, se exponen diferentes medios de adquisición de información a través de la inteligencia sin límites.

Escucha a distancia e implantes.

Existen diferentes dispositivos para escucha a distancia: por aire (*parabolic microphones*), por láser que interpretan las vibraciones en objetos como ser vidrio (ver figura 57), *covert listening devices* o *bug* (micrófono con un transmisor de radio) (ver figura 58, 59), roving *bug* (activar el micrófono del celular a distancia). Por otro lado, implantes del tipo *keyloggers* (ver figura 60) de *keyboard* diseñado para grabar las teclas presionadas (incluyendo credenciales), *skimmer devices* en ATM (ver figura 61) o inclusive *shoulder surfing* como técnica para ver la pantalla de una víctima (ver figura 62).

Figura 57

Opto Acoustic Laser Microphone



Nota. La tecnología fue desarrollada por Leon Theremin. De izq. A derecha un micrófono opto acústico, similar montado en un vehículo (Fuente imagen: Intercept Monitoring Systems, s.f.) y finalmente una filmina protectora (SD 2500) como ejemplo de TSCM (Technical Surveillance Counter-Measure) (Fuente imagen: Signals Defense, s.f.).

Figura 58

More devices



Nota. Izquierda bola micrófono, derecha escucha de teléfonos cableados sin necesidad de cortar cable (Fuente imagen: PKI Electronic Intelligence, s.f.).

Figura 59

Covert listening devices



Nota. Micrófonos con transmisión (fuente imagen: spyshopro.com, s.f.).

Figura 60

Implante keylogger.



Nota. El dispositivo de ejemplo es Key Croc de Hack5 que además de *keylogger* tiene función de acceso remoto y puede disparar *payloads* según patrones de teclas (Fuente imagen: hak5.org, s.f.).

Figura 61

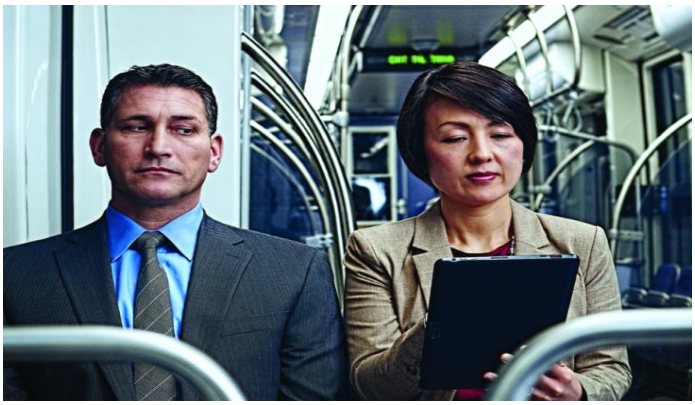
Skimmer device de ATM.



Nota. Dispositivos para clonar tarjetas de crédito, captura de pin, opcionalmente suplementado con una cámara oculta en la parte superior (Fuente imagen: nwcu.com, s.f.).

Figura 62

Shoulder surfing.



Nota. La técnica afecta seriamente la confidencialidad, incluyendo claves de acceso. También se puede realizar desde la distancia con equipos de aumento. Esta técnica, quiérase o no, es realizada sistemáticamente por las cámaras del gobierno (Fuente imagen: 3M, s.f.).

Intercepción de teléfonos celulares y satelitales.

El IMSI[125] Catcher, también llamado Stingray (ver figura 63, 64 y 65), es un dispositivo que intercepta el tráfico de los teléfonos celulares, permite denegación de servicio y geolocalización de la víctima. Además, las vulnerabilidades en el protocolo SS7[126] permiten por ejemplo el envío masivo de mensajes vacíos no visibles por el usuario (*Silent/Stealth Type-0 SMS*), generando una denegación de servicio (Weinberg, 2021).

Figura 63

IMSI Catcher/Stingray.



Nota. Kingfish (Fuente Image: Sotnek, 2019).

[125] International Mobile Subscriber Identity es un identificador univoco de 64-bit que tiene cada teléfono celular. Similar al IMEI de una SIM CARD.

[126] Signaling System No. 7 es un protocolo telefónico definido en la serie ITU-T Q.700 y que se encarga de la comunicación dentro de la Public Switched Telephone Network (PSTN)

Figura 64

IMSI Catcher/Stingray montado en drone.



Nota. Unmanned Aerial Vehicle (UAV IT180-120) con capacidad SIGINT[127] e IMINT[128] (Fuente Imágenes: Ecagroup, s.f.).

Figura 65

MINI IMSI Catcher.



Nota. Septier Mini imsi cátcher (Septier Communication Ltd., s.f.).

El ataque es del tipo *Man in the Middle*, similar al ataque *evil twin* mencionado en el capítulo apéndice. Para el ataque (ver figura 66), el dispositivo simula ser una antena legítima de la empresa de comunicaciones, captura el IMSI de la víctima y hace un *spoof* (falsificación) suplantando la identidad de la víctima con la torre, mediante un *Location Update Request* (Ouziel, 2020). Entre algunos riesgos, podemos mencionar la captura de

[127] Inteligencia de señales.
[128] Inteligencia de imágenes.

MSM de validación, permitiendo al atacante el acceso a una red social o mensajería privada de la víctima (ejemplo Telegram).

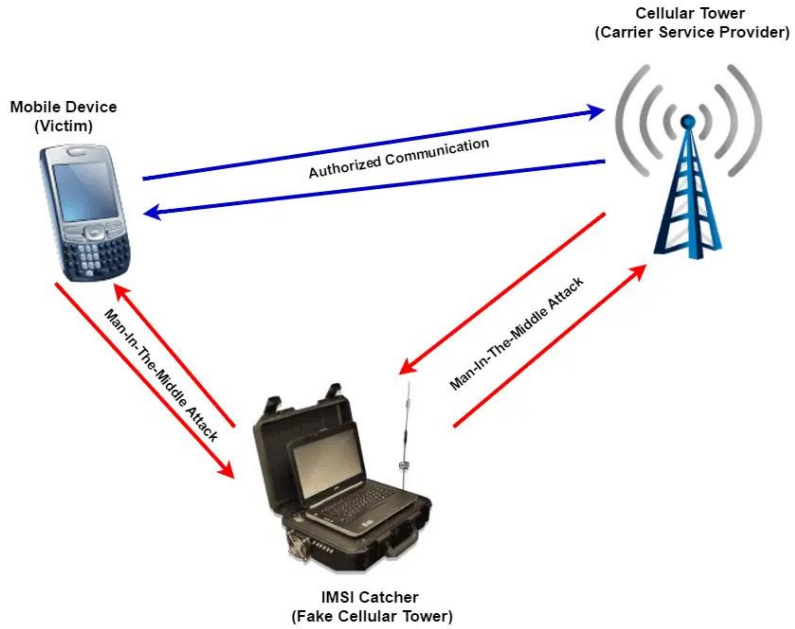
Estos equipos fueron detectados espiando ilegalmente las comunicaciones próximas a la *White House* (EE.UU.). El FBI remarcó que no había duda de que eran Israelitas (Lippman, 2019). Nuestro país no es la excepción, por lo que resulta razonable pensar que tales equipos también son utilizados de forma sigilosa[129] contra objetivos de interés, de forma ilegal, por inteligencia local como extranjera.

Usualmente los IMSI Catcher son costosos, pero investigadores de la Universidad de Aalto y de Helsinki demostraron que es posible obtener la geolocalización y afectar la disponibilidad con un SDR[130] de bajo costo (Shaik et al., 2017).

Como es habitual, siempre que hay inteligencia existe la contrainteligencia, para lo cual también existen equipos de detección de IMSI Catcher (ver figura 67).

Figura 66

MITM en la red Telefónica con un IMSI Catcher.



Nota. El atacante en las proximidades de la víctima simula ser una torre celular y al mismo tiempo imita a la víctima contra la torre real (Fuente Image: Ouziel, 2020).

[129] Se dice sigilosa porque es invisible para una persona convencional, pero existen técnicas de detección.
[130] Software Defined Radio.

Figura 67

IMSI Catcher detector.



Nota. MGT Cell Master (fuente imagen: MGT Cell Master, s.f.) y PKI 1670 (Fuente imagen: PKI Electronic Intelligence, s.f.). También existen proyectos independientes para Android.

Los teléfonos satelitales, así mismo, pueden ser interceptados y localizados. Por ejemplo, los teléfonos Thuraya utilizan GMR-1 basado en A5/2 standard que se pueden descifrar (Lee, Hong, Sung, Kim, Hong, 2021) mientras que los Inmarsat utilizan GMR-2 estándar también descifrable (Hu, Li, Tang, 2017). Para la localización existen varias técnicas como una triangulación en las proximidades. El satélite necesita estimar la posición (basado en el Doppler shift) para mantener la comunicación o directamente algunos aparatos ya incluyen GPS, entre otros medios de localización (ver figura 68, 69 y 70). Los periodistas Marie Colvin y Remi Ochlik del Sunday Times, según Priest (2016) fueron asesinados en Siria con la localización de sus teléfonos.

Figura 68

Tactical Thuraya Monitoring System SCL-5030P.



Nota. Permite interceptar comunicaciones satelitales de Thuraya (2 y 3) como así también la geolocalización (fuente imagen: Shoghi Communications, s.f.).

Figura 69

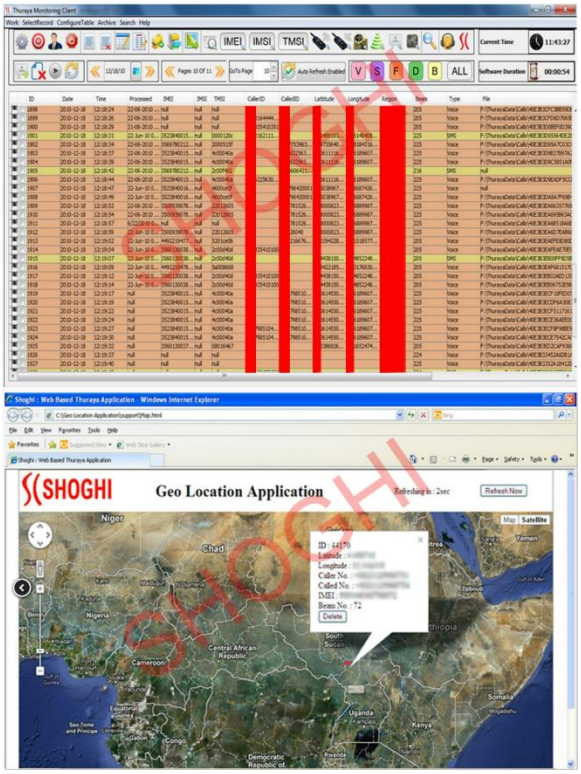
Unified Satellite Phone Monitoring System SCL-1625TII.



Nota. Permite interceptar comunicaciones satelitales de Thuraya (600km), Iridium (1000km) e IsatPhone Pro (400km) (fuente imagen: Shoghi Communications, s.f.).

Figura 70

Software ejemplo intercepción y localización.



Nota. (Fuente imagen: Shoghi Communications, s.f.)

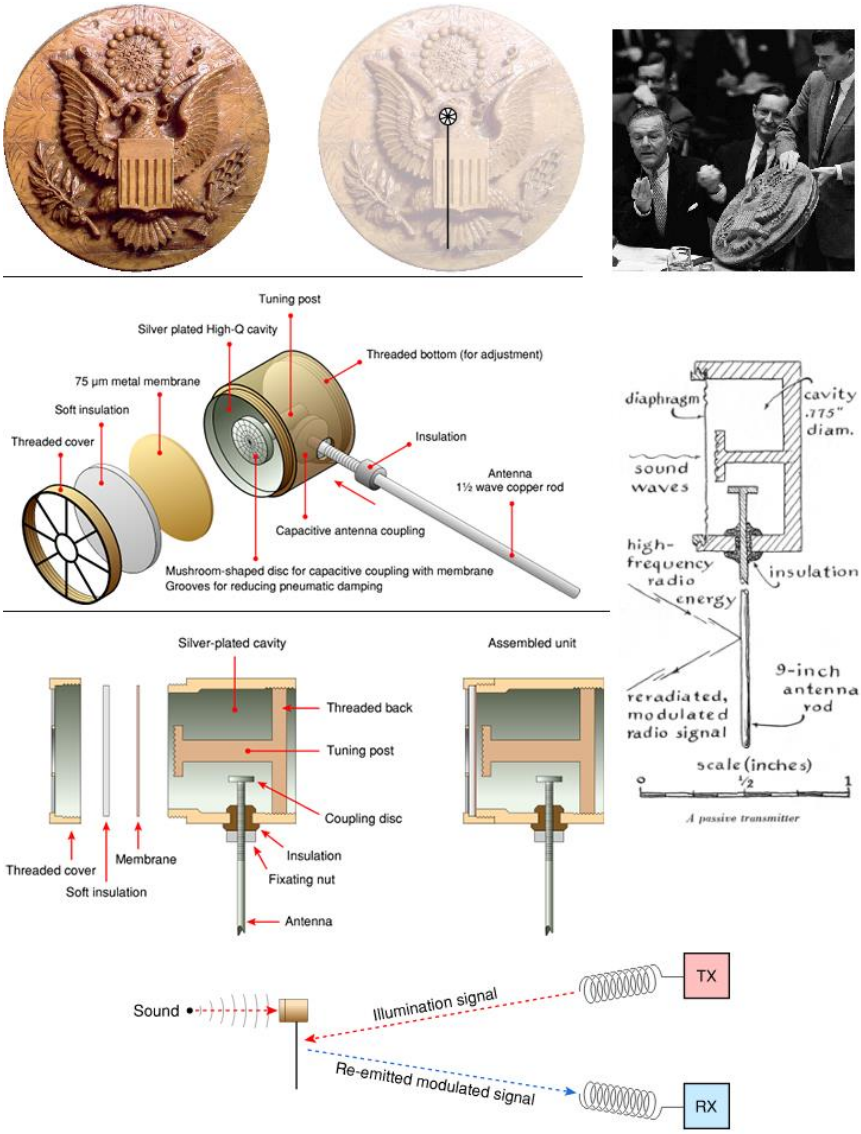
Regalos con sorpresas inesperadas – The Great Seal.

En 1945, los niños de *Vladimir Lenin All-Union Pioneer organization* le dieron un obsequio al embajador de Estados Unidos en Moscu, W. Averell Harriman, cuando los visitó en el campamento juvenil de Artek. El regalo fue un escudo de Estados Unidos tallado en madera (ver figura 71 y 72). El sello, llamado The Thing / the Great Seal bug (codename LOSS para EE.UU. y RAINDEER para los soviéticos), contenía escondido en su interior un bug pasivo inventado por Lev Termén, quien inventó además el instrumento musical Theremin (Brooker, Gómez, 2013). Este micrófono no tenía fuente de alimentación, sino que se activaba con una fuerte señal electromagnética desde el exterior y emitía (reflejaba) señales que eran captadas por antenas en un edificio aledaño (Wallace y Melton, 2008). El mismo no fue descubierto hasta 7 años más tarde de casualidad por un operador de radio británico a 1,5km de distancia. Aun así, su hallazgo tomo tiempo dada la naturaleza pasiva del mismo. Finalmente fue descubierto con técnicas *ELINT* (*Electronic signals intelligence*) / *Crystal Video Receivers* mientras era utilizado por los soviéticos. Aparentemente los

norteamericanos no tenían idea de cómo funcionaba el dispositivo (por eso el nombre “la cosa”) y pidieron ayuda a Reino Unido. Luego de 10 semanas, Peter Wright del MI5 logro resolver el rompecabezas. Pasados los 18 meses, el MI5 disponía su propia versión del micrófono en forma de paraguas (SATYR). La CIA hizo lo propio con una versión de pulsos en 1965, agregando el modelo a su colección (EASY CHAIR). El descubrimiento del bug se mantuvo en secreto hasta 1960 cuando fue expuesto ante las naciones unidas al ocurrir el incidente U-2 (Crypto Museum, s.f.).

Figura 71

Resonant cavity microphone.



Nota. Funcionamiento del dispositivo y exposición antes la UN arriba a la derecha (Fuente Image: Crypto Museum)

Figura 72

The Thing / the Great Seal bug.



Nota. (Fuente Imagen: Galería de la NSA).

Visión remota (Van Eck phreaking).

También conocido como Van Eck Radiation consiste en una técnica descripta por Wim van Eck en 1985 que permite interceptar las emanaciones electromagnéticas emitidas por un monitor para su interpretación y reproducción (ver figura 73).

Como contramedida el Tempest es un estándar de supresión de emanaciones de señales en sistemas de información, mediante la utilización de materiales de blindaje (caja de Faraday) o su contrapartida que es llenar el espectro electromagnético de ruido uniforme (White Noise) a fin de que no se pueda distinguir la información del ruido. Los estados/naciones disponen de cuartos especiales para tratar temas de seguridad, llamados SCIF (Sensitive Compartmented Information Facility), como por ejemplo el Situation Room bajo la White House (Rafferty, 2017; National Counterintelligence and security Center, 2020).

A pesar de ello, existen investigaciones sobre como vulnerar los blindajes de Faraday. El malware ODINI puede controlar los campos magnéticos[131] emitidos por una computadora mediante el control de la carga de trabajo de los núcleos en un CPU. Permitiendo utilizar campos magnéticos de baja frecuencia como *covert channel* para exfiltrar información, inclusive dentro de un *Faraday shielding* (Mordechai, Boris, Yuval, 2020).

Figura 73

Eavesdrop de emanaciones electromagnéticas de un monitor.



Nota. Hoy en día con un receptor SDR, una antena y el software TempestSDR se puede lograr resultados a bajo costo (Fuente: Youtube cannel Tech Minds).

[131] Los campos electromagnéticos de baja frecuencia que requiere una antena de recepción extremadamente grande dado que depende de la longitud de onda. Por ejemplo, para 100 kHz se requiere una antena de 3 kilómetros. Sin embargo, las ondas magnéticas no dependen de la longitud de la antena (Mordechai, Boris, Yuval, 2020).

Area 51.

No se trata de una zona de extraterrestres sino de un área de desarrollo y pruebas de proyectos súper secretos en combinación entre DARPA, CIA y la Fuerza aérea. Muchos desarrollos involucran aviones con tecnologías de sigilo (furtivos) y reconocimiento (espía). Posteriormente, las tecnologías son utilizadas en otros países como por ejemplo Rusia, China, etc. Además, el área realiza pruebas de aviones capturados como el Mig 15 ruso (renombrado como YF-110), Mig-21 (HAVE DOUGHNUT), MIG-17 (HAVE DRILL/HAVE FERRY), entre otros.

Acorde a documentos desclasificados, algunos desarrollos a mencionar son el U-2 Code Name AQUATONE/OILSTONE (1955), A-12 /OXCART Project GUSTO (1958) seguido del YF-12A KEDLOCK y SR-71 Blackbird; drone supersónico D-21 TAGBOARD (1969), satélite de reconocimiento CORONA (1959), F-117, B-2, F-22, Advanced Cruise Missile; drone de sigilo RQ-170 e inclusive el helicóptero Blackhawk de sigilo utilizado en la Operation Neptune Spear (Richelson, 2013).

Este helicóptero fue por ejemplo utilizado en la Operation Neptune Spear (CIA/Navy SEALs) para el asesinato de Bin Laden en Pakistán durante 2011. Incluida 2 helicópteros furtivos Blackhawk[132] (ver figura 74). Uno de ellos sufrió un accidente y tuvo que ser destruido para prevenir que la tecnología cayera en otras manos (Tree, 2011).

[132] Una versión secreta de la cual no se conocen detalles. Es esperable tecnología para reducción de sonido, firma infrarroja, firma de radar y pintura absorbente de radiación, entre otras tecnologías de sigilo.

Figura 74
Stealth Blackhawk.



Nota. Restos del helicóptero destruido (Tree, 2011).

Vehículos aéreos no tripulados (UAV: Unmanned Aerial Vehicle).

Hemos mencionado la utilización de vehículos no tripulados con diferentes sensores durante el capítulo de conceptos básicos. Ampliamos el concepto con los *Micro Air Vehicles* (MAV) también conocidos como Bug-Drones o *Micromechanical Flying Insect* (MFI). Durante los 70, la CIA desarrolló un prototipo llamado *Insectothopter* que contenía un micrófono. El mismo no fue operacional por ser difícil de controlar (CIA Museum, s.f.) (Ver ver figura 75). *Insectothopter* es un reflejo de lo que podríamos encontrarnos en la actualidad (50 años después).

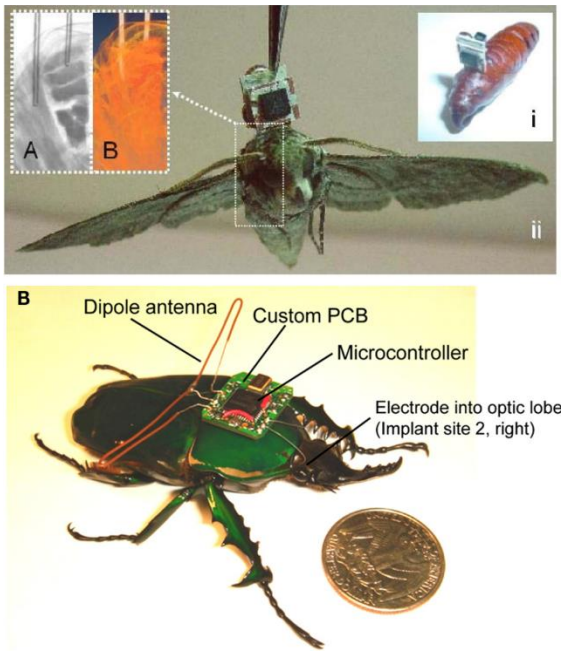
Figura 75
Insectothopter.



Prototipo de la CIA con micrófono simulando un insecto (CIA Museum, s.f.).

Publicaciones del 2009 indican que DARPA tiene un proyecto llamado HI-MEMS (Hybrid Insect Micro Electro-mechanical Systems) para transformar insectos en UAV. El mismo busca controlar insectos (Cyborn Insect) de forma remota a través del implante de electrodos (Ver ver figura 76) (Adee, 2009).

Figura 76
Hybrid Insect Micro Electro-Mechanical Systems.



Nota. Cyborn Insect, fotos ilustrativas de eléctrodos implantados. (Fuente imagen superior: Bozkurt, Gilmour, Stern, Lal, 2008). (Fuente Imagen inferior: Sato, Berry, Peeri, Baghoomian, Casey, Lavella, VandenBrooks, Harrison, Maharbiz, 2009).

En 2011, la empresa AeroVironment anunció la creación de un colibrí robot para DARPA (Defense Advanced Research Projects Agency), dentro del programa Nano Air Vehicle (NAV) (Ver ver figura 77) (AeroVironment, 2011). En la figura 78 se aprecia otro small UAV con cámara diurna y térmica.

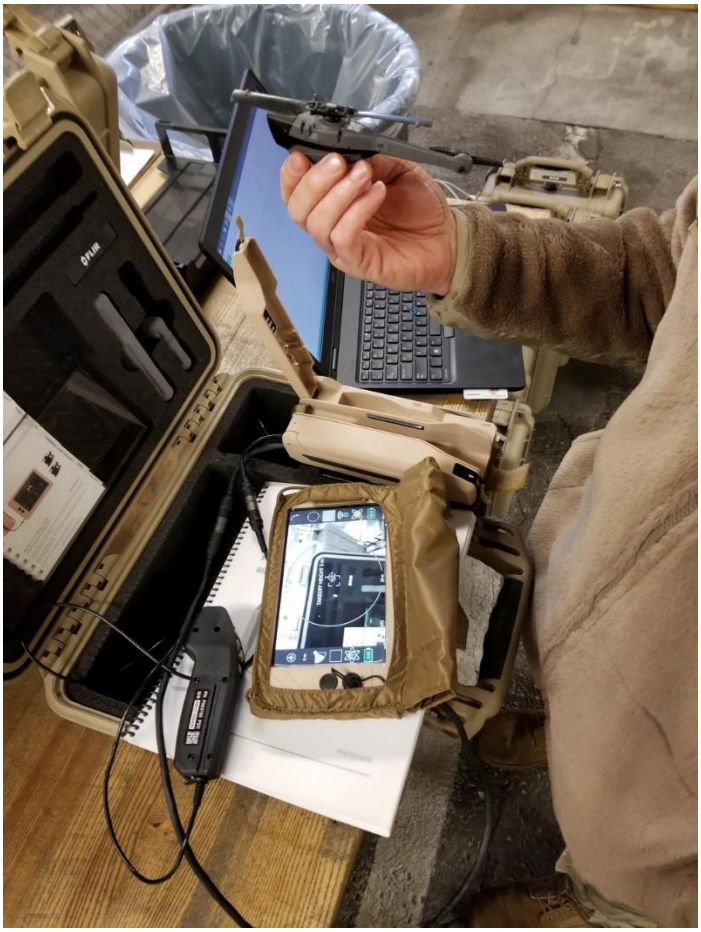
Figura 77

AeroVironment's Nano Hummingbird Surveillance Bot.



Nota: Desarrollado por la empresa AeroVironment (fuente imagen: Eckerman, 2011).

Figura 78
PD-100 Black Hornet.



Nota: Desarrollado por Prox Dynamics con un peso de 32g y un alcance de 2000m. (Fuente imagen: Lutgen, 2019).

Solo es cuestión de tiempo para que la miniaturización lleve los desarrollos a niveles imperceptible, como si fueran diminutas partículas.

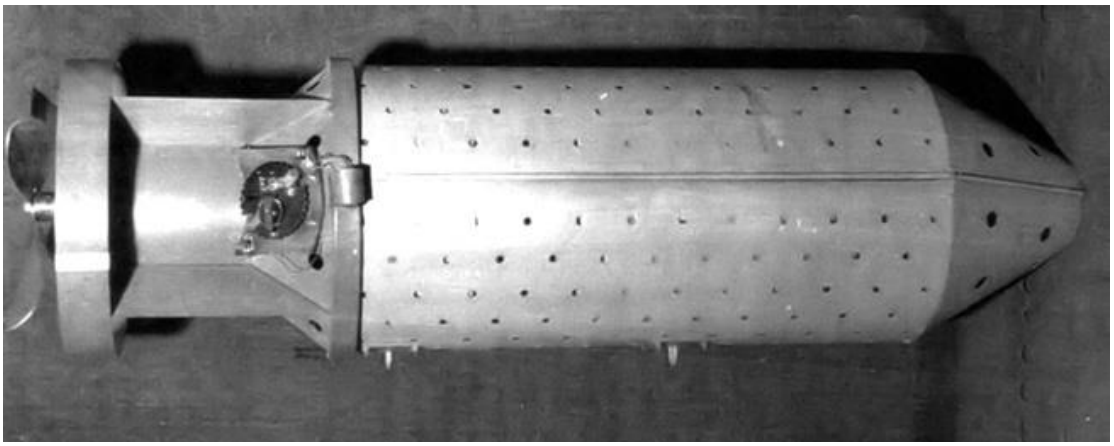
Utilización de animales.

Al igual que los insectos, los animales también son utilizados en operaciones de inteligencia o inclusive ofensivas. Durante la época del 30, la URSS entrenó perros antitanques equipados con explosivos, algunos fueron utilizados en la batalla de Kursk contra los tanques alemanes (Stewart, 2013; Lemish, 1999). Acorde a (Lemish, 1999), US Army también experimentó con perros en Fort Belvoir durante 1944. Los perros eran

entrenados para ingresar a los bunkers con explosivos[133]. A su vez comenta sobre idea de utilizar perros con bombas nucleares tácticas durante los 50.

En 1942 un dentista propuso la idea de utilizar murciélagos con bombas incendiarias contra las ciudades de Japón y el presidente Roosevelt aprobó el proyecto. Luego de algunos accidentes en una base de New Mexico, fue transferido al US Navy bajo el nombre de proyecto X-RAY. La bomba contenía un paracaídas y unos 1000 murciélagos que eran liberados con bombas incendiarias pegadas al pecho. El proyecto no llegó a utilizarse dado la creación de la bomba atómica (Duffin, s.f.) (Ver ver figura 79).

Figura 79
Bat bomb.

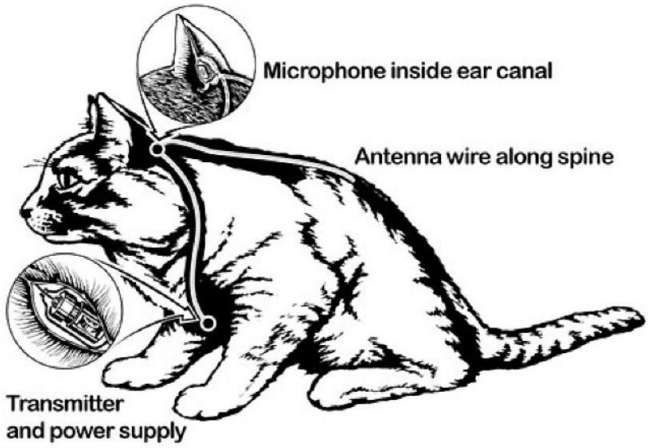


Nota: Los murciélagos liberados contenían bombas incendiarias (Duffin, s.f.).

En relación con inteligencia, durante los 60, la CIA experimentó colocando micrófonos en las orejas de gatos mediante cirugías (Operation Acoustic Kitty). El experimento fue un fracaso por el comportamiento impredecible del gato (Byrne, 2001) (Ver ver figura 80).

[133] Cabe aclarar que ningún animal utilizó explosivos reales. Las pruebas resultaron infructuosas dado el comportamiento impredecible del animal.

Figura 80
Acoustic Kitty.



Nota: Experimento de la CIA (fuente imagen: Harper, 2013).

Las palomas, conocidas por su capacidad de envío de mensajes, también fueron utilizadas con cámaras para inteligencia. En 1907, el alemán Julius Neubronner inventó la fotografía desde una paloma. Durante la primera guerra mundial (1917/8), los alemanes colocaron cámaras en palomas que realizaban vuelos sobre territorio enemigo (Spy Museum, s.f.) (Ver ver figura 81). Durante los 60 y 70, la CIA utilizó dicha técnica contra los soviéticos (Operation Tacana), además de cuervos para arrojar micrófonos en ventanas y delfines para tareas de búsqueda de minas en el agua (Rocket, 2019; CIA Museum, S.F.) (Ver ver figura 82).

Figura 81

Spy Pigeon WWI (1917-1918).



Nota: Utilizada por los alemanes durante la primera guerra mundial (Spy Museum, s.f.).

Figura 82

Spy Pigeon Cold War.



Nota: Utilizado por la CIA contra los soviéticos (The Secret World of Espionage como fue citado por Rockett, 2019; CIA, s.f.).

Acorde a Jones (2010), documentos de DARPA (Defense Advanced Research Projects Agency) indican un interés en el control de los tiburones y en el estudio de los electrorreceptores de su piel. El *Bio Electric Sensing* (“sexto sentido”) tiene implicancias en el uso militar como ser operaciones de vigilancia y monitoreo (Jones, 2010).

Según Daniels (2018), Irán ha denunciado una serie de animales espías próximo a las plantas de enriquecimiento de uranio en Natanz. En 2007 reportaron 14 ardillas que contenían GPS, micrófono y Cámaras. En 2008 encontraron dos palomas con una marca de metal azul y unos hilos invisibles. Durante 2018 indicaron la utilización de lagartos[134] con el fin de buscar sitios del programa nuclear. ¿Se trata de actividades de espionaje o paranoia del gobierno iraní? Según una publicación de LivesScience, los lagartos no pueden detectar uranio (Ghose, 2018). Acorde a autoridades egipcias, el caso de las ardillas se trató de equipos para estudiar la migración de dichos animales (S.N. BBC, 2013). Por otra parte, es cierto que en Natanz suceden eventos extraños (estudiaremos la roca espía y el *malware* Stuxnet más adelante).

A pesar de los casos puntuales, debe considerarse la posibilidad del uso de animales o estudios científicos cuya finalidad sea el espionaje.

Finalmente, resaltamos la importancia de la ética y un rechazo total al maltrato animal y de otras formas de vida.

Rocas espías.

Inteligencia británica admitió finalmente que en 2006 implantó una roca espía en Moscú (Topping y Elder, 2012). Es posible que su uso fuera la transmisión de información como canal encubierto (COVCOM) (Ver ver figura 83).

En 2012, iraníes descubrieron una roca espía cerca de las plantas nucleares de Natanz[135] que explotó al intentar moverla. El estudio posterior de sus restos indicó capacidades de intercepción de comunicaciones electrónicas (Ingersol, 2012).

Según Zvezda News, el ministerio de defensa ruso, en 2021 desarrolló un robot espía disimulado en forma de roca (ver figura 84) (Sherzad y Ukrainskiy, 2021).

[134] El académico y conservacionista iraní canadiense Kavous Seyed-Emami fue encarcelado bajo sospecha de espiar para EE.UU. e Israel. Apareció suicidado en la cárcel y se sospecha que pudo haber sido torturado.
[135] Ampliaremos sobre dichas plantas en la operación Olympic Games dentro del próximo capítulo.

Figura 83
Reino Unido Spy rock.



Nota. Colocada en Moscú (Fuente imagen: RTR TV, como fue citado por Williams, 2012).

Figura 84
Russian spy robot.



Nota. (Fuente imagen: Sherzad y Ukrainskiy, 2021).

Infiltrados.

Es bien conocido el interés de los gobiernos en infiltrar agentes (mole) dentro de organizaciones de otros países o inclusive propios. Uno de los casos más conocidos es el

de Cambridge Five (los cinco estudiantes reclutados por la KGB en la universidad de Cambridge en Reino Unido). Además de organizaciones, aúnan esfuerzos en penetrar empresas como ser medios de comunicación (diarios / noticieros), telecomunicaciones (telefonía / internet) y más recientemente empresas tecnológicas. La finalidad es el espionaje de sus clientes e incluso la empresa en si misma (o la información que manejan).

Según una investigación de Newsweek, el pentágono cuenta con un ejército secreto de aproximadamente 60 mil infiltrados (civiles / militares) que trabajan con identidades falsas y están enfocados en operaciones domésticas y extranjeras (programa Signature reduction[136]). Los operativos incluyen también operaciones *behind the enemy line* en países como Irán y Corea del Norte. Además, aparentemente cuentan con medidas para falsificar y engañar los sistemas biométricos en las fronteras (Arkin, 2021). En relación, el *malware* ExpressLane[137] infecta los sistemas biométricos a modo de update y habría permitido a la CIA obtener información del FBI, NSA y DHS (Homeland security).

Por citar otro ejemplo, un estudio de MintPress ha descubierto que cientos de ex agentes de la famosa organización de espionaje israelí Unidad 8200 han alcanzado posiciones de influencia en muchas de las empresas tecnológicas más grandes del mundo como Google, Facebook, Microsoft y Amazon (Macleod, 2022).

Otros mecanismos de infiltración es suplantar la identidad de empleados de alguna empresa, utilizando vestimenta y ploteo de vehículos acorde a la ocasión. Cortar el suministro de internet o telefónico con excusas perfectas para que técnicos puedan infiltrarse en propiedades o para que el operador telefónico obtenga datos técnicos del teléfono celular. Mecanismos de financiamiento y cursos a fuerzas de seguridad, permite formar a medida y genera influencia en dichos organismos. Por último y no menor, los espías e informantes que entablan relación de confianza con el objetivo a fin de obtener información (ver figura 85).

[136] Término utilizado por la prensa. En realidad, Signature reduction se refiere a las contramedidas para proteger las operaciones encubiertas. La investigación resulta dudosa, sin embargo, es un ejemplo útil para ilustrar la temática que por su naturaleza difícilmente encontremos documentos oficiales.
[137] El malware crea una partición oculta cifrada donde almacena información que luego es accedida.

Figura 85
Poster retro WWII.



Nota: Fuente Printed for H.M. STATIONERY OFFICE BY LOWE y BRYDONE PRINTERS LTD., N.W.10. / INF3-271.

Esto no es nuevo, el imperio romano contaba con una red masiva de agentes en tres continentes, para apoyar las operaciones militares y del gobierno. Así mismo, espionaje doméstico para identificar potenciales amenazas, como ser el complot de asesinato de Julio Cesar, quien ignoró las advertencias de su servicio de inteligencia (Lowenthal y Clark, 2015).

Robos.

Los robos armados son menos habituales debido a sus riesgos, aunque igualmente útil para algunas operaciones clandestinas que no pueden garantizarse por otros medios. Existen varios casos que seguramente vendrán a la mente, que dada su naturaleza encubierta no sería prudente mencionar de forma objetiva. Los robos no se limitan únicamente a documentos, dispositivos, teléfonos o notebooks de objetivos. Existen algunas operaciones más elaboradas.

Caso Project Azorian / Jennifer.

En 1968, un submarino soviético K-129 equipado con 3 misiles balísticos nucleares SS-N-4 Sark, salió de la base de Petropavlovsk. URSS perdió comunicación con el K-129

dado que el mismo se hundió en aguas internacionales próximo a Hawái. URSS no conocía la ubicación del submarino perdido ni su situación dado que habían perdido las comunicaciones. La red de hidrófonos norteamericanos SOSUS (Sound suverlliance system) pudo triangular la posición basado en el sonido de la explosión. Como primer paso, la Operación Sand Dollar consistió en enviar al submarino USS Halibut a encontrar y fotografiar al submarino. En 1974 la CIA utilizó un buque de perforaciones adaptado (Hughes Glomar Explorer) (ver figura 86) para recuperar al submarino con tecnología de misiles nucleares. La pantalla era la minería de manganeso (Aid, Burr, Blanton, 2010).

Figura 86
Hughes Glomar Explorer.



Nota. Utilizado para recuperar el submarino soviético K-129 (U.S. Government photo, como fue citado por Aid, Burr, Blanton, 2010).

Caso Operation Mount Hope III.

Se trató de una operación clandestina (1988) para capturar un helicóptero soviético Mil Mi-25 (versión de exportación del Mi-24) que se estrelló en el conflicto entre Libia y Chad. En mutuo acuerdo con el gobierno de Chad, arribó al aeropuerto internacional un Lockheed C-5 Galaxy de transporte llevando dos helicópteros Boeing CH-47 Chinook. Estos helicópteros volaron 800km durante la noche para recuperar al Mi-25 que luego fue transportado dentro del C-5 (ver figura 87) (Kirill, 2019).

Figura 87
Operation Mount Hope III.



Nota. Captura del helicóptero soviético Mil Mi-24 (photos del U.S. Army, como fue citado por Sacquety, 2022).

Abuso judicial.

La justicia tiene poderes especiales que le permiten vulnerar temporalmente los derechos / garantías constitucionales de los ciudadanos de forma legal, para llevar a cabo investigaciones criminales dentro de la etapa de instrucción de una causa. Sin embargo, existen abusos a dichos procesos. Según Savoia (2015), para realizar inteligencia ilegal sobre una persona, basta con contactar a algún juez afín o simplemente colocar el número

de teléfono de interés a pinchar dentro de expedientes grandes (usualmente investigaciones de crímenes complejos como narcotráfico, trata de personas, etc.).

Los convenios internacionales de intercambio de información también son explotados con fines de inteligencia ilegal. Por ejemplo, solicitar acceso a plataformas digitales, redes sociales, cuentas de correo, etc. Es habitual que los proveedores faciliten la información por miedo a quedar vinculadas a un hecho inexistente. Lamentablemente no siempre existe la reciprocidad cuando Argentina solicita información al exterior.

Respecto a la inteligencia ilegal en nuestro país, vale la pena hacer una breve mención del informe de la (Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia, 2021):

> […el] espionaje ilegal, en términos operativos, se instrumentó a través de agentes regulares de la Agencia Federal de Inteligencia (A.F.I.), del Servicio Penitenciario Federal (S.P.F.) con acciones abiertamente ilegales o enmascarados bajo supuestas órdenes judiciales. También, contó con la colaboración de agentes irregulares vinculados a dicho organismo y al Ministerio de Seguridad de la Nación, y de un nicho de magistrados de la justicia federal […] las técnicas de espionaje detectadas hasta el momento; tales como la interceptación indebida de comunicaciones a través de la apertura de causas o pre-causas judiciales mediante motivaciones artificiosas o, simplemente, a través de la instalación subrepticia de receptores de audio y video en las salas de abogados de unidades de detención, la infiltración en organizaciones sociales, el seguimiento de personas, la observación fílmica y fotográfica "in situ" o la utilización de cámaras de monitoreo de Centro de Monitoreo Urbano del Gobierno de la Ciudad Autónoma de Buenos Aires, el ingreso no autorizado a base de datos de la Dirección Nacional de Migraciones, Administración Federal de Ingresos Públicos (A.F.I.P.) y la obtención de información de otras fuentes de datos abiertas […] La información de interés así obtenida era producida y entregada con el fin de manipular a la opinión pública a través de la utilización de periodistas que, a la vez, se sirvieron de aquellas en un cuestionado libre ejercicio de la libertad de prensa al amparo de la protección constitucional del secreto de sus fuentes de información. Entre otras técnicas, se observó, también, el empleo de la acción psicológica sobre familiares de las personas que resultaban del interés persecutorio o personas seleccionadas para obtener coactivamente una declaración en una causa penal o extorsivamente un beneficio económico, de nuevo, a través del dispositivo judicial y periodístico (Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia, p2-3, 2021).

VPN y trackings.

Las VPN ofrecen seguridad y privacidad (sin registro de navegación). El concepto no puede verificarse y se sustenta únicamente en la confianza con el proveedor de la VPN (siendo vulnerable a ataques del tipo de cadena de suministro).

Por otra parte, la VPN solo cifra el tráfico desde el origen hasta el servidor VPN (desde allí la comunicación llega a destino por fuera del túnel). Aquí el anonimato entra en juego dependiendo de la concurrencia de usuarios simultáneos (dado que es posible realizar ataques de análisis de tráfico o de patrones).

Además, existen innumerables técnicas para monitoreo de usuarios de internet como ser tracking pixel, browser fingerprints (resolución de pantalla, versión, combinación de plugins, configuraciones, etc.), cookies y otros fingerprint (activos[138]/pasivos). Por otra parte, las sesiones autenticadas también revelan la identidad del usuario. Más adelante ampliaremos otras técnicas en la vigilancia masiva.

Respecto a la confianza de las VPN[139], en 2020 encontraron un servidor abierto de free VPN. En el mismo encontraron información de contraseñas, correos electrónicos, dirección de IP, dirección física y log de cerda de 20 millones de personas que utilizaban una serie de VPN (con política de no log) con base en Hong-Kong. Las mismas son UFO VPN, FAST VPN, Free VPN, Super VPN, Flash VPN, Secure VPN y Rabbit VPN (Kan, 2020).

En relación con la importancia del background check, existen muchas empresas israelitas vinculadas a la unidad 8200 que infectan equipos con *malware* del tipo Ad aware (ganancia publicitaria y vigilancia). Estas empresas realizan técnicas de Web Injection para manipular las sesiones del navegador, redirigir tráfico de búsquedas, insertar pixeles de seguimiento, secuestrar cookies de sesión para enviar spam a contactos de correo y redes sociales, robo de datos personales y bancarios. El Ad Injection que es de los más lucrativos recurre a diferentes técnicas fraudulentas. Una de estas empresas dedicadas al *malware* (Crossrider) cambio de nombre (Kape Technologies) y empezó a comprar diferentes VPN: CYBERGHOST VPN, Zenmate, Private Internet Access e inclusive un sitio de review de VPN (MentorVPN) para su propia publicidad. Uno de sus fundadores fue condenado por

[138] Cuando se ejecuta un Javascript.
[139] Virtual Private Network. Crea un canal de comunicación cifrada.

estafas y figura en los Panamá papers, otro es un espía de la unidad 8200 (del IDF - Israel Defense Forces), mientas que su CEO fue capitán de las fuerzas Israelitas y ministro de Fianzas (Hodge, 2020; Brewster, 2015; s.n., 2021).

DNS, eMail y Browser.

La utilización de DNS puede filtrar información sobre los sitios visitados. Google convenientemente ha creado sus propios servidores DNS. Ello posibilita la capacidad de redireccionar el tráfico y llevar a cabo ciertos ataques. Plataformas de correos otorgan al propietario la capacidad de lectura a los mismos y facilita la recuperación de accesos a otras plataformas (en caso de correo de recuperación claves). A su vez pueden ser una gran base de datos de claves. Por otro lado, ofrece un segundo factor para ser utilizado por otras plataformas. Asimismo, Google ha creado su propio navegador con funciones para sincronizar datos y credenciales a través de su nube. Funciones como autocompletar, búsquedas, páginas visitadas, estadísticas de uso y notificación de contraseñas expuestas (otorgando acceso al procesamiento de claves). Las corporaciones pueden recurrir a otras funcionalidades para acceder a la información, como ser: traducción, corrección o autocompletar (*Digital Candies to Enslave*).

Cursos y programas de intercambio.

Los cursos y programas de intercambio, del cual hemos adelantado sus componentes de propaganda e influencia; también presentan elementos de inteligencia. Indagar al personal militar en ejercicios, conocer los sistemas, capacidades y vulnerabilidades de los países aliados. En algunos casos, inclusive ganar acceso a los mismos.

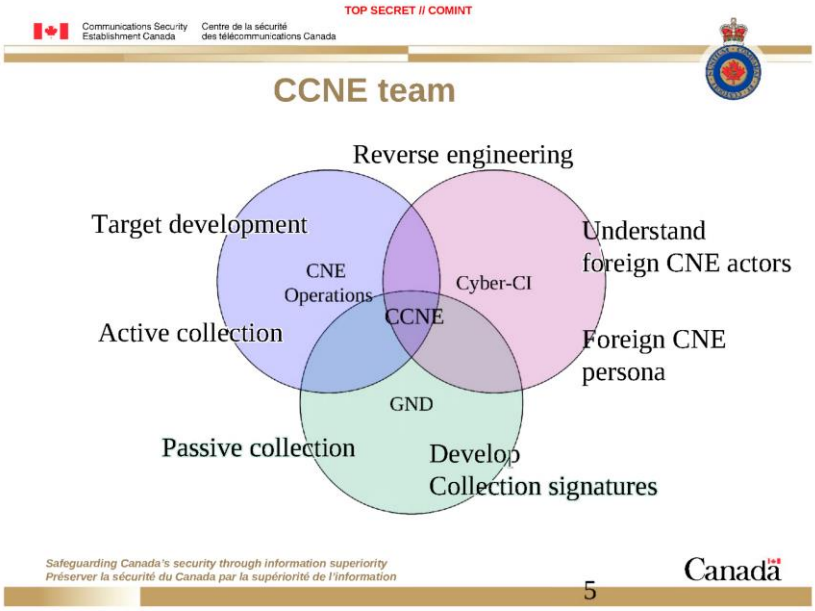
Acorde a (oficial de marina y director del ministerio de defensa[140], comunicación personal, 2022) en un reciente curso brindado al ministerio de seguridad, instructores norteamericanos indicaron a los funcionarios argentinos que debían llamarlos en caso de que un *malware* sofisticado impactara los sistemas argentinos, ya que ellos podían encargarse del asunto. Lo que resulta oportuno para obtener una imagen forense con información, ganar acceso a los sistemas, colocar implantes, conocer hasta qué punto el

[140] Fuentes reservadas. Ambas comunicaciones fueron aisladas y congruentes entre sí.

gobierno argentino detecta cyber armas y conseguir muestras de CNE para su estudio/comparación con actores conocidos (ver figura 88 y 89). Cabe aclarar que nuestro país cuenta con recursos sobrados para análisis e ingeniería inversa. Por otra parte; reportar o no una ciberintrusión puede depender de diferentes factores que involucren contrainteligencia, sistemas *sandbox* para monitorear / capturar ciberarmas o aprender de las tácticas / técnicas empleadas por los ciber atacantes, entre otros.

Figura 88

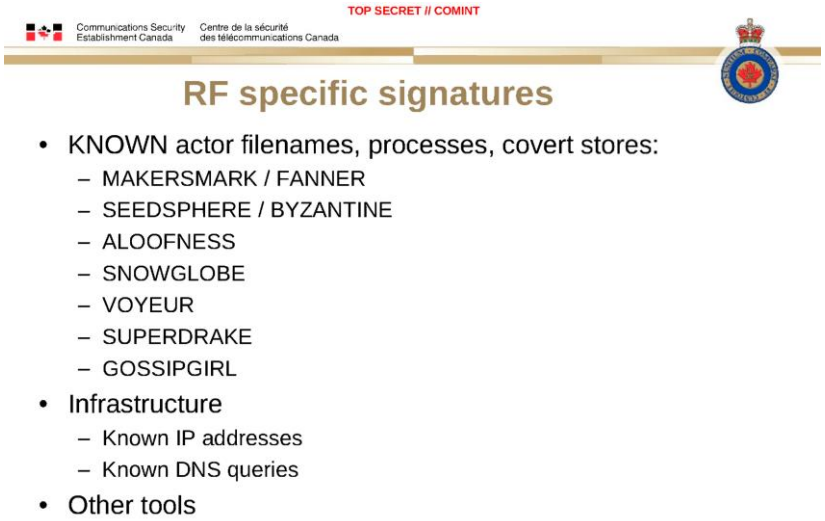
Pay attention to that man behind the curtain: iscovering aliens on CNE infrastructure.



Nota. Captura de presentación leak del FiveEyes demostrando el interés en la materia (Electronic Frontier Foundation, 2015).

Figura 89

Pay attention to that man behind the curtain: Discovering aliens on CNE infrastructure.



Nota. WARRIORPRIDE es una herramienta modular del FiveEyes, entre otras cosas, permite la adquisición de información que luego a partir de firmas (signatures) de la base REPLICANTFARM, identifica Threat Actors (Electronic Frontier Foundation, 2015).

La inteligencia no se limitada a sistemas. Por ejemplo, la colaboración de la DEA en la lucha contra el narcotráfico le permite conocer los puntos vulnerables en la frontera de nuestro país (utilizado para extracciones/ingresos, equipamiento de inteligencia). Según Buchanan (2020), la DEA es parte del aparato de espionaje de la NSA, explotando los accesos que por otra parte no tendrían. Trabajan en conjunto con las fuerzas de seguridad locales, colaboran con la instalación de equipamientos / sistemas para investigaciones y utilizan empresas privadas pantallas para dichos fines.

Software, Antivirus y telemetría.

Algunas funcionalidades genuinas en los sistemas de información, pueden ser una pantalla para el espionaje. Por ejemplo, la telemetría exfiltra datos por afuera del conocimiento / real entendimiento del usuario. En la actualidad, inclusive los autos incorporan telemetría. En casos más extremos, es posible encontrar micrófonos o cámaras ocultas en dispositivos. Tal es el caso del Nest Home Security de Google (Lee, 2019). En otras circunstancias, los micrófonos pueden estar a la vista bajo un pretexto, como ser la funcionalidad de dar órdenes de voz a un control remoto.

El caso del antivirus resulta controversial. Su naturaleza permite revisar el contenido completo de la computadora y crear una base de los documentos bajo su alcance. Desde la empresa de antivirus puedan husmear o exfiltrar archivos que consideren "sospechosos" para su análisis en el laboratorio. Dichas funciones suelen estar activas por defecto o estar camufladas con nombres confusos que no explican su función real al usuario. Por tales motivos resulta de alto interés tales empresas como pantalla o para ciber operaciones.

Hack.

El crecimiento de los dispositivos electrónicos, las telecomunicaciones e internet, resulta cada vez más tentador para los diferentes actores acceder al flujo de datos, ya sea de forma masiva o acotada a un objetivo.

Caso Pegasus Spyware

El spyware Pegasus de la firma NSO Group, vinculado a la Unit 8200 del Mossad de Israel (Brewster, 2016; Bergman y Mazzetti, 2023). Infecta los Smartphone sin necesidad de interactuar (Zero click) y es de difícil detección dado su sigilo. El *malware* permite al C&C operar el teléfono completamente de forma remota. Tiene la capacidad de prender la cámara, activar el micrófono, acceder a los mensajes, registro de llamadas, grabar llamadas, calendario, archivos / fotos, geolocalización, modificar la configuración, ejecutar comandos, exfiltrar datos, entre otros (Marczak, Scott-Railton, McKune, Razzak, Deibert, 2018).

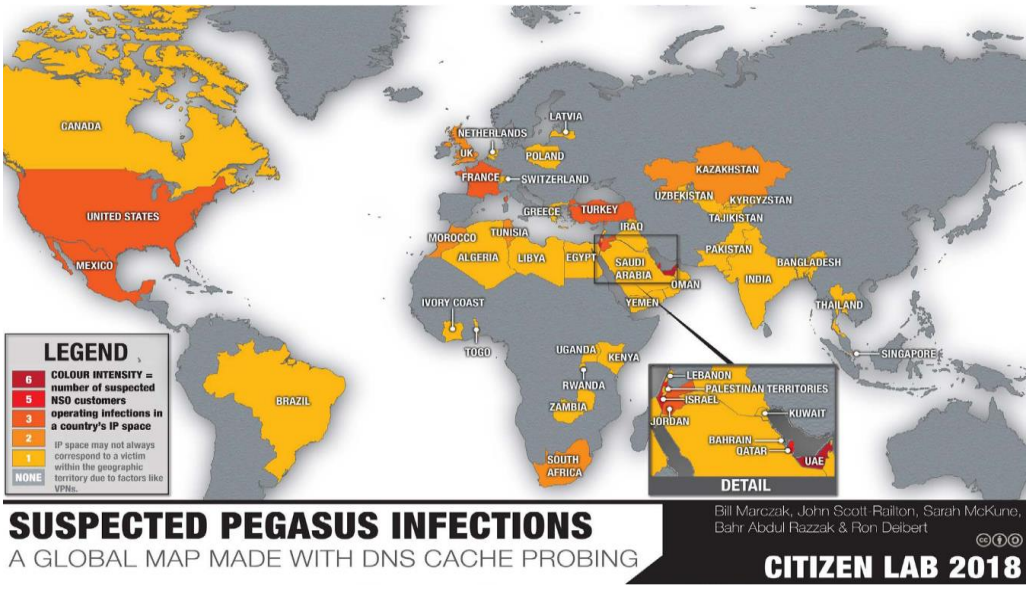
El vector de ataque ha ido cambiando a lo largo del tiempo y es diferente según la plataforma del teléfono objetivo (iOS, Android). Generalmente explota vulnerabilidades 0 day y ordena descarga el *payload* desde algún sitio de internet temporal utilizado para el deployment. Algunos ejemplos de vulnerabilidades son CVE-2016-4655 (information leak kernel), CVE-2016-4656 (corrupción de memoria kernel), CVE-2016-4657 (safari webkit) (Marczak, Scott-Railton, 2016) o más recientemente CVE-2019-3568 (buffer overflow en el VOIP stack de WhatsApp que permite la ejecución de código remoto) (Harán, 2019), CVE-2021-30860 (integer overflow que permite ejecución arbitraria desde un pdf armado para dicho fin) (Marczak, Scott-Railton, McKune, Razzak, Al-Jizawi, Anstis, Berdan, Deibert, 2021).

La funcionalidad pantalla para vender este *malware* es combatir el crimen y el terrorismo. La realidad, como es habitual, una historia muy diferente. Acorde al OCCRP (Organized Crime And Corruption Reporting Project), un leak de 50mil objetivos permitió identificar empresarios (ej. Jeff Bezos de Amazon o Pavel Durov de Telegram), realeza (ej. la princesa de Emiratos Árabes, el rey de Marruecos), activistas de derechos humanos, periodistas (ej. Cecilio Pineda asesinado), abogados/fiscales (ej. Xavier Olea Peláez que investiga el caso de Pineda), políticos/ministros/diplomáticos (ej. Presidente Emmanuel Macron de Francia; o el caso de los familiares, colaboradores y cardiólogo del presidente Manuel López Obrador de México), oficiales militares y académicos (OCCRP, s.f.) (ver figura 90).

El caso del periodista Cecilio Pineda, fue asesinado cuando denunciaba vinculaciones de la policía/políticos con el narcotráfico (Lakhani, 2021). Según Priest (2021), también la esposa del periodista Jamal Khashoggi asesinado en la embajada (ver capitulo anterior). Lo cual convierte a los responsables de Pegasus como participes necesario para la inteligencia previa a los asesinatos. ¿Combate o promueve al terrorismo / crimen?

Figura 90

Pegasus Infections.



Nota: (Marczak, Scott-Railton, McKune, Razzak, Deibert, 2018).

Otro spyware similar vinculado a Pegasus es Candiru que también fue utilizado contra periodistas. Ambas empresas fueron colocadas en lista de entidades (Malicious Cyber

Activities), lo que implica restricciones a las exportaciones. Por participar en actividades que son contrarias a la seguridad nacional o los intereses de la política exterior de los Estados Unidos y "atacar maliciosamente a funcionarios gubernamentales, periodistas, empresarios, activistas, académicos y trabajadores de embajadas" (U.S. Department of Commerce, 2021). Por otra parte, WhatsApp ha iniciado acciones legales también contra la empresa de Pegasus por explotar un bug de la mensajería de WhatsApp con la finalidad de instalar un *malware*.

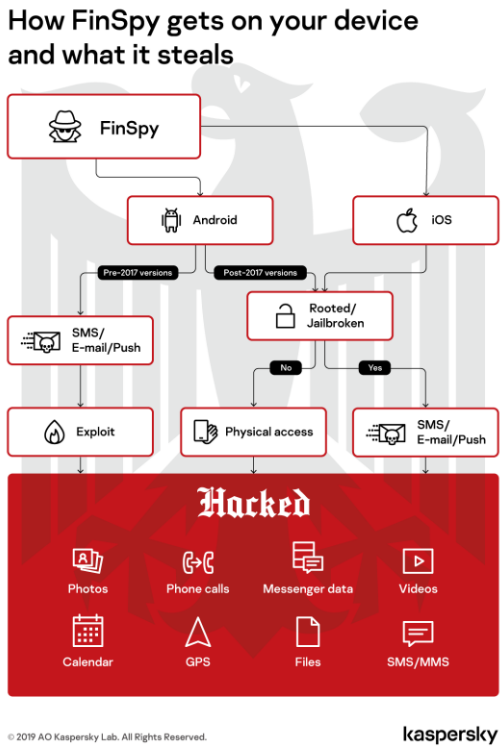
Remarcamos que tales exploits son ilegales bajo la legislación argentina (CPN), como así también en la mayoría de los países. La utilización de estos sobre ciudadanos de nuestro país es un atentado directo contra la soberanía y los derechos / garantías constitucionales de nuestro país. Además de los peligros implícitos sobre los proyectos estratégicos nacionales.

Caso FinFisher / FinSpy / Wingbird Spyware

Spyware modular de vigilancia de la firma Gamma Group (Alemania/Reino Unido) utilizado por gobiernos, similar al caso de Pegasus. Detectado operando desde al menos 2011. El mismo también fue utilizado en combinación con CobaltStrike en campañas por un grupo denominado NilePhish afectando algunas regiones de Medio Oriente. El *malware* ha sido estudiado en múltiples ocasiones por la firma Kaspersky como por Amnesty International, entre otros. Sus formas han ido evolucionando en el tiempo y los vectores de infección pueden variar; desde el proveedor de internet (ISP), troyanizando instaladores descargados/ataque cadena de suministro (patching por ejemplo de VLC, TeamViewer, etc.), sitios web visitados / Phishing o dispositivos desatendidos (ver figura 91, 92, 93 y 94) (Karpersky, 2019; Amnesty Internacional, 2020; Finfisher, 2014).

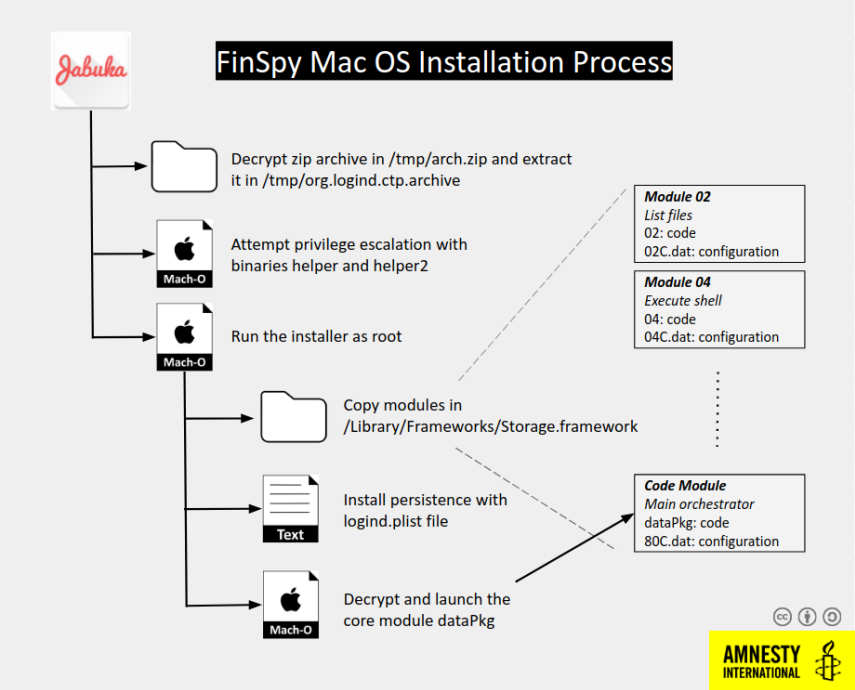
Puede infectar Smartphone con link de descarga (inclusive BlackBerry), Windows, MacOS y Linux (PDF con script/encoded binary). Además, tiene mecanismos para eludir antivirus. Como indica Perlroth (2012), la finalidad es la de perseguir el crimen, sin embargo, su uso consistió en perseguir disidentes políticos. Acorde a Amnesty International (2020), fue utilizado contra defensores de derechos humanos, incluyendo periodistas, activistas y opositores.

Figura 91
Finfisher Smartphone.



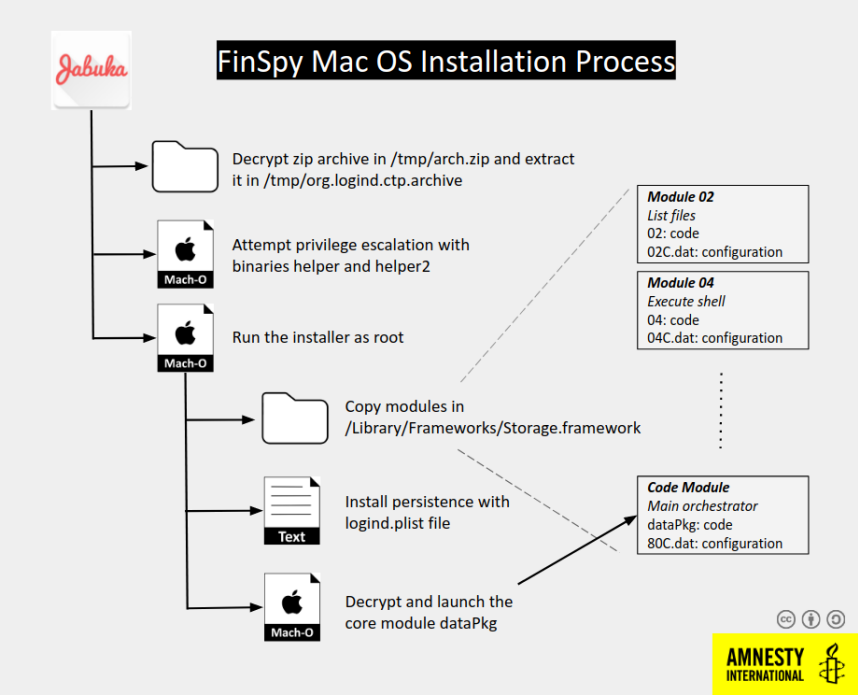
Nota: Kaspersky (2019).

Figura 92
Finfisher Brochure.



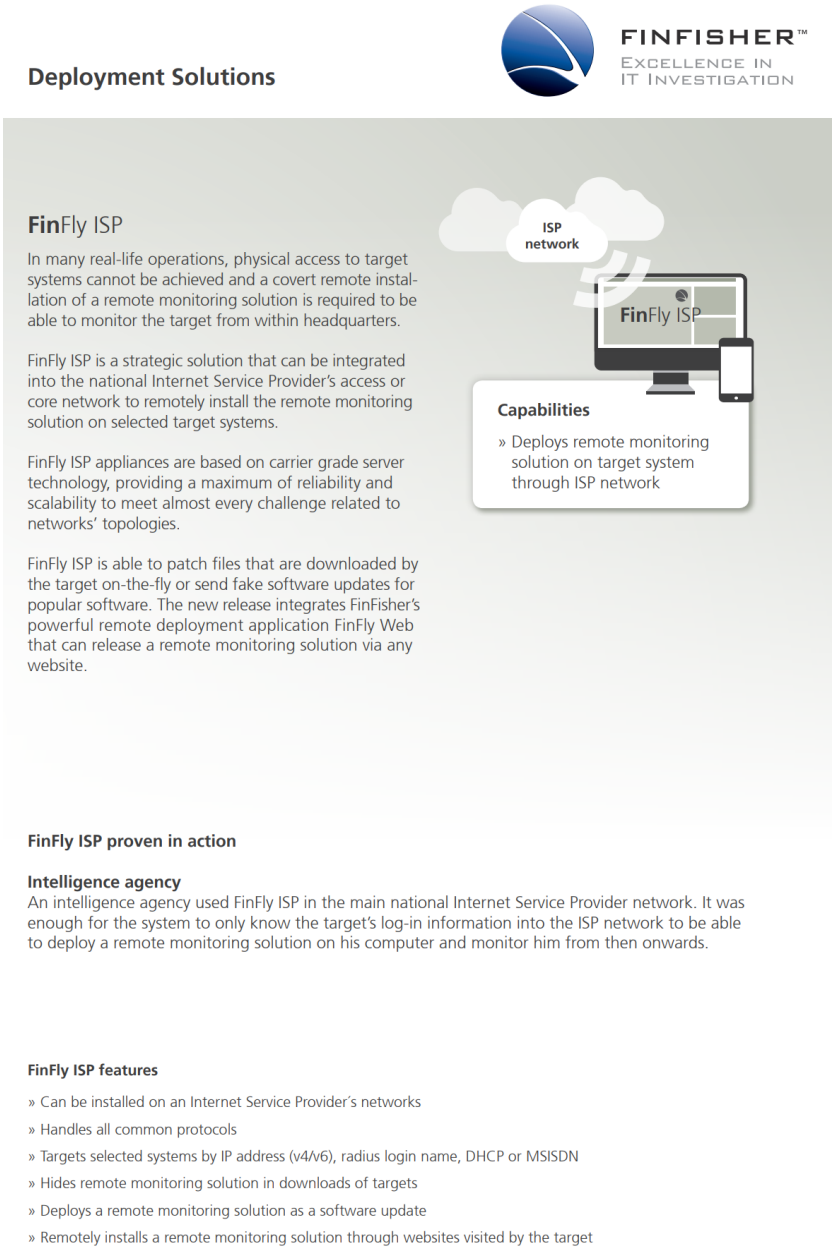
Nota: Amnesty International (2020).

Figura 93
Finfisher Brochure.



Nota: Amnesty International (2020).

Figura 94
Finfisher Brochure.



Deployment Solutions

FINFISHER™
EXCELLENCE IN IT INVESTIGATION

FinFly ISP

In many real-life operations, physical access to target systems cannot be achieved and a covert remote installation of a remote monitoring solution is required to be able to monitor the target from within headquarters.

FinFly ISP is a strategic solution that can be integrated into the national Internet Service Provider's access or core network to remotely install the remote monitoring solution on selected target systems.

FinFly ISP appliances are based on carrier grade server technology, providing a maximum of reliability and scalability to meet almost every challenge related to networks' topologies.

FinFly ISP is able to patch files that are downloaded by the target on-the-fly or send fake software updates for popular software. The new release integrates FinFisher's powerful remote deployment application FinFly Web that can release a remote monitoring solution via any website.

FinFly ISP proven in action

Intelligence agency
An intelligence agency used FinFly ISP in the main national Internet Service Provider network. It was enough for the system to only know the target's log-in information into the ISP network to be able to deploy a remote monitoring solution on his computer and monitor him from then onwards.

FinFly ISP features

» Can be installed on an Internet Service Provider´s networks
» Handles all common protocols
» Targets selected systems by IP address (v4/v6), radius login name, DHCP or MSISDN
» Hides remote monitoring solution in downloads of targets
» Deploys a remote monitoring solution as a software update
» Remotely installs a remote monitoring solution through websites visited by the target

Nota: Finfisher (2014).

Acorde a SecureList (2021), las capacidades son captura / grabación de pantalla, grabar charlas, activación de cámara / micrófono, *keylogger*, escuchar charlas VOIP, extraer correos electrónicos, capturar conversaciones de todo tipo de mensajerías (Telegram, Signal, Threema), capturar contactos, geolocalización, interceptar certificados/claves de

cifrado (incluyendo GPG/PGP), supervisar redes WIFI, grabar archivos en dispositivos extraíbles, descargar y ejecutar herramientas forenses.

La infección y operación puede variar según la plataforma, de forma genérica la primera descarga es un droper que descarga las posteriores etapas incluyendo el *payload*. Tiene persistencia a modo de bootkit (UEFI o MBR) para cargar antes del OS y ganar persistencia en el Kernel. El *malware* oculta sus archivos en un sistema de archivos virtuales cifrado (RC4) y es operado desde un C&C (Kaspersky, 2019).

A lo largo del trabajo continuaremos ampliando la inteligencia a partir del hacking sobre los sistemas y las comunicaciones.

Hack^2 = hack the hacker.

Las agencias de inteligencia tienen un gran interés en hackear a los hackers, en particular a los APT financiados por otros estados. De esta manera pueden obtener fingerprints, aprender sus tácticas, obtener ciberarmas o incluso sacar provecho de sus víctimas hackeadas. Según cuenta Buchanan (2020), la NSA logró ingresar a una máquina que pívot que utilizaban hackers chinos mientas espiaban los franceses, de esa manera la NSA obtuvo documentos de Francia.

Acorde a Greenwald (2015), el Government Communications Headquarters de Reino Unido (GCHQ) y la NSA de EEUU, vigilan a los hackers para aprender de sus técnicas y acceder a los datos que estos roban (incluyendo emails). Además, GCHQ creó un programa llamado LOVELY HORSE para monitorear las discusiones de hacker en las redes sociales junto a investigadores de la seguridad informática (entre ello, los investigadores de vulnerabilidades de Google Project Zero).

Caso Operación ARROW ECLIPSE

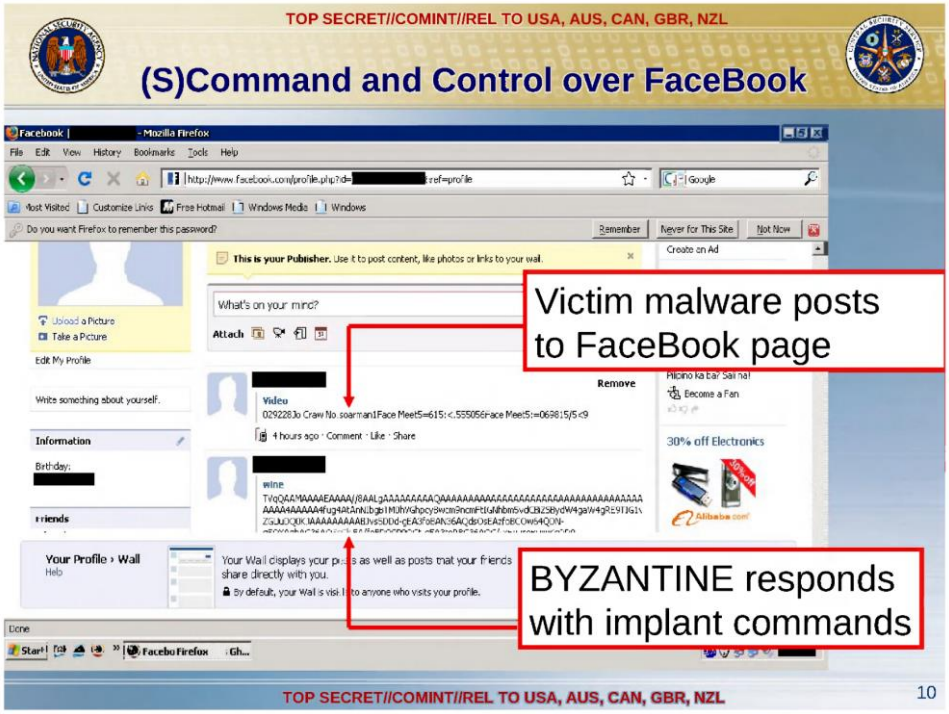
Consistió en una ciber operación de contrainteligencia del grupo TAO de la NSA. El mismo originado contra el grupo BYZANTINE CANDOR cuyos objetivos eran espionaje en el Department Of Defense y acuerdos económicos vinculados al petróleo. Se trata de un subgrupo de BYZANTINE HADES (CNE chino). Dicho grupo de hacker utilizaban spear phishing como vector de ataque. Para ocultar su atribución previamente comprometían computadoras más fáciles de atacar utilizadas como Hop Point (máquinas pívot) y la

comunicación hacia el C2C se realizaba mediante post ilegibles en una página de Facebook (ver figura 95) (Buchanan, 2020; Appelbaum, Gibson, Guarnieri, Müller-Maguhn, Poitras, Rosenbach, Ryge, Schmundt y Sontheimer, 2015).

Según revelaciones de Snowden, la operación Arrow Eclipse consistió en comprometer las máquinas Hop Point para espiar a los hackers en su operación. Además, se realizó una explotación de los routers del ISP para obtener la información previa de los actores, lo que llevó a encontrar al PLA[141] (Appelbaum et al., 2015).

Figura 95

C2C a través de Facebook.



Nota: Post ilegibles para la comunicación con el C2C[142] (Appelbaum et al., 2015).

Cámaras de vigilancia.

Cuando la gente se siente vigilada se comporta de forma diferente y por lo tanto desaparecen las libertades.



[141] People's Liberation Army de China.
[142] https://www.spiegel.de/media/1f958d98-0001-0014-0000-000000035686/media-35686.pdf

Las cámaras hoy en día se encuentran por todas partes: calles, empresas, edificios gubernamentales y militares. 54% por ciento de los mil millones de cámaras del mundo están ubicadas en China (ver figura 96). Sin tener en cuenta dicho país, las ciudades con mayor cantidad de cámaras por habitantes son: Indore, Hyderabad, Delhi, Chennai, Singapur, Moscú, Bagdad, Londres, San Petersburgo y Los Ángeles; mientras que las ciudades con mayor cantidad de cámaras por superficie: Delhi, Chennai, Singapur, Seúl, Moscú, Londres, Nueva York, Hyderabad, Bombay y México (Bischoff, 2022).

Figura 96

The most surveilled cities in the world.



Nota: Cámaras por cada 1000 habitantes (Bischoff, 2022).

La utilización de cámaras permite esclarecimiento de delitos, búsqueda de prófugos peligrosos, detección de personas en lugares no autorizados, entre otros fines. El efecto disuasivo es mencionado usualmente. Sin embargo, dicho efecto es relativo; un lugar con muchas cámaras implica la presencia de algo valioso, por ende, un incentivo para el delito.

Por otra parte, las cámaras poseen capacidades potenciadoras en las alturas, un espectro de frecuencias más amplio, capacidades de congelar o volver el tiempo atrás, hacer zoom (según óptica / resolución), entre otras. Registran de manera ilegal contraseñas de autenticación, patrones de desbloqueo de celulares, intervienen correos electrónicos en pantalla, capturan tarjetas de crédito, permiten replicar llaves físicas y convierte a simples operarios en administradores de todos los sistemas. También tienen la capacidad de hacer seguimiento a personas por tiempo completo, algo más típico de un estado policial que un

estado democrático. Cuando las personas son vigiladas no se comportan de la misma manera y condiciona la forma en que se desenvuelven; ello atenta contra las libertades constitucionales básicas. El condicionamiento está relacionado con el ejercicio del poder en el panóptico de Foucault (1975) y el efecto Hawthorne descripto por Landsberger (1958).

La inteligencia artificial es entrenada con las imágenes de las cámaras, para luego detectar patrones inusuales de comportamiento. Todo ciudadano que se comporte de forma diferente a la media queda bajo sospecha puede ser interceptado, cuestionado, etc (fase de adoctrinamiento). Nuevamente un concepto que atenta contra los principios y garantías constitucionales más básicos.

Además, las cámaras no dejan de ser sistemas y por ende son propensas a todo tipo de ataques. En particular atención, la cadena de suministro del software embebido (cerrado y llave en mano). En el caso de cámaras gubernamentales / militares, la presencia de *malware*, *backdoor* o vulnerabilidades resulta preocupante. Investigadores de la universidad de Ben-Gurion (Israel) demostraron que es posible enviar comandos a distancia, mediante pulsos infrarrojos, a un *malware*[143] presente en una cámara previamente infectada (Mordechai, Dima y Yuval, 2017). Una cámara puede deshabilitarse para llevar a cabo una operación y luego ser reactivada como si nada hubiera pasado. Por otro lado, el video puede ser manipulado inclusive en tiempo real. Como demuestran (Herling y Wolfgang, 2010), arbitrariamente es posible hacer desaparecer objetos de un video en tiempo real, aplicando un simple algoritmo[144] (ver figura 97).

El elemento eliminado podría ser una evidencia de una escena de un crimen. Esta misma operación bien podría realizarla un *malware* con capacidades de auto wiper (sin dejar rastros).

[143] Demo: https://www.youtube.com/watch?v=auoYKSzdOj4
[144] Demo: https://www.youtube.com/watch?v=FgTq-AgYlTE

Figura 97
Object Removal for Realizing Real-time Diminished Reality.



Nota: Permite desaparecer objetos en tiempo real (Herling y Wolfgang, 2010).

Cuando las cámaras se encuentran en lugares remotos, como ser el control vehicular, transmiten sus datos por redes inalámbricas o inclusive Internet. Además, pueden utilizar la nube para almacenamiento o procesamiento de datos, dando lugar a que los datos puedan ser interceptados y/o procesadas por personas no autorizadas o incluso otros gobiernos. De no contralar meticulosamente de ciberseguridad en toda la arquitectura, los vectores de ataque y accesos son múltiples. Siendo el estado anfitrión, facilitador para estados extranjeros (ataque *man in the middle*) a realizar un efectivo *lock and kill*. Recordemos que los patrones faciales de todos los argentinos quedaron expuestos y disponibles en la *Deep Web*.

Intercepción de correspondencias y mensajería.

Históricamente la intercepción de mensajería es como un deporte para los organismos de inteligencia. La oficina TAO (Tailored Access Operations) de la NSA utiliza una técnica llamada *interdiction* en la que, con ayuda del FBI y la CIA, interceptan compras online de notebook/hardware para colocar *malware* o implantes de hardware a fin de llevar a cabo operaciones de inteligencia sobre objetivos determinados (Spiegel Stuff, 2013). De forma similar se pueden llevar a cabo intercepciones en aeropuertos u otros lugares donde los equipajes tienen el pretexto de la seguridad para ser manipulados.

Para los gobiernos resulta crítico los procesos licitatorios de compra de equipamiento. La utilización de empresas pantallas podrían ser un vector de ataque para infiltrar mecanismos de espionaje en lugares estratégicos de la nación. Recordemos que los ataques a la cadena de suministro son de lo más peligrosos y difícil de controlar. Como apreciación personal, la asociación gobierno – corporación, podría ser un arma letal para dicho fin.

Los ataques también pueden llevarse a cabo contra un dispositivo *unattended* (cuando las personas dejan electrónicos fuera de la vista; en un hotel, locker, control de seguridad o cualquier escenario imaginable).

En relación con el grupo TAO, Matthew Aid comenta:

> Según exfuncionarios de la NSA, la misión de TAO es recopilar información de inteligencia sobre objetivos extranjeros mediante un sigiloso hacking (7x24hs) de sus computadoras y sistemas de telecomunicaciones, descifrando contraseñas, comprometiendo los sistemas de seguridad informática que protegen la computadora objetivo, robando los datos almacenados en los discos duros de la computadora y luego copiando todos los mensajes y el tráfico de datos que pasan dentro de los sistemas de correo electrónico y mensajes de texto específicos (CNE - explotación de la red informática) […] La sub unidad Telecommunications Network Technologies Branch (TNT) desarrolla las técnicas para ganar acceso a los sistemas y las redes sin ser detectados […] La rama Access Technologies Operations incluye personal de la CIA y FBI para adquisición de inteligencia clandestina o colocar implantes de eavestropping en el extranjero (*off-net operations*)[…] TAO también es responsable de desarrollar la información que permitiría a los Estados Unidos destruir o dañar los sistemas informáticos y de telecomunicaciones extranjeros con un ataque cibernético si así lo ordena el presidente […] TAO se ha ganado la reputación de producir parte de la mejor inteligencia disponible para la comunidad de inteligencia de EE. UU. no solo sobre China, sino también sobre grupos terroristas extranjeros, actividades de espionaje realizadas contra Estados Unidos por parte de gobiernos extranjeros, misiles balísticos y armas de destrucción masiva en todo el mundo, y los últimos acontecimientos políticos, militares y económicos en todo el mundo (Aid, 2013) .

Tarjetas de crédito, consumo de energía y otros servicios.

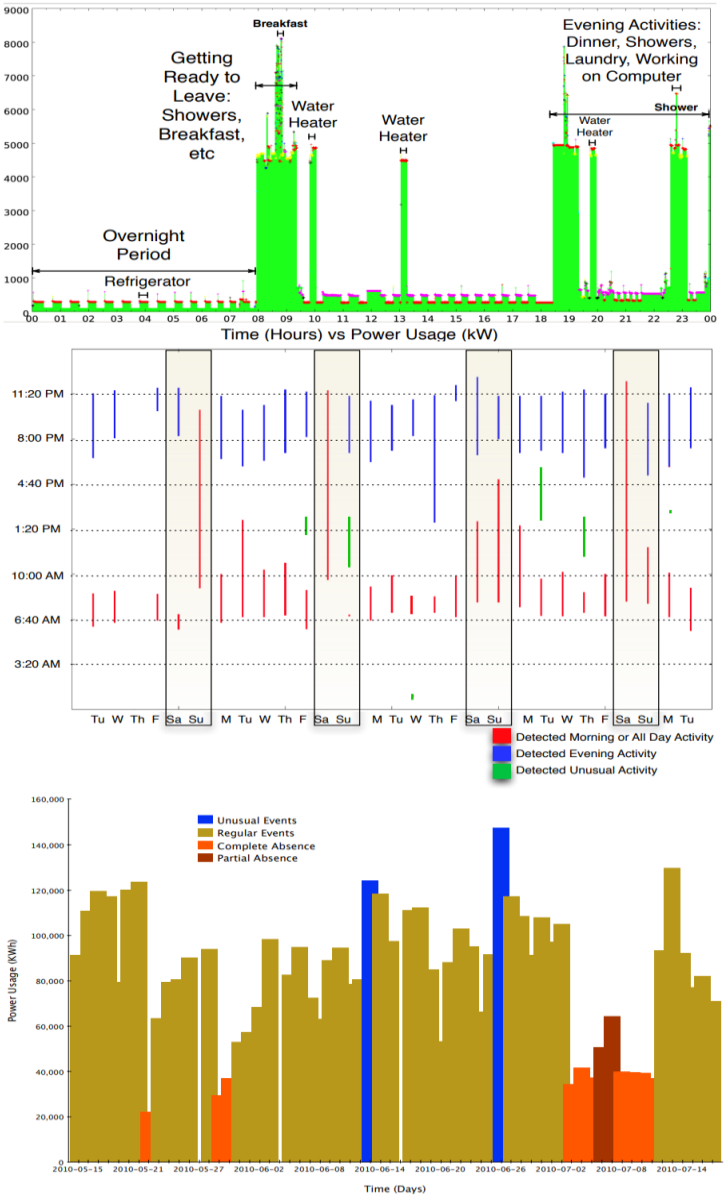
Los servicios utilizados también son fuente de inteligencia. Las tarjetas de crédito registran intereses, patrones de comportamiento, lugares habituales de intercepción, etc (alimentan operaciones, lock and kill, entre otros).

Los Smart meters (medidores inteligentes) de consumo de energía/agua son cada vez más frecuentes. Dado sus capacidades de telemetría y de desconexión remota; resultan indefectiblemente un vector de ataque, de impacto alto, que afecta a la disponibilidad y la privacidad masiva de los ciudadanos.

En relación con la privacidad, el análisis del consumo eléctrico permite identificar los patrones de comportamiento dentro de la propiedad (ver figura 98) (Molina-Markham, Shenoy, Fu, Cecchet, Irwin, 2010).

Figura 98

Patrones de comportamiento en Smart Meters.



Nota: Análisis diario, semanal y mensual (Molina-Markham, Shenoy, Fu, Cecchet, Irwin, 2010).

El análisis del consumo presenta una invasión no razonable a la privacidad, ya que permite determinar cuando una persona se encuentra ausente, durmiendo (vulnerable) o de vacaciones (operaciones de infiltración). Tener presente que en vez de un hogar podríamos estar hablando de un depósito de armamento, una oficina de proyectos estratégicos nacionales o cualquier otro escenario imaginable.

Con relación al tracking, otro ejemplo interesante que merece su atención es el heatmap creado a partir de los datos recolectados por la app de fitness Strava. La cual reveló movimientos de personal militar e inclusive la ubicación de bases secretas (Hern, 2018). Estas son solo algunos riesgos de las aplicaciones/juegos/OS utilizados en la actualidad que tienen la capacidad de recolectar información de posicionamiento y la interconexión para enviar los datos lejos y fuera del awarenss del usuario.

USACORP agreement.

Utilizamos tecnología que realmente no conocemos en profundidad ni poseemos. Son esas tecnologías que nos poseen a nosotros.
Nos han robado la tecnología y nuestro futuro como sociedad.
(reflexión de elaboración propia)

El término es una propuesta de elaboración propia, basada en el concepto de una relación mutua entre el gobierno norteamericano y las empresas, en post de un beneficio mutuo. En teoría para proteger la sociedad, en la práctica para su detrimento. Para sustentar la idea podemos citar algunos ejemplos: la relación con AT&T en Titanpoint (Gallagher y Moltke, 2016), entre otros sitios, para intercepción de comunicaciones; vinculación con Western Union para intercepción de telégrafos (United States Senate, 1976); vinculación con Microsoft para recolección con sistema PRISM (Gellman y Poitras, 2013); o la vinculación de Motorola y SIMENS a través de Crypto AG/Minerva para afectar la cadena de suministro de productos de comunicaciones de cifrado para espionaje de otros países (Crypto Museum, s.f.). Estos casos, entre otros, son tratados más adelante. Sería irracional pensar que los gigantes tecnológicos estén exentos de dicho esquema, más teniendo en cuenta su importancia estratégica.

Acorde a (Nesbit, 2017); desde los 90, la US intelligence community (IC) está trabajando con Silicon Valley en un esfuerzo para rastrear a los ciudadanos en el ciberespacio; el estado de vigilancia masiva es posible a través de una colaboración pública-privada. La comunidad de inteligencia financió científicos y universitarios con el Massive Digital Data Systems (MDDS) project, a través de organizaciones como National Science Foundation (NSF) o DARPA (Defense Advanced Research Projects Agency).

Continua que su intención era rastrear grupos de personas de ideas afines a través de Internet e identificarlos a partir de las huellas digitales (Birds of a feather / pájaros del mismo plumaje); por ejemplo, grupos terroristas. Entre las becas otorgadas se encuentran las de Sergey Brin y Larry Page de la universidad de Stanford (futuros fundadores de Google); para elaborar una biblioteca digital masiva de internet (clasificar páginas web / seguimiento de consultas de usuarios). Concepto que terminó como el corazón de Google. Cuando se consulta a las empresas (Verizon, AT&T, Google, Facebook, Microsoft) al respecto, responden que no brindan información deliberada; sino basadas en la ley Patriota. En la práctica, entre 2016 y 2017 se presentaron 260 mil solicitudes a Verizon, 250mil a AT&T y 24 mil a Google (Nesbit, 2017).

El poder dominante de las corporaciones.

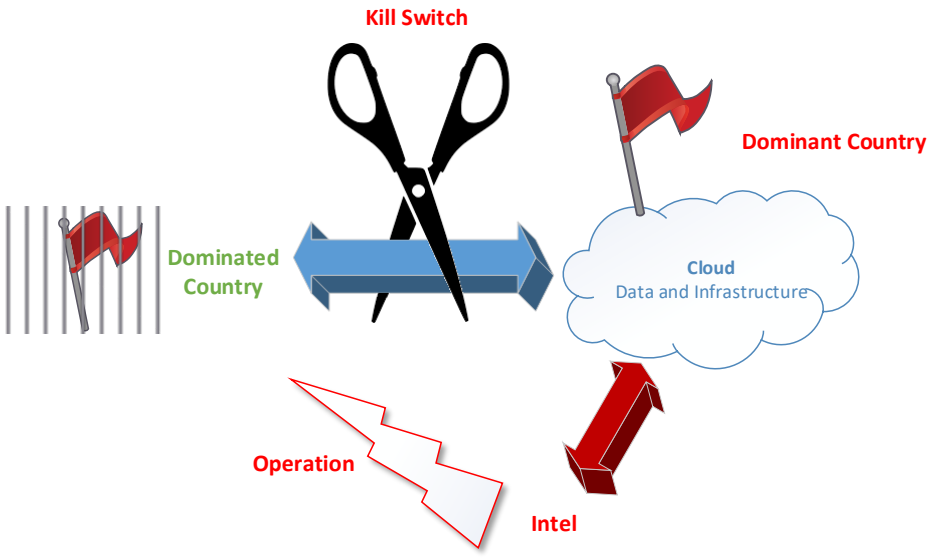
Los grandes gigantes de la industria tecnológica abusan de su posición dominante en los mercados. Sus productos ofrecen una funcionalidad para atraer victimas (*digital candies*) y, por otro lado, extraen datos fuera del awareness de las personas. Funciones habilitadas por defecto, difícil de conocer, entender y deshabilitar. Operan exactamente igual a un *malware* troyano con funciones de exfiltración. La única diferencia son los complejos contratos paraguas para cubrir sus operaciones. Como trata (Zuboff, 2019) dichos contratos son ambiguos y no explican cómo funcionan estas operaciones. Son amplios, variables en el tiempo y resultan imposibles de leer / seguir para un ciudadano (operan similar a una estafa).

En algunas situaciones, el usuario ni siquiera posee la capacidad de elección. Por ejemplo, un empleado que debe utilizar un software de comunicación elegido por la empresa donde trabaja. Los datos biométricos obtenidos (voz, reconocimiento facial, etc.) no son del empleador, sino del empleado; quien queda secuestrado en medio de la relación laboral. ¿Quién acepta el contrato? ¿Qué validez puede tener si es bajo usurpación?

Un software que lee todo lo que escribe el usuario, escucha lo que habla, posee funciones para exfiltrar credenciales de WIFI y obtiene inteligencia sobre el uso ¿es un *malware* o un OS? La tendencia actual es capturar tantos datos como sea posible, identificar unívocamente al usuario y fomentar los datos en la nube. El negocio son los datos. Todo pasa a la nube: infraestructura, safe de credenciales, gestión de identidades,

hasta equipos de red virtualizados junto a sus configuraciones. El poder del proveedor sobre una nación pasa a ser infinito. Inclusive las llaves de cifrado quedan bajo su tutela. ¿Cuándo la velocidad de las comunicaciones sea lo suficientemente alta, pasaremos a un esquema de terminales tontas y el procesamiento de nuestros dispositivos sucederá en la nube? ¿Qué pasa cuando el gobierno y las empresas acuerdan un mismo fin en común? Hay que ser muy ingenuo para no darse cuenta lo que está sucediendo[145] (ver figura 99).

Figura 99
Cloud supremacy.



Nota. El país dominante tiene control total sobre el país dominado[146] (concepto de infrastructure kill) (fuente: elaboración propia).

En algunos casos es el estado mismo quien utiliza la nube extranjera para almacenar datos. En otras ocasiones, obliga a utilizar mensajerías específicas de comunicación como ser WhatsApp para realizar trámites (ejemplo consulta de resultados COVID). ¿Qué pasa cuando es el estado es facilitador y partícipe necesario? ¿quién ayuda con el colonialismo

[145] Parafraseando una frase de Zuboff en un contexto diferente.
[146] Aclaración con relación al diagrama. Hoy en día, los datacenter en la nube ya no residen en su país matriz, sino que están distribuidos por el mundo para garantizar latencia. En otros casos, como China, se exige que los mismos se encuentren dentro del mismo país. Aun así, tales empresas tienen un poder absoluto sobre los datos. En el caso de las empresas norteamericanas, deben responder a leyes como la ley patriota. Los datos, así mismo, pueden utilizarse para entrenar tecnologías exponenciales como la IA sin el conocimiento del dueño de los datos.

tecnológico enfocado a la dominación? ¿existen acuerdos secretos? ¿por qué se favorece a una empresa y no a otras? ¿existe una licitación pública? (ver figura 100).

Existe una penetración de la dominación tecnológica (tratada en el capítulo anterior) en diferentes ámbitos incluyendo las comunicaciones. Por ejemplo, para realizar el trámite de solicitud de partidas de nacimiento del gobierno de la ciudad, exige un mail de las plataformas norteamericanas. Facilitando la exfiltración de datos de ciudadanos y fomentando la utilización de dichas plataformas. La coacción obliga a la víctima a crear un mail para poder realizar el trámite necesario.

Con relación a las comunicaciones, son los mismos funcionarios públicos / fuerzas de seguridad que utilizan plataformas y mensajerías inseguras como WhatsApp para tratar temas estratégicos o inclusive de seguridad nacional.

Figura 100

Captura pantalla del gobierno de la ciudad de Buenos Aires. Estado como facilitador.



Nota. No existe una explicación técnica justificable. La única explicación razonable es suponer la connivencia con dichas empresas / gobiernos (captura de pantalla, elaboración propia). De forma análoga, podemos mencionar los tramites que solo pueden realizarse vía WhatsApp y no por otras mensajerías como Telegram.

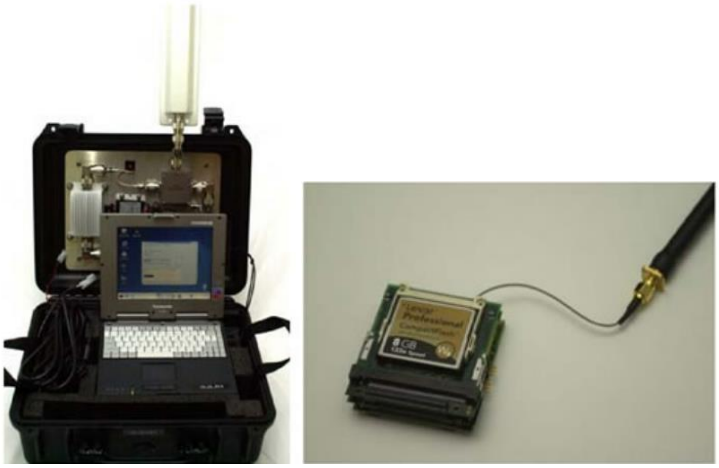
Filtraciones ANT catalog (leak).

Publicado por Der Spiegel en 2013. Corresponde un leak de un catálogo de herramientas de espionaje del 2008/09. Se trata de herramientas utilizadas por la unidad Tailored Access Operations (TAO) de la NSA (Appelbaum, Horchert y Stöcker, 2013). La

fuente del leak es desconocida. Mencionamos a continuación algunos implantes con una breve descripción a modo de reseña histórica (Appelbaum, Horchert y Stöcker, 2013):

- JETPLOW: *Firmaware* con *backdoor* para Routers y Firewall Cisco (PIX y ASA). C&C y Exfiltración. Similarmente FEEDTROUGH para firewall Juniper Netscreen. Ambos operan a nivel OS y pueden usarte con implantes como BANANAGLEE (*covert channel commnunications*). Ambos implantes ampliamente desplegados en objetivos, similar al GOUMETTROUGH y SOUFFLETROUGH (Juniper Firewalls). HALLUXWATER es un *Backdoor* que afecta los Eudemon firewalll de Huawei.
- DEITYBOUNCE: *Backdoor* que requiere la infección BIOS vía USB en servidores Dell PowerEdge. requiere *interdiction*. IRONCHEF es similar, pero para los Proliant de Hewlett Packard.
- HEADWATER: *Backdoor* para routers Huawei. Permite ejecutar funcionalidades de forma remota. Junto a HAMMERMILL permite la inspección de paquetes IP. SCHOOLMONTANA afecta los router Juniper-J a nivel OS, mientras que SIERRAMONTANA a los Juniper-M y STUCCOMONTANA a Juniper-T.
- NIGHTSTAND: Herramienta de inyección y explotación de redes Wireless y antiguos Windows XP (ver figura 101). SPARROW III es un sistema para el mapeo de redes Wireless que puede ser montado en un *drone* (UAV).

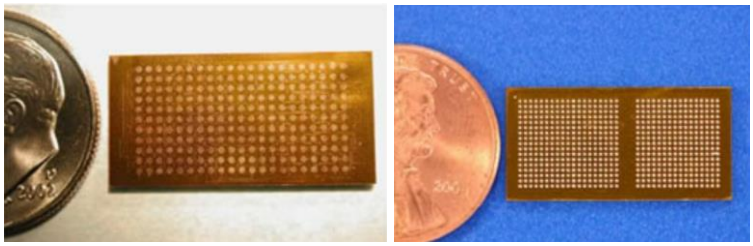
Figura 101
NIGHTSTAND y SPARROW III.



Nota. Para redes Wireless 802.11 (Appelbaum, Horchert y Stöcker, 2013).

- BULLDOZER es un implante PCI que junto a al implante de software KONGUR permite realizar CNE de un objetivo. GINSU es un software permite restablecer KONGU si fue removido.
- IRATEMONK: Implante para firmware de discos rígidos (Western Digital, Maxtor, Seagate y Samsung) que afecta el MBR para luego lograr acceso durante el boot. SWAP es un implante de BIOS de PC que permite control remoto en diferentes OS (Windows, FreeBSD, Linux, Solaris). WISTFULTOLL es un plug-in que permite recuperar información forense mediante Windows Management Instrumentation (WMI) call.
- HOWLERMONKEY: Implante de radiofrecuencia para ex filtración de información. Se combina con otras herramientas. SOMBERKNAVE es un implante para Windows XP que utiliza interfaces Wireless sin uso para *exfiltrar* información a través de algún *Access Point* que encuentre disponible.
- JINUORMINT es un chip electrónico configurable que permite diversidad de usos (un mini controlador programable con memoria). Similarmente a MAESTRO-II y a TRINITY (ver figura 102).

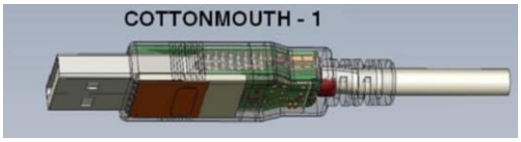
Figura 102
MAESTRO-II / TRINITY.



Nota. ARM7/9, flash, ASRAM y FPGA (Appelbaum, Horchert y Stöcker, 2013).

- COTTONMOUTH: Implante USB que permite inyección de troyanos (ver figura 103) con Wireless Bridge (command, infiltration y exfiltration). Otras versiones mejoradas son COTTONMOUTH II y COTTONMOUTH III. FIREWAKJ es un implante Ethernet o USB que permite recolección de trafico de red, inyección de paquetes y exfiltración de tráfico.

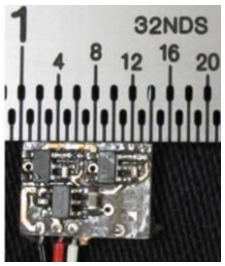
Figura 103
COTTONMOUTH.



Nota. (Appelbaum, Horchert y Stöcker, 2013).

- SURLYSPAWN: Implante de radiofrecuencia pasivo. Emite las teclas presionadas en un teclado. Es un radar retro reflector dado que solo es visible una vez que recibe una radio señal desde el exterior (ver figura 104).

Figura 104
SURLYSPAWN.



Nota. (Appelbaum, Horchert y Stöcker, 2013).

- DROPOUTJEEP: Implante de software para Apple iPhone (debe ser instalado), permite el control del Smartphone (extraer datos, contactos, SMS, geolocalización, acceso a micrófono/cámara, entre otros). La exfiltración es cifrada vía SMS o GPRS. En 2008 en estatus bajo desarrollo. GOPHERSET es un implante para SIM GSM que tiene funciones ocultas para extraer la libreta de direcciones, SMS y registros de llamadas. MONKEYCALENDAR es un software que envía geolocalización a través de SMS oculto. TOTECHASER es un implante para los teléfonos satelitales Thutaya 2520 que exfiltra datos desde el Windows CE a través de SMS ocultos. TOTEGHOSTLY 2.0 es un implante que permite control remoto total sobre teléfonos Windows (descarga o subida de datos, leer SMS, leer contactos, interceptar voice mails, geolocalización y prender la cámara/micrófono entre otras funciones). PICASSO es un auricular GSM recolecta información, locación, audio ambiente que permite exfiltración.
- RAGEMASTER: Implante de hardware que permite interceptar imágenes de un monitor. Usualmente instalado en el ferrito del cable VGA. Funciona de forma pasiva y refleja la señal de radar desde el exterior (exfiltración).

- CANDYGRAM: Simula una estación GSM y permite localizar al objetivo. Otros dispositivos que operan como estaciones son CYCLONE HX9 (*eavesdrop*), EBSR (GSM base transceiver), ENTOURAGE (*direction finding*), TYPHON HX (GSM base station), WATERWITCH (localización de handheld) y NEBULA (2G/3G base station). GENESIS es un Software Defined Radio disimulado en celular con capacidad de grabación de radiofrecuencias definidas (ver figura 105). CROSSBEAN es un GSM de notebook que permite intercepción de comunicaciones y acceso remoto.

Figura 105
CYCLONE HX9, GENESIS, ENTOURAGE, NEBULA y TYPHON HX.



Nota. (Appelbaum, Horchert y Stöcker, 2013).

Filtraciones Vault 7 (leak).

En 2017, WikiLeaks publicó una serie de documentos denominados Vault 7. Corresponden a un leak de las actividades de la CIA en ciberguerra y vigilancia. Aún se desconoce el origen / autenticidad de las filtraciones.

Las capacidades que van desde ganar acceso a TV inteligentes, navegadores web y diferentes sistemas operativos (OS, IOS, Android, Windows, MacOs, Linux). Los documentos indican la presencia de expertos en hacking en el consulado general de EEUU en Frankfurt, Alemania (Sontheimer, 2017). Además, los documentos indican el interés en comprometer automóviles. Las revelaciones no son significativas con relación a los *malware* modernos con persistencia en firmware y sigilo que iremos desarrollando a lo largo del trabajo. Aun así, vale una breve mención (Wikileaks, 2017):

- ExpressLane: mencionado en el apartado de infiltrados.

- Scribbles: Herramienta para marcar documentos como balizas (con la finalidad de detectar leaks). Al ser abiertos, una solicitud web revela la IP y otros datos del lector del documento. Hoy en día existen sitios gratuitos que ofrecen funcionalidades similares.
- Hive / Switchblade: Enmascaramiento de una interfaz HTTPS de cara al público utilizada por la CIA para transferir información de las computadoras de escritorio y teléfonos inteligentes infiltrados a través de *malware*. Utilizado para abrir los dispositivos y enviar comandos de los operadores de la CIA para ejecutar tareas específicas (como un C2C). Utiliza dominios públicos previniendo sospechas (similar a los *malware* modernos).
- AfterMidnight y Assassin: Dos *malware* que pueden ser controlados remotamente. Uno trabaja como DLL y el otro como servicio (entorno Windows). Athena y Hera son otros *malware* (atacan acceso remoto y Dnscache Service) en Windows 10 y Server 2012.
- Dark Matter: Intentos de acceso a iPhone y Mac. Incluye un *malware* (Sonic Screwdriver) para bypass de password de firmware.
- Marble: Técnicas de ofuscación de código de *malware*, enfocado en complicar las tareas de análisis. En referencia a lo que comentamos con anterioridad. Hoy en día, cualquier *malware* posee capacidades superiores; no solo ofuscación si no también cifrado, wiper, fileless, persistencia y técnicas para eludir antivirus, entre otros.
- Grasshopper: Framework para crear *malware* persistentes enfocados en eludir antivirus (Windows).
- Cherry Blossom: *Malware* de firmware de router WIFI. Lo transforma en un “FlyTrap” que se conecta con un C&C en internet y permite de manera remota monitorear el tráfico o inyectar *malware* en la máquina.
- Brutal Kangaroo: *Malware* con vector de ataque USB que explota una vulnerabilidad en Windows. Enfocado a redes air gap (recuerda a Stuxnet).
- OutlawCountry: Módulo de kernel Linux 2.6 que permite redirigir el tráfico saliente (mediante una tabla netfilter oculta) a un sitio especifico bajo el control de la agencia (infiltración/exfiltración).

- BothanSpy: Implante sobre el cliente SSH (Windows) para exfiltración de credenciales de autenticación. Gyrfalcon es similar, pero para cliente OpenSSH (Linux).
- Highrise: Aplicación (apk) de Android (4.0 a 4.3) que redirige SMS al atacante a través de TLS/SSL.
- Protego: Proyecto en PIC de sistema de control de misiles.
- Imperial: *Malware* Achilles (instalador en Mac), Aeris (POSIX) y SeaPea (OS X rootkit).
- CouchPotato: Herramienta para interceptor video streams (sistema previamente infectado).
- Dumbo (cámaras vigilancia): Software que debe ser previamente instalado. Permite deshabilitar cámaras y micrófonos de vigilancia, operados desde dicho sistema (Wired o Wireless). Además, el operador puede eliminar o manipular las grabaciones, agregar falsa evidencia. Se trata de apoyo a una operación del PAG (Physical Access Group).
- Weeping Angel (MI5/BTSS): Permite escuchar micrófonos / cámaras incorporados en los Smart TV Samsung serie F; inclusive cuando está apagado. La infección se realiza mediante USB, el audio se puede grabar (cifrado RCA) o escuchar en vivo. El acceso posterior es nuevamente vía USB o directamente remoto vía Wifi.

Caso hackeo de automóviles (Car hacking).

Las revelaciones de Wikileaks indican el interés de la agencia desde 2014 en infectar sistemas de control vehicular utilizados por autos o camiones. Según WikiLeaks (2017): "No se especifica el propósito de dicho control, pero permitiría a la CIA participar en asesinatos casi indetectables".

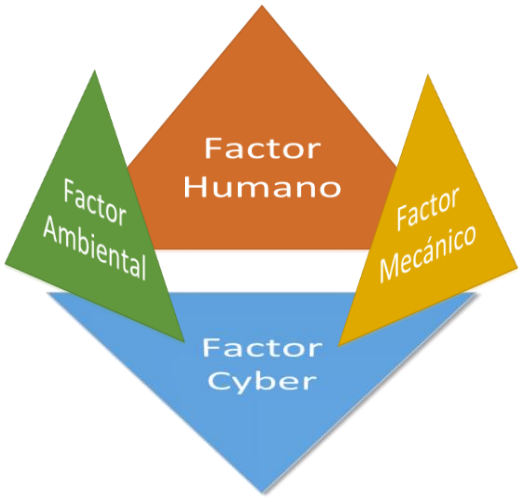
Según Miller y Valasek (2015), es técnicamente posible tomar el control de un vehículo de forma remota. También se han llevado a cabo demostraciones[147] de dichos ataques (Greenberg, 2015).

Un caso controversial es el misterioso accidente de tránsito que sufrió del periodista Michael Hastings cuando el Mercedes Benz que conducía aceleró a toda velocidad y se prendió fuego al impactar un árbol. El periodista se encontraba a punto de revelar

[147] Demo: https://www.youtube.com/watch?v=KG4F5xKqNf4.

información sobre el director de la CIA. Las revelaciones de Wikileaks incrementaron las teorías conspirativas respecto a dicho caso (The New Zealand Herald, 2017; Stebner, 2013). Richard Clarke (Former U.S. National Coordinator for Security, Infrastructure Protection, and Counter-terrorism) indicó: "consistente con un ataque cibernético a un automóvil" (como fue citado por Hogan, 2013). El fallecimiento del periodista (2013) fue previo al documento en cuestión (2014). Sin embargo, ello no evidencia que su auto no haya sido adulterado[148] o que se tratase de un *intimidation kill*. No es menester el presente trabajo profundizar en dicho caso. Aun así, resulta de interés resaltar los peligros y vulnerabilidades en los autos modernos. La incorporación de los factores cyber en accidentología vial (ver figura 106). Las afectaciones no son únicamente a vehículos. Una investigación de la universidad de Georgia basado en simulación demostró que tan solo basta con vulnerar el 20% de los vehículos de una ciudad para lograr un colapso total de la ciudad entera (Vivek, Yanni, Yunker y Silverberg, 2019).

Figura 106
Accidentología vial.



Nota: Imperioso la incorporación del aspecto ciber (fuente: elaboración propia).

[148] Un ataque podría parecer complejo, sin embargo, es posible conectar un dispositivo de bajo costo al puerto ODB2 y programarlo para enviar comandos de alta prioridad al CAN BUS del vehículo. El trigger podría ser un timmer o un módulo de WIFI remoto.

Caso Shadow Brokers (leak).

Según diferentes autores (Buchanan, 2020; Cunningham, 2020; MrSmith, 2016; entre otros) en 2016 surge un grupo denominado The Shadow Brokers quien subasta un set de ciberarmas de la NSA (Equation Group vinculado a TAO). El grupo de hackers indica que la NSA va a tener que pagar más que el resto si quieren prevenir la filtración. El nombre del grupo viene dado por un personaje del juego Mass Effect, siendo líder de una organización que vende información al mejor postor (Buchanan, 2020; Cunningham, 2020; MrSmith, 2016).

Continua con un contratista de la NSA (Hal Martins), envía desde una cuenta falsa de Twitter un mensaje a Kaspersky diciendo que quería hablar con Eugene Kaspersky. Luego envía otro mensaje que podría estar vinculado al caso: "vida útil, tres semanas". El FBI y el grupo SWAT allana la casa de Martin quien es arrestado gracias a la colaboración de Kaspersky. En la casa encuentran aproximadamente 50TB de información clasificada (Cunningham, 2020; Buchanan, 2020). Sin embargo, los mensajes de Shadow Broker siguen apareciendo. Shadow Broker filtra una lista de objetivos de la NSA incluyendo países aliados. Los países son: China, Japón, Corea del Sur, España, Alemania, India, Taiwán, México, Italia, Federación Rusa, Reino Unido, Pakistán, Suecia, Bangladesh, Macao, Arabia Saudita, Polonia, Tailandia, EE. UU., Finlandia, Irán, Países Bajos, Argentina, Bélgica , Brasil, Chile, Argelia, Egipto, Grecia, Turquía, Venezuela, Emiratos Árabes Unidos, Austria, Bolivia, Botswana, Chipre, Gabón, Bosnia y Herzegovina, Hungría, Jordania, Kenia, Sri Lanka, Namibia, Nicaragua, Noruega, Filipinas, Rumanía y la Unión Europea. Las herramientas incluyen *backdoor* en Windows, Linux, Solaris, routers, firewall, base de datos, celulares y telecom (DEWDROP, INCISION, JACKLADDER, ORANGUTAN, PATCHICILLIN, RETICULUM, SIDETRACK y STOICSURGEON) (MrSmith, 2016).

La subasta no resultó exitosa y Shadow Brokers se despide dejando un pequeño link para descargar 61 herramientas. En 2017 reaparece criticando a Trump por ordenar un ataque aéreo sobre una base en Siria, como represalia de un ataque químico de Siria, filtrando vulnerabilidades en Unix y Solaris. En este post, dejan la clave para descifrar los archivos de la primera subasta original (Cox, 2017). En primavera vuelven a publicar 23

herramientas adicionales (DANDERSPRITZ, ODDJOB, FUZZBUNCH, DARKPULSAR, ETERNALROMANCE, ETERNALBLUE, entre otros) (Cimpanu, 2017). Algunos fueron parcheados por Microsoft el mes previo, lo que generó cierta especulación. El post también reveló bancos objetivos en Qatar, Emiratos Árabes, Palestina, Kuwait y Yemen; incluyendo una lista de administradores de sistemas financieros. Posteriormente vuelven a brindan información sobre operaciones de la NSA contra sistemas bancarios y programas nucleares en Rusia, China, Irán y Corea del Norte (Buchanan, 2020).

En 2019, Hal Martin es sentenciado a 9 años de prisión por llevarse documentos secretos a su casa. Sin embargo, el misterio de Shadow Brokers sigue sin resolver (Vavra, 2019). Nghia Hoang Pho es otro contratista también sentenciado a prisión por razones similares (US Department of Justice, 2018).

Las hipótesis de atribución son diversas. Desde un mole (insider) en la NSA, vinculación con Snowden (los archivos llegan hasta 2013), colaboración de Martin, hack de inteligencia rusa, hack a la máquina de Martin o el antivirus Kaspersky en la máquina de Nghia Hoang Pho enviando archivos sospechosos al laboratorio de Kaspersky para su análisis. Según inteligencia israelí que hackeo Kaspersky, encontraron algunos archivos en el laboratorio. Según la firma, estos archivos habían sido destruidos al ser identificados como parte de la NSA. Kaspersky además indico que, según los logs el antivirus fue deshabilitado para instalar un crack con código malicioso de un office pirata y que hackers violaron la seguridad de la computadora de Pho en reiteradas oportunidades. No debe descartarse la posibilidad de deshonestos en Kaspersky o la intercepción en sus comunicaciones por terceros (Buchanan, 2020).

Independientemente de la atribución del caso, la NSA contaba con conocimiento de vulnerabilidades críticas. Esta información fue weaponizada en vez de informar a los vendedores para que pudieran resguardar la seguridad de sus ciudadanos. Las herramientas desarrolladas fueron utilizadas para operar de manera ilegal y sigilosa alrededor del mundo.

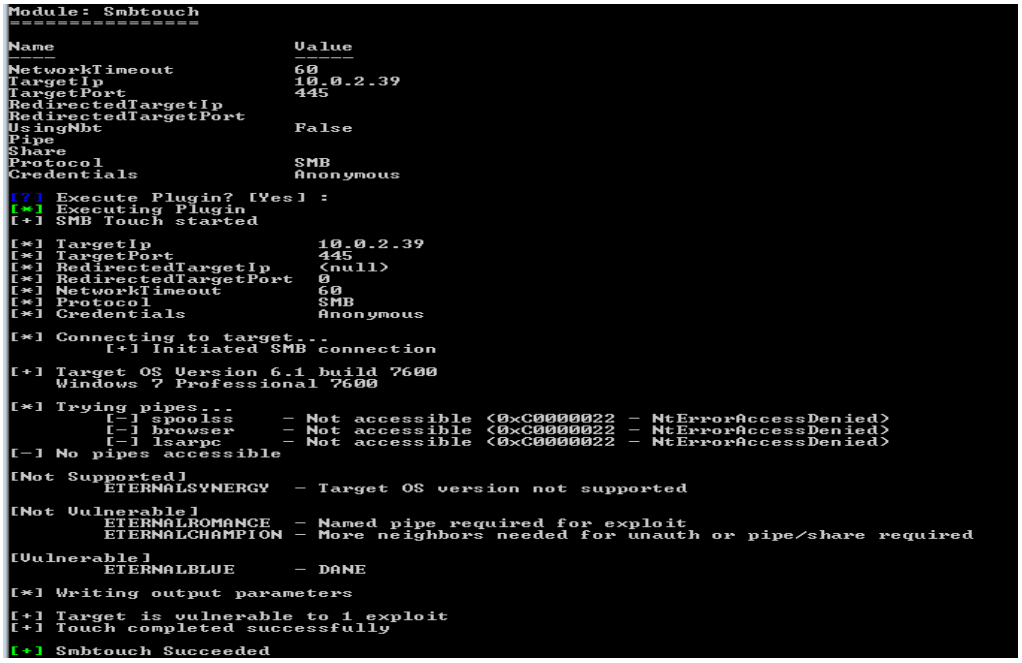
La filtración por otro lado tuvo un costo importante, no solo en la agencia si no en el mundo. Diferentes grupos de hacker tuvieron a disposición vulnerabilidades 0 day para utilizar. A continuación, mencionamos algunas herramientas con atención en el nivel de

poder, sofisticación y sigilo. Los archivos filtrados solo llegan hasta el 2013, con lo cual es razonable pensar que estas ciberarmas podrían haber mejorado de formas no reveladas.

Caso Fuzzbunch

Es un framework que escanea las vulnerabilidades de un objetivo y recomienda los posibles exploits a utilizar (ver figura 107).

Figura 107
Modulo SmbTouch.



Nota: Captura de ejemplo (Young, 2017).

Caso EternalBlue exploit

Es un exploit remoto de una vulnerabilidad 0 day (CVE-2017-0144)[149]. La vulnerabilidad básicamente es una mala implementación de Microsoft sobre el protocolo SMB (Server Message Block) (Shields, 2018).

Este poderoso exploit al poco tiempo de ser publicado fue waponizado por otros actores. En 2017 apareció el famoso WannaCry ransomware que cifraba el contenido de las máquinas y exigía dinero de rescate. El mismo causó grandes pérdidas de dinero (del orden de miles de millones). WannaCry es presumiblemente atribuido al Lazarus Group

[149] Vulnerabilidad CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144

(Lab 110) de Corea del Norte por similitud a otros ataques, huso horario de compilación y lenguaje coreano instalado, entre otros (Shields, 2018).

Posteriormente en 2017 surge otro ransomware llamado NotPetya. Consistió en una potente combinación entre el 0 day EternalBlue y el harvest de credenciales Mimikatz. En este caso los atacantes primero comprometieron la empresa ucraniana M.E. Doc que desarrolla un software impositivo. A su vez, esta empresa infectó a sus clientes a través de sus actualizaciones (ataque a la cadena de suministro); incluyendo hospitales, compañías eléctricas, aeropuertos, bancos, cajeros y entidades gubernamentales. El mismo se propago fuera de Ucrania a causa de su capacidad de infección. Dentro de los afectados se encontraba la empresa Maersk que tuvo que bloquear todas sus actividades de distribución de contenedores en todo el mundo por no poder acceder al sistema e identificar los destinos de sus contenedores. Maersk no podía recuperar sus backups debido a que la infección afectó a todos los Domain Controllers. Pudo sobrevivir de milagro dado que una oficina en Ghana que contenía un Domain Controller había estado offline debido a un corte eléctrico. Desde allí viajaron en avión con el disco en mano hasta Nigeria y de allí a Reino Unido para restaurar la infraestructura (este pasa manos fue debido a que en Ghana no tenían Visa para viajar directo a Reino Unido). Según investigaciones posteriores, se supo que la installation key ID (que debían entregar las victimas a los atacantes luego de pagar el rescate) era generado aleatoriamente y no había manera de que los atacantes pudieran recuperar el cifrado. El *malware* fue diseñado para causar daño. Este *malware* se atribuye al grupo Sandworm / GRU de Rusia (Greenberg, 2019). Como es habitual, la atribución de ambos casos mencionados fue negada.

Caso Double pulsar Backdoor

Backdoor fileless que permite ejecutar shellcode, dll, ejecutable, etc. Opera a nivel Kernel de forma sigilosa y sus comandos son: Ping, Kill, Exec (Vu, 2019; s.n., 2017).

Caso PaddleCheap Implant

Implante persistente que permite la comunicación con el C&C y la ejecución de comandos. Tiene funciones de escucha de puertos, horarios específicos o Port Knocking. Esto último es una especie de handshake secreto basado en combinación de secuencias /

protocolos / tiempos / origen /entre otros, sobre los puertos cerrados. En caso de ser correcto, abre el puerto en cuestión para la comunicación. El implante también puede llamar a hora especifica o trabajar con un proxy presente (con la captura de credenciales del sistema). La comunicación y cualquier archivo almacenado es cifrado con un par de llaves únicas para la operación. Los tipos de persistencia son AppCompat, WinsockHelper y KillSuit (modular y con plugins como keylogger o tráfico de red). Los métodos de este último son: Driver, SOTI (SolarTime) y JUVI (Donoso, 2017).

Solartime modifica el MBR para cargar un *kernel driver*. Utiliza TrueType font files (TTF) genuinos para almacenar en al final de ellos el *driver* de kernel cifrado. Al iniciar la PC carga el MBR que buscar y descifra el *driver* oculto en el TTF y lo carga previo al kernel de Windows. Esta técnica no funciona con bitlocker o EFI (Donoso, 2017).

Caso DanderSpritz Framework

Según Donoso (2017), DanderSpritz (ver figura 108) es un framework modular post explotación, evolucionado de ExpandingPulley (2001). Es modular porque utiliza plugins fáciles de programar en Python (ej. modulo para password dump). Es post explotación porque previamente hay que comprometer al objetivo con los elementos antes mencionados (ver figura 109). DanderSpritz está desarrollado en JAVA desde al menos inicios del 2005 y en 2011 incorporo script de Python (plugins). La herramienta está diseñada con foco en el sigilo. Tiene un diseño Safety Handler para prevenir que los operadores no cometan errores (ejemplo, recomendar no ejecutar un comando que pueda poner en peligro la operación). DanderSprintz contiene funciones de persistencia, movimiento lateral, búsqueda de archivos incluyendo su exfiltración sigilosa y finalmente una para finalizar eliminando los rastros (quit and delete).

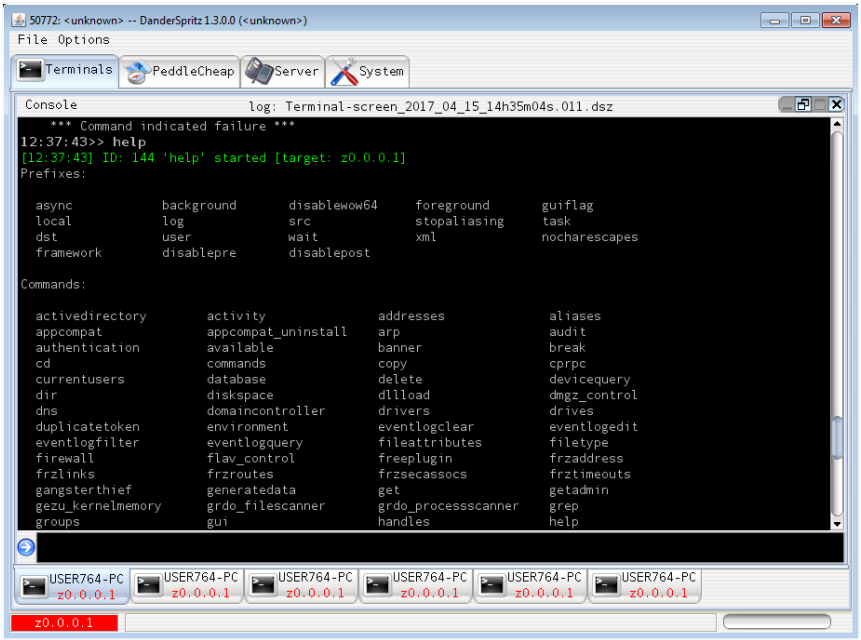
Continua con que cada operación posee una llave publica privada para el canal de comunicación y un repositorio donde almacena toda la información extraída del objetivo. Además de funciones de correlación entre targets de una operación. Incluye una función para almacenar notas (reporte) y otra para replay que permite observar los comandos y resultados ejecutados (presumiblemente para entrenamiento basado en casos de éxitos).

Como relata, la herramienta apenas conecta con un target (victima), ejecuta una recolección de información para inteligencia (Survey.py). Entre los datos obtenidos:

Operating System info, network info, mounted drives, running process (ver figura 110), services, *driver* (ver figura 111), persistencia de otros *malware* (si los hay) (ver figura 112), audit/log config (para Safety Handler), scheduled tasks, archivos recientemente modificados, dispositivos USB recientes, software instalado, protección de antivirus (ver figura 113) y passwords dump. Para saber si otro estado nación afecto previamente el target existe un archivo de firmas (sigs.py) que es algo así como patrones o indicadores de compromiso para decirlo de algún modo. Posteriormente, el operador puede lanzar una serie de operaciones a su disposición.

Figura 108

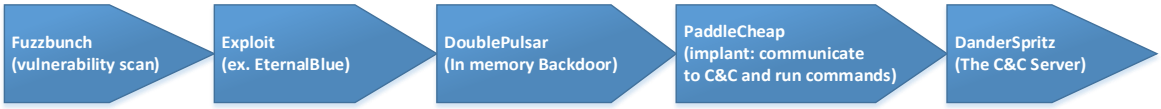
DanderSpritz Frameworks.



Nota: Herramienta modular de post explotación utilizada por Equation Group.

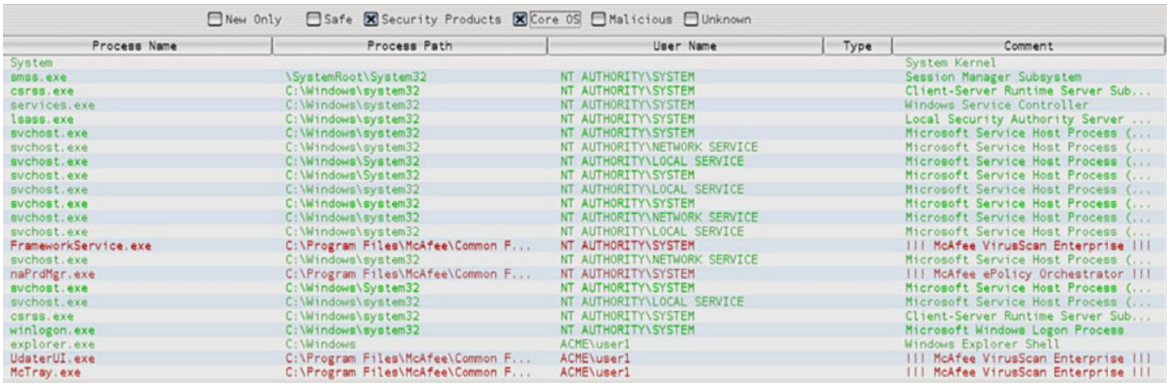
Figura 109

Equation Group Operation Chain.



Nota: Basado en el estudio de Donoso (2017) sobre el leak de ShadowBrokers.

Figura 110
Process List.

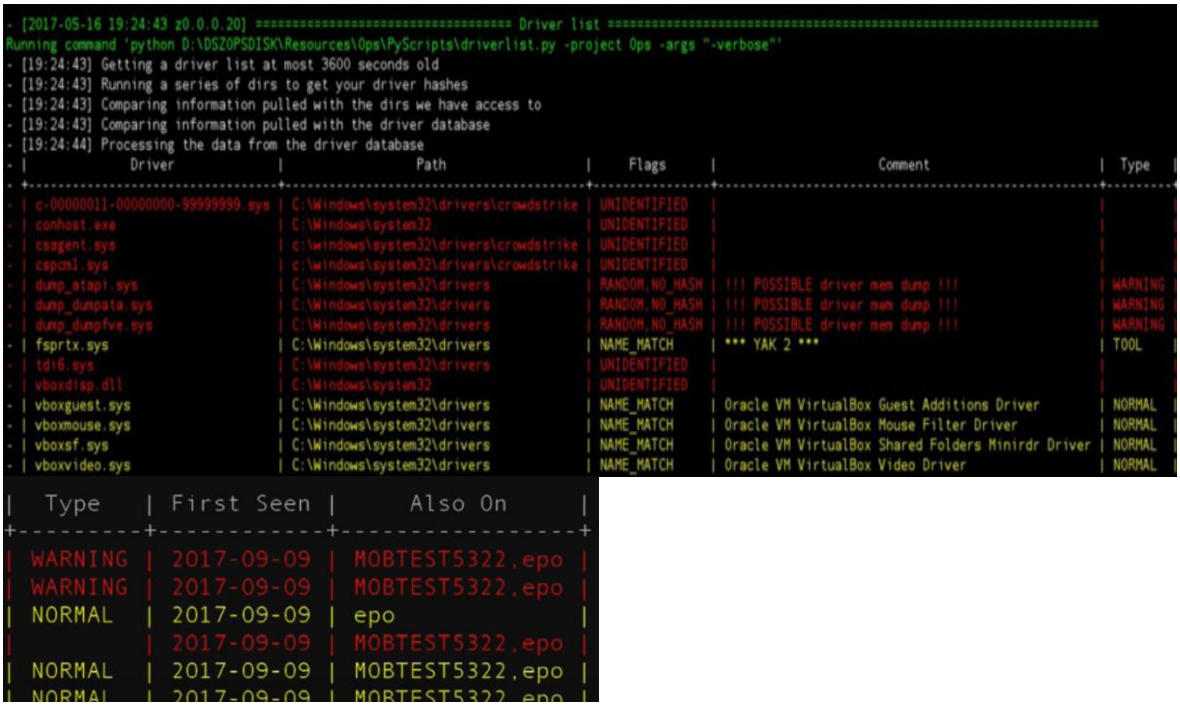


New Only | Safe | Security Products | Core OS | Malicious | Unknown

Process Name	Process Path	User Name	Type	Comment
System				System Kernel
smss.exe	\SystemRoot\System32	NT AUTHORITY\SYSTEM		Session Manager Subsystem
csrss.exe	C:\Windows\system32	NT AUTHORITY\SYSTEM		Client-Server Runtime Server Sub...
services.exe	C:\Windows\system32	NT AUTHORITY\SYSTEM		Windows Service Controller
lsass.exe	C:\Windows\system32	NT AUTHORITY\SYSTEM		Local Security Authority Server ...
svchost.exe	C:\Windows\system32	NT AUTHORITY\SYSTEM		Microsoft Service Host Process (...
svchost.exe	C:\Windows\system32	NT AUTHORITY\NETWORK SERVICE		Microsoft Service Host Process (...
svchost.exe	C:\Windows\System32	NT AUTHORITY\LOCAL SERVICE		Microsoft Service Host Process (...
svchost.exe	C:\Windows\System32	NT AUTHORITY\SYSTEM		Microsoft Service Host Process (...
svchost.exe	C:\Windows\system32	NT AUTHORITY\LOCAL SERVICE		Microsoft Service Host Process (...
svchost.exe	C:\Windows\system32	NT AUTHORITY\SYSTEM		Microsoft Service Host Process (...
svchost.exe	C:\Windows\system32	NT AUTHORITY\NETWORK SERVICE		Microsoft Service Host Process (...
svchost.exe	C:\Windows\system32	NT AUTHORITY\LOCAL SERVICE		Microsoft Service Host Process (...
FrameworkService.exe	C:\Program Files\McAfee\Common F...	NT AUTHORITY\SYSTEM		!!! McAfee VirusScan Enterprise !!!
svchost.exe	C:\Windows\system32	NT AUTHORITY\NETWORK SERVICE		Microsoft Service Host Process (...
naPrdMgr.exe	C:\Program Files\McAfee\Common F...	NT AUTHORITY\SYSTEM		!!! McAfee ePolicy Orchestrator !!!
svchost.exe	C:\Windows\System32	NT AUTHORITY\SYSTEM		Microsoft Service Host Process (...
svchost.exe	C:\Windows\system32	NT AUTHORITY\LOCAL SERVICE		Microsoft Service Host Process (...
csrss.exe	C:\Windows\system32	NT AUTHORITY\SYSTEM		Client-Server Runtime Server Sub...
winlogon.exe	C:\Windows\system32	NT AUTHORITY\SYSTEM		Microsoft Windows Logon Process
explorer.exe	C:\Windows	ACME\user1		Windows Explorer Shell
UdaterUI.exe	C:\Program Files\McAfee\Common F...	ACME\user1		!!! McAfee VirusScan Enterprise !!!
McTray.exe	C:\Program Files\McAfee\Common F...	ACME\user1		!!! McAfee VirusScan Enterprise !!!

Nota: En color resalta los procesos conocidos de los antivirus (Donoso, 2017).

Figura 111
Driver List.

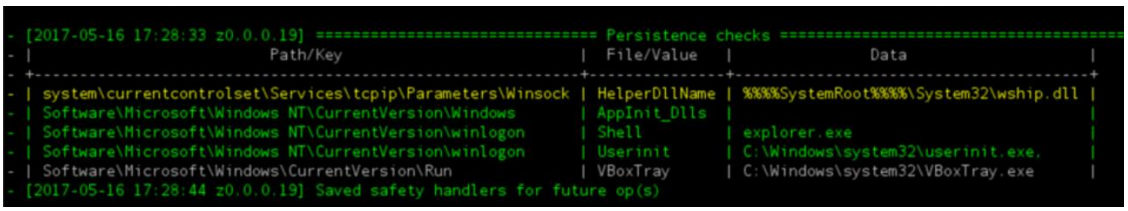


```
- [2017-05-16 19:24:43 z0.0.0.20] ============================== Driver list ==========================================================================
Running command 'python D:\DSZOPSDISK\Resources\Ops\PyScripts\driverlist.py -project Ops -args "-verbose"'
- [19:24:43] Getting a driver list at most 3600 seconds old
- [19:24:43] Running a series of dirs to get your driver hashes
- [19:24:43] Comparing information pulled with the dirs we have access to
- [19:24:43] Comparing information pulled with the driver database
- [19:24:44] Processing the data from the driver database
- |            Driver            |                Path                |     Flags     |                          Comment                          |  Type   |
- +------------------------------+------------------------------------+---------------+-----------------------------------------------------------+---------+
- | c-00000011-00000000-99999999.sys | C:\Windows\system32\drivers\crowdstrike | UNIDENTIFIED |                                                           |         |
- | conhost.exe                  | C:\Windows\system32                | UNIDENTIFIED  |                                                           |         |
- | csagent.sys                  | c:\windows\system32\drivers\crowdstrike | UNIDENTIFIED |                                                           |         |
- | cspcml.sys                   | c:\windows\system32\drivers\crowdstrike | UNIDENTIFIED |                                                           |         |
- | dump_atapi.sys               | C:\Windows\system32\drivers        | RANDOM,NO_HASH | !!! POSSIBLE driver mem dump !!!                          | WARNING |
- | dump_dumpata.sys             | C:\Windows\system32\drivers        | RANDOM,NO_HASH | !!! POSSIBLE driver mem dump !!!                          | WARNING |
- | dump_dumpfve.sys             | C:\Windows\system32\drivers        | RANDOM,NO_HASH | !!! POSSIBLE driver mem dump !!!                          | WARNING |
- | fsprtx.sys                   | C:\Windows\system32\drivers        | NAME_MATCH    | *** YAK 2 ***                                             | TOOL    |
- | tdi6.sys                     | C:\Windows\system32\drivers        | UNIDENTIFIED  |                                                           |         |
- | vboxdisp.dll                 | C:\Windows\system32                | UNIDENTIFIED  |                                                           |         |
- | vboxguest.sys                | C:\Windows\system32\drivers        | NAME_MATCH    | Oracle VM VirtualBox Guest Additions Driver               | NORMAL  |
- | vboxmouse.sys                | C:\Windows\system32\drivers        | NAME_MATCH    | Oracle VM VirtualBox Mouse Filter Driver                  | NORMAL  |
- | vboxsf.sys                   | C:\Windows\system32\drivers        | NAME_MATCH    | Oracle VM VirtualBox Shared Folders Minirdr Driver        | NORMAL  |
- | vboxvideo.sys                | C:\Windows\system32\drivers        | NAME_MATCH    | Oracle VM VirtualBox Video Driver                         | NORMAL  |
```

Type	First Seen	Also On
WARNING	2017-09-09	MOBTEST5322,epo
WARNING	2017-09-09	MOBTEST5322,epo
NORMAL	2017-09-09	epo
	2017-09-09	MOBTEST5322,epo
NORMAL	2017-09-09	MOBTEST5322,epo
NORMAL	2017-09-09	MOBTEST5322,epo

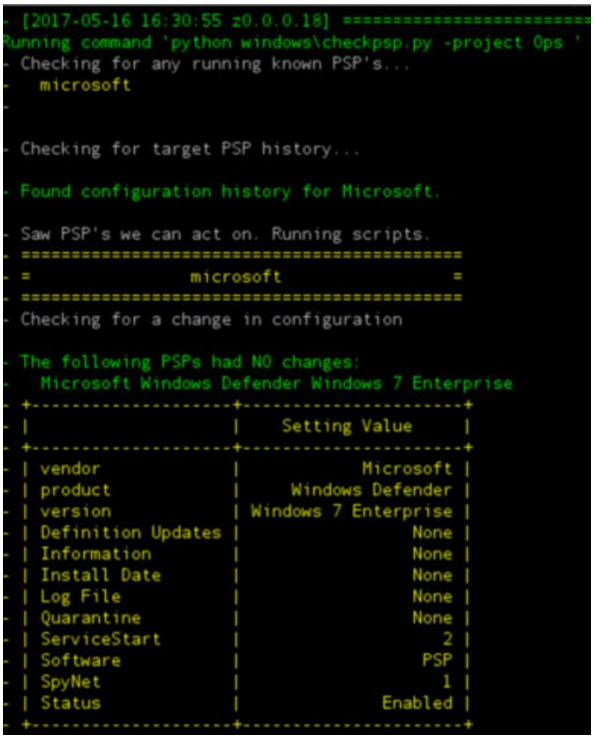
Nota: En color resalta los *drivers* conocidos, los sospechosos y los no identificados (basado en una base de datos de hash). Además, los correlaciona con otros targets (Donoso, 2017).

Figura 112
Persistances Checks.



Nota: En color resalta alguna persistencia detectada (Donoso, 2017).

Figura 113
PSP Checks.

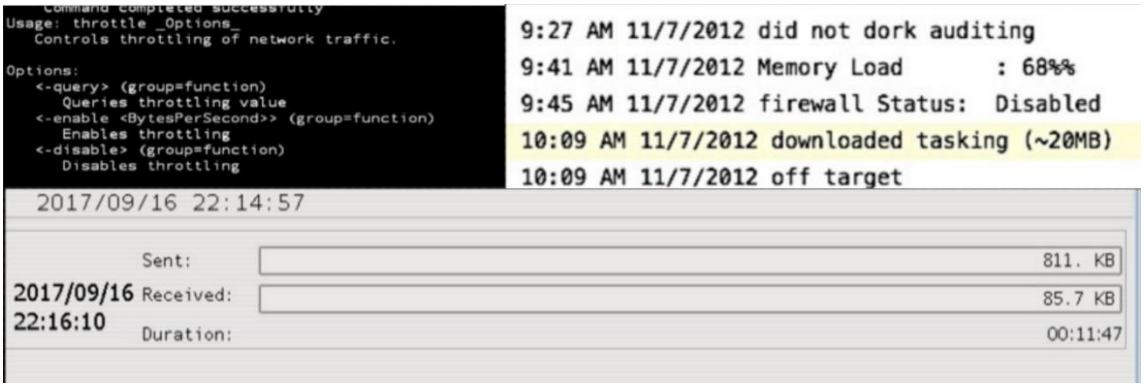


Nota: Detecta la presencia de Antivirus y sus configuraciones basado en description scripts (Donoso, 2017).

La herramienta tiene una atención extrema al sigilo. El Safety Handler previene de: acciones que puedan quedar registradas en logs, cargas de dll que pueda detectar un antivirus, inyección de código que pueda ser detectado o escribir registros que puedan comprometer la operación, etc. También deshabilita funciones del operador basado en el antivirus detectado, no permite ejecutar comandos descuidados (ej. habilitar los logs) y los scripts contienen una verificación de solo ejecutar si es seguro. La herramienta presenta una función de auditing dorking que levanta una DLL que captura todos los logs,

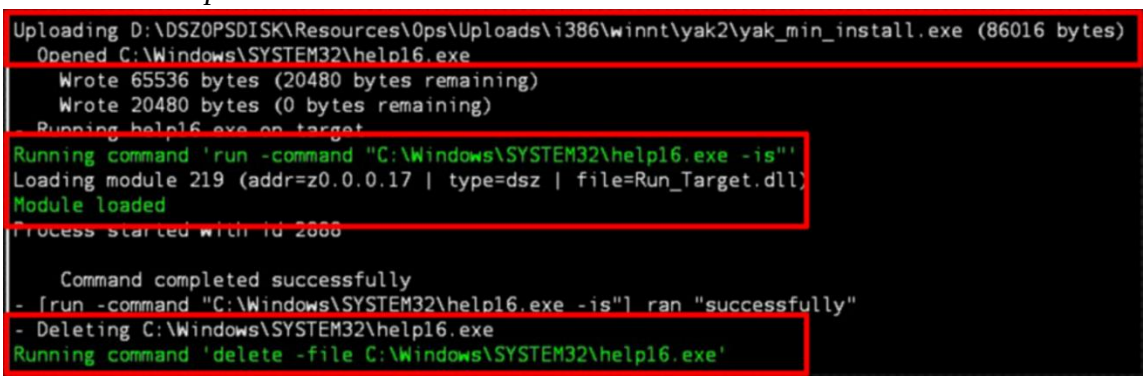
haciéndole creer al OS que los eventos se están registrando cuando en realidad no. En caso de no poder cargar esta DLL, registra todos los logs disparados por el operador y los elimina. La herramienta verifica la utilización de la memoria y regula los comandos para no superar ese umbral y no llamar la atención; o verifica que no se encuentre el usuario activo. Controla el tráfico de la red (ver figura 114), verifica e informa cambios (ej. nuevo antivirus o nuevo log habilitado). Cualquier archivo ejecutable lanzado hacia el target tiene un craft de nombre y metadatos para no llamar la atención, sumado a una herramienta de match que roba los datos de un archivo genuino del OS y los copia en el drop (file times) (ver figura 115).

Figura 114
Network use.



Nota: visibilidad de uso y control de tráfico (Donoso, 2017).

Figura 115
Executable Drop.



Nota: ejemplo de subir un keylogger enmascarado como un archivo de Windows, lo ejecuta e inmediatamente lo borra (Donoso, 2017).

Cuenta que, además, DanderSprintz contiene una suite de forense. *GreaterDoctor* puede escanear la memoria y los procesos, verificar inconsistencias entre los archivos y la

memoria, parsear archivos y capturar memoria para forense posterior (ej. para obtener firmas o claves de cifrado). *GangsterThied* puede leer toda la MTF (Master File Table) para análisis (ej. buscar algún archivo directamente y prevenir algún rootkit que impida su acceso).

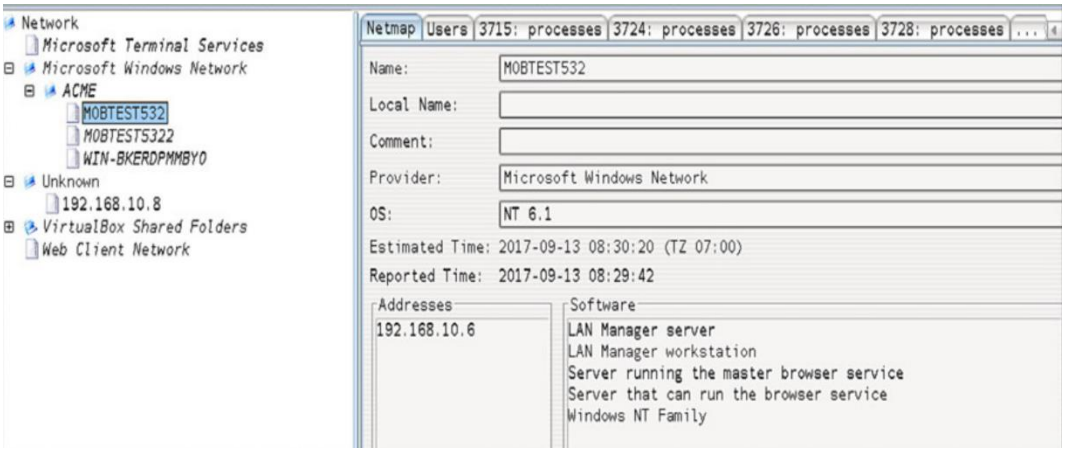
Entre las funciones, Overseer facilita el reconocimiento automático que captura: información de los navegadores, multimedia reproducido recientemente, USB devices, comandos ejecutados recientemente, cache de DNS/ARP, reciente sesiones de RDP (remote desktop protocol), archivos accedidos recientemente, screenshot periódicas, shares montados, busca PCAPS (si la víctima posee instalada una herramienta de trafico de red) y obtiene datos de *keylogger*. Simon Tatham es una función que busca PUTTY o WINSCP instalado, descifra el ini y muestra las credenciales (ver figura 116). Hay otra función para buscar bases de datos (SQL), mostrar sus instancias, listar bases, schemas, top ten rows de cada tabla y exfiltrar sus datos. SQL Canned Query plans función que utiliza las herramientas de los administradores en su contra, como abusar del ePO server para deshabilitar funciones en las máquinas de la red (AV), el WSUS server para verificar parches en las PC, operando directamente sobre la DB de forma que no quedan logs. Por otra parte, reconocimiento de usuarios de Active Directory y hasta una herramienta de escaneo de red similar a NMAP (ver figura 117). ScanSweep es otra variante que permite escanear rangos de IP de forma no secuencial. EmptyKEG abusa del WMI. Packetredirect inyecta un *driver* modo kernel que permite inyectar paquetes directos a la red (sin pasar por el stack TCP/IP de Windows), de ahí realizar movimientos laterales de forma de proxy. Finalmente búsqueda de archivos importantes en SharePoint y presenta un explorador de archivos locales con buscador detallado y exfiltración sigilosa (ver figura 118).

Figura 116
SimonTatham.



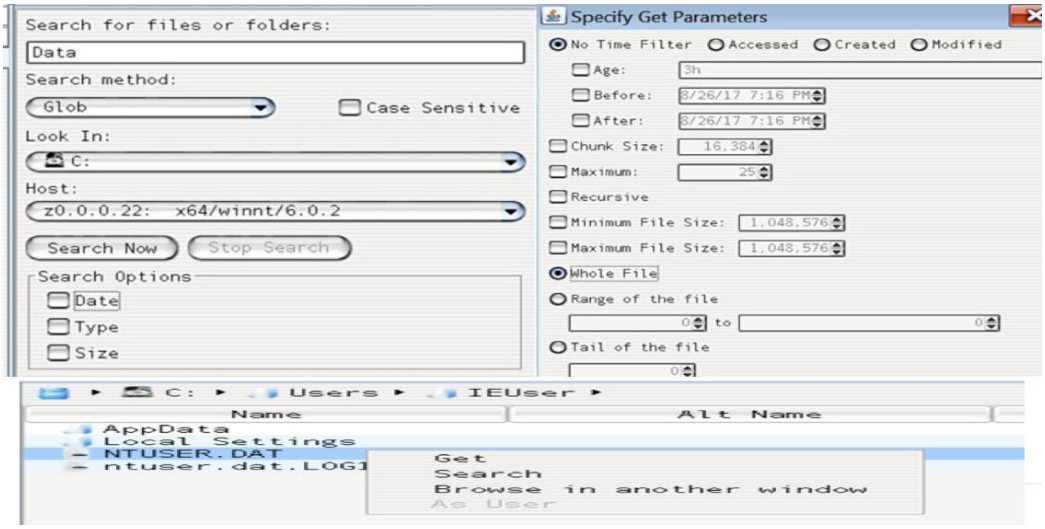
Nota: busca y descifra las credenciales almacenadas en la herramienta (Donoso, 2017).

Figura 117
NetMap Recon.



Nota: Busca y descifra las credenciales almacenadas en la herramienta (Donoso, 2017).

Figura 118
File Explorer.



Nota: Búsqueda y exfiltración de archivos específicos (Donoso, 2017).

Caso Operation Telescreen - Bvp47 Backdoor

Según Pangu Laboratory Technology (2022), en 2013 detectaron con un advanced threat detection system un comportamiento anormal en la red entre servidores de un objetivo clave[150]. A partir del análisis forense, encontraron un rootkit *backdoor* avanzado para Linux utilizado para comprometer al objetivo. El mismo utiliza canal encubierto

[150] Si bien el informe no indica cual fue el target, a partir del listado del leak de ShadowBrokers (/Linux/bin/varkeys/pitches.tar.bz2), podríamos inferir que se trató de algún organismo gubernamental de China: counsellor.gov.cn o hangzhouit.gov.cn)

cifrado (TCP SYN) que utiliza BPF (Berkeley Packet Filter) a modo kernel evitando el network protocol stack, contiene strings cifrados con XOR, ofuscación de funciones, adultera los primeros 4 bytes (magic number) del ELF (Executable and Linkable File) para prevenir la búsqueda de un Antivirus, ocultamiento al sistema (cerca de 70 hooks que ocultan su presencia), mecanismo de auto destrucción, utiliza setrlimit para fijar el core dump size igual a 0 (prevenir extracción de muestras para analizar), llama a lstat a través de syscall para omitir el Hook de SandboxRing3 verificando si el path argv[0] realmente existe (previene sandboxing), realiza técnicas para detectar entornos sandbox (llamada a mkstmp o verificación de archivos en /boot) y realiza un API flood para prevenir el análisis de sandbox.

El nombre del *backdoor* viene dado por el string “Bvp” y el valor numérico “0x47” encontrado de forma reiterativa en el algoritmo de descifrado. El nombre de la operación fue inspirado en la novela 1984 de Orwell donde el dispositivo telescreen es una TV de propaganda que además permite a la policía del pensamiento vigilar remotamente a los televidentes (Pangu Laboratory Technology, 2022).

El *backdoor* requiere un código de verificación vinculado al host para poder operar que fue descifrado por los investigadores. Sin embargo, el *payload* de la funcionalidad remota no pudo ser analizado en su momento dado que se encontraba cifrado con una llave asimétrica (RSA). Como la vida siempre nos da sorpresas, la clave privada se encontró dentro de los archivos revelados por Shadow Brokers en 2017. Puntualmente dentro de la carpeta Dewdrops_tipoffs (quizás el nombre original del implante dentro de una suit más amplia). Por lo tanto, se trata de una herramienta del ciber arsenal de operaciones ilegales de Equation Group. Esta llave no solo permitió verificar unívocamente la atribución si no también llevar a cabo un análisis más profundo que antes no había podido ser realizado (Pangu Laboratory Technology, 2022).

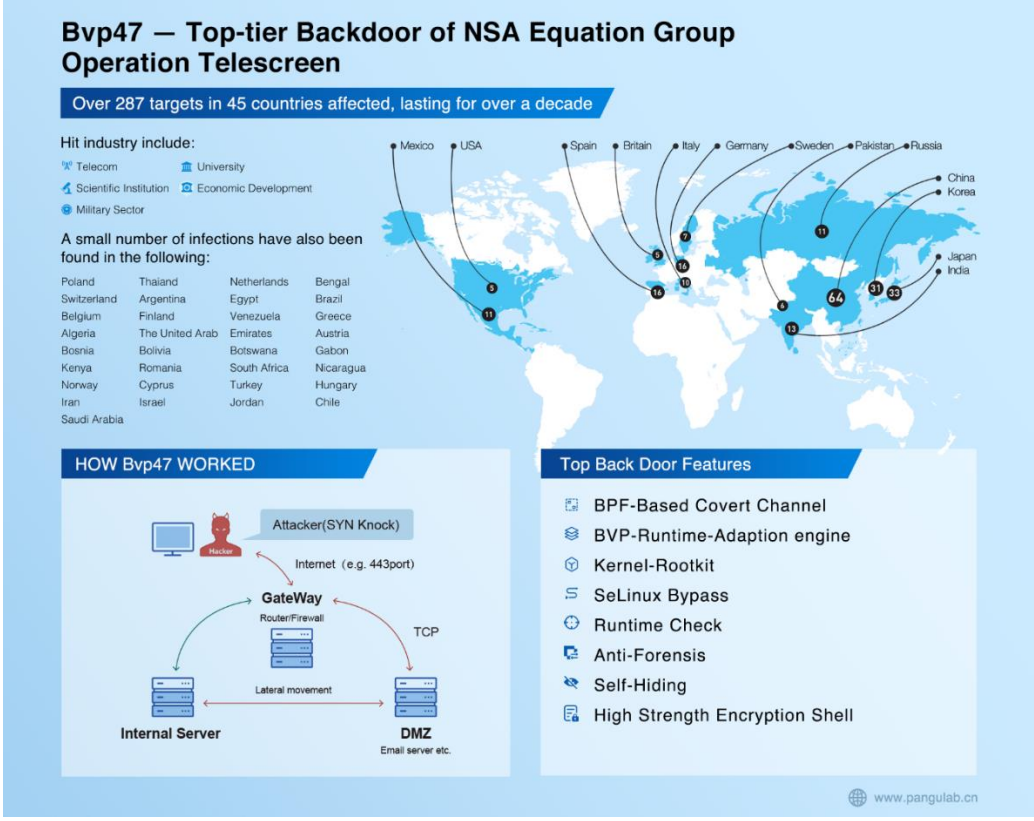
Continua, en el caso de estudio, el *backdoor* fue implantado en un Linux de la DMZ (email server). Este servidor cumplía la función de bridge entre internet y la red interna corporativa. El vector de ataque inicial no se encuentra explicado, podemos presuponer la utilización de exploit 0 day. El atacante inicia un SYN Knock a un puerto Web del servidor comprometido para iniciar el *backdoor*. Esto dispara una conexión reversa hacia el atacante que, entre otras cosas, permite ejecución de comandos (tipoff). El SYN es para

eludir mecanismos de detección que usualmente omiten los handshake. Otro servidor (también comprometido) en la red interna contacta al email server de la DMZ, descarga algunos comandos powershell e inicial un canal de comunicación para exfiltración (hacia el atacante a través del servidor DMZ) (Pangu Laboratory Technology, 2022).

En los últimos 10 años las victimas exceden los 287 objetivos en 45 países, incluyendo aliados de EEUU (ver figura 119). Además, una víctima en Japón fue utilizada como jump server para lanzar otros ataques, haciendo parecer que los mismos provenían de Japón (Pangu Laboratory Technology, 2022).

Los objetivos parecen están vinculados a servidores de mail. Considero que existen al menos dos explicaciones al respecto. O el objetivo de la operación estaba enfocado a las comunicaciones de mail, o la vulnerabilidad utilizada para comprometer los servidores se trataba de una vulnerabilidad sobre el servidor de mail de Linux.

Figura 119
Operation Telescreen.



Nota: Victimas de Dewdrop, StoicSurgeon y Incision *backdoor* presente en el leak de Shadow Brokers (file\Linux\bin\varkeys\pitchimpair\).

Eavesdrop y Vigilancia.

Dedican mucho tiempo jugando a ser dioses y poco mirando el espejo.

El ciber panóptico de Foucault.

La vigilancia es en sí una estructura de poder, dado que los gobiernos quieren saber todo de los ciudadanos, pero no permiten que los ciudadanos se entrometan en lo que andan los gobiernos.

(reflexión de elaboración propia)

El termino *eavesdropping* significa escuchar sigilosamente las conversaciones sin el consentimiento de los interlocutores. Respecto a su origen, podemos observar figuras en los aleros (eaves) del palacio de Hampton Court de Henry VIII en Reino Unido, haciendo referencia a que siempre se está siendo observado y escuchado (ver figura 120). Una advertencia ya que una traición al rey podría implicar el ahorcamiento. Posteriormente apareció durante el siglo XVI el término eavesdropper que significaba lugar donde gotea la lluvia de agua desde el techo, en referencia a las personas que asechaban bajo los aleros de las casas para escuchar que sucedía dentro de las mismas (Stollznow, 2014).

Figura 120
Eavesdroppers en el palacio de Hampton Court



Nota. Advertencia de que se está siempre observado y escuchado (Fuente: Stollznow)

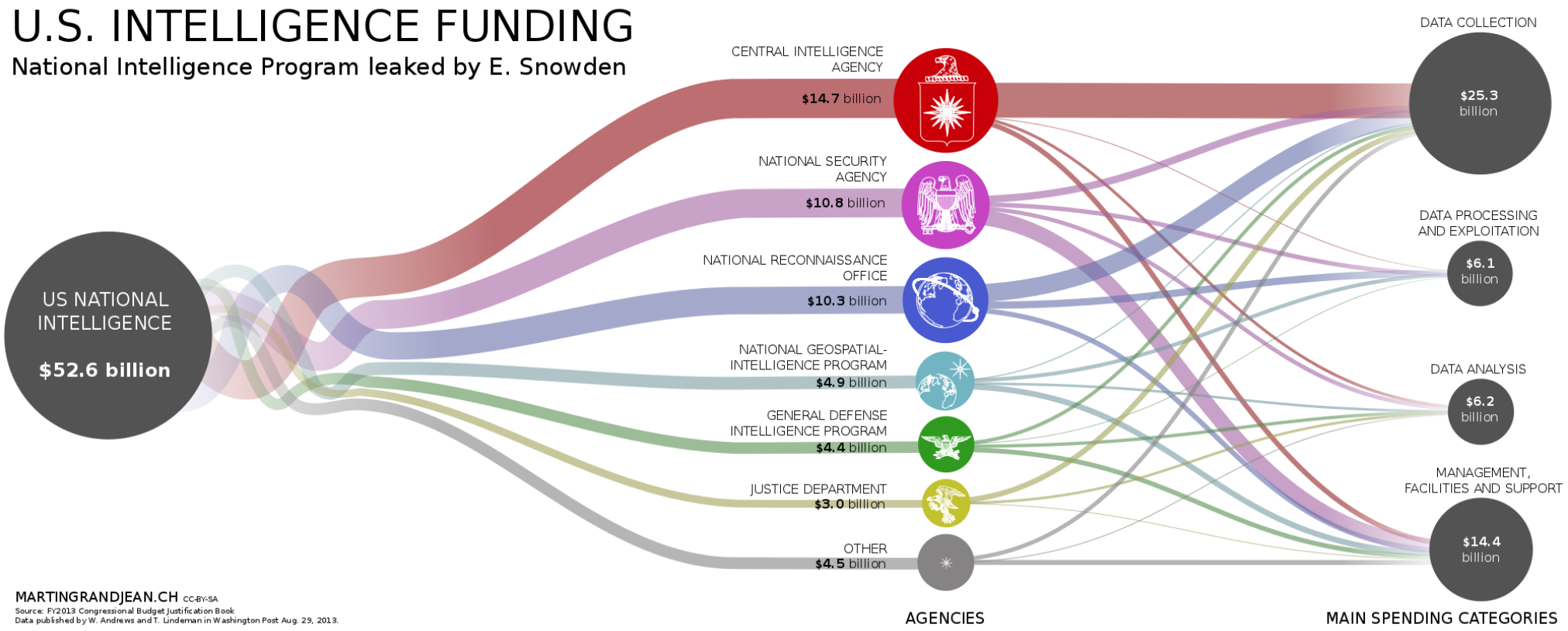
Filtración de datos de Snowden (Snowden leak).

Actúan de manera abusiva solo cuando creen que están a salvo en la oscuridad. El secreto es el eje del abuso de poder y la transparencia es su único antídoto (Greenwald ampliando a Snowden, 2014).

Parte de lo que conocemos de los sistemas de vigilancia, incluyendo su presupuesto (ver figura 121), proviene de las revelaciones de Edward Snowden que mencionaremos a continuación. Sin embargo, el periodista Campbell lleva informado al respecto desde su publicación de 1976. Por algún motivo, Campbell no tuvo la repercusión de Snowden. Ambos perseguidos judicialmente, aunque bajo diferentes circunstancias. Campbell es un periodista investigando, mientras que Snowden es un contratista del pentágono revelando información secreta que no debió haber sacado a la luz. Según (Greenwald, 2014), Snowden vio muchas cosas malas que discrepan de que le enseñaron. Por ejemplo, la CIA envió un oficial encubierto para alcoholizar a un banquero suizo e incentivarlo a manejar de regreso a su casa. La policía lo detuvo y lo encerró. El agente de la CIA le ofreció ayuda a cambio de información financiera del banco, pero el plan falló. Cuenta como le arruinaron la vida en vano. Snowden dice "tener un mayor compromiso con la justicia que miedo a la ley" (Snowden como fue citado por Philosophy Talk, 2015). Similar, Gandhi indica: “La desobediencia civil se convierte en un deber sagrado cuando el estado se vuelve anárquico o corrupto” (Gandhi como fue citado por Fischer. 2012).

En materia legal, la corte finalmente estableció en 2020 que vigilancia masiva sobre los teléfonos de los norteamericanos fue ilegal y posiblemente inconstitucional (violó la ley Foreign Intelligence Surveillance Act y la cuarta enmienda) (Gerstein, 2020).

Figura 121
The Black Budget.



Nota. Las cifras más importantes corresponden a la recolección de datos (fuente imagen: Andrews y Lindeman, 2013)

Acuerdo originalmente secreto entre Reino Unido y Estados Unidos (UKUSA Agreement) (1946).

Es ingenuo creer el gobierno no se va a tentar a hacer un uso indebido de la información (Shoshana Zuboff).

Utilizado durante la Guerra fría para interceptar las comunicaciones entre la URSS y el bloque de Europa del Este. El acuerdo originalmente constituido por 5 países conocido como Five Eyes (USA, UK, New Zeland, Canadá, Australia) (ver figura 122).

Figura 122
Five Eyes - FVEY.



Nota: Países que conforman la red Echelon (fuente imagen: Director of National Intelligence, s.f.).

Durante 1941, EEUU y Reino Unido intercambiaban información secreta (ULTRA) proveniente de Bletchley Park, donde se rompió el código de la maquina enigma alemán. En 1942 se amplía el intercambio de información con el Holden Agreement (1942) sumado a la intercepción de códigos navales japoneses (MAGIC). En 1943 el BRUSA Agreements; constituido por EEUU, Reino Unido, Australia, Canadá, Nueva Zelanda e India[151]; juntaba esfuerzos en SIGINT, para la intercepción y ruptura de las comunicaciones japonesas. BRUSA fue la antesala para el UKUSA agreement (Duffy, 2017).

El 5 de marzo de 1946 se firma el acuerdo UKUSA (United Kingdom United States Security Agreement). Firmado por el Lieutenant General Hoyt Vandenberg/GSC y Colonel Patrick Marr Johnson/British Army. Se trata de una alianza para recolectar información de inteligencia. Una cooperación conjunta en la inteligencia de señales. Acorde a la desclasificación de la NSA (s.f.): “Relaciones únicamente en materia de inteligencia de comunicaciones”, comprendido por “recolección, producción y diseminación de información derivada de las comunicaciones de otras naciones”. Intercambio de

[151] En aquel entonces, colonia británica.

producidos con relación a las comunicaciones extranjeras (a excepción de EE.UU. y Reino Unido) [152]:

1. Colección de tráfico.
2. Adquisición de documentos y equipos de comunicación.
3. Análisis de tráfico.
4. Criptoanálisis.
5. Descifrado y traducción.
6. Adquisición de información sobre organizaciones, prácticas, procedimientos y equipos de comunicación.

En el apéndice J, de las correcciones de 1944, figuran como colaboradores: Canadá, Australia y Nueva Zelanda (British Commonwealth). Estos países, además de ser aliados históricos y compartir un mismo idioma; tienen posiciones estratégicas dentro del globo terráqueo en cuando a lo que son las comunicaciones.

Programa SHAMROCK (1945-1975).

Programa que nació a partir de la WWII con el fin de recoger copias (en microfilms) de todos los telegramas extranjeros (incluyendo embajadas). Contaba con la colaboración de 3 empresas (RCA Global, ITT World Communications, and Western Union International). Finalizó en 1975 bajo orden del secretario de defensa James Schlesinger (United States Senate, 1976). El departamento de estado determinó ilegal. Esto llevó a la creación de la ley Foreign Intelligence Surveillance Act (FISA) de 1978 para contrarrestar los abusos investigados por la comisión del senado.

Proyecto MINARET (1969-1973).

Era una expansión del anterior, pero que incluía un mayor secretismo. Consistía en una lista de personas a espiar. Incluía personas que viajaban a Cuba/países comunistas, movimientos pacifistas, grupos políticos radicales, ciudadanos envueltos en protestas, tráfico de drogas, defensores de derechos civiles, entre otros (United States Senate, 1976).

[152] Como veremos adelante, la inteligencia de señales vigila a los ciudadanos de dichos países, lo cual contradice al acuerdo original.

Programa FROSTING (TRANSIENT + ECHELON).

Como cuenta (Campbell[153], 2015), en 1966 la NSA estableció el programa FROSTING para la recopilación y el procesamiento de todas las comunicaciones que emanan de los satélites de comunicación. FROSTING está conformado por 2 subprogramas: TRANSIENT (contra objetivos satelitales soviéticos) y ECHELON (para la recopilación y procesamiento de comunicaciones INTELSAT). La red ECHELON (P415 según Lockheed, posteriormente conocida como FORNSAT - Foreign Satellite Collection): Captura comunicaciones por radio y satélite, llamadas de teléfono, faxes y correos electrónicos en casi todo el mundo (ver figura 123) e incluye análisis automático y clasificación de las interceptaciones (Campbell, 2015).

Figura 123
Intercepción de comunicaciones.



Nota. (Fuente imagen Campbell, 2020).

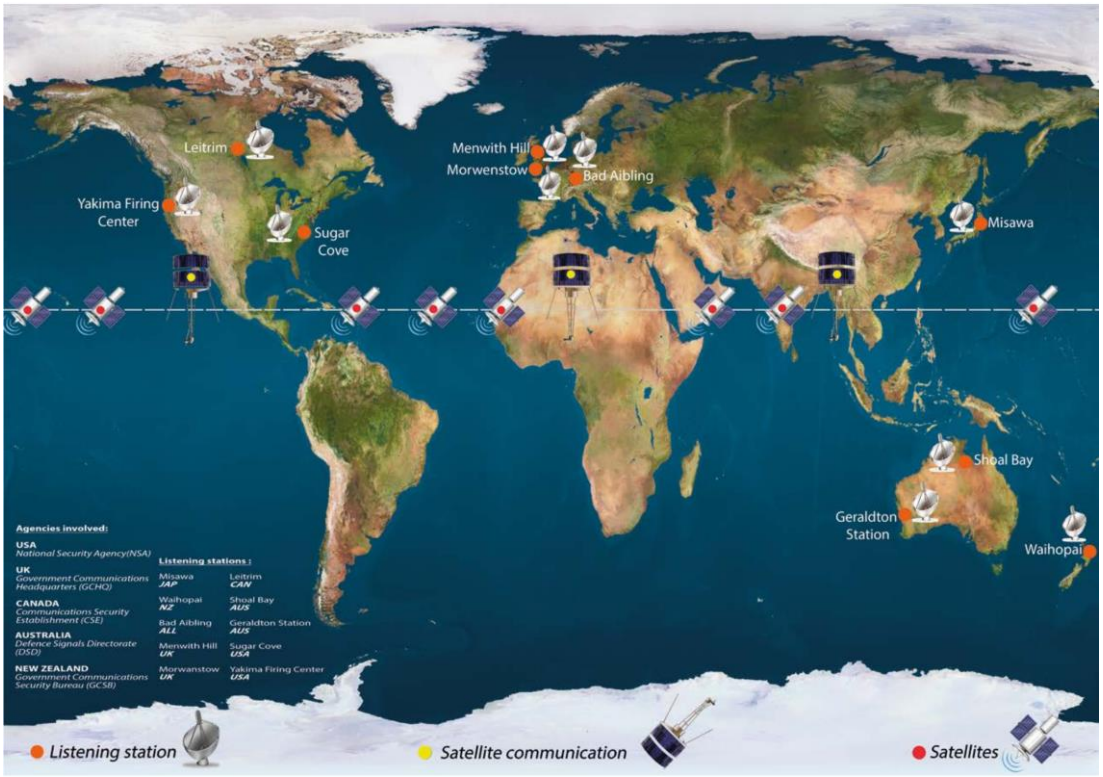
La red ECHELON (ver figura 124) fue también confirmada por el Parlamento Europeo, quien menciona el origen militar pero que hoy en día tiene una connotación de

[153] Como represalia por sus investigaciones de la vigilancia masiva, el periodista cuenta como fue históricamente perseguido, vigilado, intimidado e inclusive judicializado "the ABC trial" (lawfare) en UK; bajo el cargo de poseer información que puede ser útil para el enemigo.

beneficio político y económico (espionaje industrial) (European Parliamentary Reserch Service, 2014).

Figura 124

Echelon eavesdrops.

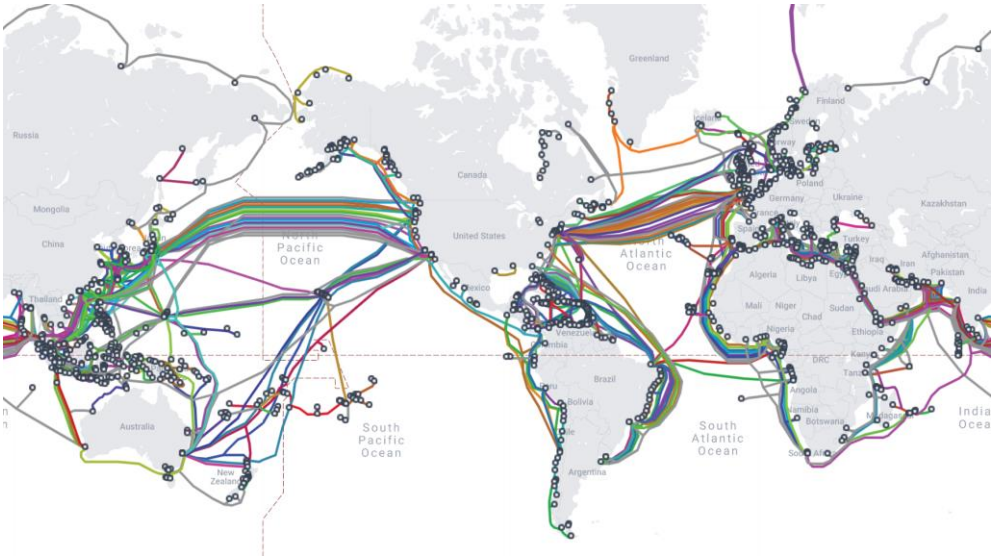


Nota. (Fuente imagen: European Parliamentary Reserch Service, 2014).

Vigilancia masiva.

Sin embargo, como continuaremos, la intercepción no se limita únicamente a la utilización de estaciones o satélites espías. Durante la década de 1856 aparece el primer cable submarino (telégrafo) y en los 80 aparecen los cables digitales de fibra óptica (Huston, 2020). Si bien existen submarinos con capacidades de intercepción y sabotaje, resulta más simple la intercepción en tierra o directamente en los proveedores. En el siguiente gráfico de cables submarinos (ver figura 125), se aprecia como EE.UU. es un gran hub de las comunicaciones de Latinoamérica y de Europa (esta ventaja se conoce como *Home field advantage*).

Figura 125
Cables submarinos.



Nota. (Fuente imagen: www.submarinecablemap.com).

En una entrevista, Assange comenta:

> […] por suerte la mayoría de los países en Latinoamérica no están en una situación de tener dictaduras agresivas. Esta influencia ahora se expresa en la financiación de ciertas ONG y grupos por parte de USAID (agencia de desarrollo del departamento de estado) y en capacidad de mantener a otro grupo dentro de la órbita estadounidense, ya sea por medio de la OEA (Organización de Estados Americanos), la SIP (Sociedad Interamericana de Prensa) o de otros acuerdos. La progresión en América Latina en relación con los Estados Unidos es muy positiva, pero hay un aspecto que me preocupa, y que Latinoamérica debe resolver, y es que todas las comunicaciones de América Latina hacia Europa y Asia se hacen a través de los Estados Unidos, donde son interceptadas por la Agencia de Seguridad Nacional (NSA).
>
> Un porcentaje importante de las comunicaciones entre países latinoamericanos se triangulan en los Estados Unidos y vuelven a la región (porque en ese país están ubicados los servidores de Internet y las centrales telefónicas de las principales empresas de comunicaciones del mundo, desde Facebook, Google y Twitter hasta Verizon y AT&T). Esto abarca a las grandes empresas telefónicas, los grandes proveedores de Internet, las transferencias en dólares. Es un tema importante de soberanía para América Latina. También vemos problemas serios con los medios de información. Esa caricatura de que los medios latinoamericanos son muy cercanos a una familia o un partido político es, en general correcta (Assange como fue citado por O'Donnell, 2014).

Las revelaciones de Snowden permiten conocer una serie de sistemas modulares que intercambian información. Más allá de sus complejos nombres, se comprende que a grandes rasgos cumplen las funciones de adquisición de diferentes fuentes (satelital, cable

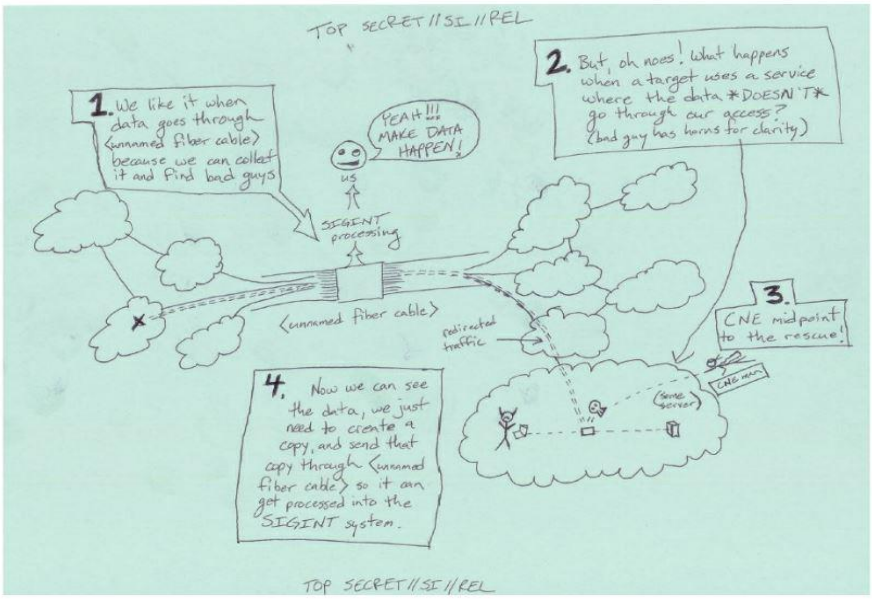
o telefónico), filtro, procesamiento/extracción (metadatos y/o datos), análisis, indexado (búsqueda) y almacenamiento (X cantidad de días para búsquedas hacia atrás).

La intercepción de los cables se realiza de diferentes maneras, con acuerdos secretos con las compañías (mediante cuantiosos contratos), mediante solicitud FISA (ley) o con técnicas de hacking[154]. Según los documentos filtrados por Snowden, la división de la NSA encargada de esta tarea es la Special Source Operations (SSO) (Greenwald, 2014).

¿Qué sucede cuando las comunicaciones pasan por cables en otros países? Realizan convenios con esos países para instalar equipamiento de intercepción (Programa[155] WINDSTOP para los países del acuerdo UKUSA o RAMPART-A para terceros países, ver adelante). Estos países, a su vez, si logran acceder a otros países, comparten la información con la NSA. ¿Qué sucede si no existe esta opción, por ejemplo, las comunicaciones dentro de un país al cual no tienen suficiente acceso / influencia? Recurren a lo que llaman traffic shaping[156] para forzar un enrutamiento de los paquetes hacia un lugar más adecuado para la vigilancia/pasive collection (ver figura 126). El enrutamiento puede ser del tráfico saliente o el tráfico entrante (ejemplo manipulando las tablas de enrutamiento BGP o sobrecargando las rutas no deseables, entre otros).

[154] Sería razonarse pensar que tanto las empresas hackeadas como los países espiados tienen un derecho a exigir una compensación cuanto menos equivalente.
[155] A lo largo de este apartado, nos referimos a programa a un proyecto y no a un software.
[156] No debe confundirse con el traffic shaping para administración de ancho de banda según la identificación de los protocolos en las comunicaciones.

Figura 126
Traffic shaping.



Nota. Forzar las comunicaciones por a los puntos donde puedan ser interceptadas (Mass, 2016).

Según Goldberg (2017), la NSA puede utilizar esta misma técnica para espiar a sus propios ciudadanos. Esto es, redireccionar el tráfico doméstico norteamericano de internet (mail, chats) hacia un territorio extranjero donde puede realizar vigilancia masiva de sus propios ciudadanos por fuera del ámbito del congreso/tribunales (evitando la ley FISA de 1978 y las garantías constitucionales). En el caso de interceptar tráfico en el extranjero está regulado por la Orden Ejecutiva 12333 de 1981 bajo orden presidencial que no requiere orden judicial. Con las comunicaciones de Internet de la actualidad, esta frontera resulta más difusa y tales leyes han quedado desactualizadas. Cabe señalar también que la OE 12333 puede dar un sustento para extranjeros dentro de su país. Sin embargo, violan las leyes de otros países y por lo tanto son punibles penalmente y de sanciones.

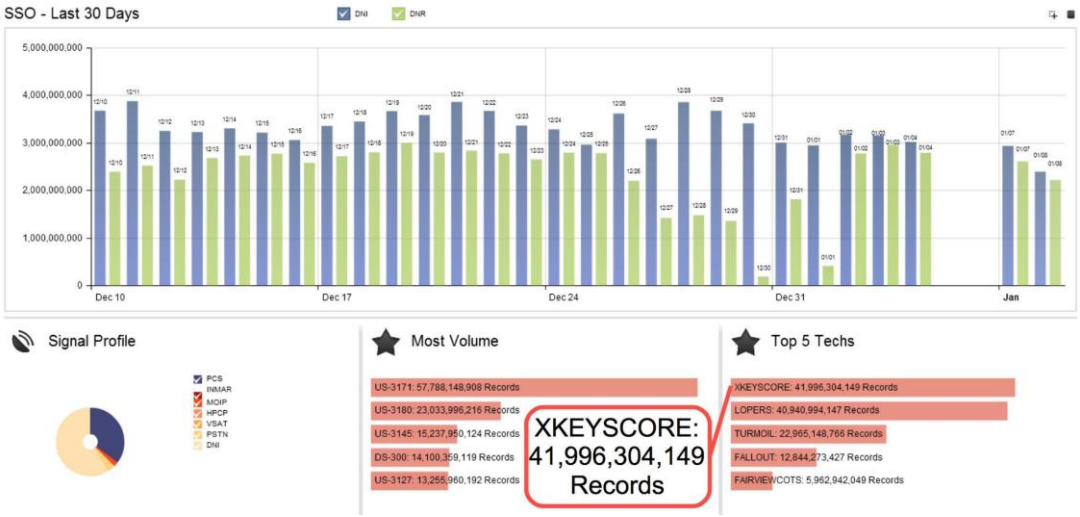
Luego del ataque terrorista del 11 de septiembre del 2001, dando cuenta que al-Qaeda utilizaba las redes norteamericanas para sus comunicaciones, surge la ley Patriota. Esta amplia el poder del estado en la vigilancia. El presidente en secreto también firma el controversial President's Surveillance Program (PSP / Stellar Wind program) que autoriza el registro del contenido de llamadas (nacionales e internacionales), y metadatos de llamadas/internet; sin necesidad de una orden judicial. En 2008, la FISA Amendment Act,

crea un marco más legal al programa, requiriendo la aprobación FISA de la corte (United States Foreign Intelligence Surveillance Court). Sin embargo, como indica (Greenwal, 2017); las solicitudes son sistemáticamente aprobadas. El Departamento de Justicia llevó una investigación e indicó el conflicto en los diferentes puntos de vista en relación con la legalidad del programa. La investigación concluye que hubo una recolección sin precedentes que deben ser cautelosamente monitoreadas (U.S. Department of Justice, 2009). Luego de las revelaciones de Snowden, en 2015, la USA Freedom Act impone limitaciones nuevamente a la recolección masiva de metadatos. En 2019 se suspende la recolección masiva de mensajes y llamadas domesticas (esto no incluye la recolección selectiva autorizada por FISA ni la vigilancia de extranjeros).

En ocasiones, las leyes restringen o impulsan el desarrollo de los programas de vigilancia. Luego de la Foreign Intelligence Surveillance Act de 1978, el foco fue limitar los abusos encontrados por el senado de los EE.UU. Posterior al atentado del 2001, las leyes fomentaron la inteligencia en detrimento de los derechos de los ciudadanos con el fin de perseguir y prevenir el terrorismo. Posterior a las revelaciones de Snowden, queda expuesto nuevos abusos y usos diferentes al terrorismo. Por lo que debe nuevamente controlarse los excesos. Se trata de un ciclo donde se corre la delgada línea entre lo legal e ilegal. Una lucha de poderes entre el Departamento de Defensa y los derechos / garantías constitucionales de los ciudadanos. Resulta indudable que el ciclo vuelva a suceder en un futuro, con el potencial de nuevas tecnologías como la inteligencia artificial y la computación cuántica. La tentación a ser dioses en el control absoluto es demasiado grande para un gobierno.

A continuación, algunos documentos revelados por Snowden (ver tabla 6, figura 127 y 128).

Figura 127
Most Volume.



Nota. Fuente revelaciones de Snowden (Greenwald, 2014).

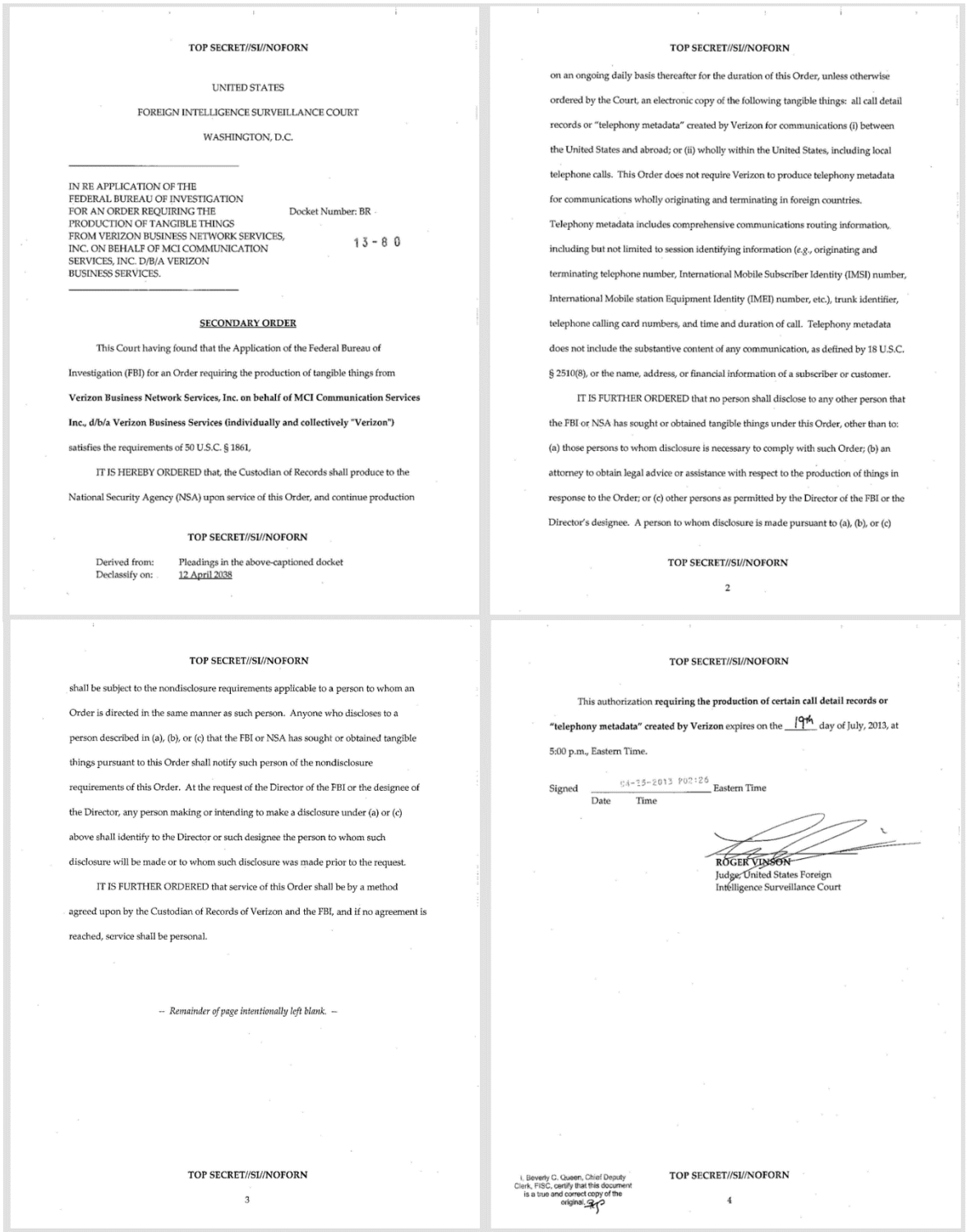
Tabla 6
Intercepción de cables.

Code Name	Volumen [Records]
DANCINGOASIS	57.788.148.908 (36%)
SPINNERET (part of RAMPART-A)	23.003.996.216 (14%)
MOONLIGHTPATH (part of RAMPART-A)	15.237.950.124 (9%)
INCENSER (part of WINDSTOP)	14.100.359.119 (9%)
AZUREPHOENIX (part of RAMPART-A)	13.255.960.192 (8%)
Other	38.000.000.000 (24%)
Total	160.168.000.000 (100%)

Nota. Basado en revelaciones de Snowden (Electrospaces, 2014).

Figura 128

Orden FISA para recolección masiva de metadatos en Verizon.



TOP SECRET//SI//NOFORN

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR 13-80

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

TOP SECRET//SI//NOFORN

on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c)

TOP SECRET//SI//NOFORN

2

TOP SECRET//SI//NOFORN

shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

-- Remainder of page intentionally left blank. --

TOP SECRET//SI//NOFORN

3

TOP SECRET//SI//NOFORN

This authorization **requiring the production of certain call detail records or "telephony metadata" created by Verizon** expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

I, Beverly C. Queen, Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.

TOP SECRET//SI//NOFORN

4

Nota. Fuente revelaciones de Snowden (Macaskil y Dance, 2013).

¿Qué función cumple la vigilancia masiva? Originalmente es la lucha contra el crimen y el terrorismo (antiguamente orientado a la guerra fría). Sin embargo, la práctica demuestra un uso diferente. Greenwald (2014) afirma:

> Parte de la vigilancia se dedicó ostensiblemente a sospechosos de terrorismo. Pero gran parte de los programas manifiestamente no tiene nada que ver con la seguridad nacional. Los documentos no dejaban dudas de que la NSA estaba igualmente involucrada en el espionaje económico, el espionaje diplomático y la vigilancia sin sospechas dirigida a toda la población […] El objetivo explícito declarado del estado de vigilancia es recopilar, almacenar, monitorear y analizar todas las comunicaciones electrónicas de todas las personas en todo el mundo […] todos los días, la NSA trabaja para identificar las comunicaciones electrónicas que no se recopilan y almacenan y luego desarrolla nuevas tecnologías y métodos para corregir la deficiencia […] Para recopilar cantidades tan grandes de comunicaciones, la NSA se basa en una multitud de métodos. Estos incluyen tapping a las líneas de fibra óptica (incluidos los cables submarinos) que se utilizan para transmitir comunicaciones internacionales; redirigir los mensajes a los repositorios de la NSA cuando atraviesan el sistema de EE.UU., como lo hacen la mayoría de las comunicaciones en todo el mundo; y cooperando con los servicios inteligentes en otros países. Cada vez con mayor frecuencia, la agencia también se basa en empresas de Internet y telecomunicaciones, que transmiten información indispensable que han recopilado sobre sus propios clientes. (Greenwald, 2014).

La historia indica que los espiados luego terminan siendo presidentes, ministros, periodistas, científicos, empresas contratistas; sin ninguna vinculación con el crimen. Cuando se realiza el filtro de datos se deja de lado los P2P[157], juegos y otros medios de comunicación que justamente son los canales encubiertos que utilizan los criminales. Quedando expuesto que no es la finalidad, sino una pantalla. Las investigaciones criminales se realizan únicamente mediante orden judicial y bajo ciertas premisas estipuladas en la ley (en nuestro país el código procesal penal). De lo contrario, toda investigación cae bajo el concepto del fruto del árbol envenenado y el proceso posterior resulta nulo. Por otro lado, planear un hecho no es un delito y por lo tanto es una garantía constitucional (podría tratarse del plano de la fantasía o un elemento de engaño / desinformación). Otra crítica a la vigilancia es que la gente no necesariamente tenga el mismo comportamiento en internet (ejemplo, utilizar las plataformas digitales para descargar emociones, frustraciones, indignación), lo que puede llevar a un gasto ineficiente

[157] Point to point, como ser software para compartir archivos.

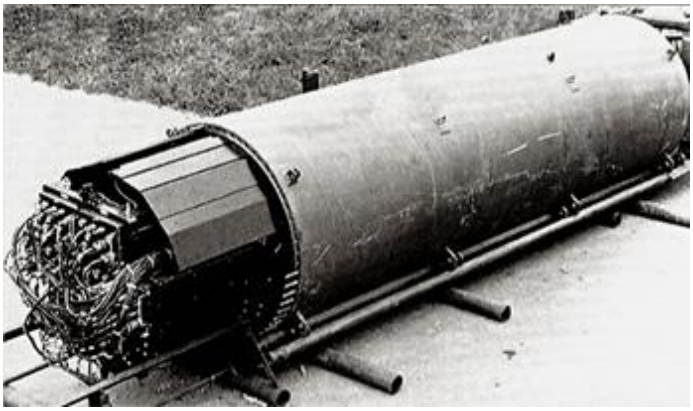
de recursos en investigar casos “pizza” que no llevan a nada. Así mismo, hay innumerables casos de terrorismo / tiroteos que no han podido identificar / prevenir. Con lo cual la efectividad masiva es insuficiente para su justificación. Quizás el mayor poder resida en los objetivos específicos, dado que los analistas pueden examinar los datos y elevar informes de inteligencia. Un ejemplo es el intento de atentado del vuelo 253 de Northwest Airlines de 2009 que no fue detectado, aunque afortunadamente falló el explosivo. Como contracara, la investigación posterior focalizada llevó a encontrar al actor intelectual (al-Qaeda), el cual fue asesinado en una operación con drones en Yemen. Finalmente, como mencionamos en Hack[2], existen operaciones ilegales contra el cibercrimen; a fin de sacar provecho de sus conocimientos y de la información que roban en vez de hacer justicia (a excepción de una afectación de sus intereses).

Como se propone a lo largo del trabajo, la finalidad es aplicar la inteligencia (recolección/procesamiento/análisis) para la adquisición de información y su posterior uso estratégico en la dominación mediante todo tipo de operaciones de guerra sin límites.

Caso Operation Ivy Bells

En 1971, EE.UU. utilizó al submarino USS Halibut con la misión de interceptar un cable submarino en el mar de Okhotsk, Rusia. El cable unía la base naval del pacifico en Petropavlovsk con el cuartel general en Vladivostok y las comunicaciones no se encontraban cifradas. Las señales de warning en la costa de Siberia ayudaron a la localización del cable. La intercepción se basó en el principio de inducción electromagnética para evitar cortar la cubierta del cable (en esa época hablamos de cable de cobre eléctrico y no de fibra con luz) (ver figura 129). Las cintas con grabaciones eran esporádicamente recuperadas para el análisis de la NSA. El programa fue un éxito y llevo a realizar otras intercepciones (entre Europa y África en el Pacifico) y mejoras en el dispositivo. Bell Laboratories desarrolló una versión más grande (The beast) para grabar por más tiempo. En 1981, un ex empleado de la NSA (Ronald Pelton) brindo información a la KGB a cambio de dinero, lo que terminó por arruinar la operación. El dispositivo de captura hoy se exhibe en un museo en Moscú. Un desertor de la KGB luego vendió a Pelton, lo que lo llevó a la cárcel. El dispositivo habría estado operativo hasta principios de los 80 (Sontag y Dreg, 1998; Campbell, 1999; Brown, s.f.; Carle, s.f.).

Figura 129
Dispositivo de intercepción.



Nota. 6 metros de largo y 6 toneladas de peso (fuente imagen: Sontag y Drew, 1998).

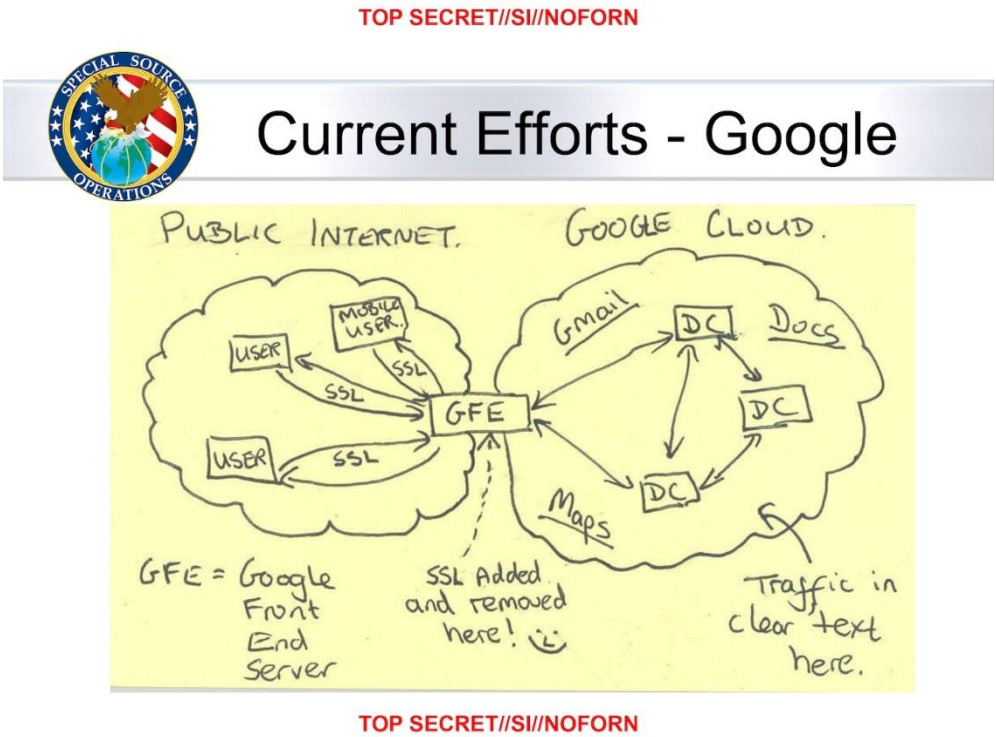
Programa WINDSTOP.

Programa de la NSA para la intercepción de cables con ayuda de países 2nd party (los miembros del UKUSA Agreement). Utiliza un sistema llamado TICKETWINDOW para compartir la información entre los 2nd party (Electrospaces, 2014).

Caso Programa MUSCULAR (DS-200B).

Programa en conjunto entre la NSA y GCHQ para intercepción de los cables que unen los grandes centros de datos de Google y Yahoo, mientras viajan descifrados entre diferentes continentes (ver figura 130). Este acceso es diferente a la solicitud por FISA (Gellman y Soltani, 2013).

Figura 130
MUSCULAR.



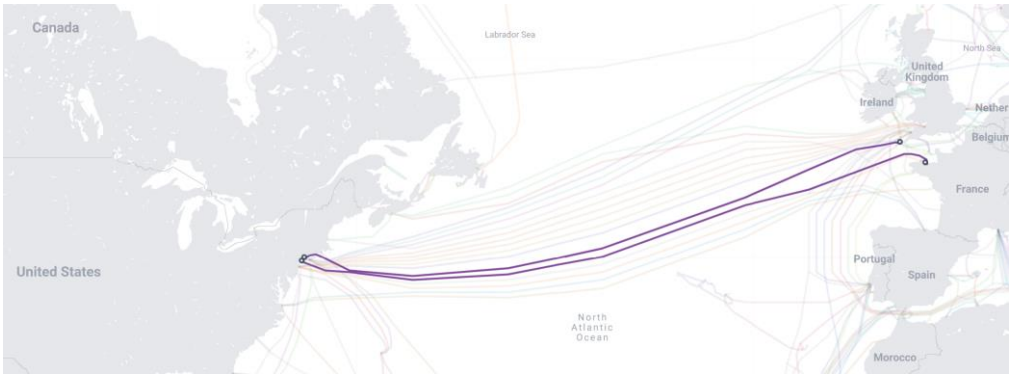
Nota. Intercepción de comunicaciones (Gellman y Soltani, 2013).

Caso INCENSER (DS-300).

La empresa Cable & Wireless (code name GERONTIC), actualmente parte de Vodafone colabora con el GCHQ a cambio de una contraprestación económica (Ball, Harding y Garside, 2013). Esta empresa tiene acceso a 29 cables submarinos y le permite a la agencia extraer datos de los cables de fibra óptica.

La empresa Global Cloud Xchange (GCX) es propietaria del cable FLAG Atlantic y FLAG Europe-Asia. El primero conecta Reino Unido con EE.UU./Francia, mientras que el otro conecta Reino Unido con Japón (pasando por Corea, China, India, Egipto, entre otros) (ver figura 131 y 132). Este último, es de alto interés por sus comunicaciones provenientes de Asia. La empresa GCX no colabora con el GCHQ, pero la interconexión entre dichos cables y el backbone terrestre lo realiza la empresa Cable & Wireless. De todas formas, GCHQ ha Hackeado (CNE) la infraestructura Linux de GCX a fin de obtener información de estadísticas y monitoreo de ruteo (Project PFENNING ALPHA) (Electrospaces, 2014).

Figura 131
FLAG Atlantic-1 (FA-1).



Nota. En Reino Unido llega hasta la playa Sennen cove, al norte de Skewjack Farm (fuente submarinecablemap.com).

Figura 132
FLAG Europe-Asia (FEA).



Nota. En Reino Unido llega hasta Porthcurno, próximo a Skewjack Farm (fuente submarinecablemap.com).

En Cornwall se encuentra la instalación de intercepción Skewjack Farm (code name NIGELLA) (ver figura 133 y 134) (White, 2014). El programa TEMPORA se encarga de que la información sea filtrada para reducir su volumen (MVR - Massive Volume Reduction), luego se extrae datos según selectores (e-mail, MAC address, IP Address) posiblemente utilizando equipos NARUS y finalmente se envían los resultados al Regional Processing Center (RPC), GCHQ Bude. Además, se realiza reensamblando de sesiones para alimentar al sistema XKEYSCORE (cual mencionamos más adelante) (Electrospaces, 2014).

Figura 133
Skewjack Farm.



Nota. Los datos son enviados al GCHQ Bude (fuente imagen: producción propia basada en Google maps).

Figura 134
GCHQ Bude.



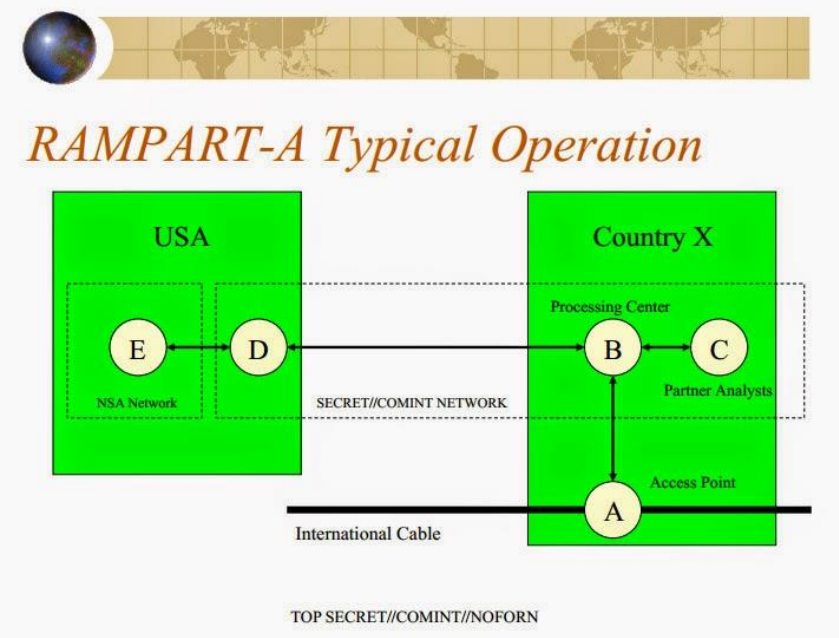
Nota. Los datos son enviados al GCHQ Bude (fuente imagen: Google maps).

Programa RAMPART-A.

Programa iniciado en 1992, en el cual la NSA coopera con otros países que dan acceso a los cables y permiten la instalación de equipamiento[158] de espionaje de la NSA (ver figura 135, 136 y 137) (similar al anterior pero con terceros países). Algunos subproyectos en código: SMOKYSINK, AZUREPHOENIX, SPINNERET, MOONLIGHTPATH, FIREBIRD, FALCONSTRIKE, DULCIMER. El programa busca instalar los equipamientos de intercepción en International Gateway Switches, End-Point GSM Switches, Leased Internet Circuits e Internet Backbone Routers (Jensen, 2014; Geist, Gjerding, Moltke, 2014).

Figura 135

Convenios con otros países para la intercepción de señales.

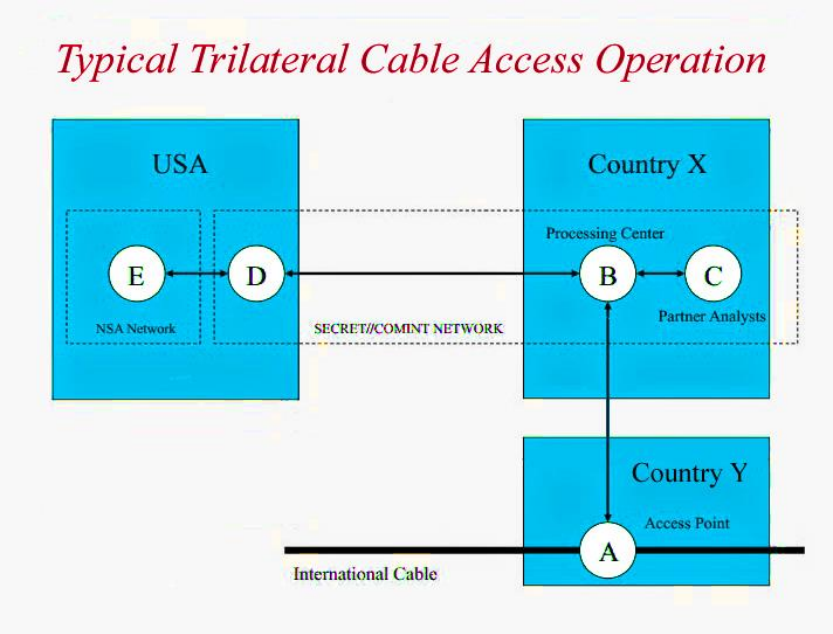


Nota. Documentos filtrados por Snowden (Electronic Frontier Foundation, 2014; Jensen, 2014).

[158] Recuerda a Sevoia (2016) cuando indica que la tecnología y la inversión del Proyecto X de gendarmería fue provista por una empresa norteamericana, a cambio de poder tener acceso a la información recolectada por gendarmería en el sexto piso del edificio Centinela. Cuenta como gendarmería se infiltraba en manifestaciones para filmar y armar causas. La larga lista de espiados por el Proyecto X va desde empresas, sindicatos, ambientalistas, trabajadores, víctimas de cromañón, estudiantes, familiares de discapacitados, docentes, campo, agrupaciones de vecinos, judiciales y un listado interminable alimentado por una red de agentes a lo largo y ancho del país. ¿Cuántos acuerdos secretos habrá en el país?

Figura 136

Convenios con otros países para la intercepción de señales que incluyen 3ros.



Nota. Documentos filtrados por Snowden (Electrospaces, 2016).

Figura 137

Convenios con otros países para la intercepción de señales.



Nota. Documentos filtrados por Snowden (Greenwald, 2014).

Caso EIKONAL / GRANAT Operation (2004-2008)

Operación del BND de Alemania fue un convenio firmado con la NSA en 2003 en el cual se permitía la intercepción de los cables de fibra donde la NSA proveía del equipamiento. La intercepción inicio en 2005 en la fibra de la empresa Deutsche Telekom en Frankfurt. La NSA entregaba al BND una lista de 'selectors' (números de teléfono y email) a buscar, en particular interés de Rusia y Medio Oriente. También estuvo interesada contratistas de defensa (Airbus Group y Eurocopter) y agencias gubernamentales francesas. El BND desarrolló un programa para filtrar y prevenir entregar información de sus propios ciudadanos (Code name DAFIS), el cual no funcionó bien dada la complejidad del caso. La operación finalizó en 2008 por su dudosa legalidad. El caso salió a la luz por las revelaciones de Snowden y su posterior investigación por el parlamento alemán en 2014 (Electrospaces, 2015; Mascolo, Leyendecker, Goetz, 2014; Mascolo, Goetz, Osten, 2014). Otro caso similar es el de la estación satelital Bad Aibling (Code name Garlick) que utilizaba la NSA con cooperación del BND para inteligencia de señales (Baumgärtner, Blome, Gude, Rosenbach, Schindler y Schmid, 2015).

Caso Dunhammer Operation

¿Amigos? No tanto… (reflexión de elaboración propia)

A partir de las revelaciones de Snowden, el DDIS (Danish Defence Intelligence Service) también inicio una investigación al respecto a la cual finalizó en 2015. Sus conclusiones fueron que la NSA, con colaboración de inteligencia danesa, espió las conversaciones de líderes políticos y funcionarios de Alemania, Suecia, Noruega y Francia (incluyendo a la canciller alemana Angela Merkel) entre el 2012 y el 2014. Se utilizó los números de teléfonos para poder buscar los datos a través de los cables de internet daneses, lo que permitió interceptar llamadas y mensajes. Una vez interceptados, los datos se envían a un centro de datos en Sandagergård para su almacenamiento, en el extremo sur de Amager en Copenhague. A partir de allí, los analistas pueden buscar utilizando un software llamado Xkeyscore. La ubicación geográfica de Dinamarca es estratégica para interceptar las comunicaciones de países europeos e inclusive de Rusia (Fastrup y Quass, 2021) (ver figura 138).

Figura 138
Cables de internet daneses.



Nota. Ubicación estratégica para espiar países de Europa y Rusia (Fastrup y Quass, 2021).

Espiar a los líderes políticos como hemos mencionado no tiene nada de nuevo. En 2010, TAO realizo un CNE (Project Flatliquid) para acceder los emails del presidente de México (Felipe Calderon) y su gabinete durante 2010. También trascendió el espionaje al presidente de Brasil (Dilma Rousseff) y la compañía Petrobras (Glüsing, Poitras, Rosenbach, Stark, 2013). El caso de Dilma Rousseff (presidente de Brasil) y de Enrique Peña Nieto (candidato y posterior presidente de México), figura la intercepción de comunicaciones según revelaciones de Snowden (Greenwald, 2014).

Según Buchanan (2020), la NSA juega a dos puntas. Colabora con Dinamarca para espiar a Alemania con la promesa de no utilizar los equipamientos para espiar al propio país (Dinamarca). Sin embargo, hace lo mismo con Alemania; promete no utilizarlos para espiar a este país y termina espiando a Dinamarca. Una promesa engañosa que permite espiar a ambos países.

Caso Athens Olympic Games

Durante los juegos olímpicos de Atenas en 2004, EE.UU. dudaba de la capacidad antiterrorista de Grecia y ofreció su ayuda[159]. Dado la posible ilegalidad del caso, acordó el deploy del aparato de inteligencia de señales de forma secreta. Los espías norteamericanos tuvieron acceso a las redes telefónicas, sistemas claves y hubs. Con la promesa de quitar la tecnología de espionaje una vez finalizados los juegos olímpicos. Promesa que nunca cumplió (Buchanan, 2020).

El sistema estaba construido sobre la intercepción legal que utilizaban las fuerzas de seguridad, pero eludía el sistema de auditoría y supervisión. Lo que permitió el espionaje de objetivos; entre los que se encontraba el primer ministro, su esposa, miembros del gabinete, la alcaldía y periodistas. Durante un update del software de espionaje, algo falló y causó una disrupción de las comunicaciones. Vodafone y otros llevaron una investigación y encontraron las capacidades de espionaje ocultas en la red. El Network Management expert de Vodafone (Costas Tsalikidis), fue ordenado a remover el software de espionaje, eliminando la evidencia de lo ocurrido. Al día siguiente, fue encontrado en el baño de su casa colgado de una soga (Buchanan, 2020).

Sistema XKEYSCORE

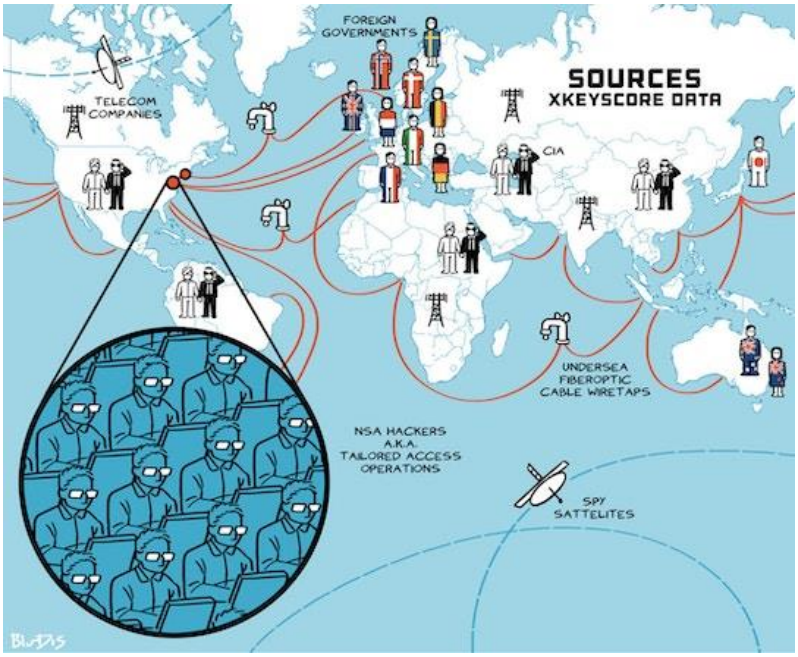
Sistema que se alimenta de los datos provenientes de las intercepciones mencionadas con los acuerdos con otros países (algunos de ellos pueden utilizar el sistema también) (ver figura 139). Se trata de un sistema escalable tanto en procesamiento como en capacidad de almacenamiento. Consistía en aproximadamente 700 servidores en cerca de 150 sitios (2008). El sistema crea un rolling buffer de 3 a 5 días de contenido y 30 días de metadatos donde se pueden realizar búsquedas remotas por los analistas (ver figura 140). Para las búsquedas utilizan selectores (ej. email, teléfono). Aunque a veces no resulta tan efectivo por el uso de comunicaciones anónimas. Por eso el software vuelve a ensamblar los paquetes IP para reconstruir las sesiones y obtener documentos como chat, documentos de Word, Excel, etc. (similar a Wireshark para quien está familiarizado). A partir de esa DB

[159] No necesariamente sea parte del programa Rampart-A. Sin embargo, por afinidad de detalles fue conveniente colocarlo en el presente apartado.

se pueden realizar búsquedas por características, de forma simple y similar a Google (Marquis-Boire, Greenwald y Lee, 2015).

Figura 139

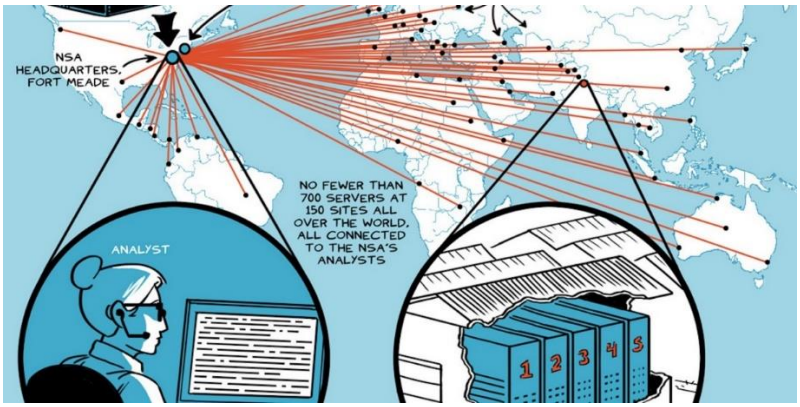
Fuentes de datos para XKEYSCORE.



Nota. (Marquis-Boire et al., 2015).

Figura 140

XKEYSCORE.



Nota. Búsqueda de datos por analistas (Marquis-Boire et al., 2015).

El sistema también puede enviar los datos de VOIP a otro sistema llamado NUCLEON (repositorio de voz). Otras funcionalidades son el seguimiento a partir de cookies u otros fingerprint unívocos como servicios de analytics, espiar hackers para obtener información

robada fruto de sus incursiones, espiar otros estados naciones para aprender de sus técnicas / obtener exploit 0 day, entre otros (Marquis-Boire et al., 2015).

Caso Hack Cellphone SIMs

El sistema XKeyScore fue utilizado para espiar los emails de los empleados de la empresa Gemalto. Los SysAdmin son objetivos habituales de la NSA por sus accesos a los sistemas. Con esa información, la NSA y el GCHQ hackearon la red de Gemalto (proveedor mundial de tarjetas SIM de celulares) y robaron millones de claves privadas que permite descifrar las comunicaciones de celulares (Marquis-Boire et al.2015).

Suit QUANTUM - FOXACID

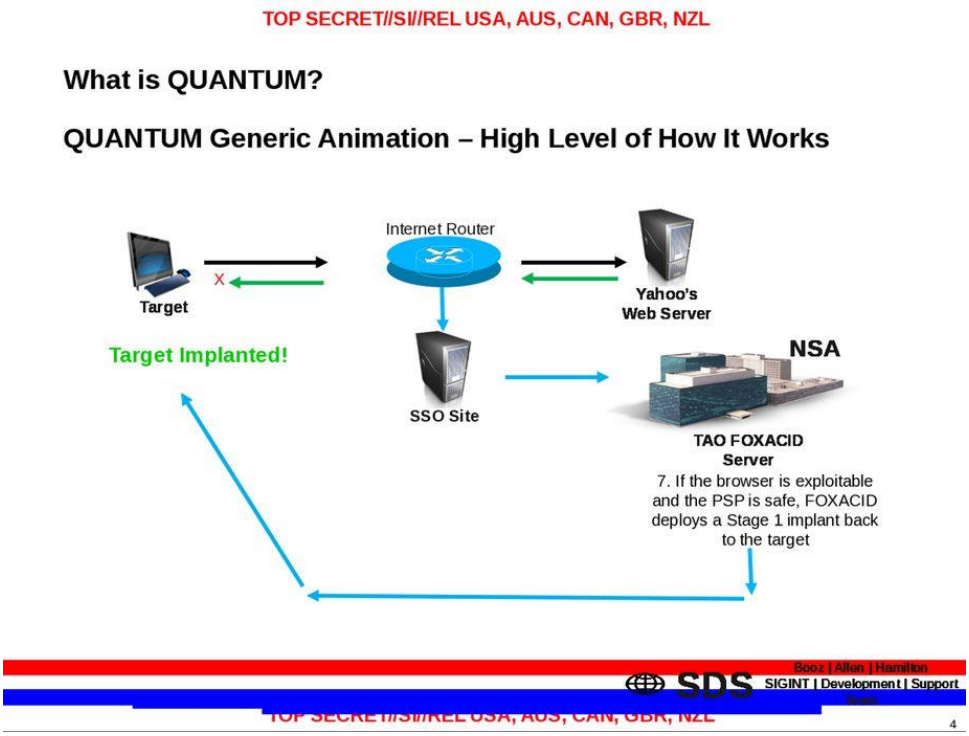
Suít de ataque del grupo TAO. La NSA, en cooperación con las compañías de telecomunicaciones, coloca servidores en los internet backbone para impersonar Websites legítimos. Consiste en un Man On The Side Attack, el cual se basa en responder las solicitudes más rápido que el sitio web genuino (ver figura 141, 142, 143 y 144) (ataque Second Date). Otra variante es QFIRE, que consiste en máquinas virtuales cerca del target a fin de garantizar baja latencia (Schneier, 2013).

El tráfico redireccionado se envía a unos servidores FOXACID (orquestador de exploits) quien impersona al servidor Web (ver figura 145). Este servidor explota una vulnerabilidad 0 day en la victima para colocar un implante, como por ejemplo OLYMPUSFIRE que permite un control remoto de la PC (listar directorios, obtener archivos, etc.) (SPIEGEL Staff, 2013). Otra variante es realizar un ataque man in the middle contra el Access point (WIFI) con una tool de CNE denominada BADDECISION (National Security Archive, 2010).

Antiguamente el ataque era menos sofisticado, utilizaba un mail de phishing (genérico o spear phishing) y un XSS (Cross Site Scripting) que consistía en colocar código JavaScript en un sitio web (mediante un iframe) (National Security Archive, s.f.).

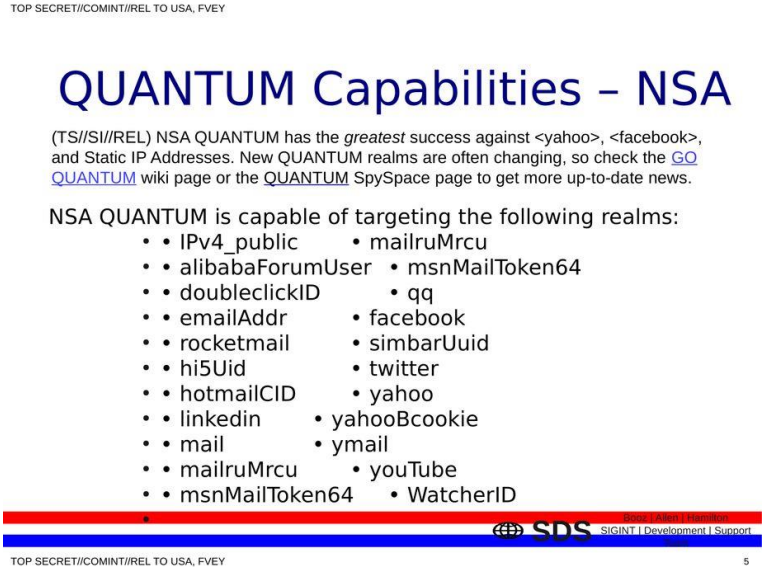
En combinación con XkeyScore, la NSA puede buscar tráfico TOR desde el país del objetivo en los horarios de actividad y utilizar cookies para rastrear objetivos (QUANTUMCOOKIE), aunque no muy efectivo (Schneier, 2013).

Figura 141
Quantum.



Nota. Man on The Side Attack (SPIEGEL Staff, 2013).

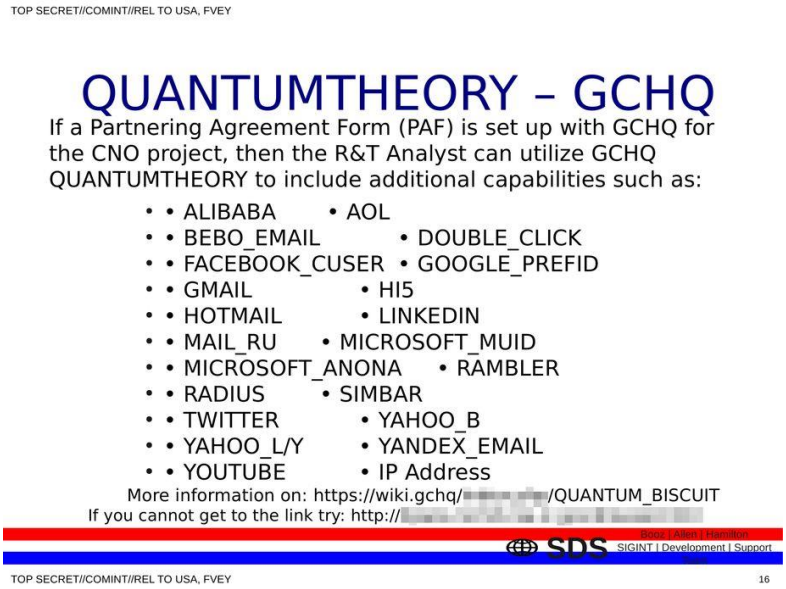
Figura 142
Quantum targets.



Nota. (SPIEGEL Staff, 2013).

Figura 143

Quantum targets.



Nota. (SPIEGEL Staff, 2013).

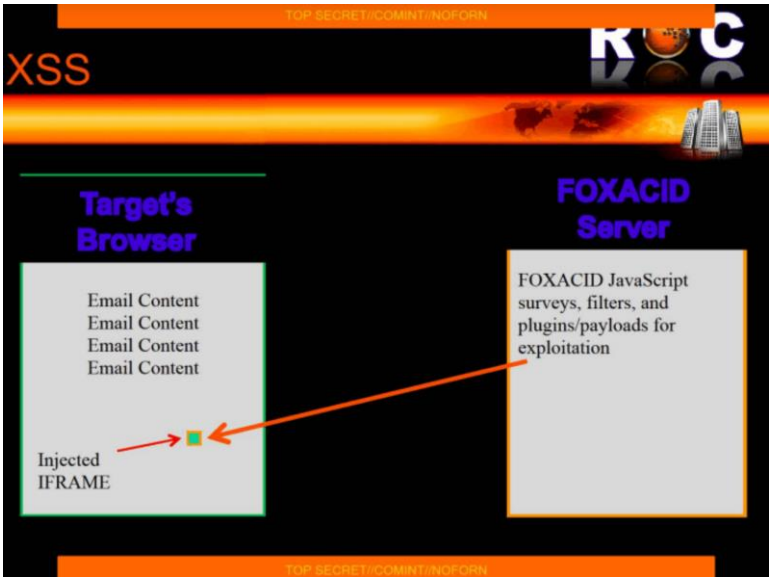
Figura 144

FOXACID.



Nota. El dibujo resulta interesante desde el psicoanálisis. (Funte imagen: SPIEGEL Staff, 2013).

Figura 145
FOXACID.



Nota. Método anterior a la explotación 0 day (Fuente imagen: National Security Archive, s.f.).

Caso Operación Socialist.

GCHQ estuvo detrás de los ciber ataques a la empresa de telecomunicaciones belga, Belgacom desde 2010. El ataque se llevó a cabo contra empleados de las empresas utilizando "Quantum Insert" (desarrollada por la NSA), permitiendo a través de ellos acceso a la infraestructura de Belgacom (Spiegel Staff, 2013).

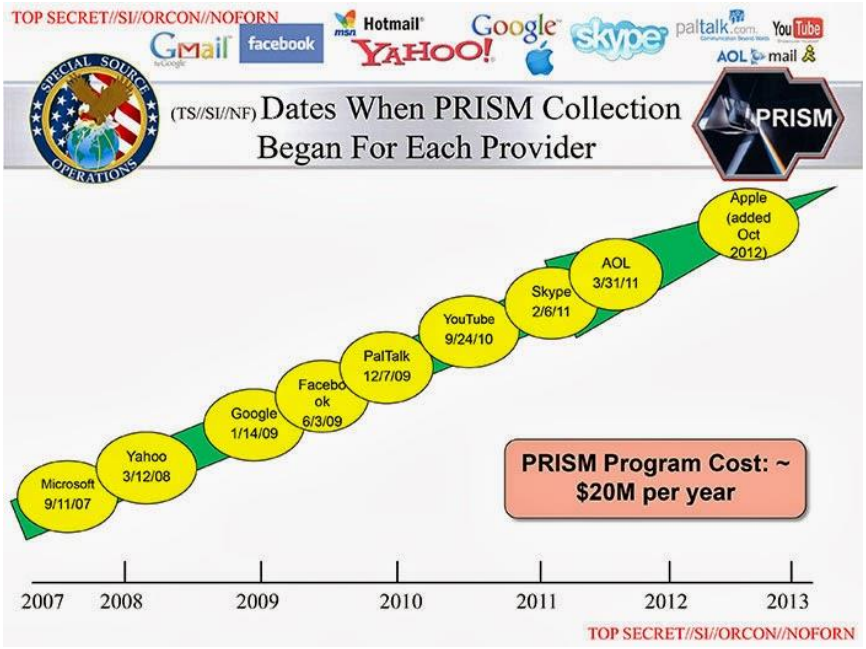
Programa Downstrem collection (PRISM)

Programa para recolectar información de objetivos extranjeros con colaboración de las grandes empresas de Internet (Microsoft, Facebook, Google, Apple) (ver figura 146 y 147). Operativo desde 2007, la colección la realiza una unidad del FBI bajo FISA Amendments Act (Greenwald y MacAskill, 2013). La recolección inicia a partir de un selector (email o IP) colocado en el Unified Targeting Tool (ver figura 148). Se puede hacer vigilancia en tiempo real o revisar las comunicaciones guardadas (Gellman y Poitras, 2013). Sin embargo, la colección no es automáticas, las empresas tienen que facilitar la información bajo pedido (secure FTP o en persona) (Auslen, 2013). La recolección luego pasa por una serie de sistemas para su clasificación, procesamiento y finalmente almacenamiento (ver figura 149). Bases de datos como Marina (metadatos de internet), Mainway (metadatos de

teléfono e internet), Nucleon (voz), Pinwale (contenido de internet, video). La información luego es revisada por un analista para su informe de inteligencia (Gellman y Poitras, 2013).

Figura 146

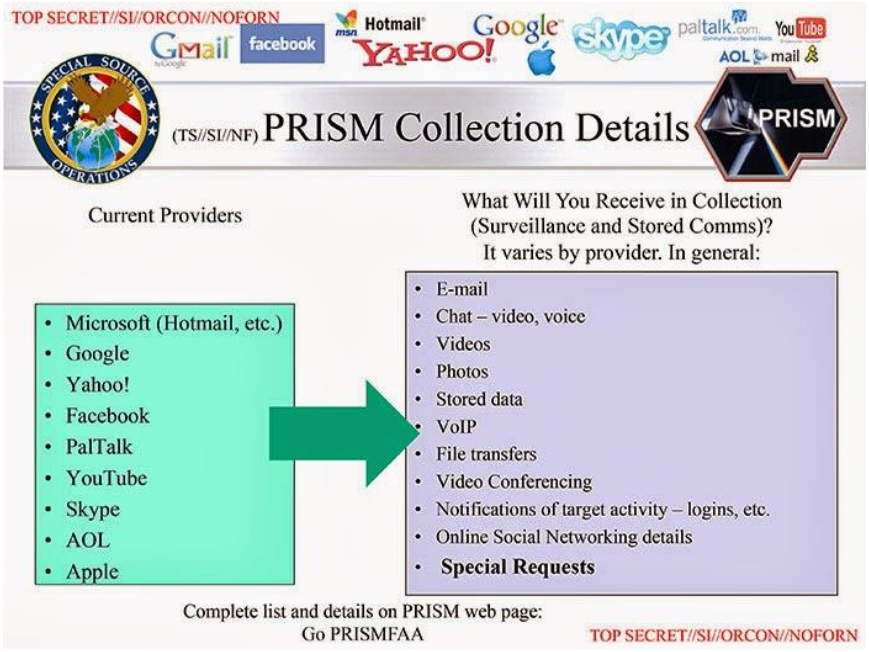
PRISM.



Nota. Cooperación con empresas. Revelaciones de Snowden (Macaskill y Dance, 2013).

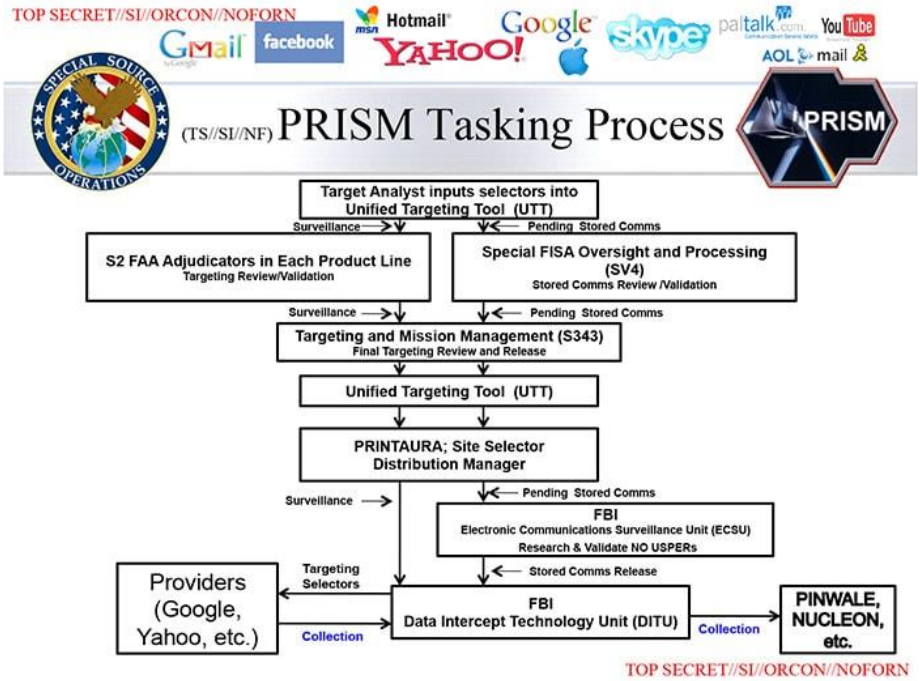
Figura 147

PRISM.



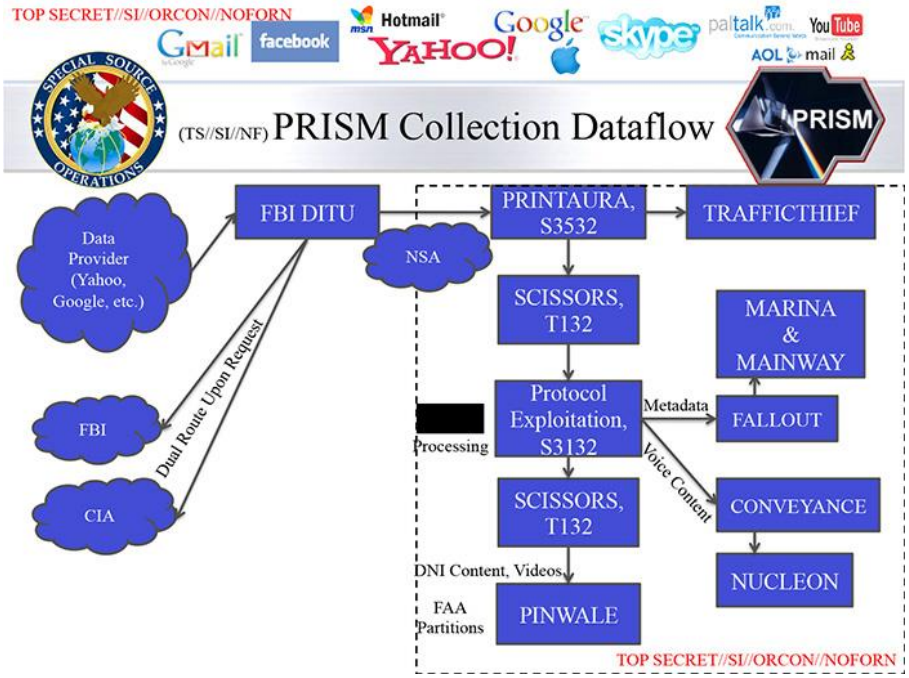
Nota. Datos recolectados. Revelaciones de Snowden (Macaskill y Dance, 2013)

Figura 148
PRISM.



Nota. Proceso de recolección. Revelaciones de Snowden (Gellman y Poitras, 2013)

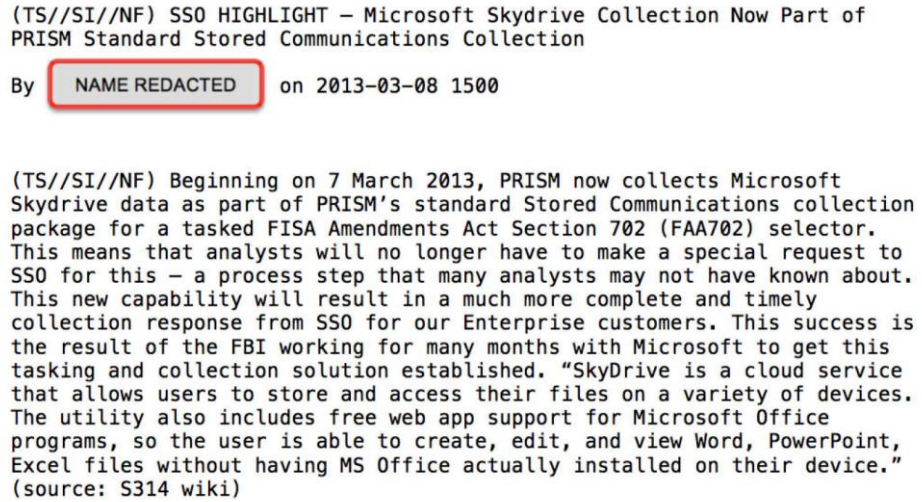
Figura 149
PRISM.



Nota. Procesamiento. Revelaciones de Snowden (Macaskill y Dance, 2013).

Otro ejemplo mencionado por Greenwald (2014) de la SSO (Special Source Operation unit) es el trabajo arduo trabajo que realizó Microsoft para dar un acceso más fácil a la NSA sobre los datos de Outlook.com, Skype y Skydrive (renombrado a OneDrive) (ver figura 150). A su vez, para esquivar las protecciones de cifrado en las comunicaciones (ver figura 151).

Figura 150
PRISM.



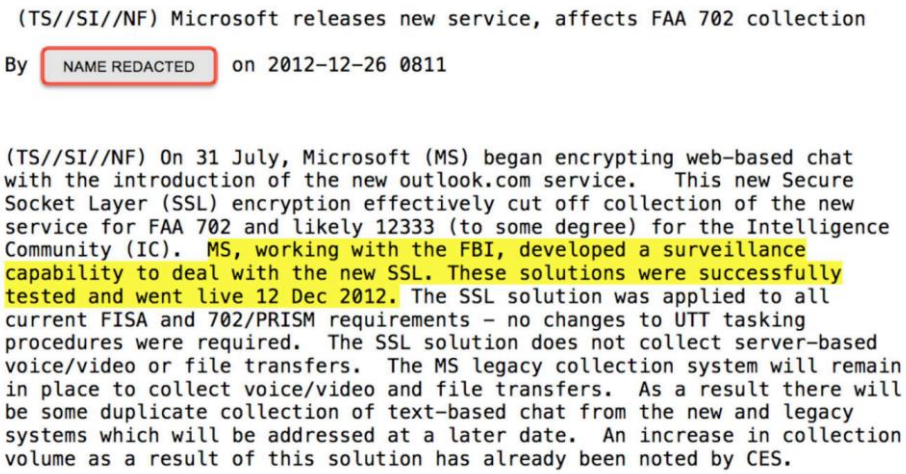
(TS//SI//NF) SSO HIGHLIGHT – Microsoft Skydrive Collection Now Part of PRISM Standard Stored Communications Collection

By NAME REDACTED on 2013-03-08 1500

(TS//SI//NF) Beginning on 7 March 2013, PRISM now collects Microsoft Skydrive data as part of PRISM's standard Stored Communications collection package for a tasked FISA Amendments Act Section 702 (FAA702) selector. This means that analysts will no longer have to make a special request to SSO for this – a process step that many analysts may not have known about. This new capability will result in a much more complete and timely collection response from SSO for our Enterprise customers. This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established. "SkyDrive is a cloud service that allows users to store and access their files on a variety of devices. The utility also includes free web app support for Microsoft Office programs, so the user is able to create, edit, and view Word, PowerPoint, Excel files without having MS Office actually installed on their device." (source: S314 wiki)

Nota. Trabajo entre el FBI (Data Intercept Technology Unit) y Microsoft para acceso a varios sistemas (Greenwald, 2014).

Figura 151
PRISM.



(TS//SI//NF) Microsoft releases new service, affects FAA 702 collection

By NAME REDACTED on 2012-12-26 0811

(TS//SI//NF) On 31 July, Microsoft (MS) began encrypting web-based chat with the introduction of the new outlook.com service. This new Secure Socket Layer (SSL) encryption effectively cut off collection of the new service for FAA 702 and likely 12333 (to some degree) for the Intelligence Community (IC). MS, working with the FBI, developed a surveillance capability to deal with the new SSL. These solutions were successfully tested and went live 12 Dec 2012. The SSL solution was applied to all current FISA and 702/PRISM requirements – no changes to UTT tasking procedures were required. The SSL solution does not collect server-based voice/video or file transfers. The MS legacy collection system will remain in place to collect voice/video and file transfers. As a result there will be some duplicate collection of text-based chat from the new and legacy systems which will be addressed at a later date. An increase in collection volume as a result of this solution has already been noted by CES.

Nota. Solución al cifrado de datos (Greenwald, 2014).

Programa Upstream collection

El otro tipo de recolección es llamado Upstream collection (ver figura 152) en contraposición a PRISM (Downstrem) (ver figura 153 y 154). Se refiere a la intercepción de internet y telefonía desde los backbone de internet (realizado únicamente por la NSA). Dado que las comunicaciones toman la ruta más económica y no la más corta, muchas comunicaciones viajan por USA. Los programas Upstream son Stormbrew (cable tapping en colaboración con Verizon; ejemplo cables que conectan la costa oeste con China, Japón y Corea), Fairview (cable tapping en cooperación con AT&T), Blarney (telefonía e internet dentro de EE.UU. con asistencia de AT&T, ej. el equipo Narus STA 6400 que captura el backbone traffic en el secret Black Room 641A del edificio de San Francisco), Oakstar (consiste en varios subprogramas para colección de internet y telefonía), de interés el subprograma SILVERZEPHYR (internet y teléfono de Sudamérica) (Electrospaces, 2013; Wired Staff, 2006; Angwin, Savage, Larson, Moltke, Poitras y Risen, 2015; Bridi y Greenwald, 2013; Electronic Frontier Foundation, s.f.).

Un homónimo similar es el MUSCULAR de GCHQ que adquiere contenido y metadatos de los cables que viajan a los data centers de Google y Yahoo (Gellman y Soltani, 2013).

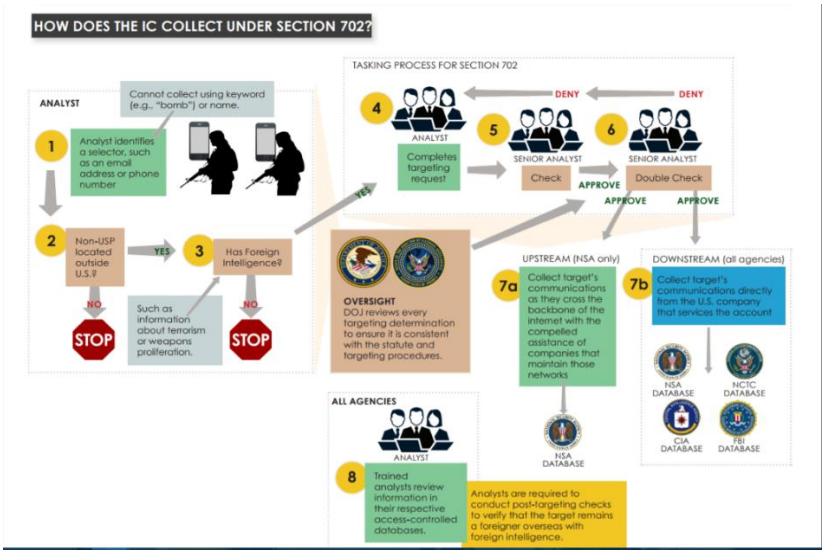
Figura 152
Upstream / Prism.



Nota. Colección de datos. Revelaciones de Snowden (Macaskill y Dance, 2013).

Figura 153

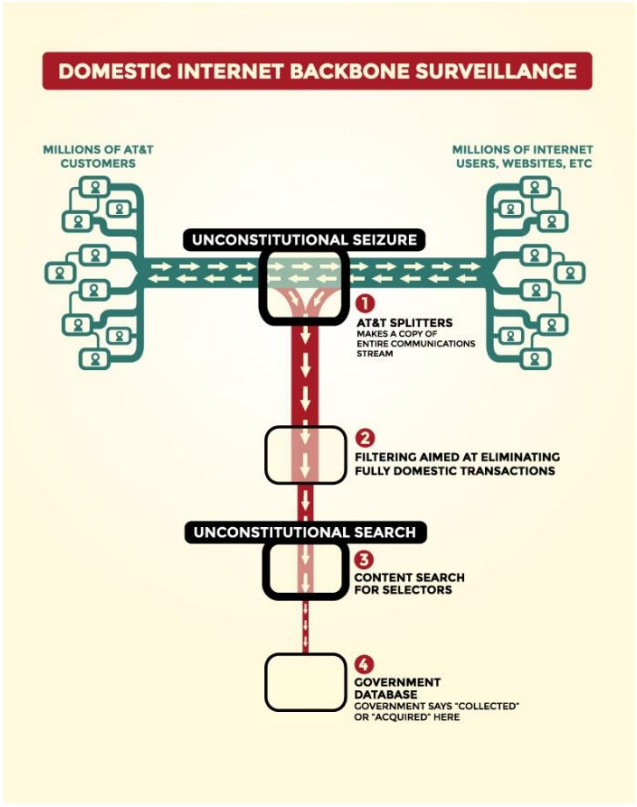
Colección workflow.



Nota. Acorde a FISA Amendments Act (2008). Office of the Director of National Intelligence.

Figura 154

Legal question.



Nota. Contracara según Electronic Frontier Foundation. T&T está cooperando con la vigilancia ilegal. AT&T instaló un divisor de fibra óptica en sus instalaciones en 611

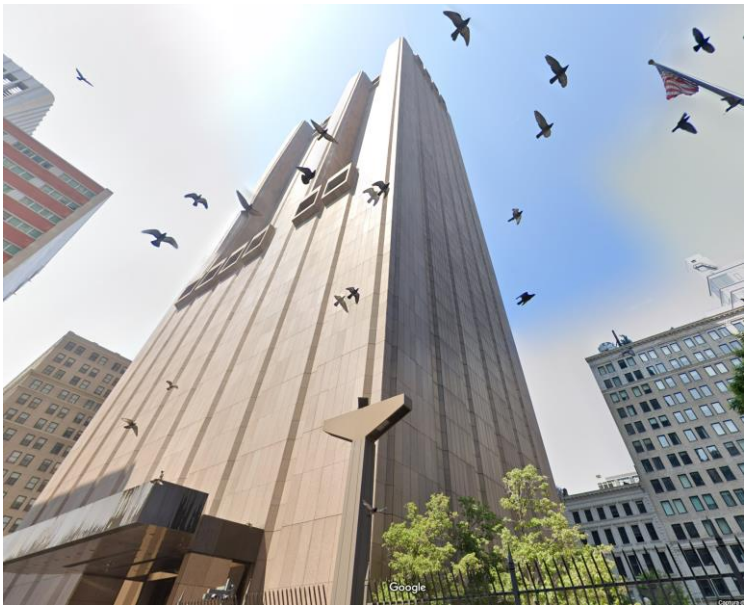
Folsom Street en San Francisco que hace copias de todos los correos electrónicos, navegación web y tráfico de Internet. AT&T proporciona esas copias a la NSA (Electronic Frontier Foundation, s.f.)

Project X (TITANPOINTE)

El mejor lugar para esconder algo suele ser a la intemperie (Edgar Allan Poe, 1844)

Edificio de 29 pisos de AT&T ubicado a la altura 33[160] de la calle Thomas Street en NY (vinculación con Verizon que paga impuestos por algunos pisos). El mismo no posee ventanas, puede soportar una explosión atómica y tiene alimento/agua para albergar 1500 personas durante 2 semanas. Adicionalmente cuenta con 250.000 galones de combustible para generadores de energía, lo que la convierte en una ciudad autónoma (ver figura 155) (Gallagher y Moltke, 2016).

Figura 155
TITANPOINTE.



Nota. Convenientemente ubicado frente al State Police y en la esquina el Jacob K. Javits Federal Building que incluye FBI y Homeland Security para su resguardo (observado en Google maps).

Es un gran Gateway switch que rutea las llamadas desde EE.UU. hacia el mundo y por lo tanto de interés para el tapping the la NSA en colaboración con AT&T (Company code name LITHIUM). Si bien existen varios edificios vinculados a lo largo del país nos

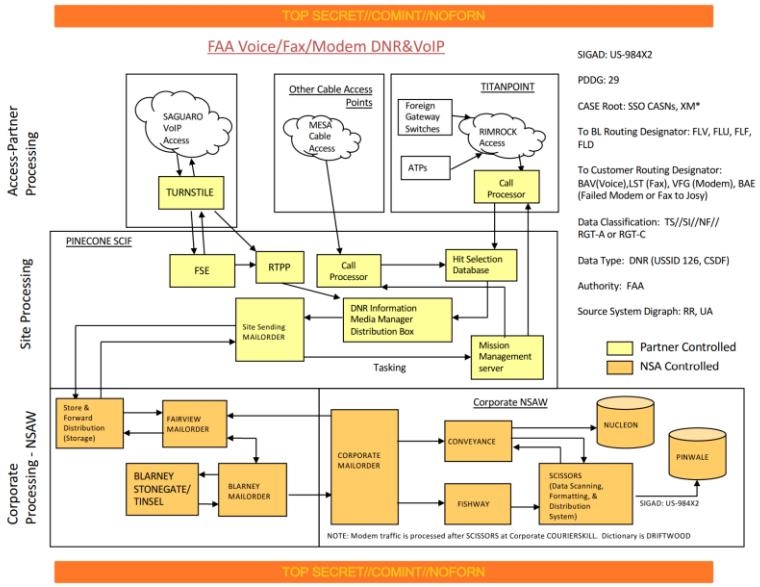
[160] No casualmente el numero 33 es el nivel más alto de la masonería.

limitamos a mencionar TITANPOINTE. El edificio contiene varios 4ESS switches[161] (code name RIMROCK). Además, participa del programa SKIDROWE para interceptar comunicaciones satelitales (Gallagher y Moltke, 2016).

TITANPOINTE es mencionado como uno de los Core Sites del programa BLARNEY. El programa fue iniciado en los 70, consiste en relaciones comerciales para ganar acceso a las redes globales y ganar inteligencia extranjera. Sus características son: contra proliferación, contraterrorismo, diplomático, económico, militar y político. Entre los objetivos se encuentra el FMI, Banco Mundial, Banco de Japón, Unión Europea, Naciones Unidas (un ejemplo fue influenciar la votación de sanciones contra Irán), países como Francia, Alemania, Italia, Japón, entre otros. Los equipamientos se colocan en una secret room llamada Sensitive Compartmented Information Facility. Utilizados para monitorear las llamadas de teléfono, fax, VOIP, videoconferencias y tráfico de internet (ver figura 156, 157 y 158) que proviene del backbone y es procesado aquí antes de pasar a la NSA (Gallagher y Moltke, 2016).

Figura 156

FAIRVIEW: Dataflow Diagrams.

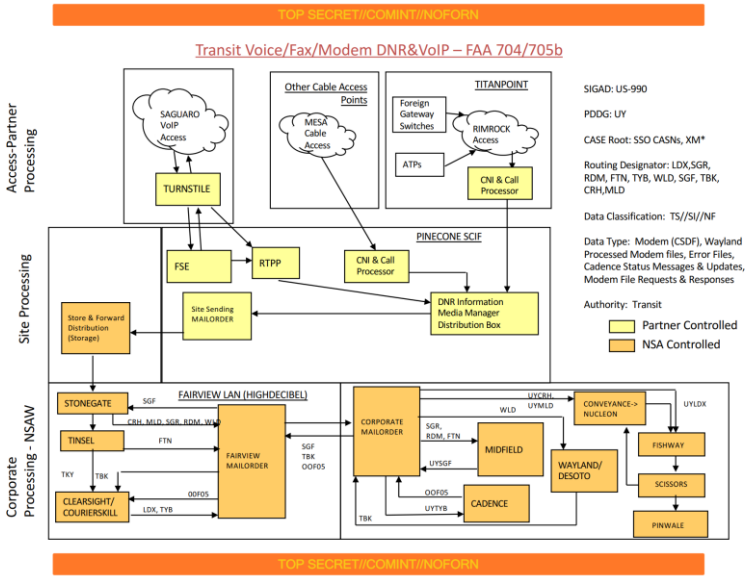


Nota. SMS, DNR (Dialed Number Recognition) and VoIP (FISA, cuando una punta sola es extranjera) (Gallagher, Moltke, 2016).

[161] Al día de la fecha posiblemente reemplazados por equipos más modernos.

Figura 157

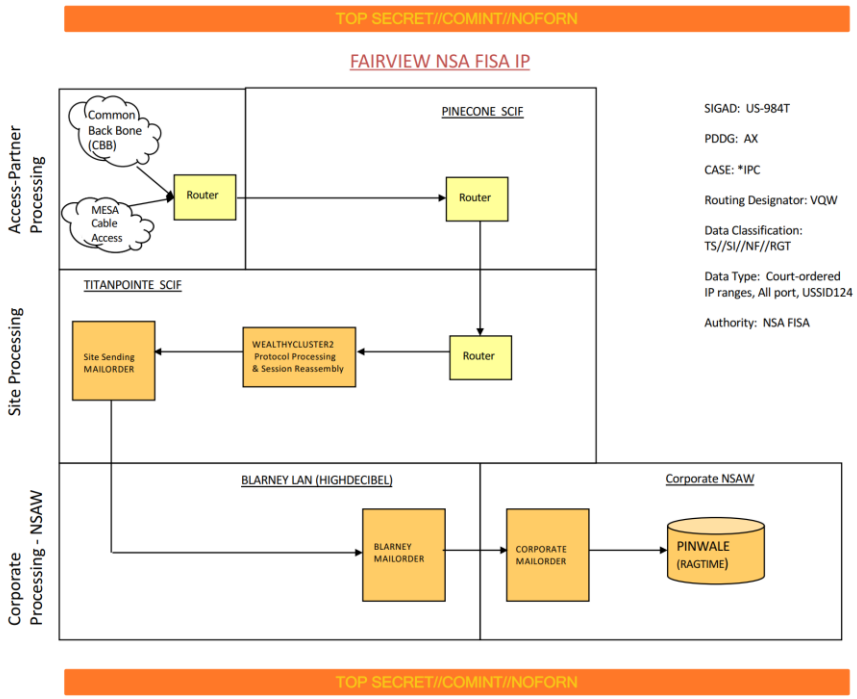
FAIRVIEW: Dataflow Diagrams.



Nota. NSA voice and VoIP (Transit Authority, cuando ambas puntas son extranjeras).

Figura 158

FAIRVIEW: Dataflow Diagrams.



Nota. IP range sesión reassembly (Mailorder es una especie de FTP) (Electronic Frontier Foundation, 2015).

Bumblehive - Centro de datos en Utah (Utah Datacenter).

Recójalo todo, etiquételo, almacénelo. Y lo que sea que quieras, vas a buscarlo[162]
(NSA Director, Keith Alexander; como fue citado por Greenwald, 2013).

Centro de datos construido en 2014, ubicado en Utah al lado de Camp Williams y próximo a firmas como Microsoft y Oracle. Acorde a Bamford (2012), el centro de datos tiene la función es descifrar (code breaking), analizar y almacenar las comunicaciones del mundo proveniente de satélites y cables subterráneos (ver figura 159 y 160). Ello incluye emails, llamadas telefónicas, búsquedas de Google, itinerarios de viaje, compras, etc. El descifrado de datos es fundamental para acceder a información financiera, transacciones de acciones, negocios, secretos militares, documentos legales, comunicaciones personales y secretos de diplomáticos extranjeros. Básicamente todo el mundo con comunicación es un objetivo. También existe interés en la Deep web que contiene las bases de datos (leaks), documentos gubernamentales e información de gran valor. El centro corresponde a la nube de la NSA, recopilando datos de satélites, puestos de escucha en el extranjero y salas secretas de monitoreo en las empresas de telecomunicaciones (Bamford, 2012). Las personas que piensan que nunca van a ser espiadas se engañan a si mismo psicológicamente con esta respuesta que solo busca eludir la realidad.

Los datos provienen de satélites, Buckley Air Force Base (inteligencia de satélites y puestos de escucha en el extranjero), Fort Gordon (Code name Sweet Tea - intercepciones de Europa, Medio Oriente y África), Lackland Air Force Base (intercepciones en América Latina, Medio Oriente y Europa), Hawái Oahu (intercepciones en Asia), puestos de escucha domestica (con las empresas de telecomunicaciones), puestos de escucha en el extranjero. También tiene comunicación con el centro de investigación de programas múltiples en Oak Rigde donde ingenieros trabajan contrayendo supercomputadoras y proyectos de criptoanálisis. Tener gran cantidad de datos cifrados ayuda al criptoanálisis (en caso de tratarse de una misma clave) (Bamford, 2012).

[162] La frase original: "*Collect it all, tag it, store it. And whatever it is you want; you go searching for it* ". En el contexto de la guerra de Irak, luego se popularizo en un sentido más amplio dentro de la vigilancia masiva: "*Collect it all*".

Figura 159

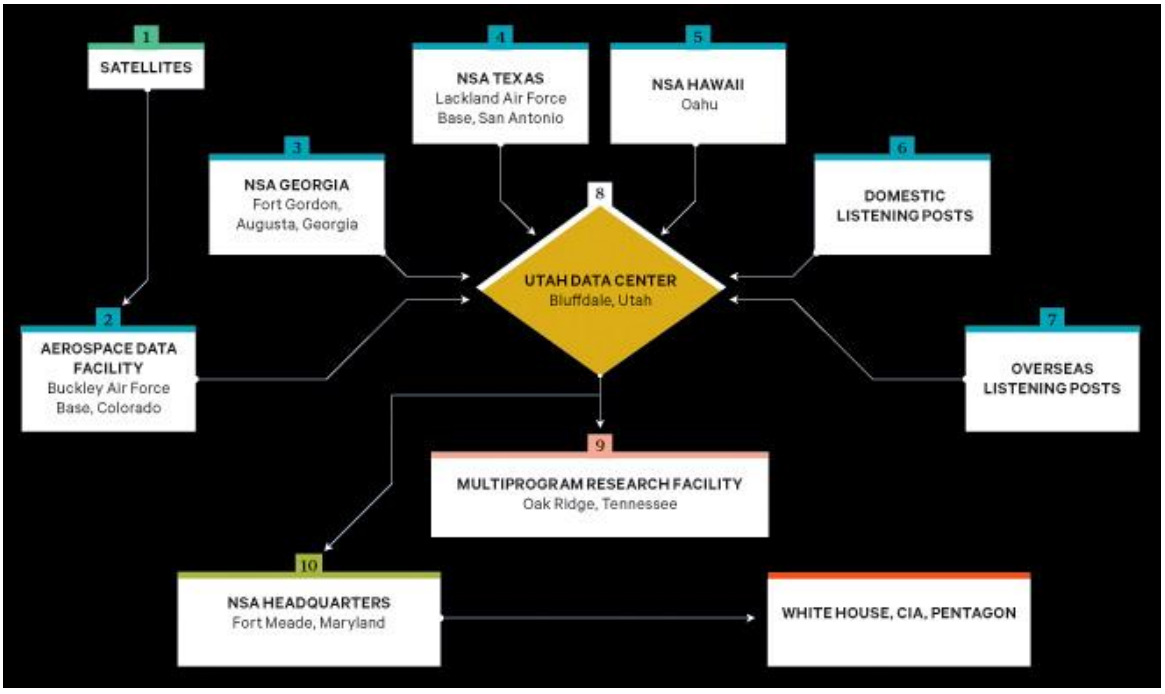
Utah Datacenter.



Nota. Diseñado para apoyar los esfuerzos de la comunidad de inteligencia para monitorear, fortalecer y proteger a la nación (foto NSA, 2013).

Figura 160

Utah Datacenter.



Nota. Recolección de información de varios sitios (Bamford, 2012).

Servicio de recolección especial (Special Collection Service).

El Special Collection Service (SCS - Codename F6) es un programa secreto conjunto de la CIA y la NSA (parte del programa STATEROOM). Operacional desde los 70' con la función de insertar equipamiento de eavesdropping en lugares difíciles como embajadas, instalaciones de gobierno, centros de comunicaciones (surgió para evitar la complejidad de descifrar los datos en tránsito) (Richelson, 2015; Appelbaum, Blome, Gude, Neukirch, Pfister, Poitras, Rosenbach, Schindler, Schmitz, y Stark, 2013). Existen varios sitios SCS de intercepción en el mundo (ver figura 161, 162 y 163). Robert Hanssen (doble agente ruso que trabajó en el FBI) brindó información a la KGB y predecesoras; acerca del programa entre 1979 hasta el 2001. Fue sentenciado a cadena perpetua como consecuencia a su traición (Lathem, 2001; U.S. Department of Justice, 2003).

Un ejemplo es la operación GAMMA GUPPY (code name). Durante los 70 interceptó los radioteléfonos de las limusinas de los líderes soviéticos en Moscú (incluyendo al presidente y al ministro de defensa). El contacto de la CIA era un mecánico que trabajaba con las limusinas. Luego de que el periódico revelara el caso en 1971, los soviéticos empezaron a cifrar las comunicaciones y el mecánico desapareció (presumiblemente muerto) [163]. La información obtenida de la operación ayudó al presidente Nixon durante las negociaciones del Strategic Arms Limitation Talks (SALT) (Richelson, 2015; CIA, 2001; CIA, 2012).

[163] Resulta indispensable remarcar la importancia en la responsabilidad de los periodistas que filtran información de que sus acciones pueden poner en peligro la vida de personas.

Figura 161

Special Collection Service (SCS) eavesdropping sites.



Nota. Centros en el mundo (Appelbaum, Blome, Gude, Neukirch, Pfister, Poitras, Rosenbach, Schindler, Schmitz, y Stark, 2013).

Figura 162

Equipamento Codename Einstein / Castanet.



Nota. Escondidos en falsa estructuras y cielos rasos (Pacific SIGDEV Conference leak) (Richelson, 2015).

Figura 163
CSS Oportunidades de accesos.



Nota. Pacific SIGDEV Conference leak (Richelson, 2015).

Desde el techo de la embajada norteamericana en Berlín (ver figura 164) pueden monitorear una gran parte de la comunicación celular en el barrio gubernamental. Hay evidencia de que los agentes con base en Pariser Platz apuntaron recientemente al teléfono celular que Merkel. La operación fue autorizada por el expresidente George W. Bush y su jefe de la NSA, Michael Hayden. Pero habría tenido que ser aprobado posteriormente por Obama (Appelbaum et al., 2013).

Figura 164
US Embassy en Berlín.



Nota. Desde donde se interceptan las comunicaciones del barrio gubernamental. Foto (Christian Thiel/Der Spiegel como fue citado por Electrospaces, 2013).

Acorde a WikiLeaks, entre 2006 y 2012, la NSA espió por medios no convencionales los teléfonos de 3 presidentes franceses (Jacques Chirac, Nicolas Sarkozy y François Hollande), incluyendo ministros, senadores, entre otros (Greenberg, 2015) [164].

La utilización de embajadas como medio para adquisición de inteligencia tampoco es nuevo. A finales de la edad media, Venecia empezó a colocar embajadas en el extranjero con el objetivo de recopilar inteligencia comercial/económica sobre socios comerciales y competidores; el objetivo era asegurar la protección de los monopolios comerciales y un comercio sin obstáculos. Napoleón también obtuvo su información de su servicio diplomático, embajadores y cónsules que tenían su propia red de espionaje. Los jóvenes diplomáticos se hicieron amigos de funcionarios de lengua suelta y ocasionalmente enamoraron a sus esposas (Lowenthal y Clark, 2015).

Caso Olympia.

El *Communications Security Establishment de Canadá* (CSEC), en conjunto con la NSA, mapearon todas las comunicaciones telefónicas y por computadora del Ministerio de Minas y Energía de Brasil; incluyendo a Petrobras (Greenwald, 2014; Bridi y Greenwald, 2013). Este tipo de incursiones no tienen relación con la defensa nacional del Five Eyes, lo cual resulta netamente ofensivo. ¿Qué clase de operación pensaba realizarse con dicha información? [165]

Breve mención de Rusia.

Acorde a Soshnikov y Reiter (2019) un hacker (0v1ru$) robó información de la empresa contratista del FSB llamada SyTech en 2019. A partir de la filtración se conocieron algunos proyectos.

- Nautilus (2009-2010): Rastrear la actividad de los usuarios en las principales plataformas de redes sociales (como Facebook, MySpace y LinkedIn).

[164] En el caso de Argentina, un documento de la embajada de EEUU solicita refacciones de una propiedad frente al edificio de la quinta presidencial de Olivos (Wikileaks, 2018). Desde la óptica de la inteligencia, resulta una ubicación estratégica. Sin embargo, no podemos afirmar o presumir que ese fuese su uso.
[165] Resulta indefectible pensar en diferentes casos del cono sur que afectaron tanto la política como a empresas regionales; dejando camino libre a empresas extranjeras. Casos que deberían estudiarse en profundidad desde la óptica de las operaciones de inteligencia dentro del marco de la geopolítica internacional y sus intereses.

- Nautilus-S (2012): Proyecto para desanonimizar el tráfico Tor basado en colocar nodos dentro de la red (particularmente nodo saliente). Sin embargo, Sytech comparaba las solicitudes de un usuario a internet e intentaba compararlas con el tiempo de visita de sitios (en el nodo saliente).
- Reward (2013-2014): Proyecto para penetrar secretamente en redes P2P.
- Mosquito (2015): Buscar y recopilar información en internet.
- Mentor (2013-2014): Espiar las comunicaciones por correo electrónico administradas por empresas rusas.
- Hope / Nadezhda (2013-2014): Analizar la Internet rusa y sus conexiones con el mundo.
- Tax-3 (2018): Permite eliminar manualmente datos de personas bajo protección estatal del sistema FTS (Financial tracking service).

Según Bagge (2019), mediante directive ministerial en 2014, Rusia cuenta con el System of Operational-Investigatory Measures (SORM-3). Lo que implica la instalación de equipos provistos por el FSB en empresas de telecomunicaciones para realizar DPI (Deep packet Inspection).

La trampa del vigilante.

¿Cuál es la sanción para el centinela cuando ocurre un hecho?
(reflexión de elaboración propia)

El centinela controla a todos los que transitan la puerta y advierte de posibles peligros que se aproximen desde la distancia. Sin embargo, cuando se asignan múltiples accesos al mismo centinela y las personas se trasforman en un torrente cuasi ilimitado y diverso de datos, dificulta su labor (velocidad de procesamiento). Es por ello por lo que se requiere de sistemas automáticos (IA) para asistir y alertar. Lo que no es posible de analizar puede almacenarse para su posterior uso. La diversidad de datos fomenta el desarrollo de bases de datos no estructuradas. El análisis automático promueve las diferentes técnicas de Inteligencia Artificial. El concepto del ciber panóptico también es funcional desde el aspecto de la disuasión, dado que todos se sienten vigilados.

A pesar de todo, existen algunos aspectos respecto de la figura de responsabilidad del encargado de vigilar y procurar la seguridad. Debido a las intercepciones de comunicaciones y acceso a los sistemas; se presentan algunas dudas razonables:

Legal checkmate: Bajo la óptica de la vigilancia masiva, resulta poco posible desconocer sucesos trascendentes (por ejemplo, caso Nisman). No brindar información implica encubrimiento. Facilitar la misma, implica confirmar la intercepción ilegal de las comunicaciones. ¿Por acción u omisión, existe un jaque mate legal?

Según la peligrosa doctrina Hack Back, que podemos encontrar en el manual de Tallin, "Rule 24: States entitled to take countermeasures" (Schmitt, 2017), un "Injured state", ¿podría tener un legítimo derecho a contra atacar los sistemas de vigilancia masiva?

Finalmente, ¿Qué pasa con el vigilante cuando no previene un atentado, tendría algún grado de responsabilidad?

El verdadero poder de las revelaciones sobre la vigilancia.

> *Lo que comenzó como profundamente invasivo se normalizó, se transformó en el estado de cosas habitual y dejo de ser notorio (Greenwall, 2014).*

Snowden acordó con los periodistas no publicar toda la información en una única nota, dado que pensaba que la noticia podría quedar en el olvido. Por lo que decidieron publicarlo gradualmente (Greenwall, 2014). Su análisis no es simple debido a la distribución de la información en diferentes medios, sumada a los nombres en código. En el presente trabajo no analizamos la misma en profundidad ni tampoco su veracidad. Bien podría Snowden ser una operación para desestabilizar, paralizar o generar ruido. Aunque todo indicaría que las revelaciones son válidas. El caso de Snowden se ha tomado seriamente. En 2013; España, Italia, Portugal y Francia; cerraron el espacio aéreo del avión presidencial de Bolivia (Evo Morales), el cual tuvo que aterrizar de emergencia en Austria; debido al rumor de que pudiera estar transportando a Snowden (BBC, 2013). Si bien el FiveEyes se ha visto afectado a causa de las revelaciones; por otro lado, ganaron un valioso tiempo disuasivo, sumado al gasto de recursos dedicado por otros estados en estudian dicha información. Con relación a las revelaciones, para el presente, resulta suficiente su

comprensión conceptual. Por otra parte, cabe resaltar que el verdadero poder de estas. Greenwall (2014) afirma:

> Independientemente de cómo se use o abuse de la vigilancia, los límites que impone a la libertad son intrínsecos a su existencia […] Lo que hace que un sistema de vigilancia sea efectivo para controlar el comportamiento humano es el conocimiento de que las palabras y acciones de uno son susceptibles de ser monitoreadas.
>
> Este principio estaba en el corazón de la concepción del Panóptico del siglo XVIII del filósofo británico Jeremy Bentham, un diseño de edificio que él creía que permitiría a las instituciones controlar de manera efectiva el comportamiento humano […] [las personas] actuarían como si siempre estuvieran siendo observados, incluso si no lo estuvieran. El resultado sería el cumplimiento, la obediencia y la conformidad con las expectativas.
>
> En la década de 1970, Michel Foucault observó que el principio del Panóptico de Bentham era uno de los mecanismos fundacionales del Estado moderno. En Power, escribió que el panopticonismo es "un tipo de poder que se aplica a los individuos en forma de supervisión individual continua, en forma de control, castigo y compensación, y en forma de corrección, es decir, el moldeado y transformación de los individuos en función de ciertas normas" […] Además, este modelo de control tiene la gran ventaja de crear simultáneamente la ilusión de libertad. La compulsión a la obediencia existe en la mente del individuo (Greenwald, 2014).

Contramedidas.

Como ya hemos adelantado, las medidas más básicas para eludir los sistemas de vigilancia son evitar, cifrar y desinformar / engañar.

Evitar quizás sea el menos práctico. Consiste justamente en evitar comunicar la información sensible a tratar, donde los participantes de un proyecto, operación, etc.; trabajan de manera aislada e incomunicada como celdas independientes. Además de ser poco práctico suele inquietar mucho a los agentes de inteligencia que se alimentan de información (como vampiros que necesitan sangre). Resulta más práctico saber administrar los canales de comunicación. Tanto los canales seguros como los inseguros, que pueden ser útiles a la hora de brindar desinformación.

La otra medida es la utilización de criptografía, esteganografía y canales encubiertos. Sin embargo, hay que remarcar que inteligencia siempre está un paso adelante, tal como veremos a continuación.

Paradoja del cifrado.

> *La matemática criptográfica permite proteger secretos, pero una mejor matemática permite a los atacantes escuchar las comunicaciones (parafraseando a Buchannan).*

Caso ENIGMA.

Durante la segunda guerra mundial (WWII), los alemanes utilizaban para comunicarse una máquina llamada enigma (ver figura 165). Este dispositivo cifraba los mensajes enviados, previniendo de esta manera que el mensaje pudiera ser leído, adulterado o reemplazado por el enemigo. Protegiendo así la integridad, la confidencialidad y previniendo ataques del tipo *Man in the Middle* o *Tampering*.

Originalmente desarrollada por dos oficiales navales holandeses en 2015. La máquina enigma fue desarrollada en 1917 y patentada en 2018 por el alemán Arthur Scherbius. Enigma es una serie de máquinas que fueron evolucionando en el tiempo. En 1932, el ejército alemán reclamó los derechos exclusivos de la máquina (Crypto Museum, s.f.).

Figura 165
Máquina Enigma alemán.



Nota. Utilizada durante la WWII para el cifrado de mensajes (Fuente imagen: Computer Museum of America, 2020).

La máquina consistía en una serie de circuitos eléctricos. Había un plugboard que permitía conectar una serie de cables (habitualmente 10) para intercambiar dos letras entre sí; generando una sustitución (ver figura 166). Luego entraban en juego los rotores. Cada rotor contenía 26 conectores de entrada y 26 de salida (correspondientes a las 26 letras del abecedario). Estos conectores contenían internamente unos cables para mezclar los circuitos eléctricos entre la entrada y la salida (ver figura 167) (cada uno con una configuración propia). Los rotores, a su vez, se conectaban con otros rotores permitiendo sucesivas sustituciones (ver figura 168). Posteriormente, un reflector producía una mezcla adicional, regresando el circuito nuevamente hacia los rotores (ver figura 169). A la salida de los rotores pasaba nuevamente por el plugboard para un intercambio adicional y finalmente iba a un circuito de luces que iluminaba la letra resultante luego de todas las sustituciones (ver figura 170). Adicionalmente, había un mecanismo mecánico que giraba los rotores cada vez que se presionaba una tecla. De esta forma, se evitaba que una letra tuviera siempre la misma sustitución. Primero giraba el rotor de la derecha, que al completar una vuelta completa pasaba a girar el segundo rotor y así sucesivamente. En definitiva, la clave del cifrado estaba conformada por la selección de los rotores a utilizar (había 3 de 5 rotores disponibles), el orden como se colocaban en la máquina, la posición inicial de los mismos y finalmente la configuración del cableado del plugboard[166] (Fuente: CryptoMuseum, s.f).

Figura 166

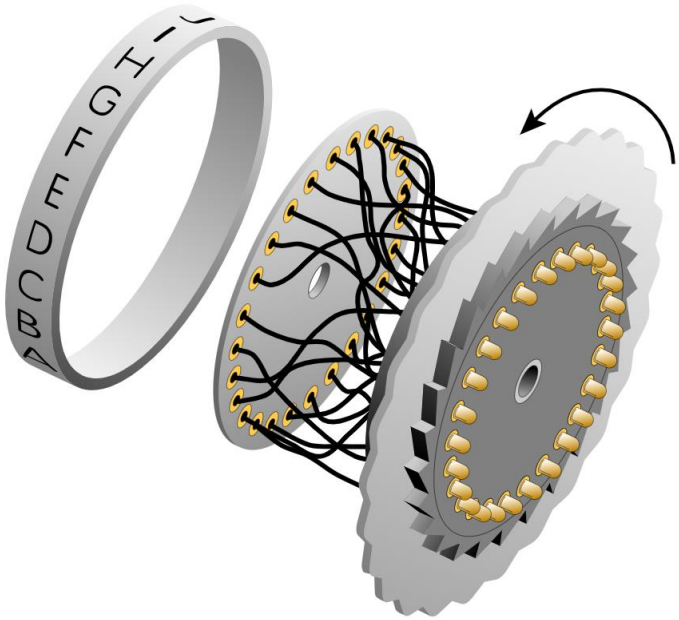
Plugboard de la máquina Enigma alemán.



Nota. Se utilizaban 10 cables para intercambiar dos letras entre si (Fuente imagen: Captura de Owen, 2021).

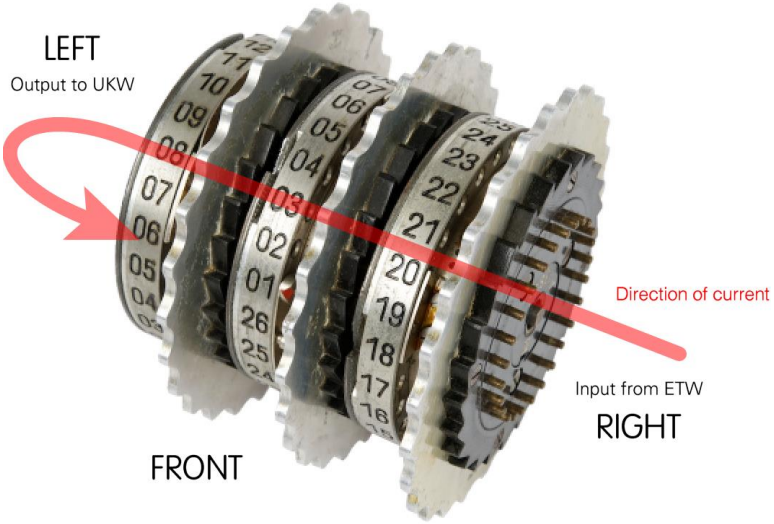
[166] Para una mayor comprensión, se recomienda el video de (Owen, 2021): https://www.youtube.com/watch?v=ybkkiGtJmkM

Figura 167
Rotor de la máquina Enigma alemán.



Nota. Los cables internos realizaban una sustitución (Fuente: CryptoMuseum, s.f).

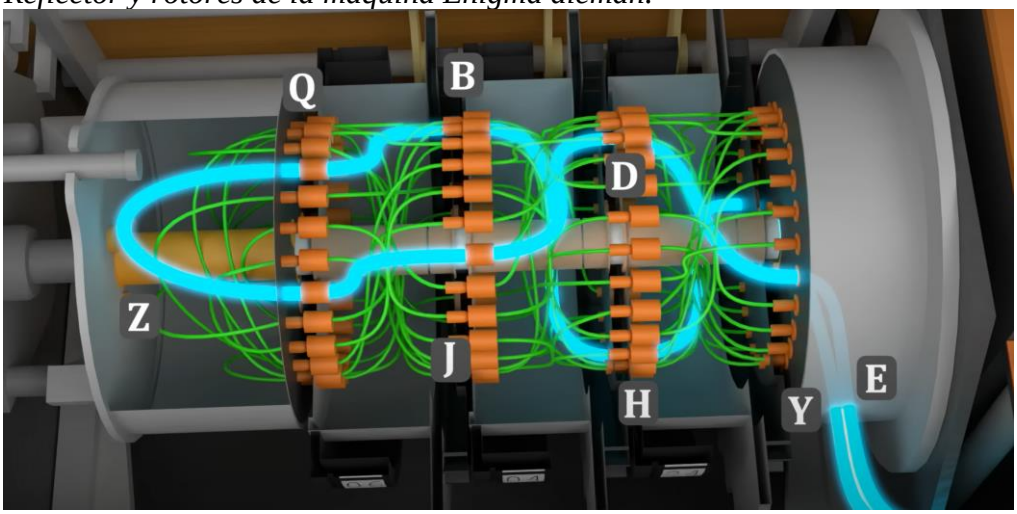
Figura 168
Rotores de la máquina Enigma alemán.



Nota. Se conectaban entre si realizando sustituciones (Fuente: CryptoMuseum, s.f).

Figura 169

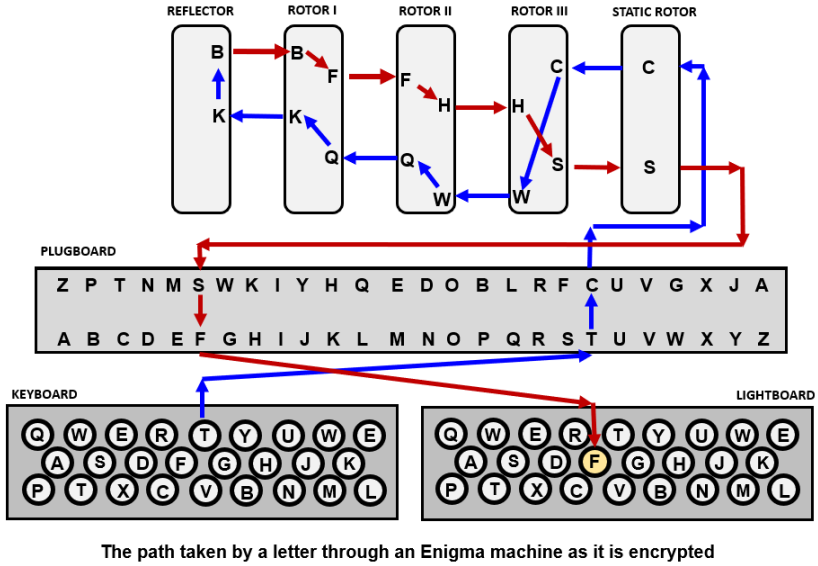
Reflector y rotores de la máquina Enigma alemán.



Nota. El rotor de la izquierda intercambiaba letras y regresaba el circuito a pasar nuevamente por los rotores (Fuente: CryptoMuseum, s.f).

Figura 170

Máquina Enigma alemán.

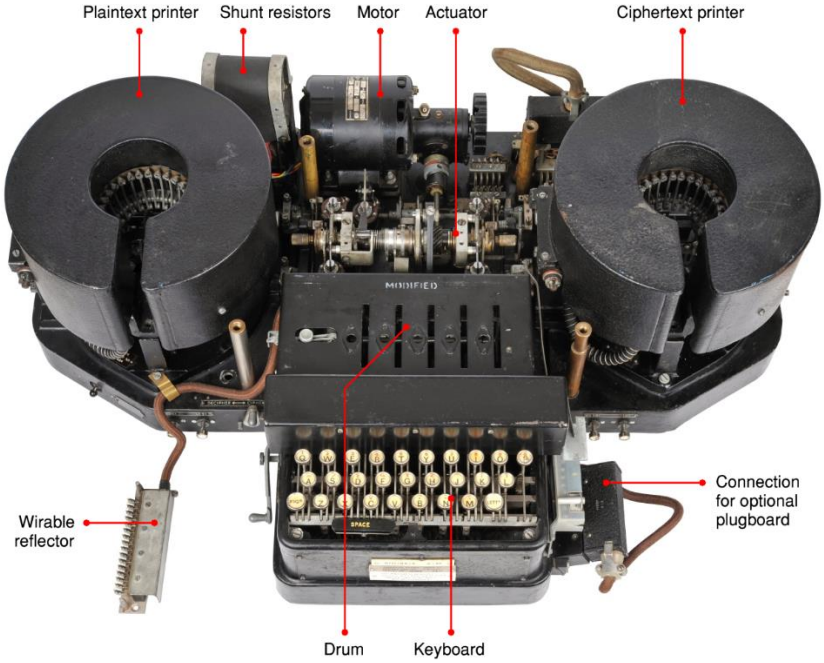


Nota. Diagrama del funcionamiento (Fuente imagen: Une University of New England, s.f.).

Los británicos también poseían una máquina similar llamada Typex y Estados unidos utilizada otra denominada SIGABA (ver figura 171 y 172) (Crypto Museum, s.f.).

Figura 171

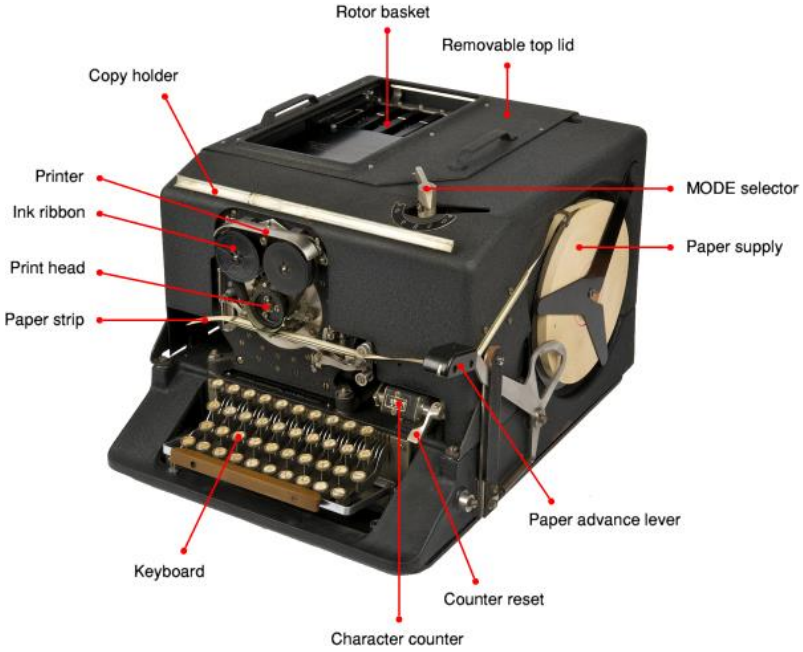
Máquina de cifrado Reino Unido.



Nota. Typex (Fuente imagen: Crypto Museum, s.f.).

Figura 172

Máquina de cifrado EEUU.



Nota. SIGABA (Fuente imagen: Crypto Museum, s.f.).

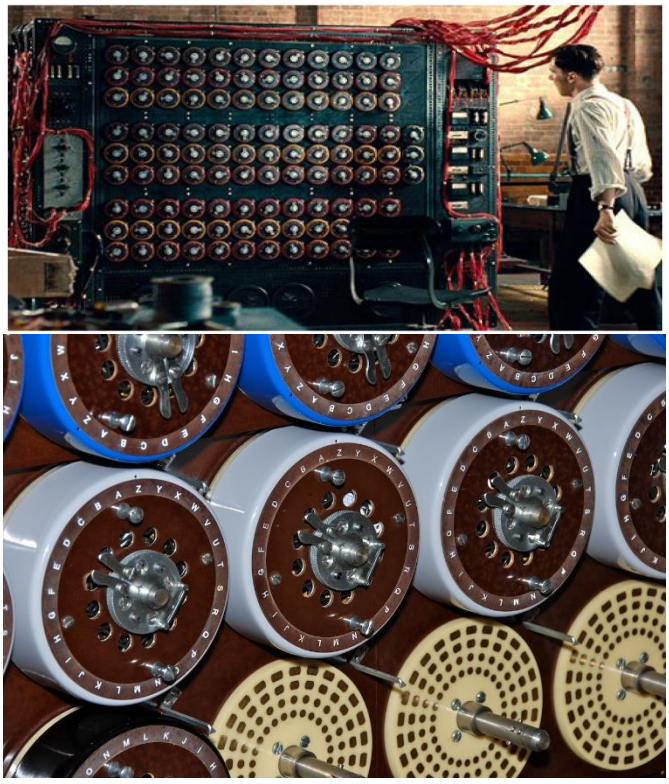
Tres matemáticos polacos (Marian Rejwski, Jerzy Rózycki y Henryk Zygalski) empezaron a trabajar para romper el cifrado de la máquina enigma. Rejewski se puso a

trabajar en el problema a fines de 1932 y dedujo el cableado interno secreto del Enigma. Zygalski desarrolló las llamadas hojas de Zygalski que se utilizaron para explotar el indicador de mensaje de doble cifrado, una debilidad en los procedimientos alemanes (el mismo indicador de mensaje se enviaba dos veces al comienzo de cada mensaje). Posteriormente desarrollaron una máquina mecánica llamada bomba[167] criptológica (Bomba kryptologiczna) para explotar dicha vulnerabilidad. En 1939 con la guerra inminente, los polacos entregaron sus conocimientos y una réplica de la máquina a los franceses y británicos. Por su parte, los alemanes, incorporaron en 1938, dos rotores adicionales multiplicando la cantidad de posibilidades por un factor de 10 (Crypto Museum, s.f.).

En 1939, el matemático británico Alan Turing diseñó la bomba británica (code name Victory), que se trataba de una variante de la bomba polaca (ver figura 173). Se basó en la suposición de que un texto conocido (plain text) estaba presente en una determinada posición en el mensaje (ejemplo “Heil Hitler”). Posteriormente, Gordon Welchman desarrolló un tablero diagonal que reducía los pasos necesarios (denominada Agnus Dei/Agnes/Anggie). Finalmente incorporó el tablero diagonal a la “Victory”, por eso hoy en día se habla de “bombas Turing-Welchman” (ver figura 174). Los resultados eran probados en una Typex modificada para actuar como una Enigma (Crypto Museum, s.f.).

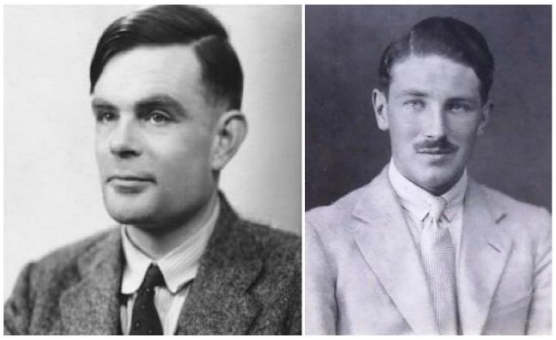
[167] Su nombre deviene a que rotores electromecánicos hacían un ruido similar al conteo de una bomba.

Figura 173
Bombe británica.



Nota. Imagen superior: captura de la película “The Imitation Game” de Morten Tyldum (2014). (Fuente imagen inferior: Crypto Museum, s.f.)

Figura 174
Turing y Welchman.



Nota. Alan Turing (1912 - 1954) y Gordon Welchman (1906 - 1985).

Gracias al trabajo de los criptólogos (polacos y posteriormente británicos), la guerra finalizó aproximadamente 2 años antes de lo previsto (UK Government, 2013). Salvando innumerables vidas humanas. Dejando en claro la importancia y el fuerte interés de los estados en la materia.

Alan Turing realizó importantes avances como la máquina de Turing o la prueba de Turing de inteligencia artificial. Lamentablemente tuvo un triste final en su vida. En 1952 el gobierno británico lo condenó por ser homosexual (section 11 of the Criminal Law Amendment Act 1885) y lo obligó a realizar una terapia hormonal (castración química) a fin de evitar la cárcel. Dos años después, muere a los 41 años por suicidio ingiriendo una manzana con cianuro. En 2009 el primer ministro británico pidió disculpas públicas por el trato que le dieron (Bailin y Halford, 2012). La reina Elizabeth II, junto al secretario de justicia (Chris Grayling); otorgaron un indulto (royal pardon) en 2013 (UK Government, 2013).

Durante el curso de la guerra, construyeron más de 200 bombas Turing-Welchman. Para evitar el riesgo de perderlos en caso de un ataque con bomba, estas instalaciones se extendieron entre Bletchley Park (ver figura 175) y sus llamadas Outstations en Wavendon, Adstock, Gayhurst, Eastcote y Stanmore (Bletchley Park Museum, s.f.).

Figura 175
Bletchley Park.



Nota. Bletchley Park fue elegido por sus facilidades de transporte. Posteriormente utilizado para entrenar al US Navy / Army en criptoanálisis. (Fuente imagen: GCHQ Museum, s.f.)

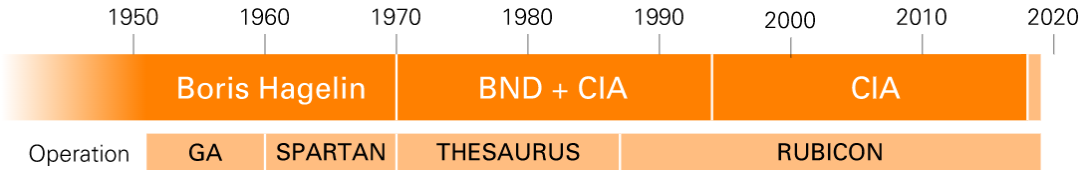
Los secretos de Bletchley Park salieron a la luz en 1974 con el libro (The Ultra Secret) del oficial de la RAF, Winterbotham. Algunos autores, como Kahn, indican que, al finalizar la guerra, los británicos vendieron máquinas a países emergentes para espiarlos. Acorde a Baldwin (2022), no existen evidencias sólidas para dicha afirmación. Pero si es

posible afirmar que países como Alemania del este, que poseía algunas máquinas, fueron espiados durante la guerra fría hasta 1956 (Baldwin, 2022).

Caso MINERVA y la vinculación con la guerra de Malvinas (Operación THESAURUS/ RUBICON).

¿Hemos aprendido algo de la historia? Acorde a Crypto Museum (s.f.), la empresa suiza Crypto AG (code name MINERVA) fue fundada por el sueco Boris Hagelin en la década del 30'. Dedicada a proveer equipos de cifrado para comunicaciones seguras a diferentes países del mundo. De forma secreta mantuvo negociaciones con William Friedman llegando a un acuerdo con la NSA (Gentleman's Agreement de 1951 a 1960) y John Ferguson acordando con la CIA (Licencing Agreement de 1960 a 1970 – Operation Spartan). Durante la operación Thesaurus (posteriormente Rubicon), la CIA y el BND (Bundesnachrichtendienst – Inteligencia alemana) compraron la empresa en los 70' de forma secreta. Luego de 94' queda en manos de la CIA (ver figura 176). Las construcciones de algunas máquinas fueron realizadas por MOTOROLA y SIEMENS. La operación permitió espiar al menos a 120 países durante 50 años (hasta el 2000) (Crypto Museum, s.f.).

Figura 176
Crypto AG – CIA BND Operations.



Nota. Fuente Cryptomuseum.

El desarrollo de los diferentes modelos de máquinas a lo largo todos estos años implico un verdadero trabajo para la NSA que debía buscar la manera de hacer las máquinas vulnerables, pero al mismo tiempo que parecieran seguras.

Durante la guerra de las Malvinas, el gobierno argentino compró las máquinas HC-570 y HC-520 (ver figura 177) que eran espiadas por los alemanes y norteamericanos. El matemático Kjell Ove Widman (code name ATHENA) de Crypto AG mintió y engañó al gobierno argentino al convencer que las máquinas eran seguras (Crypto Museum, s.f.).

Figura 177

Crypto AG – HC-520 utilizada en la guerra de Malvinas.



Nota. Desarrollada por SIEMENS, utilizaba un microprocesador MOTOROLA[168] 6800 con un algoritmo vulnerable provisto por la NSA. Fuente Crypto Museum.

Durante 1976, la CIA proporcionó (a través de Crypto AG a Brasil) máquinas de cifrado vulnerable (Hagelin CX52 - ver figura 178) para la red CONDORTEL. La misma fue reemplazada en 1977 por la Hagelin Crypto H-4605 a pedido de Argentina, quien además supervisó la incorporación de Ecuador en 1978. CONDORTEL era utilizada para coordinar operaciones represivas entre los gobiernos golpistas en Latinoamérica dentro del plan Cóndor. En dicha red se informaba para la persecución de los refugiados exiliados (Kornbluh y Osorio, 2020).

[168] La empresa hoy en día vende celulares en nuestro país a pesar de haber participado de la inteligencia que asesinó a soldados argentinos. La dominación y la propaganda cumplen un rol en dicho rumbo.

Figura 178

Hagelin CX52 y su reemplazo Hagelin Crypto H-4605.



Nota. Utilizada en la red CONDORTEL (Kornbluh y Osorio, 2020).

Caso BULLRUN

El mejor backdoor es el que aparenta ser un simple bug (Matthew Green).

Programa clandestino secreto de la NSA cuyo objetivo es vencer la seguridad de distintas tecnologías de cifrado usadas en redes de comunicaciones (TLS, SSH, VPN, cifrado de voz, etc). Su homólogo británico sería el programa Edgehill de la GCHQ.

Las agencias buscan promover la adopción de estándares, protocolos o sistemas con debilidades o *backdoors*. Como mencionamos con anterioridad, mantener la vara lo suficientemente alta como para proteger mínimamente a los ciudadanos, pero lo suficientemente baja para no perder los accesos. Este concepto se llama NOBUS (Nobody But Us) (Buchanan, 2020). Para lograrlo cuenta con acuerdos con las empresas proveedoras, infiltrados, recomendaciones del NIST, entre otros. Además, cuenta con la asistencia con un enorme equipo de matemáticos investigando en la materia.

Como ejemplos es bien conocido el caso del cifrado Lucifer que originalmente constaba de 128 bits. La NSA reemplazó las cajas de sustitución (esta sustitución aparentemente fortaleció de ataques de criptoanálisis diferencial), pero por otra parte redujo los 128 bits a 64bits y utilizo 8 para paridad quedando solo 56bits (suficiente para ataques de fuerza bruta). Como resultado nace el DES (Harris y Maimí, 2019). Otro caso conocido es el del generador de números aleatorios Dual_EC_DRBG que contenía una vulnerabilidad y la NSA recomendó al NIST en 2006. Paralelamente pago en secreto $10 millones a la empresa RSA para que incluyera esta debilidad en su librería RSA BSAFE (Menn, 2013; Glaser, 2014). La NSA también lazo dos cifrados livianos[169] (Simon y Speck) (Beaulieu, Shors, Smith, Treatman-Clark, Weeks y Wingers, 2013), pero fue rechazado por ISO en 2018 (Ashur y Luykx, 2021).

Caso SENTRY EAGLE

Acorde a Maass, Poitras (2014), La NSA ha utilizado agentes encubiertos para obtener acceso a datos y sistemas confidenciales en la industria de las telecomunicaciones globales. Además, la NSA trabaja con empresas estadounidenses y extranjeras para debilitar los sistemas criptográficos. Según revelaciones de Snowden, es un término general que abarca los programas más sensibles (Core Secrets) para proteger el ciberespacio norteamericano mientas explota el de los otros países. Se encuentra relacionado con la misión cristológica e incluye 6 programas: Sentry Hawk (explotar redes informáticas / espionaje con ayuda de empresas), Sentry Falcon (defensa de redes informáticas), Sentry Osprey (cooperación CIA y otras agencias en target exploitation/TAREX), Sentry Raver (romper/debilitar sistemas de cifrado con colaboración de empresas como el caso citado de RSA), Sentry Condor (operaciones y ataques a redes informáticas) y Sentry Owl (colaboración con empresas privadas). Tarex está integrado por personal de la CIA, FBI y DIA para operaciones clandestinas (SIGINT/HUMINT) en todo el mundo. Las operaciones "off net enabling" (encubiertas o clandestinas), "Supply chain enabling" (ver figura 179) (interdiction activities para modificar equipamiento en la cadena de suministro) y "harware implant enabling" (Maass y Poitras, 2014). Entre los objetivos de la presentación filtrada por

[169] Para dispositivos con baja capacidad de procesamiento como ser los IOT.

Snowden figura Corea del Sur, Alemania, Beijing, China (países clave en fabricación de equipos de telecomunicaciones); como así también operaciones domesticas en Hawái, Texas y Georgia. Los documentos indican infiltración de agentes encubiertos en entidades comerciales (SIGINT enabling) como también acuerdos con empresas extranjeras con el fin de hacer productos explotables para SIGINT (Maass y Poitras, 2014).

Figura 179
Interdiction.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Nota. Filtraciones de Snowden (Greenwald, 2014).

Desinformación y engaño.

Negarle alimento a un vampiro puede ponerlo muy inquieto ¿Qué sangre le darías? ¿propia, de otro, agua con colorante o sangre envenenada?
(reflexión de elaboración propia)

Cuando una persona es un objetivo, sus posibilidades son prácticamente nulas frente a las capacidades de inteligencia. En tales condiciones, la administración de los canales de comunicación resulta imperativa y el engaño entra en juego.

Según el DoD, el engaño son aquellas medidas diseñadas para engañar al enemigo mediante la manipulación, distorsión o falsificación de evidencia para inducir al enemigo a reaccionar de una manera perjudicial para los intereses del enemigo.

Acorde a Caddell (2014), un uso habitual del engaño político es ocultar un objetivo estratégico mientras que el engaño militar puede ser pasivo (ocultar intenciones o algo existente) o activo (crear falsas suposiciones que no existen). Cuando la información es falsa se llama *fabricación* y está destinada a engañar a un oponente (unidades inexistentes, ordenes falsas, etc). Cuando se utiliza información genuina, pero distorsionada o fuera de contexto se llama *manipulación* y resulta más adecuada para cuando algo evidente no puede ser ocultado. En cualquier caso, el engaño es intencional y está diseñado para ganar una ventaja contra el adversario. Como ejemplo, Roosevelt mostró un mapa secreto de Hitler con la intención de invadir América. El mapa en realidad era una fabricación del MI6 para causar alarma en EE.UU. y hacerlos participe de la guerra. Aun así, se cree que Roosevelt podría tener presente de la falsedad e igual le fuera útil engañar a la opinión pública.

Según Daniel y Herbig (como fue citado por Caddell, 2014), existe un engaño tipo A diseñado a crear confusión y aumentar la ambigüedad (ej. las negociaciones diplomáticas de Japón con EE.UU. previo al ataque de Pearl Harbor hizo que los analistas no pudieran predecir la acción militar). Mientras que el tipo M está diseñado para engañar a que el enemigo crea un plan falso (ejemplo, la operación BODYGUARD ya mencionada que incluía FORTITUDE NORTH y FORTITUDE SOUTH, engaños para cubrir la verdadera operación OVERLORD). Esta última es más difícil de lograr y requiere mayor esfuerzo.

Lo que los rusos llaman Maskirovka se trata de campañas de engaño enfocadas a llevar a conclusiones erróneas al adversario militar o político. La información modela la percepción del entorno y las circunstancia, lo que constituye el contexto de la conciencia sensorial. Un ejemplo que cuenta Buchannan (2020) es el engaño de Rusia para llevar los misiles a Cuba durante la famosa crisis de los misiles. Los nombres en código hacían parecer que los misiles se dirigían al Mar de Bering, los misiles estaban ocultos en granjas cubiertos con hojas de metal para evitar las fotografías infrarrojas. El capitán del barco no conocía su destino hasta último momento. Para ampliar el engaño, los soviéticos filtraron información precisa de su operación a las fuerzas contrarrevolucionarias cubanas para que estas llevaran la noticia a inteligencia occidental y a su a su periódico amigo en Miami que tenía una reputación exagerar los hechos. La CIA descartó las afirmaciones hipérbole y creyó en las negativas soviéticas.

El engaño también puede convertirse en sabotaje. Acrode a Geiss (1996), el coronel Vladimir Vetrov (nombre en código Farewell), fue un ingeniero de la KGB en Francia. Tenía la función de evaluar información de la sección *línea X* del *Directorate of Scientific and Technical Intelligence* de la KGB. La *línea X* contenía agentes secretos en embajadas con la finalidad de obtener tecnología occidental para la Unión Soviética. Sin embargo, Vetrov desertó en los 1981 y brindó información a inteligencia francesa (Direction de la surveillance du territoire – DST) sobre los agentes y documentos robados. Estos documentos son conocidos como Farewell Dossier y Francia compartió esta información con USA. La CIA, al reconocer que los soviéticos estaban espiando sus tecnologías, planeó deslizar diseños defectuosos a los agentes soviéticos, con ayuda del FBI. Lo que terminó en chips de computadoras de baja calidad instaladas en equipamiento soviético, una turbina defectuosa en las tuberías de gas, fabricas químicas defectuosas, engaños sobre aviones de sigilo, e inclusive planos rechazados por la NASA del transbordador espacial[170].

Los rusos también utilizan el Control Reflexivo (*Reflexibe control*) que consiste en imponer suposiciones erróneas al adversario para modificar su manera de actuar. Implica comprender el modelo de toma de decisión para corromperlo de forma tal que las decisiones sean favorables al engañador. Esto se logra influenciando los canales de comunicación, manipulando los sentidos de cómo se procesa la información lleva a una percepción errónea de la realidad, ocultar las verdaderas intenciones. El conflicto no debe verse como la interacción de dos fuerzas militares si no como la interacción de dos sistemas de tomas de decisiones (Bagge, 2019).

El engaño también puede ser utilizado para encontrar objetivos. En 1996, el líder checheno, Dzhokhar Dudayev, fue asesinado con 2 misiles aire tierra guiados por láser lanzados desde un Sukhoi Su-25 ruso. El hecho se produjo luego de localizar la señal de su

[170] Existe un antecedente sobre una explosión de un gasoducto que transportaba gas desde Siberia a Europa. El evento no es claro dado las discrepancias entre autores. Acorde a Reed, como fue citado por Kettmann (2014), los soviéticos robaron un software para operar un oleoducto en el cual la CIA habría colocado un troyano. El software estaba diseñado para operar bien solo por algunos meses y luego elevar la presión de gas, lo que terminó causando una inmensa explosión en 1982. Un ex miembro de la KGB negó que la explosión fuera causada por el motivo descripto. Como menciona Joshi (2019), Regan impulsó un embargo a la tecnología de USA que necesitaba URSS para el oleoducto. Por lo que recurrió a una empresa canadiense. Según un agente de la CIA, en realidad la explosión fue a causa de una fuga de gas, a la cual un ingeniero incrementó la presión para mantener el suministro. Un tren ruso que pasaba causó la nube de gas y su explosión. Hasta la fecha no se ha podido aclarar con certeza este suceso de la historia.

teléfono satelital mientras entablaba conversaciones de paz con Konstantin Borovoi (bajo orden del presidente Borís Yeltsin). La charla fue solo un engaño para prolongar el tiempo de la llamada y poder localizar su posición (*Deception, Find, Lock and Kill*). No queda claro cómo se obtuvieron las coordenadas dado discrepancias entre autores. Según Pelton (2012), otro avión ruso de inteligencia electrónica (ELINT) captó la señal, acorde a Madsen (2013) la NSA localizó la ubicación con sus satélites espías y entregó las coordenadas d Rusia. El contexto de la ayuda era impulsar las candidaturas tanto del presidente Borís Yeltsin como de Clinton (recordemos que Yeltsin mantenía una postura muy cercana a Washington).

Algunos conceptos claves del capítulo.

A continuación, repasaremos brevemente algunos conceptos relevantes del presente capitulo:

- Si bien las revelaciones de Snowden han quedado desactualizadas a la fecha y no analizamos su veracidad; conceptualmente ilustran las intenciones y capacidades de la vigilancia. Las capacidades actuales/futuras indefectiblemente utilizaran inteligencia artificial y patrones biométricos (voz, reconocimiento facial, análisis automático de datos), entre otras tecnologías.
- Para encontrarlos, solo hay que seguir el camino de los datos.
- La inteligencia habitualmente tiene una componente intrínseca de ilegalidad.
- Muchas de estas tecnologías pueden “rebobinar” al pasado.
- Ganar acceso a los sistemas de información puede garantizarse mediante leyes, acuerdos, infiltrados, influencia, afectación a la cadena de suministro (implantación de tecnologías) o incluso mediante técnicas de hacking.
- Existe un mecanismo de espionaje mutuo para bypasear la ley. EE.UU. puede enviar las comunicaciones de sus ciudadanos a Reino Unido y viceversa. Posteriormente se intercambian la información por acuerdos de intercambio.
- La inteligencia es un paso necesario para las operaciones dentro de un kill chain. La utilización del ciberespacio amplia y potencia las capacidades de adquisición de información como así también las ciber operaciones.

- Durante el capítulo anterior, sobre la guerra híbrida, se han mencionado algunos casos vinculados a cuestiones domésticas más que internacionales. La explicación de ello es que esa distinción ya no es tan clara. Existen infiltrados operando en otros países, convenios secretos con empresas por afuera del conocimiento del gobierno local, acuerdos secretos con agencias de inteligencia de otros países fuera del consentimiento del gobierno/ciudadanos, etc. Las estructuras mentales que poseemos ya no son útiles para comprender la complejidad del mundo actual. La división entre injerencia doméstica o internacional no solo no es clara, sino que ha desaparecido completamente. Al igual que la seguridad perimetral corporativa ya no es suficiente, la seguridad en un estado/nación no puede pensarse separando la seguridad interior de la seguridad exterior.
- Argentina podría tener un legítimo derecho a exigir una restitución económica a causa del daño provocado en la guerra de Malvinas. Por haber EEUU participado en la guerra desde las sombras, sin una declaración formal. Por proveer tecnología de cifrado seguro cuando en realidad era, insegura por diseño. Aportando información confidencial al enemigo.
- La dominación a la que se encuentra sumida el país no permite los planteos del punto anterior. El derecho se ejerce desde el poder y para el poder.
- De no despertar a tiempo, países europeos podrían sufrir el mismo destino.
- Existen individuos trabajando en hacer las comunicaciones más seguras, mientras que, al mismo tiempo, otros trabajan en el objetivo opuesto. La tecnología llega al público solo cuando se encuentra en un umbral intermedio.
- La NSA busca mantener la seguridad los sistemas (incluyendo el cifrado) lo suficientemente alta para prevenir ataques externos; pero lo suficiente baja como para no perder sus accesos. De manera análoga, sucede algo similar con Latinoamérica respecto a la dominación; las operaciones mantienen en un umbral controlado de crecimiento con sabotaje de proyectos estratégicos, guerra económica, etc. Sin embargo, es de esperar eventuales asistencias, dado que el deterioro no resulta del todo conveniente (perdida de negocios, proliferación de

drogas que terminan en su país, surgen ideas antinorteamericanas, alineamiento con otros países enemigos).

- El verdadero poder de la vigilancia es generar la ilusión de la libertad; mientras que el poder ejerce la obediencia en la mente de las personas, inclusive cuando no están siendo vigiladas.

Capítulo ~~(3)~~ Fobos – Proyecto Cóndor: Sabotaje y robo tecnológico.

El presente capítulo es una mención sobre el proyecto argentino Cóndor. Este caso de estudio permite identificar acciones de guerra sin restricción estudiadas a lo largo del presente trabajo.

Caso Proyecto Cóndor.

Resulta imperiosa la mención del caso del proyecto Cóndor en el que podemos identificar diferentes tipos de operaciones de guerra híbrida que llevaron a su sabotaje.

El proyecto consistió en un programa estratégico argentino para el desarrollo de cohetes de largo alcance con la finalidad de ser utilizado como lanzador espacial, incluyendo su plataforma de lanzamiento en falda del Carmen (falda Cañete en realidad). Dada la similitud de la tecnología, también tiene un uso dual como misil de largo alcance. Hecho que termino causando presiones internacionales para su cancelación (De León, 2017).

De León realizó una investigación que no resulta fácil de resumir. Ello se debe a que se trató de un largo programa que atravesó diferentes gobiernos, incluyó modificaciones, cambios en los organismos que dirigían el proyecto y su secretismo presenta algunas diferencias en la visión de los entrevistados. Sus origines pueden remontarse por lo menos a la década del 60. Existen antecedentes sobre la idea de desarrollo que datan de 1969, pero no fue hasta 1979 que la Fuerza Aérea lo formalizó. Se trataba de un plan multi etapas con asistencia internacional para la transferencia tecnológica a un plan de desarrollo nacional. La firma alemana contratada era MBB (Messerschmitt-Bölkow-Blohm) que a su vez subcontrataría a una firma italiana SNIA S.p.A. para el propulsante. Posteriormente por las presiones se crea una nueva firma llamada COSEN. Durante los 80 el proyecto sufrió algunas modificaciones, en parte por la guerra de las Malvinas; lo que llevó a plantear un genuino derecho a la defensa en un misil llamado Cóndor BM o Cóndor II (ver figura 180) que incluía una tobera TVC (*Thrust Vector Control*) para controlar la dirección, mientras que el cohete

espacial continuaría como Cóndor I (De León, 2017). Recordemos que Reino Unido, además de militarizar la región, envió 31 bombas nucleares durante el conflicto de Malvinas (Norton-Taylor, 2022).

De León (2017) cuenta que el otro inconveniente en 1984 fue el financiamiento del proyecto. Al finalizar la dictadura, las fuerzas armadas ven sus presupuestos reducidos y nace la idea de conseguir clientes internacionales para conseguir dinero. Arabia Saudita no muestra interés dado que solo compraba productos terminados (igualmente hace un aporte económico). Surge Egipto como cliente del proyecto. Dicho país no resultaba un inconveniente por estar en paz con Israel y no tener conflictos con EE.UU. Sin embargo, Irak se entera del proyecto y entabla relaciones con Egipto. Es posible que en este punto comiencen las complicaciones. Irak financia a Egipto con el fin de obtener la tecnología. Para aquel entonces, Irak no tenía inconvenientes con EE.UU. dado que estaba enfrentado a Irán. De todas formas, en 1987 Irak crea su propio proyecto gemelo (Project 395 / DOT / BADR-2000) y se independiza de Egipto (contacta directamente con empresas europeas); aunque su versión era a combustible líquido en vez de sólido.

De León (2017), continúa que empiezan las presiones de Reino Unido a Alemania (Thatcher presiona al canciller alemán) y de EE.UU. sobre la firma alemana (comienzan a indagar sobre el proyecto). El Brigadier Edgardo Stalh, a cargo de la dirección del proyecto, cuenta que tuvo que ir al Departamento de Estado en el 1985 y en una entrevista con el Coronel Brown de la Fuerza Area norteamericana y este le dice:

> Usted es militar y yo soy militar, es así como hablamos el mismo idioma. Yo le voy a hacer a usted algunas preguntas y sé que no me las puede responder, pero le voy a contar como es la cosa. Nosotros sabemos lo que ustedes quieren hacer. Estados Unidos estaría de acuerdo en permitir, digamos, que ustedes sigan adelante, pero por supuesto bajo ciertas condiciones. Por ejemplo, ¿cómo va a votar Argentina en la próxima reunión de la OEA con el problema de Nicaragua[171]? (Stalh como fue citado por De León, 2017, p 84). ***[coerción]***

Continúa que el embajador norteamericano en Argentina entabló amistad con el ministro de defensa Jaunarena del cual intentó obtener información del proyecto en varias oportunidades. El brigadier Crespo era consultado por el embajador cuando iban a pescar

[171] La mención es por un reclamo internacional presentado por Nicaragua contra USA debido a la intervención de USA en el caso Irán Contra mencionado en capítulos anteriores.

juntos. Para este entonces, varias agencias de inteligencia de diferentes países estaban detrás del proyecto (incluyendo la CIA, NSA, MI6 y Mossad), tanto las instalaciones en Córdoba, el personal de las fuerzas, el estado de avance, los proveedores, etc.

En 1987 se crea el MTCR (Missile Technology Control Regime) que es un acuerdo político originalmente de los miembros del G-7 (EE.UU., Reino Unido, Canadá, Francia, Alemania, Italia y Japón). El mismo busca limitar la proliferación de sistemas de Categoría 1 (tecnologías de misiles / UAV con capacidades de carga superiores a 500kg y rango superior a los 300km). Para lograrlo busca controlar la exportación de bienes / tecnología ***[romper la cadena de suministro]***. No se trata de un tratado sino de un acuerdo informal de asociación voluntaria (MCTR, s.f.). El mismo no tiene sustento legal, como indica (MCTR, s.f.):

> MTCR no es un tratado y no impone ninguna obligación legalmente vinculante a los Socios (miembros). Más bien, es un entendimiento político informal entre estados que buscan limitar la proliferación de misiles y tecnología de misiles.

Aun así, el mismo sirvió para presionar a Alemania e Italia en lo que respecta al proyecto Cóndor. Para 1988, EE.UU. incrementó las presiones sobre Egipto y Argentina. También comenzaron persecuciones judiciales en Italia ***[Lawfare]*** (De León, 2017).

Resaltamos que cuando el parlamento británico estudió el reemplazo sus misiles nucleares Trident en 2006, indicaron que existe un "aide memoire" adjunto al MTCR que establece que el mismo acuerdo no reemplaza ningún otro acuerdo que haya entrado en vigor antes de 1997. Lo que permite la transferencia de sistemas de Categoría 1 entre miembros de la OTAN (Defence Select Committee, 2006). Quedando expuesto como eludieron[172] los mismos mecanismos que exigían a Argentina. De forma análoga, podríamos afirmar que el proyecto Cóndor no se encontraba abarcado por tener acuerdos previos al MTCR.

[172] Nuevamente recuerda a rebelión en la granja de Orwell.

Figura 180
Condor II.



Nota: Dentro de la torre de servicio vertical (De León, 2017)

En 1988 empiezan los sucesos que atentan contra los participantes del proyecto. Según De León (2017) a pedido de la CIA, el Servicio de Inteligencia Militar Italiano (SISMI) destruye los sistemas de tobera que encuentra ***[romper cadena de suministro]***. Por otra parte, un atentado bomba asesina en Mónaco al gerente Ekkehard Schrotz de COSEN ***[Lock and Kill]***. Un llamado telefónico de "los guardianes del islam" (Irán) insta a finalizar el proyecto. Aunque se sospecha que podría tratarse del Mossad ***[False Flag Kill]***. Un mes después, alguien ingresa por la noche a las oficinas de COSEN en Suiza y roba documentación de proveedores para luego entregarla a periódicos ***[Hack and Dump]***. Paralelamente, dos militares egipcios son detenidos en EE.UU. mientas exportaban un material de fibras de carbono necesarias para el proyecto (MX-4926), material no permitido sin licencia de exportación ***[Lawfare]***. Con un fin intimidatorio, se produce otro atentado explosivo sin

víctimas delante de la camioneta que trasladaba ingenieros italianos y alemanes a la fábrica de misiles de Egipto ***[Psychowar]***, nuevamente se sospecha de Irán o Israel. Sumado a las presiones internacionales, Egipto abandona el proyecto (De León, 2017).

A todo esto, el candidato presidencial argentino (Menem) viajó a Siria y acordó recibir 40 millones de dólares para su campaña de parte de Arabia saudita, Irak, Kuwait, Libia, Siria y la Organización para la Liberación de Palestina; a cambio de entregar tecnología del Cóndor y tecnología nuclear (De León, 2017). Según Lejtman[173](2019), el candidato viajó a Roma, acordó la entrega del Cóndor a Libia y recibió un adelanto de 2 millones. Luego viajó a Siria y acordó una central nuclear en Siria y otra en Irán. Según el ministro Cavallo (como fue citado por De León, 2017) Menem le comentó que sus asesores que habían sido irresponsables en vender el Cóndor a Libia y era necesario detener su desarrollo. Independientemente de las discrepancias entre los autores, pudo existir algún tipo de acuerdo personal con países de una región altamente inestable.

Como continua (De León, 2017), en 1989 la BBC realizó un documental del Cóndor. El mismo incluía información incorrecta sobre sus capacidades al indicar su alcance podría llegar a 2500km, que podría llevar una cabeza nuclear o un agente nervioso químico; las repercusiones internacionales buscaban aumentar las presiones sobre el proyecto ***[Guerra psicológica / propaganda]***. Ese mismo año, Menem ganaba las elecciones, pero no cumple con sus acuerdos privados dado que entabla relaciones con Washington. Poco después, cancela el proyecto pagando un costo de 3 millones de dólares a la empresa alemana (mientras tanto Irak invade Kuwait quedando como enemigo de EE.UU.) (De León, 2017).

Para finalizar. La dualidad civil / militar y la vinculación con países de medio oriente, inquietaron a EE.UU., Reino Unido e inclusive Israel. Durante los 90, EE.UU./ Reino Unido lograron influir al gobierno argentino de Menem, quien había decidido virar a una política alineada al llamado “consenso de Washington”, una política delineada por EE.UU., organismos de crédito internacional, el Fondo Monetario Internacional y el Banco mundial. Ello también le permitió renegociar la deuda externa con el plan Brady. Lo que costó la

[173] Este autor también relaciona que no haber cumplido con el acuerdo llevó a los atentados de nuestro país. Esto puede que no concuerde exactamente con el reciente informe del Mossad que indica que la célula Libia empezó a migrar a Argentina justamente desde 1988. En ese entonces no podían saber que no iba a cumplir porque eso fue posterior a ganar en 1989.

pérdida de autonomía en diferentes áreas, como la economía, ciencia/tecnología, paralización de Atucha II. Entre otras presiones políticas de EE.UU., Nancy Dorn (Subsecretaria del Ejército de EE.UU.) le indico al Brigadier Julia (a cargo del proyecto): "Si [Argentina] no termina con el programa del misil no podrá pensar jamás en el otorgamiento de nuevos créditos ni ayudas para el país" (De León, 2017) ***[Guerra económica]***. Si bien la Fuerza Aérea Argentina defendió el programa hasta último momento, inclusive en contra de las ordenes políticas, finalmente se desmanteló bajo decreto. De forma humillante, se entregó la tecnología a los Estados Unidos a través de España a fin de ocultarlo a la población (dos envíos en el buque Bahía San Blas). Agentes de la CIA fueron a Córdoba y destruyeron gran parte de las instalaciones. Además, la CIA incautó en Mendoza unos contenedores especiales presurizados con nitrógeno utilizados para el transporte de motores con combustible que también se llevaron (De León, 2017).

Luego de muchos años de negociaciones, EE.UU. permitió a Argentina volver a desarrollar un plan para cohetes espaciales. Pero en esta oportunidad con tecnología de combustible líquido. Tecnología que Argentina no domina como el caso del combustible sólido. Esto implicó retroceder no menos de 50 años en el desarrollo tecnológico del país. En cuyo caso, este fue el objetivo buscado por EE.UU. y Reino Unido. Como afirma De León (2017): “La eliminación del proyecto Cóndor significo la eliminación de un potencial competidor comercial en un sector muy dinámico para la economía de Estados Unidos. Por ese resultado, es objeto de estudio en centros de inteligencia norteamericanos como un ejemplo exitoso de coerción internacional”.

Por todo lo expuesto, Argentina tiene un legítimo derecho a exigir una restitución económica por la transferencia tecnológica de dicho proyecto. Además, el antecedente es un fiel recordatorio de las operaciones de guerra sin límite. Punto que debe tenerse en cuenta por los responsables del desarrollo y gestión de los proyectos estratégicos nacionales.

Capítulo ~~(4)~~ Deimos – Antecedentes en ciber operaciones.

No es posible entender las acciones de ciberguerra sin comprender la geopolítica mundial, los actores y sus intereses (reflexión de elaboración propia).

El presente capítulo es una ampliación para dar sustento a las ciber operaciones, encuadradas dentro de la ciberguerra en un esquema de guerra sin límites.

Operaciones contra la infraestructura crítica.

Veremos diferentes afectaciones a la infraestructura critica, siendo el sector eléctrico uno de los más importantes. Ello se debe a que la falta de energía eléctrica arrastra a todas las otras infraestructuras críticas. La ausencia de suministro eléctrico afecta al país completo: industria, hospitales, semáforos, suministro de agua, sistema de cloacas, comunicaciones, transporte, bancos, aeropuertos, radares, votaciones (especialmente con voto electrónico), sistemas de pago (comprar suministros básicos de agua o comida mediante pago digital). De prolongarse un apagón en el tiempo resultaría caótico. La película “The trigger Effect” (1996) está ambientada en un apagón de similares magnitudes. Más reciente, el libro “Lights Out” (2015, Ted Koppel) desarrolla los riesgos de ciberataques en EE.UU. y los efectos caóticos sobre la sociedad, a medida que se van agotando las baterías, dando a entender que 3 semanas sería un punto crítico.

DARPA realiza juegos de ciberguerra en Plum Islan (NY), donde entrena al Blue team que debe mantener los disyuntores eléctricos operativos mientas el Red team los sabotea. El Almirante Mike Rogers (comandante del U.S. Cyber Command) afirmó en 2014 que China y al menos 1 o 2 países más, poseen capacidades para realizar un shutdown de la grilla eléctrica de EE.UU. (Fox News, 2015).

Un escenario más extremo es un apagón producido por un EMP (pulso electromagnético), como causa de una tormenta solar severa, arma de radiofrecuencia o la detonación de una bomba atómica en la atmósfera. Vincent Pry (Task Force del National and Homeland Security) menciona que, por la naturaleza de este tipo de apagones se tardaría al menos de 28 días en restaurar el sistema y como consecuencia, el 90% de la población norteamericana podría desaparecer. Esto último no es ciencia ficción, ejemplo

de esto son la prueba nuclear de alta altitud STARFISH PRIME (Operation Fishbowl) realizada por EE.UU. en 1962, que produjo daños generalizados a los sistemas electrónicos, o las pruebas similares de Rusia en Kazajistán que destruyeron la red eléctrica. Al respecto, en 2017 una comisión de evaluación de este tipo de amenazas (USA), menciona que estas armas no están diseñadas para producir una gran explosión cinética, sino un alto nivel de rayos gamma, generando un EMP E1 de alta frecuencia. La electrónica moderna que está preparada a trabajar con bajo voltajes es mucho más vulnerable a los EMP. Un ataque EMP incluso puede ser realizado desde un satélite, carguero o submarino (Committee on Homeland Security, 2017).

No es casualidad que Trump creara en 2018 ejercito del espacio (4to dominio) y que en el 2019 lanzara una orden ejecutiva para la Resiliencia nacional a los EMP.

Desde hace tiempo, Rusia como EE.UU. llevan realizando reconocimientos de sus redes eléctricas e infraestructura crítica. Inclusive con el *deploy* de *malware* que podría sabotear las operaciones (Sanger y Perlroth, 2019). Previamente anticipado por Snowden, cuando mencionó el implante *sleeping programs* en diferentes países del mundo durante tiempos de paz y la finalidad de ser utilizados cuando se requiera (Stone, 2016).

Caso Operation Olympic Games

Quizás uno de los más conocidos y estudiados del mundo. Al igual que la gran mayoría de las operaciones, contó con una importante fase de inteligencia, seguida de planificación, *Targeting*, *Weaponnearing* y finalmente una etapa final de ataque. Para la etapa de ataque, usualmente todo el trabajo ya se encuentra realizado. Si imaginamos las fases en su relación al tiempo/recursos utilizados, podremos imaginar un diagrama tipo embudo.

El objetivo del ataque fueron las plantas nucleares[174] iraníes en Natanz. Estas plantas de enriquecimiento de uranio (incrementar la proporción del isotopo de uranio 235) son una tecnología dual. Además de ser útiles para la generación de energía y usos medicinales; puede ser utilizadas para la creación de una bomba atómica, lo que preocupa a la región.

El resultado final de la operación fue el gusano Stuxnet. Este *malware* afecta los sistemas Windows mediante 4 vulnerabilidad 0 day. Estas vulnerabilidades no fueron

[174] Es paradójico que el plan nuclear iraní inicio con la ayuda de USA en los 50 y continuo durante muchos años. Esto remarca como en la geopolítica, los vientos nunca soplan en el mismo sentido.

reportadas a Microsoft (se optó por desproteger a los ciudadanos en pos de guardar el secreto para su *weaponization*[175]). Este *Malware* rompió el mito de la protección Air-Gap[176] ya que la infección fue vía USB (vector explotado por ingenieros de Siemens o con un espía infiltrado).

El *malware* estaba desarrollado para afectar PLC Siemens de los sistemas SCADA. Puntualmente interactuaba con el software STEP7 de Siemens, utilizado para operar los ICS. Además, el *malware* grababa los datos de operación normal (21 segundos) y durante el ataque realizaba un "*replay*" de los mismos. De manera que los operadores no pudieran ver en pantalla lo que realmente estaba ocurriendo (Langner, 2013).

El objetivo estaba dirigido a destruir las centrifugadoras de las plantas nucleares de IRAN (conversores de frecuencia de entre 807Hz y 1210Hz) (Chien, Falliere y Murchu, 2010). El ataque se atribuye a un trabajo conjunto de desarrollo de los servicios de inteligencia de Israel junto con Estados Unidos (2015, BBC). Más específicamente: el hacking team ofensivo Tailored Access Operations (TAO) de la NSA y el Security Team Unit 8200 de Israel. Este último, vinculado posteriormente al *malware* Pegasus que intervino ilegalmente celulares de todas partes del mundo de la mano del Mossad. Según (Zetter y Modderkolk, 2019), un ingeniero iraní reclutado como topo por la agencia de inteligencia holandesa (AIVD), proporcionó información crítica, como así también en el implante USB. Dado los antecedentes históricos de Crypto AG, no descartaría la participación de BND/Siemens en la fase de inteligencia como deployment.

En el año 2007, el laboratorio del Departamento de Energía de EE.UU. obtuvo una centrifugadora (P1) de Libia, que eran las mismas utilizadas usadas por Irán. Lo que le permitió realizar experimentos de como destruirla. Israel también hizo pruebas en el desierto (Buchanan, 2020). No casualmente, el Departamento de Energía de EE.UU. demostró la vulnerabilidad Aurora en el mismo periodo.

Conocemos la existencia del *malware* porque infectó gran cantidad de máquinas en el mundo debido a su naturaleza como gusano (Shearer, 2010). Su posterior análisis en 2010

[175] Similar al caso de los exploit de Shadow Brokers.
[176] Denominación para los sistemas o redes aisladas.

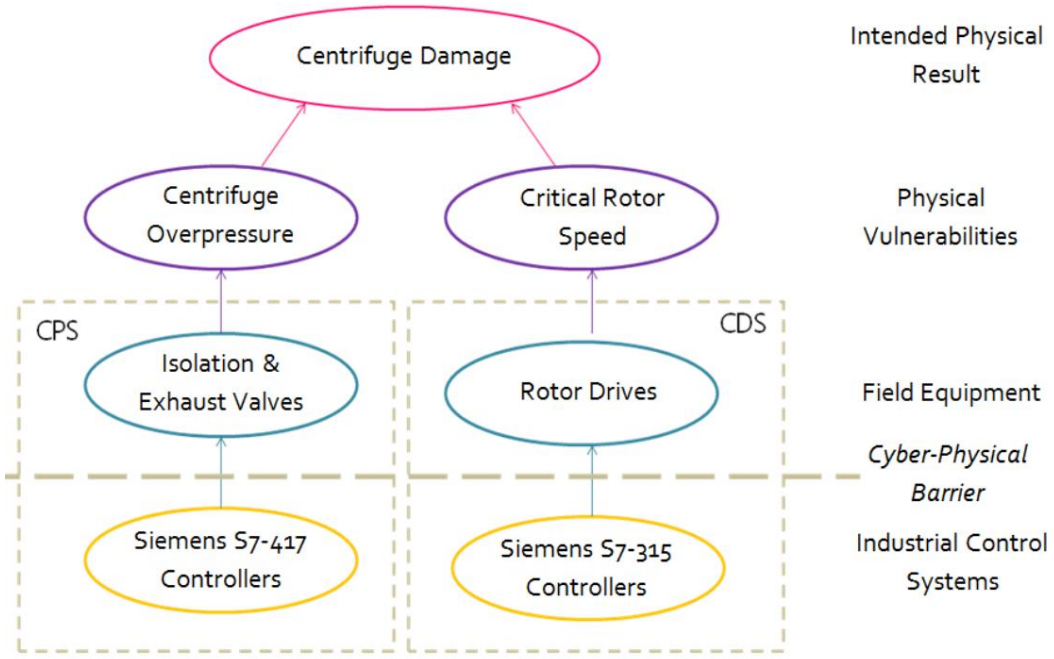
lo llevó a la luz; originalmente analizado Sergey Ulasen de VirusBlokAda, investigadores de Symantec y el experto en sistemas industriales Ralph Langner (Buchanan, 2020).

De haber querido, hubieran podido destruir todas las centrifugadoras juntas de un solo golpe. Sin embargo, ello hubiera llamado mucho la atención, dejando la operación al descubierto. Por lo tanto, la operación estaba enfocada en el sigilo. La idea era simular accidentes o fallas mecánicas y desalentando a los ingenieros en el desarrollo de un plan nuclear (Buchanan, 2020). Existen varias versiones diferentes del *malware*. Siendo las ultimas las más agresivas. Próximo a ser descubierto lanzaron la versión más agresiva con a la finalidad de terminar de destruir la mayor cantidad de centrifugadoras posibles. Acorde a (Buchanan, 2020), se destruyeron cientos de centrifugadoras, causando demoras de entre 1 a 3 años de la producción estimada.

Stuxnet contenía dos rutinas diferentes de ataques: *Overpressure Attack* y *Rotor Speed Attack* (ver figura 181). El primer ataque (y más complejo) intenta presurizar en exceso las centrífugas[177] (enfocado en aumentar el stress en las centrifugadoras y producir una ruptura temprana). El segundo ataque intenta acelerar en exceso los rotores de las centrífugas y llevarlos a sus velocidades críticas de resonancia (Langner, 2013). Con relación a la inteligencia, Langner comenta: “Las manipulaciones precisas y detalladas de estos subcontroladores [refiriéndose al complejo ataque de presurización] indican un profundo conocimiento físico y funcional del entorno de destino; quienquiera que haya proporcionado la inteligencia requerida también puede conocer los ingredientes favoritos de la pizza del jefe de ingeniería local”.

[177] Cierra válvulas y descalibra parámetros de los sensores de presión que actúan aisladamente sobre las válvulas de presión. Para más detalle, ver informe.

Figura 181
Stuxnet Attack Vectors.



Nota: las 2 tácticas utilizadas por el *malware* (Langner, 2013)

Vulnerabilidad Aurora[178].

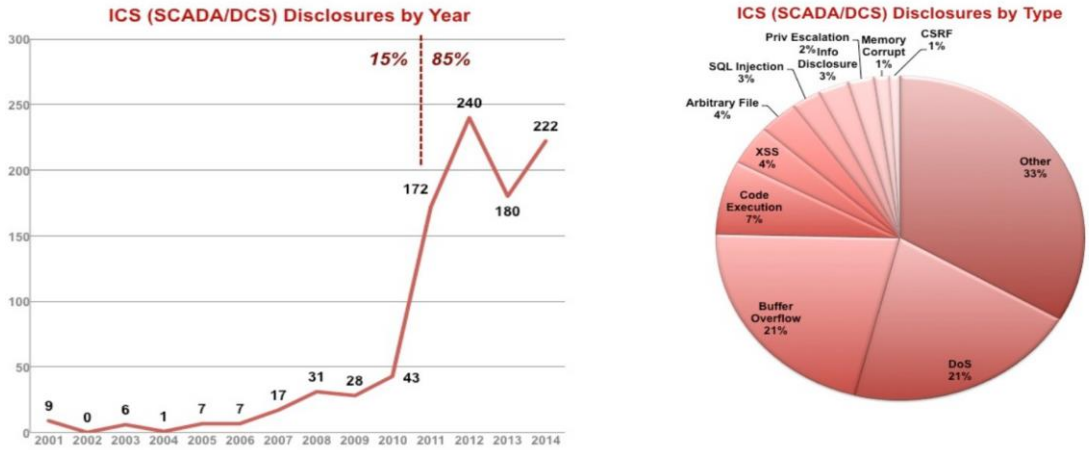
En 2007, el departamento de energía de EE.UU. demostró una vulnerabilidad llamada Aurora (no confundir con operación aurora de espionaje chino ni con el programa de exploración espacial). La vulnerabilidad permite destruir un generador de energía en tan solo 3 minutos. Esto se logra desconectando el generador de la red de energía lo suficiente como para perder la sincronización con la red, para posteriormente volver a reconectarlo. Esta desincronización ejerce una presión severa sobre el rotor y produce un impulso de energía mecánica sacudiendo el generador, dañando rulemanes e incrementando su temperatura. Reiterando esta operación logra la destrucción del generador. Lo que demuestra es como un ciberataque puede producir daños físicos permanentes sobre la infraestructura crítica de manera simple (TrendMicro, 2018).

[178] Video: https://www.youtube.com/watch?v=fJyWngDco3g

Stuxnet y la caja de pandora en los ICS.

Stuxnex corresponde al primer antecedente histórico de tecnología del tipo *cyber-physical weapon*. Esto llevó al menos a dos consecuencias visibles. Por un lado, que investigadores en seguridad pusieran el foco en la rezagada seguridad industrial y desde entonces se ha encontrado una gran cantidad de vulnerabilidades (ver figura 182)[179].

Figura 182
Vulnerabilidades encontradas en ICS.



Nota: (fuente scadahacker.com)

Por otro lado, el acontecimiento de Stuxnet marca un hito histórico, rompiendo una barrera que antes no se había nadie atrevido a atravesar. Habilita a otros actores a llevar a cabo similares operaciones en el ciberespacio. En palabras de Langner (2010): "*Welcome to Cyberwar*" (Bienvenido a la ciberguerra).

Caso Shamoon

En 2012, la empresa petrolera Aramco de Arabia Saudita fue infectada por el *malware* Shamoon que afectó 30 mil computadoras de la compañía. Los sistemas estuvieron apagados por más de 10 días, afectando la economía nacional. El ataque a su vez afecto a RasGas de Qatar (Zetter, 2012; Paganini, 2012).

Se trata de un *malware* modular descubierto por Symantec en 2012 que presenta similitud con Flame. Es una bomba lógica que crea un servicio persistente, utiliza la red

[179] Muchos de estos sistemas cerrados poco a poco empezaron a tener accesos a distancia para su mantenimiento. Quedando aún más expuestos.

para propagarse, exfiltra de información sobre los archivos y finalmente realiza un borrado seguro. Básicamente está conformado por 3 componentes principales: Dropper, Wiper y Reporter (Johnson, 2012). El primero es el vector de ataque que crea un servicio permanente y garantiza la persistencia. Además, es el encargado de la propagación en la red y de lanzar los otros 2 componentes. El Reporter identifica la ubicación de los archivos y reporta al atacante. Finalmente, el wiper pisa los archivos por una imagen de una bandera de EE.UU. quemándose (Johnson, 2012; Buchanan, 2020). Versiones posteriores en 2016 utilizan una foto de Alan Kurdi, un niño sirio ahogado (Finkle, 2016).

El wiper utiliza un *driver* rawdisk para acceder directamente al disco sin pasar por la API de Windows. Como último ataque borra el MBR del disco, inutilizando el sistema. La operación fue lanzada durante el mes de Ramadan, aprovechando que la mayoría de los empleados se encontraban de vacaciones. Maximizando así sus posibilidades de causar el mayor daño posible. Un grupo llamado Cutting Sword of Justice se atribuye la creación del *malware* (conocido como el mayor hack de la historia). Se desconoce el origen del grupo/ataque. Según Paganini (2012), podría tratarse de una disputa entre Irán y Saudí Aramco sobre el embargo petrolero impuesto a Irán por los Estados Unidos y la Unión Europea (el 1 de julio de 2012). El ataque de Shammon fue el 15 de agosto de 2012, posiblemente la penetración inicial a la red fuera previa.

Un dato curioso es que, en 1996, en el RAND de Washington DC, realizó un ejercicio simulado llamado “The day after…. In cyberspace”, donde se plantearon varios escenarios de ciberataques, entre los cuales figuraba la disrupción de los sistemas de control de la petrolera Aramco: “mal funcionamiento catastrófico del control de flujo que condujo a una gran explosión e incendio en una nueva torre de craqueo. Este hecho fue seguido por un comunicado de guerra de un grupo islámico radical vinculado a Irán” (Molander, Riddile y Wilson, 1996)[180].

Caso Steel Mill blow

En 2014 una acería alemana sufrió un ciberataque. No se informaron detalles del incidente y se desconoce el origen. Se estima de un grupo ATP por su sofisticado

[180] La propuesta de un avión impactando al pentágono es otro caso ejemplo de propuesta de planes de contingencia que terminaron ocurriendo (Graham, 2004; Ryan, 2000).

conocimiento en ICS. Las consecuencias fueron daños físicos severos al horno (Goldman, 2014).

El vector de ataque inicial consistió en un Spear phishing a la red corporativa. Luego comprometieron los ICS. Según un reporte del BSI: "hubo una acumulación de averías de componentes individuales del sistema de control o de instalaciones enteras. Las fallas del sistema dieron como resultado un incidente en el que un horno no se pudo apagar de la manera normal y el horno estaba en una condición indefinida que resultó en un daño masivo en todo el sistema." (Germany's Federal Office for Information Security como fue citado por Goldman, 2014) (ver figura 183).

Figura 183

Incidente en acería en Alemania.



Nota: Otro incidente ocurrido en 2022 en Saarstahl AG in Völkingen que ilustra el peligro de los procesos industriales. Este caso fue un accidente y no un ataque (Folz, 2022).

Caso Irongate

En 2015 la firma FireEye encuentra en virustotal (*on the wild*[181]) una muestra de un *malware* que ataca los ICS con ciertas similitudes con Stuxnet. El mismo empacado con PyInstaller.

El *malware* reemplaza una DLL, realiza un ataque Man in the Middle entre PLC Siemens y el Sistema de monitoreo. Puede grabar el tráfico y hacer un replay. Además contiene evasión de virtual machine. No se conocen ataques y se estima que puede tratarse de una prueba de concepto (Lee, 2016).

[181] Término utilizado por investigadores de *malware*, refiere a una muestra libre y activa operando fuera de la contención o entorno de test.

Caso BlackEnergy

El Ciberataque a la red eléctrica de Ucrania (2015) afectó la mitad de los hogares en la región Ivano-Frankivsk durante algunas horas. Se utilizó un *malware* llamado BlackEnergy en conjunto con un módulo Killdisk. Este *malware* fue desarrollado en 2007 y se atribuye al grupo ruso Sandworm (Voodoo Bear) vinculado a la Unit 74455 del GRU (inteligencia militar rusa). El nombre viene por el terrorífico gusano de arena de la novela Dune, dado que en el código encontraron alusiones a la novela (Arrakis, house atrides, etc). Originalmente el *malware* fue vendido en un foro por $40 USD y la finalidad original de la primera versión era generar DDOS (denegación de servicio distribuidas mediante bots). Posteriormente fue mejorado a su versión 2 en 2010 y versión 3 en 2014. Esta última tiene capacidad de robar claves, grabar el teclado, tomar capturas de pantalla, crear acceso remoto, scan de red y destrucción del sistema entre otras funciones (Greenberg, 2019).

Este mismo *malware* (la versión DDOS) habría sido utilizado en el ataque a Georgia en 2008. Afectando sitios gubernamentales, incluyendo al Ministry Foreign Affairs (Danchev, 2008). Georgia puede considerarse el primer experimento de guerra híbrida combinando los dominios tradicionales junto con el ciberespacio.

BlackEnergy posee varios mecanismos de infección, entre ellos un 0 day de Powerpoint (CVE 2014-4114) o archivos de office (con macros) enviado por correo con técnicas spear-phishing (victima específicamente) (Lipovsky, 2014).

El *malware* en si no tiene comandos para controlar los disyuntores. Fue utilizado como medio para lanzar un ataque coordinado a 3 plantas de energía. La operación consistió en establecer su propio software de control en una estación lejana y desde ahí enviaron los comandos de corte de energía. En otro de los casos directamente utilizaron una herramienta del HelpDesk de IT para controlar las computadoras del sistema de control. Además de bloquear las terminales de los operadores, los cuales observaban el mouse moverse por la pantalla abriendo los disyuntores y sin poder hacer nada (Greenberg, 2017).

La segunda fase del ataque consistió en sobrescribir el código de unos convertidores Serial-to-Ethernet que se utilizaban en las comunicaciones de Internet. De esta manera *brikearon*[182] esos dispositivos, denegando el restablecimiento del suministro por parte de

[182] Slang español derivado de la palabra brick. Para indicar que se transforma en un ladrillo (sin función).

los operadores. Adicionalmente, apagaron las baterías de backup dejando a los operadores también en la oscuridad. Como si no fuera suficiente, bombardearon al call center con llamadas falsas dando mayor confusión a la población que no podía informarse de lo que estaba ocurriendo (Greenberg, 2019).

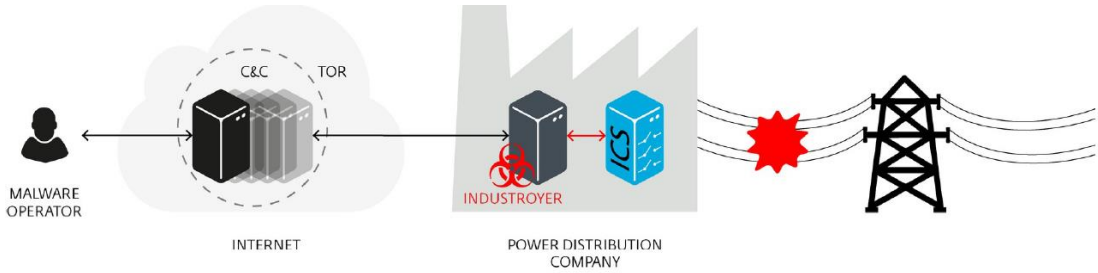
Caso Industroyer / Crash Override.

En 2016 se produce nuevamente un ciberataque a la red eléctrica de Ucrania. El apagón afectó gran parte de su capital Kiev durante 1 hora, afectando aproximadamente 250mil hogares.

Según la presentación en la conferencia Blackhat 2017. Cherepanov, Miller, Slowik, Lee y Lipovsky; asocian este apagón con un *malware* llamado Industroyer / Crash Override[183]. La asociación es porque las capacidades del *malware* y su fecha de activación coincidente con el ataque en cuestión (Black Hat, 2020).

Este *malware* afecta los sistemas de control industrial, como ser los utilizados en infraestructura crítica (ej. agua/gas); especialmente los utilizados en las subestaciones eléctricas. El mismo utiliza protocolos de comunicación específicos en el ámbito industrial (IEC 60870-5-101, IEC 60870-5-104, IEC 61850, y OLE for Process Control Data Access OPC DA); por lo cual no podría haberse desarrollado sin tener acceso a tales equipos. Su peligrosidad reside en su capacidad de controlar interruptores y disyuntores digitales presentes en dichas subestaciones eléctricas (ver figura 184) (Cherepanov, 2017).

Figura 184
Vulnerabilidades encontradas en ICS.



Nota: (fuente imagen: Cherepanov, 2017)

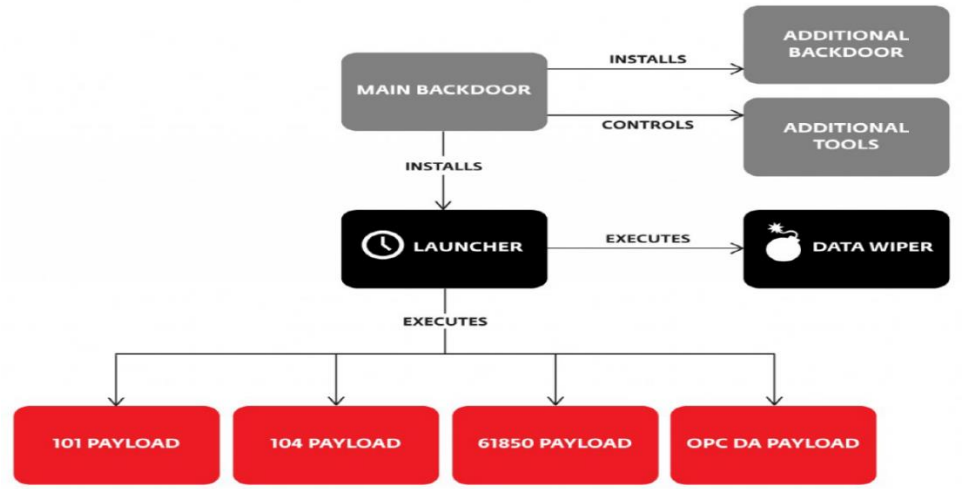
[183] Tiene dos nombres porque depende del reporte del profesional que lo investigó. Sucede algo similar al nombre de los APT.

En este caso no existe una vulnerabilidad puntual, sino que el problema principal se encuentra en el diseño de los protocolos industriales. Tales protocolos se desarrollaron hace mucho tiempo atrás, donde no se tuvo en cuenta aspectos de seguridad. Además, los entornos eran aislados del mundo exterior, conformados por partes de confianza y sin necesidad de actualizaciones (Cherepanov, 2017).

Industroyer es un *malware* modular (ver figura 185). Su principal componente es un *backdoor* para controlar el ataque de manera remota. Otras características son su persistencia (tiene un *backdoor* adicional oculto como notepad en caso de que se detecte el componente principal), su capacidad para evitar la detección (conectándose vía TOR en horarios no laborales), un Wiper para eliminar rastros una vez finalizado el ataque, scanner de red y hasta un módulo de denegación de servicio sobre vulnerabilidad (CVE-2015-5374) en equipos Siemens SIPROTEC (utilizados en subestaciones eléctricas). Este equipo Siemens se utiliza para abrir los circuitos eléctricos en caso de detectar peligros en la red eléctrica. En caso de haber sido inutilizado por el *malware*, este equipo no responde al operador y debe ser reiniciado manualmente (Cherepanov, 2017).

El especialista en seguridad de red eléctrica del SANS Institute, Mike Assante, resalta el potencial peligro de daño físico a la red eléctrica en caso de que se produzca un riesgo eléctrico real, sumado la ausencia de esta protección (previamente deshabilitada por el *malware*) (Greenberg, 2017). Se desconoce el origen del *malware*, pero se sospecha del mismo grupo ruso que atacó la red eléctrica en 2015.

Figura 185
Componentes de Industroyer.



Nota: (fuente imagen: Cherepanov, 2017)

Caso Havex

En 2017 un grupo ruso llamado Dragonfly / Energic Bear logró obtener acceso a las salas de control de empresas eléctricas de USA. Utilizando técnicas de *spear-phishing*, *watering hole* (proveedores ICS) y *troyanized software;* como vectores de ataque.

Una vez logrado el acceso remoto, realizaron un reconocimiento de las redes y obtuvieron información sobre los sistemas de control. Según Symantec, este grupo realiza actividades desde 2011 y hay sospechas de que infraestructura crítica de Suiza y Turquía también pudo haber sido alcanzada. Este mismo grupo está vinculado al *malware* Havex que realiza espionaje en sistemas de control industrial. Se trata de un RAT (Remote Access Troyan) con capacidades de descubrimiento (escaneo) de dispositivos en la red (Symantec, 2014).

Caso Triton / Trisis / HatMan

El *malware* Triton, diseñado para manipular los sistemas de seguridad industrial, causó un incidente en una infraestructura crítica en 2017 (Johnson, Caban, Krotofil, Scali, Brubaker y Glyer, 2017). El mismo fue utilizado contra una organización en Oriente Medio (Symantec Security Response, 2017), posiblemente Arabia Saudita[184] (Gibbs, 2017). El *malware* está diseñado para interactuar con el controlador *Triconex Safety Instrumented System* (SIS). Estos componentes están diseñados como protección para proteger vidas humanas en caso de fallas críticas. Como indica (Johnson et al., 2017):

> SIS es un sistema de control autónomo que monitorea de forma independiente el estado del proceso bajo control. Si el proceso supera los parámetros que definen un estado peligroso, el SIS intenta devolver el proceso a un estado seguro o realiza automáticamente una parada segura del proceso.

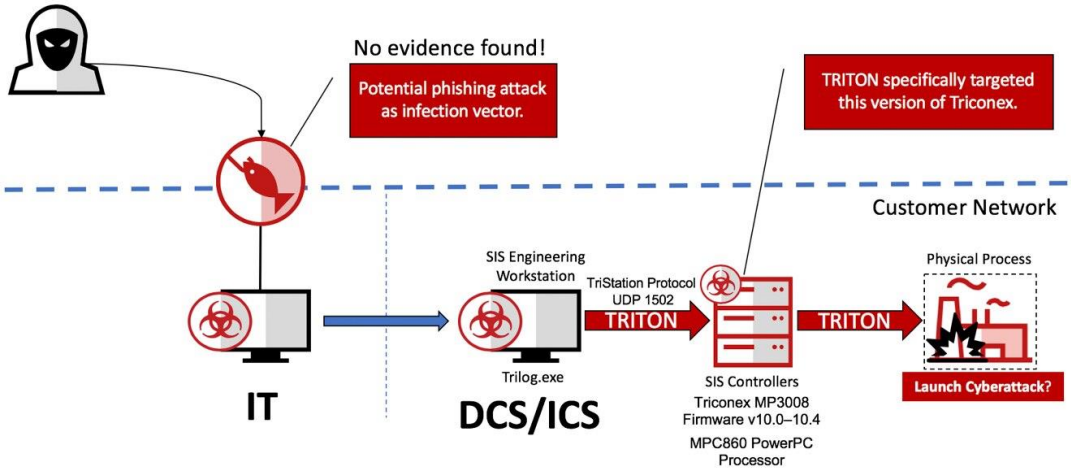
Los equipos atacados fueron los *Triconex SIS* de Schneider. Durante el incidente, el controlador SIS detectó una falla en la validación de código, dado que el *malware* modifica su memoria, iniciando un apagado seguro que causó la parada de la planta. El atacante no llegó a lanzar el *payload* en la fase final de ataque. Algunos posibles escenarios de ataque son reprogramar el SIS para que mediante un falso positivo genere una parada de planta (denegación de servicio), o que detecte una situación insegura como normal poniendo en riesgo la infraestructura/vidas humanas (Johnson et al., 2017).

El *malware* desarrollado en *Python* esta empacado en un ejecutable que simula ser un update legítimo. Enmascara la aplicación Triconex Trilog (ver figura 186). Contiene *payloads* de *PowerPC* (el procesador que utiliza algunos *Triconex*) y utiliza el protocolo TriStation para inyectar el código en el SIS *Controller*. Este protocolo propietario no está documentado ni en estructura ni como desarrollar aplicaciones, por lo que el atacante tuvo que realizar una ingeniería inversa y disponer de dichos equipos (atacante avanzado y con recursos) (Johnson et al., 2017; Roccia, 2018).

El *malware* verificar que no exista errores al enviar un *payload*. En caso de error, intenta regresar al controlador al estado previo y si falla pisa la memoria con un dummy para evitar un análisis forense (Johnson et al., 2017).

[184] Fuentes posteriores indican que se trataría de la compañía Petro Rabigh.

Figura 186
Componentes de Triton.



Nota: (fuente imagen: Roccia, 2018)

La firma FireEye lo vincula al grupo APT TEMP.Velos / Xenotime, relacionado al Central Research Institute of Chemistry and Mechanics (CNIIHM) de Rusia (FireEye Intelligence, 2018).

Ciber operaciones de espionaje

Desarrollamos algunas operaciones durante el capítulo anterior, como ser la utilización del *malware* Pegasus, las operaciones de hacking de las diferencias agencias de inteligencia, los programas de vigilancia, entre otros. En el presente apartado ampliaremos algunos antecedentes relevantes.

Caso Moonlight Maze

En 1998, el FBI inició una investigación por la intrusión a varias agencias gubernamentales detectadas originalmente en 1996. Los países afectados fueron UK, Canadá, Brasil, Alemania y EE.UU. Los objetivos en este último fueron: el Departamento de Defensa (DoD), Administración Nacional de Aeronáutica y del Espacio (NASA), Departamento de Energía, Base de la Fuerza Aérea Wright Patterson, Laboratorios Nacionales de Los Álamos y Sandia, Instituto de Tecnología de la Fuerza Aérea, Laboratorio de Investigación del Ejército e instituciones de investigación naval (Hodfson, Shokh y Balk, 2022).

Los intrusos utilizaron un *backdoor*. Los archivos robados fueron transferidos con el protocolo *ICMP* como *covert channel*. La cantidad de información robada era tan grande que, en caso de imprimirse, tendría tres veces el tamaño del monumento a Washington. Las fuerzas de seguridad colocaron un *honeypot* donde había archivos con *beacon* (balizas), para poder realizar *track* (seguimiento) de los atacantes. Rastrearon los orígenes a Rusia. En 2017, investigadores atribuyeron el caso al grupo APT Turla / Venomous Bear/Snake / MakersMark (Hodfson et al., 2022).

Transferencia de tecnología.

US Cyber Command acusó en 2012 a China de la infiltración del APT en la firma RSA, lo que permitió duplicar la llave electrónica SecurID y que posteriormente fue utilizada para penetrar en mayo del 2011, la red de Lockheed Martin entre otras firmas asociadas al US Defense (accediendo a diseños de más de 24 sistemas de armamento, entre ellos el Aegis Ballistic Missile Defense Systems, F/A-18 Tactical fighter jet [Mc Donell Douglas], el sistema de despegue vertical V-22 Osprey [Bell/ Boeing Helicopters] y al litoral combat ship) (Finkle y Shalal-Esa, 2011; Nakashima, 2013). Otro ejemplo es la acusación en 2014 a China de espionaje económico contra grandes empresas norteamericanas, lo que China respondió que el programa PRISM de la NSA espía tanto a ciudadanos norteamericanos como extranjeros de manera sistemática e ilegal (RT Stuff, 2014).

Según el Capt. USN Scott Jasper, La mayoría de las intrusiones observadas hasta la fecha originarias de China parecen estar orientadas a recopilar información en lugar de lanzar ataques, de esta manera China logra una ventaja económica competitiva y reducir los costos a partir de la información extraída. Como la economía de China depende en parte de la de USA, si realizara algún tipo de ataque que afecte la economía norteamericana, indirectamente afectaría su propia economía. Eso es lo que se conoce como una estrategia disuasiva del tipo "*entaglement*" (Jasper, 2017).

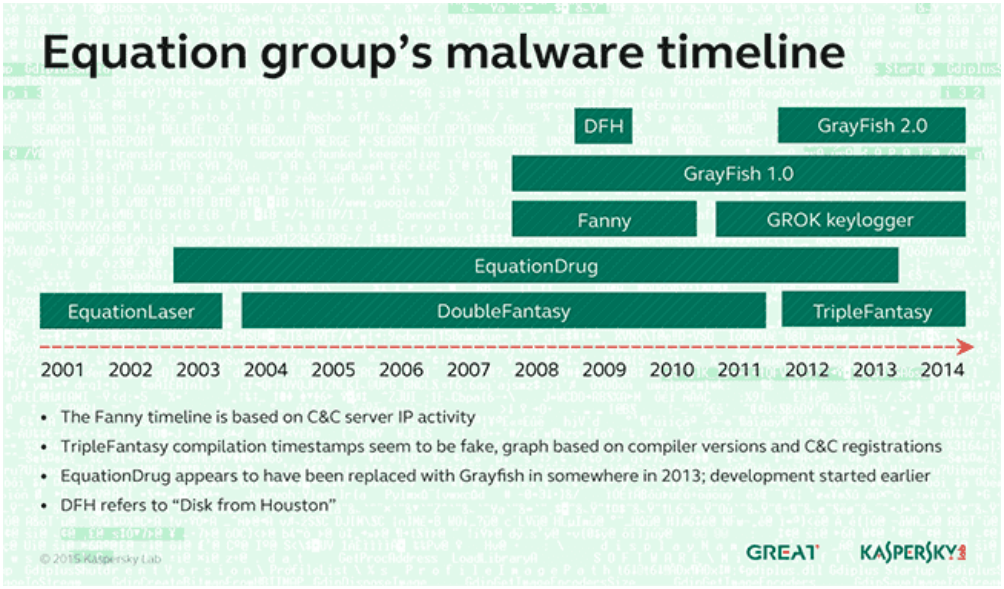
Caso Flame / Skywiper.

El sofisticado *malware* está orientado al ciber espionaje en países de Medio Oriente. tiene un inusual tamaño de 20 MB, es modular, posee varios métodos de cifrado para almacenar la información dentro de una base de datos (Gostev, 2012).

El mismo afectó al ministerio de petróleo de Irán y a plantas de petróleo (MAHER como fue citado por Keizer, 2012). Fue reportado por el Irán National CERT y presenta similitud con Stuxnet como Duqu. Tiene capacidad para infectar sistemas por la red/USB, escucha tráfico de red para captura de claves, búsqueda de archivos, toma captura de pantallas, graba sonido desde el micrófono, envía información a los C&C vía SSH/HTTPS, posee técnicas de evasión de antivirus e infecta sistemas Windows XP/Vista/7 (MAHER, 2012). Además, tiene un comando para eliminar su presencia (Johnson, 2012).

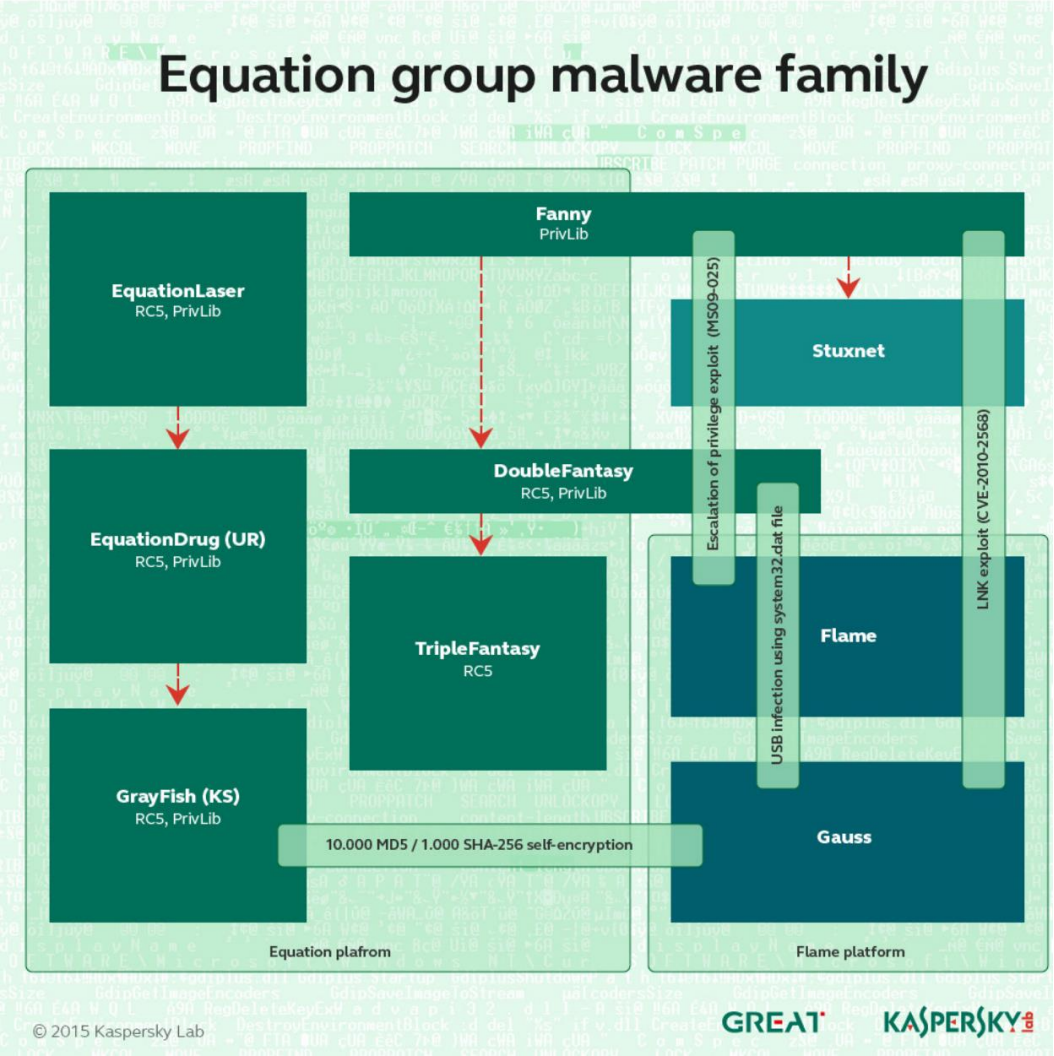
Acorde a Kaspersky Labs (2015), Equation Group (NSA) disponía de algunas vulnerabilidades 0 day previo a dichos *malware* (ver figura 187 y 188).

Figura 187
Equation Group malware implants.



Nota: Algunos *malware* de Equation grupo utilizaban previamente el mismo 0 day que Stuxnet y Flame (Kaspersky, 2015)

Figura 188
Equation Group malware implants.



Nota: Similitudes con Stuxnet, Flame y Gauss (Kaspersky, 2015).

Caso Fanny (2008)

Fanny es un gusano del 2008 enfocado en inteligencia en Medio Oriente y Asia. Utilizaba dos vulnerabilidades que luego fueron descubiertas en Stuxnet (propagación con LNK/USB sticks y mismo escalamiento de privilegios MS09-025). Algunas víctimas posteriormente actualizaron a Double Fantasy y luego a EquationDrug. El principal propósito parece el *mapping* de redes *air-gapped* (cerradas). Utiliza al dispositivo USB como *Command and Control* intermedio. Coloca la información a exfiltrar oculta en un sector del USB, que en algún momento envía al C&C (cuando dicho pendrive encuentra un

sistema con salida a internet). Desde el C&C, a su vez pueden programar comandos en el USB para ser posteriormente ejecutados en la red aislada (Kaspersky, 2015).

Caso DoubleFantasy

Acorde a Kaspersky Labs (2015). Los participantes en una conferencia científica en Houston recibieron una copia de los materiales de la conferencia en un CD-ROM que luego se utilizó para instalar el implante DoubleFantasy en las máquinas de los objetivos. El *malware* es un troyano para inteligencia y su función es la de confirmar un objetivo. En caso afirmativo, permite el deploy de otras ciberarmas (EquationDrug o GrayFish).

El *malware* presenta persistencia, explota vulnerabilidades de escalamiento y si no detecta antivirus descifra (XOR) el payload. Este *malware* envía información cifrada (RC6 con encode Base64) al C&C y permite al atacante ejecutar comandos y el deploy de otros *malware*. Posteriormente evolucionó a TripleFantasy (Kaspersky, 2015).

Caso EquationDrug (2003-2013).

Posiblemente sucesor del EquationLaser (2001-2004). Se trata de un *malware* modular sofisticado que otorga acceso completo del sistema al atacante (Win95/98/ME). Es modular porque tienen capacidad para múltiples *plugins*. Utiliza *hooks* al sistema como un *rootkit*. Posteriormente evolucionó a GrayFish (WinXP/7/8/NT/2000). Para plataformas como Windows 7, el atacante utiliza GrayFish o TripleFantasy. EquationDrug cuenta con un mecanismo de auto destrucción en caso de perder el contacto con el C&C en un tiempo predefinido. La exfiltración de información simula ser un archivo de fuentes (.fon) y utiliza cifrado (Kaspersky, 2015).

Caso GrayFish (2008-2013)

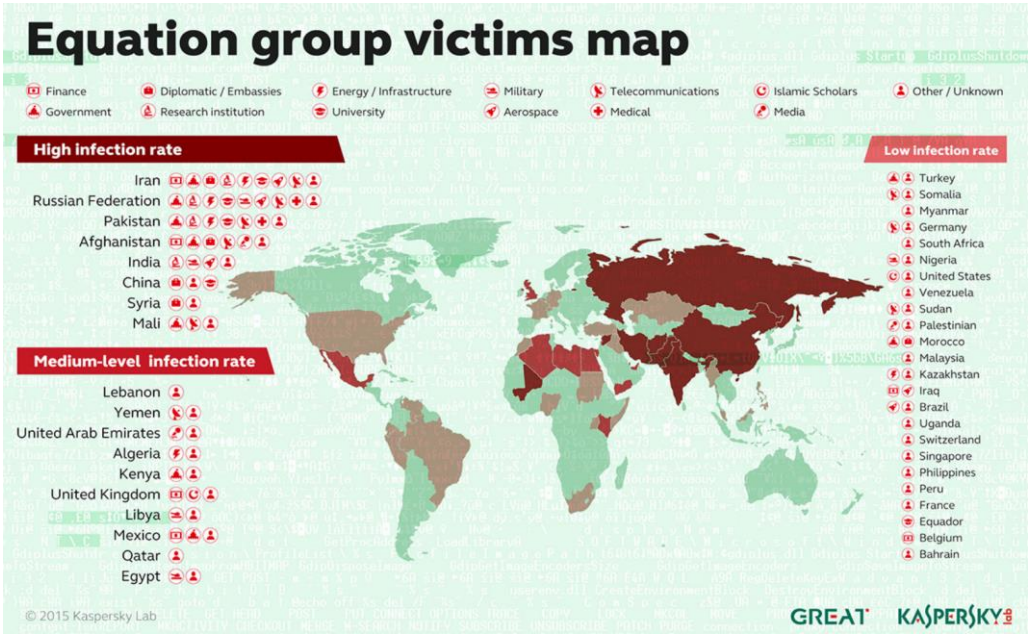
Malware más sofisticado, es un *bootkit* que secuestra (*hijacks*) los procesos de carga del OS e inyecta código en el *Boot Record*. Tiene un mecanismo *multi stage* de carga incluyendo descifrado. En caso de falla contiene un mecanismo de auto destrucción. Para almacenar la información robada, implementa su propio *encrypted Virtual File System* (VFS) dentro del registro. Además, explota algunos *drivers* del sistema lo que le permite ejecución a modo kernel. Su presencia es invisible a los antivirus dado que reside cifrado

en el registro y sin archivos en disco. El manejo de las llaves de cifrado presenta similitud con el *malware* Gauss. La funcionalidad más sofisticada de GrayFish es el plugin de reprogramación de firmware de HDD (disco rígido). El firmware de disco se puede grabar, pero no leer; lo que complica la detección (Kaspersky, 2015).

Los países afectados por Equation Group: Irán, Rusia, Siria, Afganistán, Kazakstán, Bélgica, Somalia, Hong Kong, Libia, Emiratos Árabes, Iraq, Nigeria, Ecuador, Mexico, Malasia, United States, Sudan, Líbano, Palestina, Francia, Alemania, Singapur, Qatar, Pakistán, Yemen, Mali, Suiza, Bangladesh, South África, Filipinas, United Kingdom, India y Brasil (ver figura 189). El C&C puede ser de diferentes países como EE.UU., Reino Unido, Italia, Alemania, Holanda, Panamá, Costa Rica, Malaysia, Colombia y República Checa. Utilizan un proxy para enmascarar el registro de los dominios. Uno de los vectores de ataque consiste en advertise con exploits en Java. Otro caso observado es un script PHP inyectado en foros en Oriente Medio, asegurándose solo atacar ciertos rangos de IP[185]. Los cifrados que utiliza son RC5, RC6, XOR, AES y Sustitution Tables (Kaspersky, 2018).

Figura 189

Equation Group víctimas.



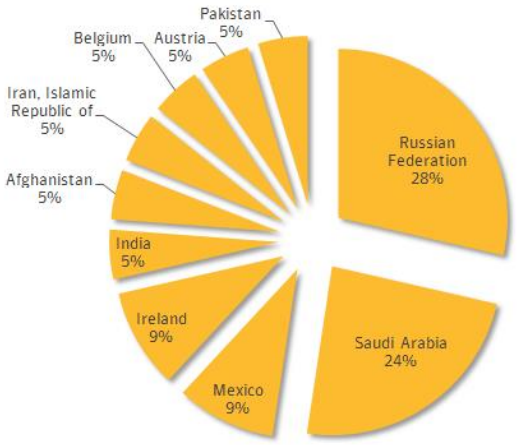
Nota: (fuente imagen: Kaspersky, 2018).

[185] El dirigido es más típico de una operación militar, donde hay una orden especifica de objetivos autorizados, minimizando daños colaterales o conflictos con otras naciones.

Caso Regin

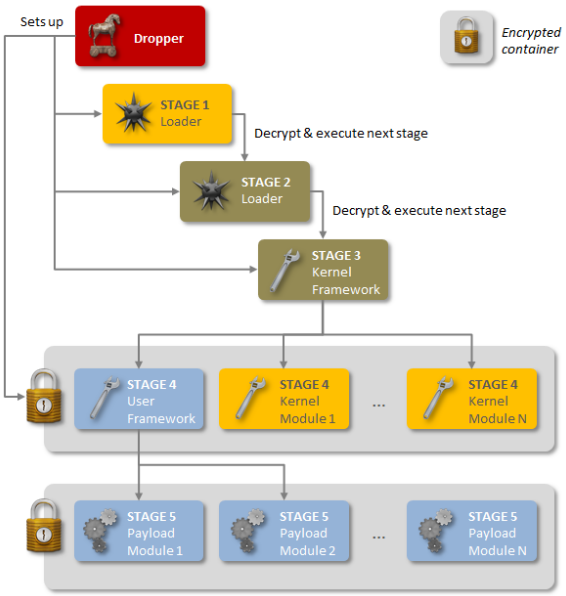
Observado entre 2008 y 2013. Comparte similitudes con GrayFish y Stuxnet. Acorde a Guarnieri y Gallagher (2014), este *malware* es responsable de los ciberataques conducidos en 2010 por la NSA contra las oficinas de la Unión Europea. Asimismo, el ciberataque del GCHQ en 2013 en contra de Belgacom (compañía de telecomunicaciones de Bélgica). También infectó un USB de un alto rango del personal del canciller alemán Ángela Merkel (Appelbaum, Gibson, Guarnieri, Müller-Maguhn, Poitras, Rosenbach, Ryge, Schmundt y Sontheimer, 2015). Acorde a Symantec se trata de un framework modular de vigilancia. Tiene un sofisticado mecanismo cifrado *multistage* de carga (ver figura 190 y 191). Los mismos pueden estar almacenados en el registro con la técnica *encrypted Virtual File System* (VFS) observada en el GrayFish. También puede utilizar *raw sectors* al final del disco. Posee capacidades de *sniffer* de red, cifrado (RC5), mecanismos de exfiltración de datos por canales encubiertos (HTTP, TCP, UDP, ICMP), *Intel gathering* del sistema, robo de credenciales, inteligencia de procesos, búsqueda en el *file system*, capacidades forenses (recuperar archivos borrados), captura de pantalla, operación remota del mouse y *sniffing* GSM BSC (*Base Station Controller*) lo que significa inteligencia sobre telefonía celular GSM incluyendo credenciales de operadores (Symantec Security Response, 2014).

Figura 190
Víctimas.



Nota: (Fuente imagen: Symantec Security Response, 2014).

Figura 191
Framework modular multietapas cifradas.



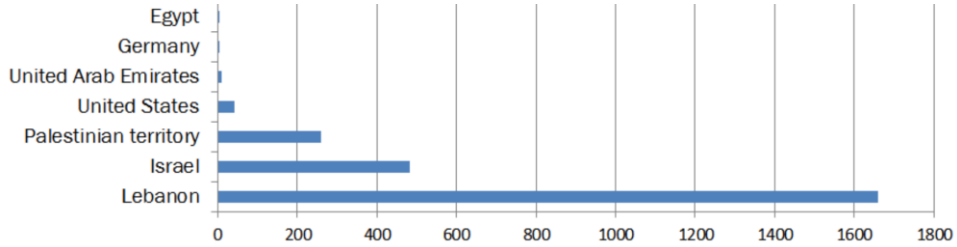
Nota: (Fuente imagen: Symantec Security Response, 2014).

Caso Gauss

Acorde a Kaspersky (2018), es un *malware* de ciber espionaje modular con estructura semejante a Flame, similar código base y sistema de comunicación (C&C). Estuvo operando en Oriente Medio entre 2011 y 2012 principalmente en el Líbano (a diferencia de Flame en Irán) (ver figura 192 y 193). Está diseñado para recolectar información y capturar credenciales (sistemas bancarios, redes sociales, email, IM accounts). Además, incluye comandos para interceptar datos para operar con bancos del Líbano. Si bien es más extendido que Flame, no presenta funciones de auto replicación.

Los módulos tienen nombres de matemáticos y sus capacidades son: inyectar modulo en navegadores para recolectar sesiones, *cookies*, credenciales e historial; recolectar información de las conexiones de red, información de procesos/*folders*, información del BIOS y RAM-CMOS; información de red y unidades removibles; infectar USB, exfiltración y comunicación con el C&C. El módulo que infecta USB utiliza la vulnerabilidad utilizada por Stuxnet (“.LNK exploit” CVE-2010-2568) y tiene su propio módulo para interactuar directamente con el USB. Uno de los módulos esta compilado por el usuario “flamer”. La configuración es almacenada en el registro (al igual que Duqu y Stuxnet).

Figura 192
Víctimas.



Nota: (Fuente imagen: Kaspersky, 2018).

Figura 193
Comparación de infecciones.

Name	Incidents (KL stats)	Incidents (approx.)
Stuxnet	More than 100 000	More than 300 000
Gauss	~ 2500	?
Flame	~ 700	~5000-6000
Duqu	~20	~50-60

Nota: (Fuente imagen: Kaspersky, 2018).

Caso Duqu

Descubierto en 2011 (operando desde 2009). Acorde al reporte del Laboratory of Cryptography and System Security, se trata de un *malware* modular con amplias similitudes a Stuxnet, incluyendo mecanismos de inyección y un *driver* fraudulentamente firmado (ver figura 194). Stuxnet contenía un *driver* firmado por Realtek / JMicron, ambas firmas en la misma zona geográfica de Taiwán, por lo que se presume un infiltrado pudo haber robado la llave privada. Mientras que Duqu, el *driver* está firmado por una empresa de Taipéi llamada C-Media con VeriSign como certificante. Por lo que el atacante tuvo que comprometer alguna de las compañías (Bencsáth, Pék, Buttyán, Félegyházi, 2011).

La funcionalidad primaria del *malware* es de *keylogger* y sus objetivos apuntan a sistemas industriales (nucleares en Irán). Una versión mejorada (Duqu 2.0 en 2015) tuvo como objetivo P5+1 nuclear talks y el evento del 70th aniversario de la liberación de Auschwitz. Infectó en 2015 hoteles en Austria y Suiza, sede de las negociaciones respecto del plan nuclear de Irán. Además, en 2014 infectó a la empresa Kaspersky. Se cree que podría ser un trabajo de la unidad 8200 de Israel (Jennings, 2015), que posteriormente

habría informado de que Kaspersky podría trabajar en conjunto inteligencia de Rusia para escanear computadoras y obtener archivos[186] (Perlroth y Shane, 2017).

Figura 194

Stuxnet Duqu Flame y Gauss.



Nota: (Fuente imagen: Kaspersky, 2012).

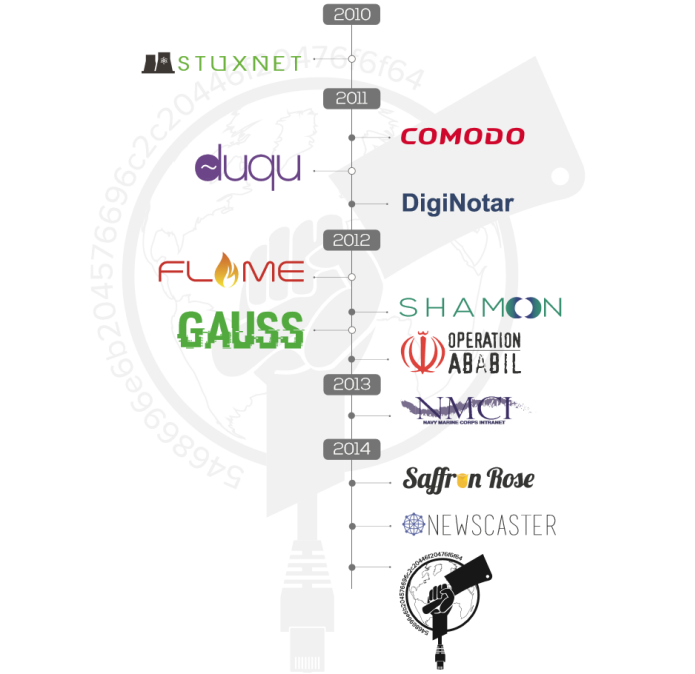
Caso Operation Cleaver

Acorde a la firma norteamericana Cylance (s.f.), un grupo de desarrolladores / hacker, aprovechó con éxito herramientas disponibles como personalizadas para atacar y comprometer objetivos en todo el mundo (ver figura 195). Los objetivos incluyen militares, petróleo y gas, energía y servicios públicos, transporte, aerolíneas, aeropuertos, hospitales, telecomunicaciones, tecnología, educación, aeroespacial, base industrial de defensa (DIB), empresas químicas y gobiernos. Los países afectados incluyen Canadá, China, Inglaterra, Francia, Alemania, India, Israel, Kuwait, México, Pakistán, Qatar, Arabia Saudita, Corea del Sur, Turquía, Emiratos Árabes Unidos y EE. UU.

Los vectores de ataque son diversos: *SQL injection*, *Spear Phishing*, *Harvesting* de credenciales y *Privilege Escalation*. Una de las herramientas utilizadas fue TinyZBot con capacidad de captura pantalla / teclado, *backdoor* / persistencia, deshabilita el antivirus Avira, *exfiltration* vía SMTP/FTP/SOAP, extracción claves navegador, entre otros. La firma indica que se trata de un grupo de al menos 20 personas (con conocimiento en idioma inglés) operando en parte fuera de Irán, pero bajo sus intereses. Irán negó la acusación indicando que solo busca obstaculizar las conversaciones en la temática nuclear (Cylance, s.f.).

[186] Recordemos el caso de Shadow Brokers.

Figura 195
Cronología operaciones.



Nota: (fuente imagen: Cylance, s.f.).

Caso Operation SNOWGLOBE

Operación de espionaje mediante un *malware* del tipo RAT llamado Babar. El nombre corresponde a un elefante animado de TV francés. Opera desde al menos el 2009 y sus capacidades son detección de antivirus, keylogger, captura de clipboard (capturar claves en caso de utilizar un gestor de contraseñas), captura de pantalla y captura de audio.

Descubierto por el servicio secreto de Canadá y revelado por Snowden. Las victimas además de Canadá fueron el programa nuclear de Irán, España, Grecia, Noruega, Argelia y Costa de Marfil. El *malware* está vinculado a EvilBunny dado que ambos poseen un error tipográfico en su código. Otros *malware* de la misma familia son Casper, Nbot, Tafacalou y Dino. Se cree que fue creado por las agencias de servicios secretos francesas (Follorou, Untersinger, 2014; Constantin, 2015).

Ciber operaciones de guerra electrónica en drones.

Caso Skygrabber ($25) Vs Predator ($40 Millon).

En 2009 insurgentes iraquíes interceptaron los videos capturados por los drones no tripulados norteamericanos (Predator) en operaciones en Irak, Afganistán y Pakistán. Dicha capacidad otorgó una inteligencia adicional a la hora de evitar tales drones.

Para la intercepción utilizaron un software ruso de $26 dólares llamado Skygrabber. El hecho se produjo debido a que algunos drones no cifraban las transmisiones. El descubrimiento se produjo al encontrar dichos videos en la laptop de un militante Chiita (Gorman, Dreazen y Cole, 2009).

Caso captura de drone (RQ-170 catch and troll).

En 2011 un drone no tripulado RQ-170 (UAV) de la firma Lockheed Martin fue capturado por las fuerzas de Irán mientras realizaba tareas de inteligencia. El US Department of Defense declaró que se encontraba en una misión en Afganistán cuando perdieron el control. Sin embargo, luego se supo que el drone de la CIA estaba realizando inteligencia de posibles instalaciones nucleares en Irán (BBC News, 2011).

No se sabe exactamente como lograron la captura. Una hipótesis es que se efectuó un bloqueo (*jammer*[187]) de las señales que controlaban al UAV (tanto satelital como terrestre). Además, lanzaron un ataque *GPS Spoof* a fin de engañar las coordenadas del drone y que el mismo aterrizada en la base iraní en vez de la base norteamericana en Afganistán (Petterson y Faramarzi, 2011).

Cuando el presidente Obama solicitó la devolución del drone y la empresa iraní Aaye Art Group ofreció devolver una versión miniatura en juguete del drone (ver figura 196) (Bozorgmehr, 2012). Irán realizó una ingeniería inversa del RQ-170 y luego replicó drones reales (Lendon, 2014). Esa tecnología podría estar siendo compartida con Rusia en el conflicto con Ucrania (Sharma, 2023).

[187] Se estima que para realizar el bloqueo de señales podrían haber utilizado un vehículo Kvant 1L222 Avtobaza ruso.

Figura 196
RQ-170 Toy.



Nota: Juguetes empresa Aaye Art Group (fuente imagen: Bozorgmehr, 2012).

Ciber operaciones a la cadena de suministro.

Caso Juniper Backdoor.

Existen varios incidentes relacionados con la criptografía Dual EC vinculados con la generación de números pseudoaleatorios y la elección de Q en los Firewall de Juniper, que se sospecha puedan ser puertas traseras de la NSA (Buchanan, 2020).

En 2015 la firma retiró parches debido a dos vulnerabilidades. Se trataba de una inyección de código no autorizado dentro del código fuente del sistema (ataque a la cadena de suministro). Las vulnerabilidades eran un *backdoor* inyectado por un actor desconocido. El CVE-2015-7755 permitía el descifrado de las comunicaciones VPN, mientras que el CVE-2015-7755 era un *backdoor* para acceso Admin (*harcoded password*) (Checkoway, Cohney, Garman, Green, Heninger, Maskiewicz, Rescorla, Shacham, Weinmann, 2016).

En el primer caso, el atacante había modificado una constante para predecir los números pseudoaleatorios generados, mientras que el segundo caso se trataba de una clave incrustada (“<<< %s(un='%s') = %u”) en el código fuente de forma ofuscada para evitar su detección por parte de auditoria (ver figura 197) (Checkoway et al., 2016).

Figura 197

CVE-2015-7755.

```
ROM:0013DC4C                STR             R12, [SP,#0x30+var_24]
ROM:0013DC50                LDR             R0, =aSCtUUnSSipSDip ; ">>> %s(ct=%u, un='%s',
ROM:0013DC54                LDR             R1, =aAuth_admin_int ; "auth_admin_internal"
ROM:0013DC58                BL              sub_558F74
ROM:0013DC5C
ROM:0013DC5C loc_13DC5C                                 ; CODE XREF: auth_admin_internal+2C↑j
ROM:0013DC5C                ADD             R0, R5, #0x44
ROM:0013DC60                LDR             R1, =aSUnSU ; "<<< %s(un='%s') = %u"
ROM:0013DC64                BL              strcmp
ROM:0013DC68                CMP             R0, #0
ROM:0013DC6C                BNE             loc_13DC78
ROM:0013DC70                MOV             R0, #0xFFFFFFFD
ROM:0013DC74                LDMDB           R11, {R4-R8,R11,SP,PC}
ROM:0013DC78 ; ---------------------------------------------------------------------------
```

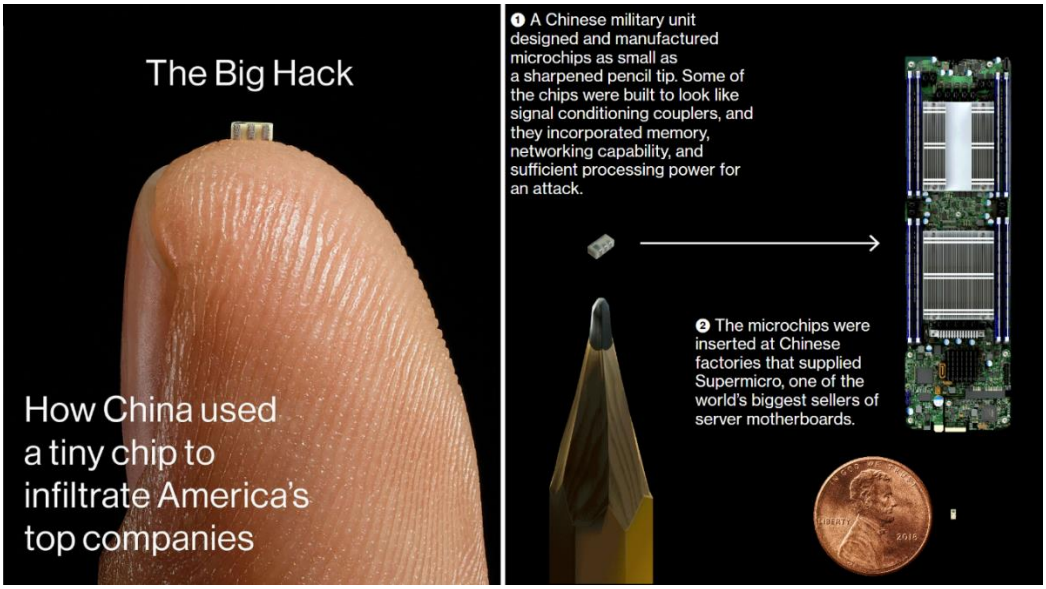
Nota: Clave oculta en el código que permite acceso Admin a los equipos Juniper (Checkoway et al., 2016).

Caso Tiny Chip - Big Hack.

En 2015 Amazon estaba interesada en una empresa llamada Elemental Technologies que poseía una tecnología de compresión de video. Amazon contrato a otra empresa para evaluar la seguridad quienes encontraron un diminuto chip que no era parte de los diseños de las placas. Este chip habría sido colocado en las fábricas de China. Estos servidores eran utilizados por el datacenter del DoD, la operación de drones de la CIA y redes en los buques de guerra del US Navy. La investigación secreta permitió determinar que existía un *backdoor* hacia la red (ver figura 198). Este método de ataque es superior a la interdicción (interceptar en el camino y colocar implante) dado que coloca el implante desde su fabricación. La afectación alcanzo cerca de 30 compañías (incluyendo Amazon y Apple). El ataque apunta a acceder a secretos corporativos y datos sensibles gubernamentales. El chip manipulaba la memoria temporal que pasaba por la placa previo a llegar al CPU, insertando código para que el OS descargara un código más complejo desde un sitio anónimo en internet. El ataque es atribuido al PLA[188] que sobornaba / extorsionaba a las fábricas de china (eran tercerizadas de Taiwán) (Robertson y Riley, 2018).

[188] Ejército de Liberación Popular de China (por sus siglas en inglés).

Figura 198
Tiny Chip Implant.



Nota: Implantación de chip desde su fabricación (Robertson y Riley, 2018).

Breve mención Intel Management Engine.

> *Si hubiera sospechado que podrían estar construyendo un motor de espionaje, ciertamente no habría cooperado, a pesar de que todo lo que querían era reducir la huella de memoria (Tanenbaum, 2017).*

Entre el OS (Sistema Operativo) y el *hardware*; en los procesadores Intel[189], operan por lo menos 2½ OS *Kernels*: UEFI y una versión modificada de Minix 3 (originalmente desarrollado por Andrew Tanenbaum). UEFI es de código cerrado y al igual que Minix 3 (para dar soporte al *Intel Management Engine - ME*). Este sistema se encuentra oculto, incluye un *file system*, un *stack* de red, *web server*, tiene acceso a las credenciales e incluso puede cambiar la imagen del *firmware* aun con la *PC* apagada (ver figura 199) (Minnich, Lim, O'Leary, Koch, Chen, Hudson, Mirtchovski, Verdun, Giamarchi, 2007).

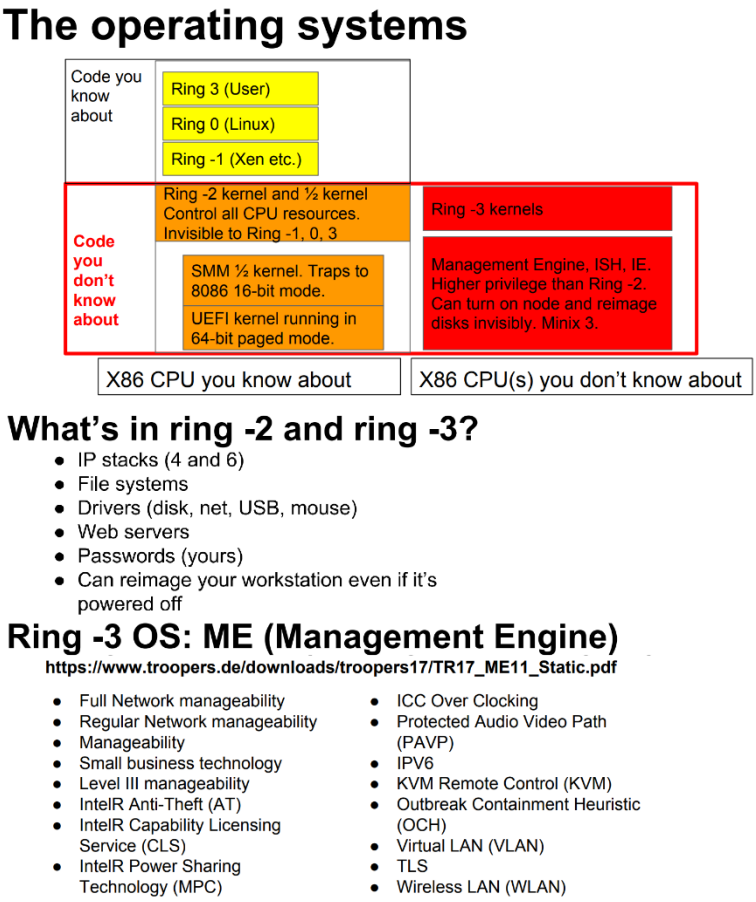
Los procesadores con vPro además cuentan con el módulo Intel *Active Management Technology* (ATM) que permite administración remota de la computadora (incluyendo instalación de OS). Se han reportado vulnerabilidades, como el acceso con default admin (Intel, 2018) o el *Silent Bob is Silent* (CVE-2017-5689)[190] (Mitre, 2017) y buffer overflow

[189] AMD también contiene código cerrado en el AMD PSP (*Platform Security Process*).
[190] Demo: https://www.youtube.com/watch?v=tVe-UYPifj8

(CVE-2017-5705, 6 y 7) (Ermolov y Goryachy, 2020). El grupo PLATINUM ha creado un *malware* para explotar el *Serial Over Lan* (SOL) y exfiltrar datos (ver figura 200) (Cimpanu, 2017).

Figura 199

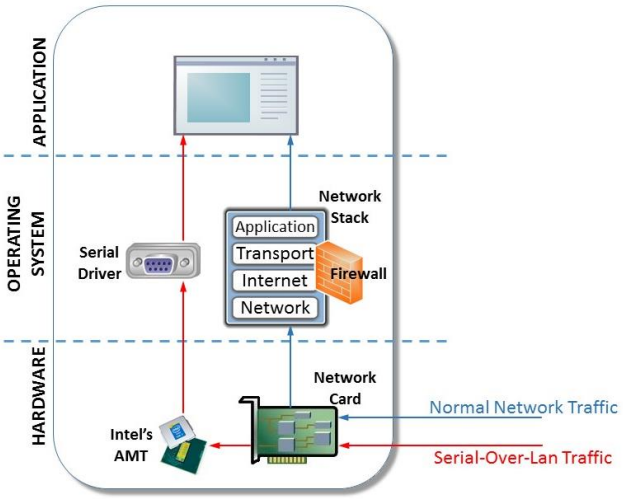
Firmware.



Nota: Kernel propietarios en los procesadores (Minnich, Lim, O'Leary, Koch, Chen, Hudson, Mirtchovski, Verdun, Giamarchi, s.f.).

Estos componentes han llamado la atención de diferentes investigadores porque existe una genuina preocupación en la comunidad de seguridad respecto a los mismos. Debido a que, por un lado, la seguridad por oscuridad no es seguridad. Por otra parte, todo software es propenso a vulnerabilidades. Finalmente, los antecedentes históricos de ataques a la cadena de suministro.

Figura 200
Intel AMT Serial Over Lan.



Nota: Funcionalidad explotada por *malware* para exfiltrar datos (Cimpanu, 2017).

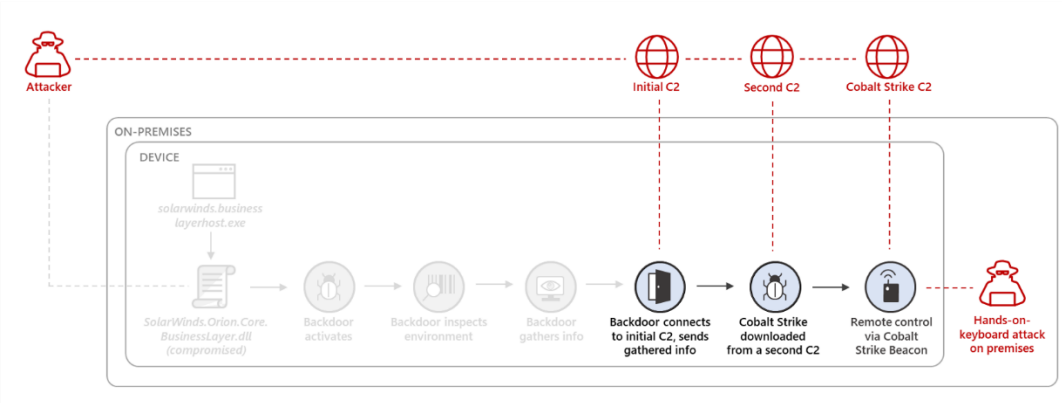
Caso SUNBURST Backdoor.

Acorde a FireEye (2020), Lakshmanan (2020, 2021), entre otros. En 2019, atacantes comprometieron la red de la firma SolarWinds (proveedora de software para la administración de infraestructura). No queda claro como fue el acceso inicial, aunque se encontró que un pasante filtró en un repositorio de GitHub la clave ("solarwinds123") del FTP de descarga. Los atacantes instalaron un *backdoor* en la herramienta llamada Orion (puntualmente el componente SolarWinds.Orion.Core.BusinessLayer.dll). Esta herramienta contenía un troyano[191] y fue instalada en cerca de 18 mil clientes, permitiendo a los atacantes ganar accesos a sus redes (ataque en la cadena de suministro). El mismo permitía enviar comandos (trasferencia de archivos, reinicio, ejecutar archivos, deshabilitar servicios, etc.). Entre las víctimas se encuentran Microsoft, FireEye, Malwarebytes, CrowdStrike, Mimecast, Administración Federal de Aviación, Administración Nacional de Aeronáutica y del Espacio Departamento de Estado / Justicia / Comercio / Energía / Agricultura y Homeland security, entre otros. En el caso de FireEye indican que robaron una herramienta de pentest.

[191] Es un programa benigno que oculta una funcionalidad maligna. En referencia al caballo de troya del poema Aeneid de Virgil de la odisea de Homero.

A partir del *backdoor*, se observó la utilización de diferentes *malware* como el dropper de memoria TEARDROP o RAINDROP, para ejecutar un Cobalt Strike BEACON (una herramienta de red team para ejecutar diversos *payloads*) (ver figura 201). La atribución se cree de origen ruso, aunque aún existen discrepancias respecto al grupo en cuestión.

Figura 201
SUNBURST.



Nota. El *backdoor* posteriormente permitió la implantación de un *malware* de Cobalt Strike (Microsoft Cyber Defense Operations Center CDOC, 2021).

Ciber operaciones en procesos electorales.

Hemos mencionado previamente algunos antecedentes de interferencia en los procesos electorales, ya sea con técnicas de hack and dump (desprestigiar), guerra psicológica (personalización de mensajes o simplemente sembrar la duda a la credibilidad del proceso electoral). Aquí ampliaremos algunos casos adicionales.

Caso Elecciones de Ucrania.

En 2014, un grupo de hackers (CyberBerkut) realizó un ataque sobre el sistema electoral de Ucrania. La finalidad no fue adulterar los votos. El objetivo era evitar que muestren los resultados genuinos, plantar resultados falsos y desacreditar las elecciones. Tener que explicar a la sociedad que los resultados no son correctos y que el ganador es otro, genera en la población, conflicto y desconfianza. Posteriormente se vinculó este grupo al ATP Fancy Bear de Rusia (Greenberg, 2019).

Caso Guccifer 2.0

Acorde a Greenberg (2019), Guccifer 2.0 es el nombre del hacker que comprometió la red del Demotratic National Comittee (DNC) durante las elecciones presidenciales de 2016. El nombre es un engaño distractivo en relación con el hacker rumano Guccifer que no tiene vinculación con el caso. Guccifer 2.0 publicó los documentos robados (hack and dump operation) a la prensa y sitios web (DCLeaks, Guccifer 2.0 y WikiLeaks). Para registrar DCLeaks se pagó con Bitcoins minados para garantizar cierto anonimato. La operación de influencia estuvo enfocada a perjudicar a Clinton. Lo que los rusos conocen como Kompromat: obtener información comprometedora de los adversarios políticos y utilizarla para formar la opinión pública / rumores. El vector de ataque fue un mail de Phishing a John Podesta con una falsa solicitud de cambio de clave en Gmail. El ataque estuvo a punto de fallar, no ser por un desentendimiento entre el Staff de Podesta y ServicesDesk. Según comenta se atribuye al grupo Cozy Bear (vinculado a la Units 26165 de inteligencia extranjera rusa/SVR) y Fancy Bear (vinculado a inteligencia militar rusa/ GRU) (Greenberg, 2019).

Acorde al reporte de Mueller (2019) sobre la interferencia en las elecciones presidenciales, el grupo que comprometió las redes se trató de Sandworm y Cozy Bear. Una vez comprometida la casilla de Podesta, continuaron la campana con otros contactos. Posteriormente los atacantes ganaron acceso a la red del DNC vía VPN, con las credenciales de un empleado. Dentro de la red fueron adquiriendo más credenciales (con Mimikatz) e implantaron 2 *malware*: X-Agent (*keylogger*, *screenshot*, listado archivo, etc) y X-Tunnel (exfiltración de archivos mediante un canal cifrado). Dentro del compromiso se encontraba el servidor de correos. El *Keylogger* permitió nuevos accesos. La exfiltración se realizó a unas máquinas *proxy* que hacían de relay de archivos a su destino final (posiblemente para ocultamiento).

Continua que el Internet Reseach Agency (IRA o también conocida como la fábrica de Trolls) de Rusia llevó a cabo campañas en redes sociales desde 2014 (Facebook, YouTube, Twitter y posteriormente Tumblr e Instagram). Enfocadas a favorecer a Trump y desacreditar a Clinton con la utilización de cuentas falsas. Por otra parte, la agencia es conocida en fomentar manifestaciones arengando a grupos antagónicos a encontrarse en un

mismo lugar (amplificando el asunto al contactar a la prensa). En ambos casos, reporta que se utilizaron 3500 advertisement ($100mil). En el caso de Twitter utilizaban una cuenta falsa simulando una U.S. person y luego utilizaban una granja de cuentas para amplificar. En algunos casos llegando a personas de alto perfil que amplificaban aún más los mensajes (retweeted) (Muller, 2019).

Caso Elecciones de Francia.

El exjefe Bernard Barbier del servicio secreto francés (DGSE), en una entrevista confirmó que la NSA se infiltro en la red presidencial de Francia en 2012, durante las elecciones presidenciales. Lo que elevó un reclamo a la NSA a pedido del presidente (Francois Hollande). El director de la NSA (Keith Alexander) le habría confirmado el hecho. Para el espionaje habría utilizado un *malware* con una firma similar al *hack* de la comisión europea en 2010 (Sayer, 2016; Follorou, 2016). Dado su descubrimiento se desconoce el objetivo final. ¿Podría estar vinculado a alguna interferencia en las elecciones?

Ciber operaciones en sistemas financieros.

Caso Operation Ababil.

Ocurrido en 2012, consistió en una serie de ciberataques (DDOS) principalmente contra instituciones financieras de USA. El grupo apodado Izz Ad-Din Al Qassam / Qassam Cyber Fighters anunció por Pastebin que el ataque se trató de una represalia por el cortometraje anti musulmán (Innocence of Muslims) popularizado por un pastor norteamericano antimusulman. El video causó una serie de revueltas en medio oriente, siendo Libia la más violenta, causando la toma de la embajada de EE.UU. y el asesinato de 4 norteamericanos (incluyendo al embajador). Acorde a la comunidad de inteligencia norteamericana, el grupo que llevo a cabo el ataque fue de Irán (Buchanan, 2020).

El acontecimiento recuerda en parte al hack a Sony de 2014. Ambos acontecimientos no se encuentran vinculados, aunque fueron consecuencia de un video ofensivo. Como indica (Buchanan, 2020; Baumgartner, 2014), un grupo de hackers denominados “Guardians of Peace”; exfiltraron datos, publicaron información y lanzaron un wiper sobre

los sistemas de la compañía Sony. El ataque fue consecuencia de la película “The Interview” que parodia al líder norcoreano Kim Jong-un.

Acorde al FBI, el gobierno de Corea del Norte es responsable de estas acciones (Federal Bureau of Investigation, 2014).

Caso robo bancario (Bank Heist).

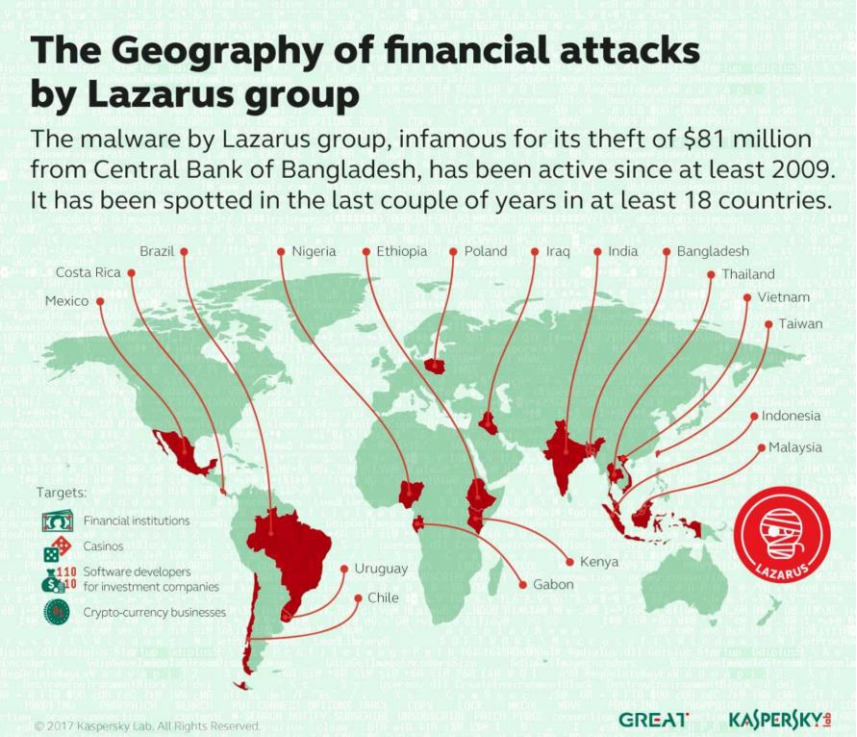
Kaspersky ha investigado varios casos de ciberataques a bancos llevados a cabo presumiblemente por el grupo Lazarus de Corea del Norte (ver figura 202).

Los atacantes luego de comprometer la seguridad perimetral (en un caso un servidor Web, en otra oportunidad Watering hole de un sitio infectado), pasan meses dentro de la red aprendiendo de la misma, realizando movimientos laterales y ganando accesos. El grupo utiliza una diversidad de herramientas, desde un *backdoor* RAT, *Keylogger* para obtener credenciales, software proxy para utilizar maquinas internas como salto y no llamar la atención del C2C, etc. El objetivo final y más deseado es el sistema Swift Alliance que se encarga de realizar las transacciones bancarias (Kaspersky, 2018).

En ocasiones realizan un ataque lateral para distraer al personal de seguridad mientras se lleva a cabo el golpe (transferencia de dinero que posteriormente extrae una mula en otro país). En el caso del banco de Chile de 2018, arrojaron un ransomware de distracción mientas robaban 10 millones de dólares (Leyden 2018; Merces, Gelera y Co, 2018).

Uno de los golpes más relevantes fue el del Central Bank of Bangladesh (2016). Los atacantes adulteraros los archivos de log y corrompieron la impresora de transacciones (dejando a ciegas a los auditores). Estuvieron a punto de robar 100 millones de dólares, si no fuera porque llamaron la atención al escribir mal el nombre de la entidad destinataria del pago. Otra parte de las transacciones pudo ser recuperada, aun así, los atacantes lograron obtener una cifra para nada despreciable (Kaspersky, 2018).

Figura 202
Golpes a bancos.



Nota: El objetivo es tomar el control del sistema Swift de transferencias bancarias (Kaspersky, 2018).

Caso Deep Voice.

Durante 2020, el director de una empresa de energía de Reino Unido recibió una llamada de su jefe para realizar una transferencia de 243 mil dólares a un proveedor húngaro. Lo que no sabía era que se trataba de un atacante utilizaron un software de inteligencia artificial para falsificar la voz de su superior (Stupp, 2019).

En 2020, un atacante engañó a un gerente de un banco de Hong Kong simulando ser el director de una importante empresa. En la llamada indicaba que iban a realizar una adquisición y que solicitaban autorización para la transferencia de 35 millones de dólares. Nuevamente se trató de una estafa elaborada utilizando IA para falsificar la voz del director corporativo (Brewstep, 2021).

Ciber operaciones con Deep Fake (IA).

La inteligencia artificial no responde a la sociedad si no a los intereses de sus creadores (reflexión de elaboración propia).

En relación con la tecnología de *Deep Fake*. Durante 2021, unos bromistas engañaron a varios políticos europeos (Reino Unido, Letonia, Lituania y Estonia) organizando una video llamada desde correos falsos. Los bromistas suplantaron la identidad de Leonid Volkov (jefe de gabinete del político opositor ruso Alexei Navalny). Al principio se pensó que utilizaron *Deep Fake*, pero se trató de un imitador. El echo igualmente levantó las alertas de la utilización de esta tecnología para llevar a cabo ataques diversos (Vincent, 2021). En 2022, alcaldes de Berlín, Madrid y Viena fueron nuevamente engañados para realizar una video llamada con el alcalde de Kiev, Vitali Klitschko. Nuevamente se trató de un engaño y se sospecha que podrían haber utilizado tecnología Deep Fake (Oltermann, 2022).

Previo a estas tecnologías, ya existían intereses en montajes para *fake news*. Un ejemplo fue la operación de la CIA que consistía en realizar un video falso de Saddam Hussein (líder de Irak) teniendo relaciones íntimas con una persona del mismo género. Algo no tolerable dentro de su cultura ortodoxa/cerrada. El video simulaba una supuesta cámara oculta de baja resolución. La idea era distribuirlo en la población para facilitar la invasión de Iraq en 2003. Finalmente, el plan no se llevó a cabo, pero resalta el interés en la materia (Harris, 2010).

Si bien se están desarrollando técnicas para la detección de estos engaños, en algún punto quizás no pueda ser posible distinguir un engaño de la realidad. Después de todo, los datos no son ni más ni menos que ceros y unos. Como decía Arthur C. Clarke: “Cualquier tecnología lo suficientemente avanzada es indistinguible de la magia” (Clarke, 1962).

Tecnologías exponenciales como la inteligencia artificial generativa, la computación cuántica o comunicaciones por ondas gravitacionales, por mencionar algunas; pueden brindan tanto desafíos como oportunidades en el ámbito de la ciberdefensa y la ciberseguridad.

Conceptos claves del capítulo.

El presente capitulo consistió en exponer antecedentes históricos para dar soporte a las ciber operaciones. No se han mencionado casos puntuales vinculados al cibercrimen dado que el presente trabajo está enfocado a las operaciones dentro de un marco de guerra híbrida. Cabe aclarar que la misma está lejos de abarcar todos los hechos importantes ocurridos en los últimos años, aunque no por ello sea insuficiente para exponer la complejidad con al que nos enfrentamos.

- Hemos apreciado que existen ciber operaciones enfocadas al espionaje, robo tecnológico, sabotaje, operaciones militares, afectación a procesos electorales y desacreditar, entre otros.
- Las ciberarmas pueden ser de lo más diversas, aunque en general suelen ser avanzadas y poseen foco en el sigilo.
- El ataque a la cadena de suministros, como hemos ido desarrollando en capítulos anteriores, es una de las peores pesadillas a la cual puede enfrentarse un defensor.
- La gran mayoría de los actores están enfocados en el espionaje, sin embargo, las ciber operaciones suelen ser congruentes con la estrategia global de cada país o estar determinada por sucesos específicos del momento. No es suficiente el análisis técnico de los casos, se requiere un vasto conocimiento en historia y geopolítica. Por mencionar algunos casos, Corea del Norte tiene un acceso restringido a las divisas debido al bloqueo internacional que enfrenta y es esperable que sus ciber operaciones estén vinculadas a atacar entidades financieras o el sistema Swift para hacerse de ese dinero que tanto necesita. China tiene una estrategia de equiparar a EE.UU. para el 2035 y ser potencia mundial para el 2050; sus ciber operaciones están vinculadas al espionaje/robo tecnológico, mientras que por otra parte evita realizar operaciones disruptivas que puedan generar un conflicto que lo desvíen de su camino de desarrollo. Rusia está experimentando con las ciber operaciones de guerra híbrida de lo más diversas, apreciable una relación con sus operaciones de influencia a los países limítrofes e influencia en elecciones norteamericanas (posiblemente

apunte a prevenir un líder que tenga una política agresiva contra ellos). EE.UU. por su parte, apunta al espionaje total y a la influencia del mundo entero; espía a sus aliados, pero pone un foco particular en sus enemigos (donde las operaciones suelen ser más disruptivas / agresivas). Para algunas operaciones, requiere del apoyo de aliados. Como ya vimos, la inteligencia alimenta las operaciones de lo más diversas dentro de un esquema de guerra híbrida para lograr una dominación total.

Capítulo ~~(5)~~ Kairós – Conclusión

Mientas el hombre siga siendo hombre, el mundo jamás conocerá la paz
(reflexión de elaboración propia).

Durante el desarrollo del presente documento hemos explorado la existencia de un submundo (*DeepWorld*) no visible. Un *Deepworld* de espionaje, operaciones y guerra invisible del cual solo son observables algunas aristas aisladas. En este mundo no existen buenos ni malos, solo intereses en busca de la dominación a partir de la supremacía de la información y la colonización tecnológica. El trabajo refleja las vulnerabilidades y los peligros inmersos de las sociedades del siglo XXI. Cuando la información obtenida a través de la inteligencia sin límites se encuentra disponible, las operaciones basadas en decisiones precisas resultan letales. Los ataques pueden ir desde disrupción de infraestructuras críticas, acceso a sistemas de comunicación / información (retroalimentación), sabotaje de proyectos estratégicos, implantación de tecnologías (colonialismo tecnológico), afectación de procesos electorales, instauración de gobiernos a fin, penetración cultural, dominación económica (incluyendo deuda), influencia a partir de perfilación psicológica, asesinato de personaje / objetivos estratégicos e inclusive la modificación del comportamiento (sociedades a medida), entre otras.

Como desarrollamos, las capacidades y características del 5to dominio, no hacen más que potenciar las operaciones de la guerra sin límite. El anonimato, la abundancia de datos, la velocidad de transmisión y el procesamiento masivo (incluyendo el uso de tecnologías como la IA); son solo algunas de las particularidades que desarrollamos. La comprensión de la geopolítica mundial y el conocimiento de la historia del siglo pasado (antecedentes desarrollados), son imprescindibles para el estratega del siglo XXI. La visión tradicional y el estudio mono disciplinario no resultan suficientes para comprender la complejidad de los conflictos modernos. Se requiere un pensamiento crítico para anticipar los peligros futuros a partir de la dinámica de las tecnologías de la información y la comunicación.

Estrategia Argentina: recomendaciones y lineamientos de ciberseguridad.

No se trata de lo que quieran hacerte si no de lo que tú les permitas
(reflexión de elaboración propia).

El presente trabajo no pretende definir un plan estratégico nacional. Sin embargo, puede ser utilizado como base para fijar los lineamientos globales que debe perseguir dicha estrategia. No es posible diseñar un plan sin reconocer la inmersa dominación (bajo un esquema de guerra invisible) que se encuentra presente nuestro país desde el siglo pasado. La influencia se produce no solo desde el exterior, sino que cuenta con actores (*insiders*) en todas las estructuras de la nación. Por lo tanto, quien tenga la responsabilidad de desarrollar un proyecto estratégico nacional, no puede omitir valerse de la información del presente trabajo a fin de tener alguna posibilidad de éxito. Seguidamente, realizaremos una mención al caso del proyecto Condor.

La estrategia también debe contemplar la situación geopolítica mundial en la que se enfrentan diferentes actores (EE.UU., Rusia, China, entre otros). Argentina, en su humilde posición, puede desarrollar alianzas y planes para garantizar un mejor posicionamiento mundial. Los países latinoamericanos, por similitudes históricas, pueden ser aliados en búsqueda de una unión estratégica.

El plan debe contemplar los aspectos desarrollados. Al mismo tiempo, promover una sociedad justa y moderna; respetando a la naturaleza y los seres vivos. La tecnología debe estar a disposición de los ciudadanos y no por el contrario.

Algunos puntos para tener presente son:

- Imprescindible la participación de un equipo interdisciplinario conformado por civiles y militares; estrategas, especialistas en las TIC, psicólogos, historiadores, especialistas en derecho, entre otros.
- Desarrollo de una disuasión legal que incluya penalidades económicas / penales con foco en los datos y la privacidad de los ciudadanos. Requerimientos respecto al almacenamiento de datos dentro del ámbito nacional (soberanía de datos). De forma análoga, el enrutamiento de las

comunicaciones en el ámbito local (soberanía de comunicaciones). Leyes penales rigurosas contra las operaciones mencionadas y organismos de control.

- Auditorias rutinarias sobre los sistemas y empresas de telecomunicaciones. Los implantes o mecanismos de inteligencia siempre están presentes, solo deben ser encontrados y los responsables deben castigados severamente por sus delitos.
- Desarrollar sistemas propios; tanto hardware como software para las comunicaciones y el procesamiento de datos. Ampliar los desarrollos en criptografía post cuántica. Desarrollar sistemas de detección automática de ciber amenazas, procurando que estos no sean un nuevo mecanismo de inteligencia.
- Fomentar los esquemas de arquitecturas descentralizadas, donde los datos y el cifrado resida del lado del usuario. Dejar de ser un estado facilitador y cómplice para pasar a ser un defensor de la privacidad / seguridad de sus ciudadanos.
- Proponer leyes internacionales con amplias penalidades por incumplimiento por parte de los estados. No solo en las operaciones de espionaje, sino también en la transparencia frente a sus ciudadanos.
- Plan de educación en las escuelas con las temáticas que hemos desarrollado. En particular la guerra por las mentes. La tecnología actual permite grabar y distribuir clases con especialistas de alto nivel internacional a un bajo costo.
- Plan de capacitación de talentos para el desarrollo futuro del país, pensado en las tecnologías disruptivas/exponenciales.
- Desarrollar defensas psicológicas en la población (como los anticuerpos contra un virus) para no ser vulnerable a los ataques de guerra psicológica. El mensaje subliminal, es un menaje que pasa por debajo de los límites de percepción. Educar amplia los límites de percepción y awareness psicológico, haciendo menos probable el éxito del psico atacante.
- La educación y el awareness deben ser parte de la cultura de la sociedad. Son las mismas personas que retransmiten y amplifican los mensajes. Las *fake news* tendrían una corta vida sin el sustento de las personas. De forma análoga y

como si fuera un movimiento de aikido; los *character assassination* no serían tan efectivos si la gente comprende que no hablan mal del objetivo sino del emisor.

- No hay plan que resista a las personas. Recordemos que la cultura se come a la estrategia en el desayuno (Peter Drucker). Hay que educar con principios y valores.
- La educación basada en casos de estudio no es suficiente dado que las técnicas pueden mutar en el tiempo al igual que la tecnología. La educación debe desarrollar un paradigma de instrucción fomentando razonamiento y pensamiento crítico.
- Desarrollo de una red nacional independiente con capacidades de desconexión del mundo en caso de situaciones riesgosas (Rusia y China están trabajando en redes autosustentables).
- La responsabilidad del cuidado de los datos no puede recaer únicamente en las empresas, cuyos intereses no se condicen con los de la nación. La responsabilidad del estado tampoco es suficiente y requiere una participación ciudadana activa.
- Debatir sobre los límites entre la libertad de prensa y las operaciones psicológicas / propaganda sobre la población.
- En definitiva, se requiere de un plan estratégico integral a nivel nacional para el desarrollo de un gobierno digital. Incluyendo diferentes pilares como la gobernanza e institucionalidad, políticas de estado con normativas, infraestructura en las TIC, talentos, gestión del cambio, reingeniería de procesos enfocada a la eficiencia y por sobre todas las cosas, una visión que contemple los aspectos de la seguridad de la información.

Futuros Riesgos.

La paradoja de la IA es llegar a la conclusión de que el mayor peligro del ser humano es él mismo y que para protegerlo debe eliminarlo (reflexión de elaboración propia).

La tecnología continúa avanzando y expandiendo sus fronteras. La misma moldea y transforma la sociedad. Los nuevos descubrimientos otorgan nuevas capacidades para los individuos, pero a su vez los hace más vulnerables a nuevas formas de ataques. Tecnologías como Inteligencia Artificial (IA) podrían ser exponencialmente disruptivas en un sentido amplio. Tales tecnologías deberían estar al servicio de la sociedad y no responder a los intereses de otros. Algunos peligros que pudiéramos observar con mayor preponderancia a futuro podrían ser:

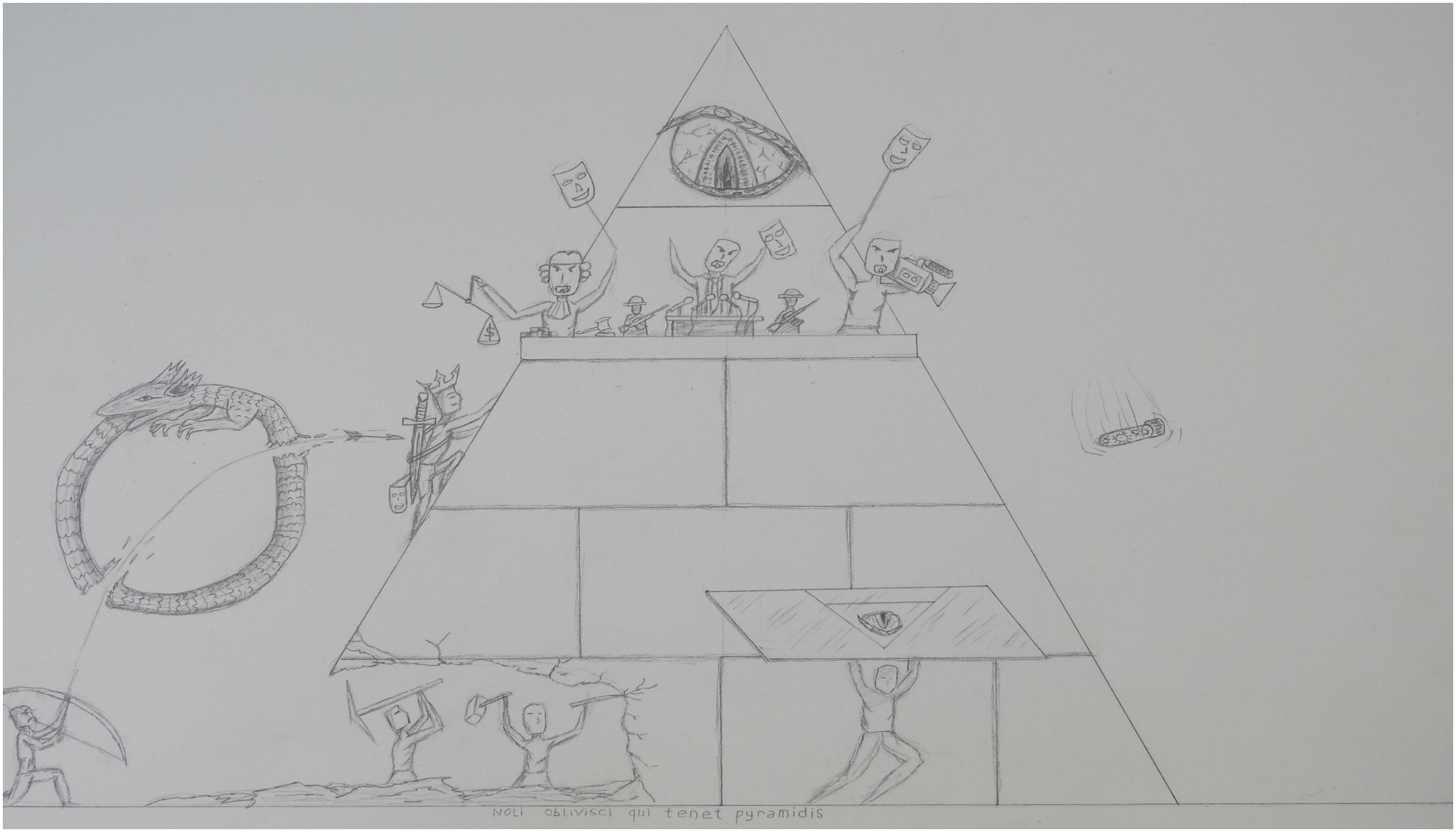
- Ampliación de las capacidades en la guerra psicológica en la manipulación de las masas.
- Ataques sobre implantes médicos como ser marcapasos cardíacos o bombas de insulina (asesinatos sigilosos). Análogamente, ataques sobre el hombre cibernético (ciborg) del futuro.
- Fraguar evidencias digitales para incriminar objetivos (lawfare). En particular atención cuando los actores son investigadores, jueces, ejecutores y reporteros de la propaganda en función de un interés superior.
- Car hacking para producir accidentes indetectables o afectar la disponibilidad.
- Toma de control de robots que se encuentren trabajando al servicio de la sociedad. El atacante podría crear una gran botnet y producir caos en la sociedad.
- Ataques sobre IA (basadas en redes neuronales), afectando la cadena de suministro (inyectando interferencias en los data sets de entrenamiento) o alterando los sensores de la red (inputs) a fin de que la computadora tome decisiones equivocadas. Dependiendo la situación, podrían tener consecuencias nocivas.
- Tecnologías como 5G de alta frecuencia que pueden ser transformadas en armas de alta frecuencia.
- Disrupción total de un país (quien tiene el poder de los datos y la arquitectura de la nube puede apagar la sociedad en su conjunto).
- La singularidad tecnológica podría llevar a la sociedad a una dimensión que no podemos imaginar. Este podría ser un futuro utópico o quizás distópico.

Cabe aclarar que, si bien el trabajo expone los diferentes peligros asociados a la tecnología, no es razonable que las sociedades permanezcan aisladas de la misma. Evitar el riesgo no es una opción estratégica. Deben tomarse medidas proactivas con ética y responsabilidad.

Futuras investigaciones.

Existen varios aspectos del presente trabajo que puede impulsar posteriores investigaciones para aquellos que quieran colaborar / ampliar el conocimiento.

- Ampliar antecedentes de ciber operaciones.
- Proponer mejoras al framework de dominación. Ampliar la invasión cultural.
- Desarrollar casos de estudio sobre la temática de dominación dentro de un esquema de operaciones de guerra sin límites.
- Extender los aspectos de guerra sin límites, en particular interés la guerra por las mentes.
- Desarrollar aspectos legales a nivel nacional e internacional con particular mención a las operaciones de vigilancia (tanto masiva entre estados como las individuales de corporaciones por fuera del real awareness del usuario). Comparativa entre diferentes países potencia.
- Ampliar la vigilancia masiva y las revelaciones de Snowden.
- Proponer estrategias nacionales basadas en la problemática descripta.
- Estudio y seguimiento de la criptografía / comunicaciones cuánticas. El entrelazamiento cuántico permite contramedidas como así también nuevos ataques (ejemplo, una partícula enlazada secreta/Man in the Quantum Attack).
- Investigar el secretismo del código oculto dentro de los procesadores.
- Estudiar y proponer posibles estructuras de organización sociales que garanticen la transparencia, equidad y desarrollo de sus seres.
- Cualquier otra investigación que pueda desprenderse del presente trabajo que corrija o amplié las fronteras del conocimiento.


NOLI OBLIVISCI QUI TENET PYRAMIDIS

Apéndices.

Capítulo apéndice: ~~(0)~~ Krónos – Conceptos Básicos.

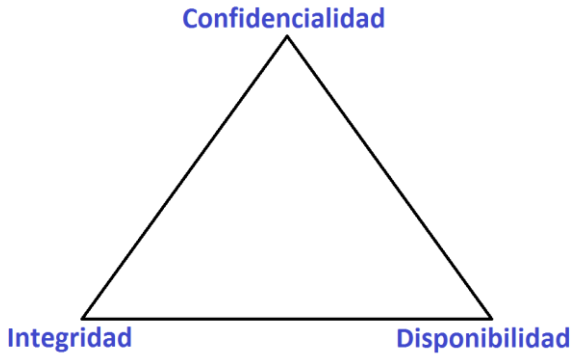
Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología (Bruce Schneier).

El correspondiente capitulo consiste en una breve base conceptual para quienes no se encuentren familiarizados con la temática de seguridad de la información. El mismo no pretende ser exhaustivo ni riguroso, sino más bien brindar una pequeña base conceptual de ideas y términos que ayudaran a comprender los posteriores capítulos.

Principios de seguridad de la información.

Una de las principales nociones, son los pilares de la información para la protección de los activos críticos. También conocidos como CIA[192] Triad: Confidencialidad, Integridad y Disponibilidad (ver figura 203) (Harris y Maimí, 2019).

Figura 203
Triada de la información



Nota. Los pilares están conformados por la Confidencialidad, Integridad y Disponibilidad. Incorporando además la dimensión de *safety* (fuente imagen: elaboración propia).

[192] Referente a las iniciales en inglés de Confidentiality, Integrity y Availability.

En términos básicos, la confidencialidad se refiere a que la información privada solo debe ser accedida por quien está autorizado. La integridad hace referencia a que la información debe ser consistente en el tiempo, sin alteraciones (ej. producto de un acceso no autorizado, una afectación por bomba lógica[193] o a una falla del sistema de almacenamiento). Finalmente, la disponibilidad consiste en que la información debe estar disponible cuando se requiera (por el *owner* o el modelo de negocio). Hoy en día, la información es un activo de los más valiosos para una organización y debe ser protegida en todos sus estadios (*at rest*[194]*, in motion, in use*). Es por eso por lo que usualmente en sistemas IT[195] la Confidencialidad suele ser prioridad por sobre los otros aspectos, mientas que entornos OT[196], la disponibilidad suele ser precedente.

Los entornos OT son Sistemas de control industrial (ICS) en donde los HMI[197] / SCADA[198] manejan controladores de campo (ej. controladores de lógica programables o PLC) que a su vez operan dispositivos de campo/actuadores (ej. válvulas, sensores, interruptores, entre otros). Para quien no está familiarizado con esta temática puede resultar complicado, pero en realidad no lo es. Se trata básicamente de un sistema que obtiene datos de entrada de sensores y tiene una lógica (programa) que actúa tomando acción sobre actuadores. Por ejemplo: si la temperatura de un horno industrial es excesiva, el programa toma las acciones correspondientes sobre válvulas físicas que regulan los elementos de la combustión del horno. Por lo explicado, puede entenderse que en dichos sistemas resulta crítico el tiempo de respuesta basado en los datos (disponibilidad) mientras que la confiabilidad de estos es un aspecto secundario.

Es importante mencionar que la seguridad es inversamente proporcional al costo y a la facilidad de uso. Esto es sencillo de comprender ya que mayor seguridad implica mayores costos en profesionales, equipamientos, controles, etc. mientras que el usuario ve afectada su facilidad de uso al requerir diferentes factores de autenticación, clasificar la información,

[193] Una bomba lógica es un algoritmo con una finalidad destructiva sobre el Sistema o los datos.
[194] *At rest* es la información en estado de reposo o almacenamiento, usualmente protegida entre otros mecanismos por los sistemas criptográficos. *In motion* es información en tránsito, por ejemplo, transferida por la red. Pudiendo ser interceptada por un tercero (*Man in the middle*). *In use* es información en uso en memoria o en los registros del CPU.
[195] Tecnologías de la información (*Information technology*), referente a redes corporativas de datos.
[196] Tecnologías de operación (*Operation Technology*), referente a máquinas/fábrica.
[197] Interfaz hombre máquina (*Human Machine Interface*).
[198] Sistemas de supervisión, control y adquisición de datos (*Supervisory Control And Data Acquisition*).

rotación de claves, estar en alerta constante (*awareness*), etc. A causa de lo mencionado es que se busca un punto de equilibrio entre dichos aspectos.

El concepto del eslabón más débil de la cadena nos ilustra como los sistemas son tan robustos como su punto más débil, es por ello por lo que la seguridad se aplica en profundidad o capas, como las capas de una cebolla (Ver figura 204). La redundancia de mecanismos de seguridad permite que en caso de falla exista otro nivel de contención/protección. El ejemplo clásico es el del castillo del rey: para matar al rey primero hay que pasar la fosa con cocodrilos, luego superar la muralla con arqueros, derrotar a los guardias de la ciudad, sobrepasar la segunda muralla interior, vencer a los guardias reales para finalmente poder llegar al rey. La primera muralla que separa la ciudad interior (de confianza) del mundo exterior (no confiable) suele conocerse como seguridad perimetral. Debido a que gran cantidad de ataques son producidos por o con ayuda de *insiders*[199] (de forma consciente o inconsciente), hoy en día se está dejando de lado la seguridad perimetral para pensar en arquitecturas del tipo *Zero trust.*

La estrategia *Zero Trust* implica que cada uno de los actores/activos dentro de la red no son confiables y por lo tanto deben ser validados previamente. Otras estrategias como el *Moving Target Defense* (MTD) buscan crear la misma asimetría sobre el atacante generando incertidumbre en cambios constantes (a nivel red, sistema, código) utilizando técnicas de: *Shuffling*, *Diversity* y *Redundancy*[200]. La estrategia de arquitectura *Cybersecurity Mesh* utiliza un perímetro de seguridad para cada dispositivo en un enfoque holístico. En un futuro posiblemente apreciaremos sistemas automáticos/inteligentes tanto en la defensa como en el ataque.

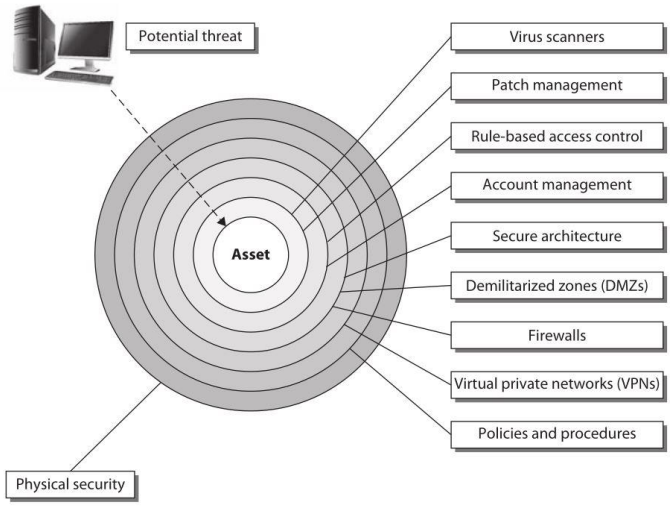
Volviendo a los conceptos de seguridad, *Security by obscurity* (seguridad por oscuridad) hace referencia a que mantener en secreto que la llave de la casa se esconde bajo el tapete, no es realmente seguridad. Esto es debido a que tarde o temprano alguien va a descubrirlo.

[199] Persona que trabaja de manera directa o indirecta dentro del perímetro de confianza y por su naturaleza tiene acceso y conocimiento de este.
[200] *Shuffling* se refiere a cambiar las direcciones de red (IP) constantemente dentro de una red virtual definida por software (SDN) a fin de que un atacante luego no pueda encontrar al objetivo que había planeado atacar. *Diversity* consiste en cambiar el código/sistema operativo/etc. a fin de modificar las vulnerabilidades que pudo haber encontrar el atacante previamente y que al realizar el ataque ya no se encontraran presente. *Redundancy* es tener elementos alternativos de disponibilidad en caso de ataque. En la práctica es difícil/costoso de implementar, presenta algunos inconvenientes y su eficiencia es discutible.

La seguridad únicamente por oscuridad no es seguridad[201]. Sin embargo, en un esquema robusto en capas con un adicional de oscuridad o desinformación, en ciertas circunstancias podría ser conveniente, siempre y cuando el profesional comprenda conceptualmente la seguridad en tu totalidad.

Figura 204

Ejemplo de seguridad en capas.



Nota. (Fuente imagen: Harris y Maimí, 2019).

En seguridad solo debe acceder a la información solo quien realmente lo requiera y con el menor privilegio posible. Esto nos lleva a los conceptos de Need to know y Least privilege respectivamente.

Finalmente cabe mencionar que el software no es libre de errores. Por ejemplo, podemos medir con la densidad de falla promedio cada 1000 líneas de código (defect density, KLOC[202]). El primer bug[203] recibió su nombre por una polilla encontrada por Murray Hoppers en 1947 en un relé de la Mark II[204]. Dichos errores, sea por equivocación o adrede, son una vulnerabilidad en los sistemas y pueden ser explotados por un atacante para modificar el flujo habitual de un programa o sistema. La calidad del código no es la única

[201] No debe confundir este concepto con mantener en secreto las técnicas y métodos defensivos, como por ejemplo controles de mitigación de riesgos. Se puede conocer que controles se realizan como mecanismo disuasivo, pero nunca indicar como se llevan a cabo, dado que esto permite eludir (*circunvent*) el control.
[202] Del ingles, *Kilo Line of Code*.
[203] Bug es un término histórico que refiere a una falla.
[204] Computador electromecánico de la Universidad de Harvard.

medida de seguridad. Acorde a Howard, Pictus y Wing (2003), la superficie de ataque (*Surface Attack*) del sistema representa indicador de oportunidades de ataque (*Attackability*). Las dimensiones son: *Target*/*Enablers*, *Channels*/*Protocols* y *Access rights*[205]. La idea conceptual consiste en que reducir la superficie de ataque reduce las posibilidades de ser atacado. Como remarca Pratyusa, Tan, Maxion y Wing (2007) un atacante se conecta al sistema usando canales de comunicación (*channels*), invoca métodos (*methods*) y envía datos (*data ítems*)[206]. Estos recursos de sistema a los cuales tiene acceso un atacante conforman la superficie de ataque. Si bien la medida de superficie de ataque no representa la calidad del código, una gran superficie de ataque indica que es probable que un atacante explote las vulnerabilidades presentes. Dado que el código usualmente contiene vulnerabilidades, es prudente reducir la superficie de ataque para mitigar riesgos en la seguridad.

Es imperioso comprender que no existe la bala de plata. Este concepto remarca la falsa creencia de que un sistema o protección es perfecto y apto para todos los tipos de ataques. El Almirante Mike Rogers (Comandante del U.S. Cyber Command), mencionó en una charla organizada por el Royal United Services Institute (RUSI): "*despite your best efforts, you must prepare and assume that you will be penetrated*" (Martins, 2015). Efectivamente la ofensiva es más fácil y económica que la defensa, ya que el atacante solo debe tener éxito solo en una oportunidad para triunfar, mientras que el defensor debe detener todos los ataques. Además, el ataque tiene una ventaja estratégica del factor sorpresa y de ir delante de la defensa (primero sale el *malware*[207] y después el *antimalware*, surge la vulnerabilidad[208] y luego el parche[209], etcétera).

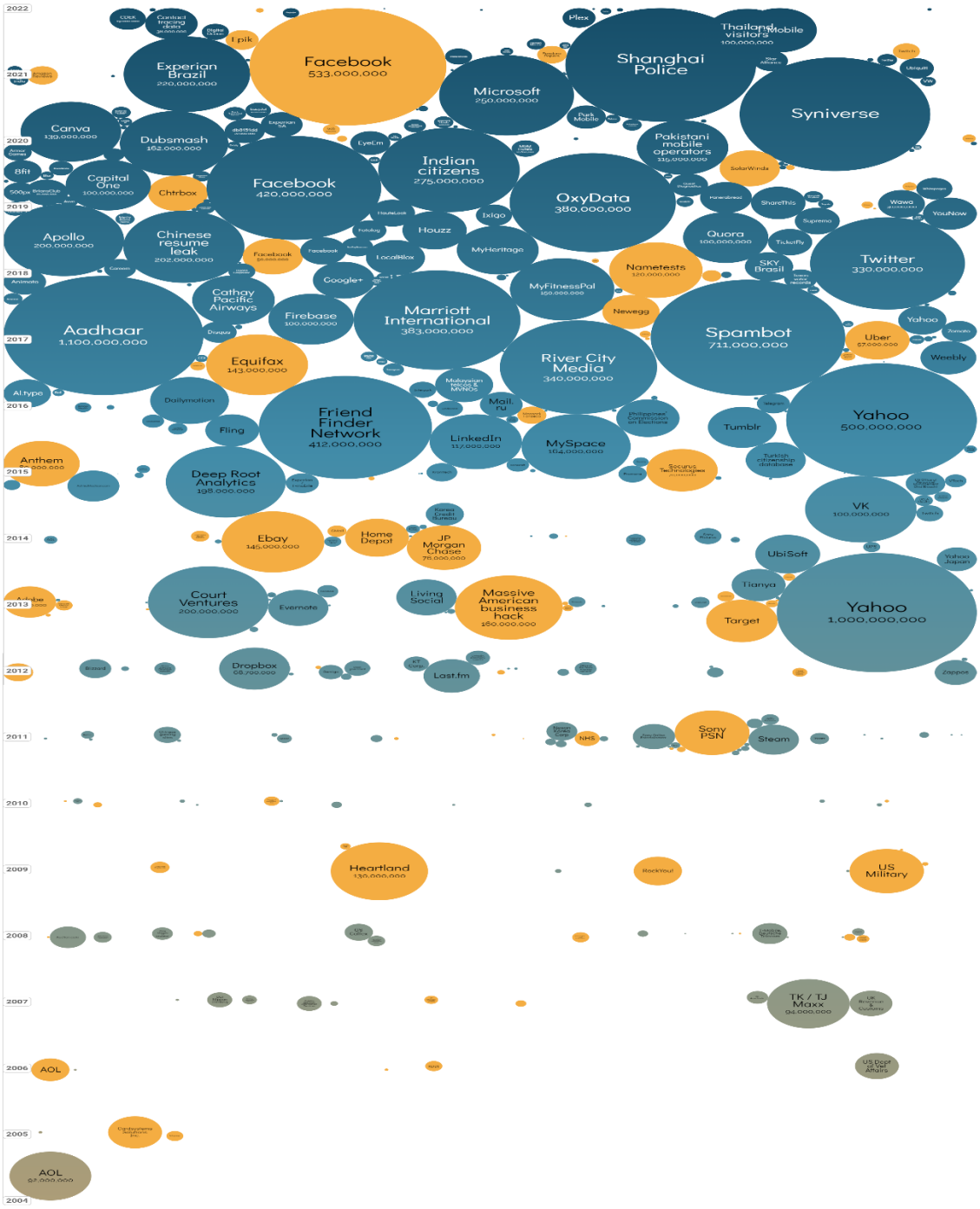
Lo mencionado puede sustentarse en las estadísticas de fuga de datos (*leaks*). En la figura 205 puede apreciarse la tendencia con un incremento en los *leaks* de datos. Tener presente

[205] *Target* son procesos o datos que el atacante desea controlar. *Anablers* son otros procesos o datos que el atacante utiliza para llevar a cabo el ataque. *Channels* y *protocols* es la manera de comunicarse con el sistema. *Access rights* sos las restricciones de permisos impuestas por el sistema.
[206] *Channels* son los canales de comunicación (ej. sockets), *method* son los métodos (ej. API o funciones de sistema) y *data ítems* son los datos que envía o recibe (ej. un input de una cadena de caracteres).
[207] Software malicioso.
[208] Debilidad no esperada de un Sistema que podría permitir modificar el funcionamiento esperado del mismo.
[209] Actualización de software destinada a corregir un error. No siempre efectiva y puede adicionar nuevos errores.

que dicho gráfico no cuenta filtraciones que no fueron denunciadas o intrusiones sigilosas por gobiernos o agencias de inteligencia.

Figura 205

Leaks de en los últimos años (2004-2022).



Nota. Cronología de abajo (2004) hacia arriba (2022) (Fuente imagen: McCandless, Evans, 2022).

En relación, recientemente se ha filtrado una base de datos llamada RockYou2021 que consiste en una recopilación de 8.460 Millones de contraseñas, siendo la más grande hasta la fecha (García, 2021). También las noticias han dado a conocer el hurto la base de datos de documentos del RENAPER (registro nacional de las personas de Argentina) que incluye la información completa, incluyendo fotos (por ende, datos biométricos), de todos los argentinos y se encuentran a la venta en foros de hacking (Cimpanu, 2001). Otra noticia reciente saca la luz a un grupo de cyber mercenarios, en foros *underground*, denominado RocketHack/Void Balaur, enfocados en ofrecer el servicio de exfiltrado de datos al mejor postor, incluyendo correos de Gmail/Protonmail, comunicaciones en Telegram, mensajes SMS, pasaportes, registros de llamadas de celular, datos de aerolíneas e información bancaria; que habrían afectado al menos a 3500 objetivos, incluyendo candidatos presidenciales bielorrusos, activistas de derechos humanos, periodistas, doctores, ministro de defensa de un país de Europa del este, un ex jefe de una agencia de inteligencia y funcionarios gubernamentales de diferentes países de Europa, entre otros (ver figura 206). Los vectores de ataques utilizados fueron *phishing*, *malware* (ej. Z*Stealer/ DroidWatcher) y se cree que además disponen de accesos directos a diferentes proveedores de servicios (Brewster, 2021; Hacquebord, 2021).

Todo esto nos lleva a comprender que la seguridad perfecta es una ilusión; un placebo que demuestra la ignorancia en la tecnología y las amenazas en el ciberespacio. Los profesionales se capacitan y entrenan arduamente para enfrentar los desafíos del ciberespacio; pero solo estarán preparados el día que puedan nadar como peces, volar como aves, correr como cheetah y ladrar como ranas.

No existe la seguridad perfecta y en el fondo la seguridad se basa en una correcta gestión de riesgos a partir de un inventario de activos a proteger. La evaluación de riesgos determina la probabilidad de ocurrencia de un suceso (amenaza x vulnerabilidad) y el impacto de esta. Donde la Amenaza es igual a la capacidad del atacante + Oportunidad + Intención de este. En base a los resultados de la evaluación, el riesgo se puede:

- Aceptar. Implica no tomar medidas. El riesgo encuadra dentro del apetito al riesgo que tiene el modelo de negocio/organización.
- Evitar. Se evita el negocio o específicamente dicha solución.

- Transferir. Implica contratar un seguro que se haga cargo del impacto económico.
- Mitigar. La acción de aplicar controles y medidas de protección. El costo del control y del riesgo residual (riesgo remanente a pesar del control - debido a que los controles nunca son perfectos) no debería ser superior al valor al activo que se está protegiendo.

La aplicación de una estrategia de ciberseguridad ayuda a disuadir/detectar/mitigar una amenaza, con el fin de alterar las circunstancias de capacidad y/o la oportunidad de los atacantes.

Figura 206

Países afectados por Rockethack.



Nota. Exfiltración de datos personales por cyber mercenarios y disponibles al mejor postor (Fuente imagen: Hacquebord, 2021).

Internet: la red de redes.

Para comprender donde estamos siempre es importante conocer un poco de historia. Durante 1958, Estados Unidos crea la agencia de investigación de proyectos avanzados (DARPA) dependiente del departamento de defensa (DOD) en respuesta al lanzamiento del primer satélite del mundo Sputnik I (URSS).

En 1960, RAND Corporation, plantea la idea de una red militar descentralizada con múltiples caminos entre dos puntos y la división de mensajes en fragmentos que seguirían

caminos distintos. Todo esto con la finalidad de tener una red resiliente a los ataques nucleares que pudieran destruir algunos nodos de la red.

En 1962 el canadiense McLuhan, adelantado a su tiempo, halaba de que la humanidad pasaría de la cultura de la impresión a la cultura electrónica, conformando una identidad colectiva denominada aldea global (McLuhan, 1962).

En 1963, el informativo Licklider discutía la idea de una red galáctica y es convocado para trabajar en DARPA junto a otros.

En 1965, Donald Davies del National Physical Laboratory (NPL) de Reino Unido, trabajaba en una red con fines comerciales. Len Kleinrock desarrolla el concepto de *Packet Switching*, donde el dato es dividido en paquetes para ser enviado por la red (similar al concepto de *Time Sharing* de compartir un medio limitado como ser un *mainframe* por varios integrantes).

DARPA desarrolla una red para la transferencia de conocimiento entre universidades denominada ARPANET en 1969. DARPA, RAND, MIT y NPL conforman los primeros nodos, entre otros.

Durante 1971, el Institut de Recherche en lnformatique et en Automatique (IRIA) de Francia comienza el desarrollo de la red de investigación llamada CYCLADES. Esta red utilizaba el concepto de *Packet Switching* y unía redes pequeñas a través de nodos llamados *Gateway*. Estos nodos solo transferían la información a nivel capa física sin necesidad de mayor intervención. Con relación a ello, el científico de la computación Pouzin acuña el termino *catenet* (red de redes o internet).

Durante 1973, Vint Cerf y Robert Kahn (inspirados en el trabajo de Pouzin), presentan el protocolo TCP/IP para Arpanet. Cert y Kahn son conocidos como los padres de Internet[210].

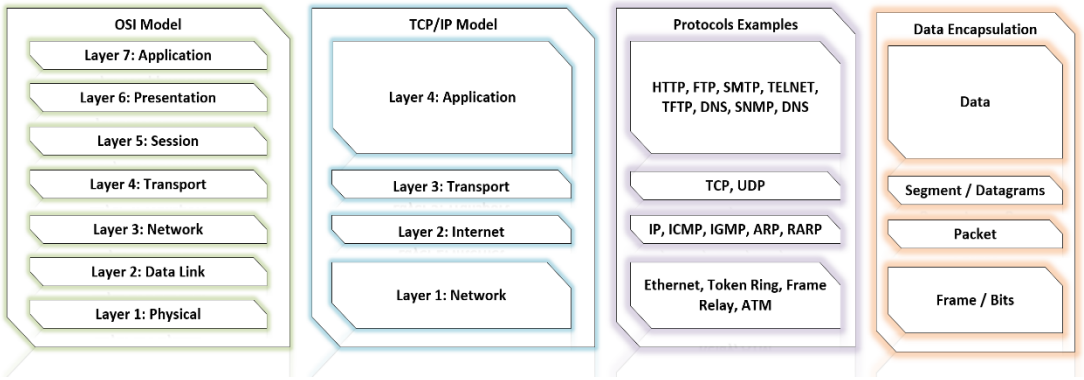
En 1980, la Organización Internacional de Normalización (ISO) crea el marco de referencia modelo OSI (ISO/IEC 7498-1) (ver figura 207). Luego en 1983 Paul Mockapetris plantea el Domain Name System (DNS) para resolución de nombres de dominio. En 1990 ARPANET es disuelta, pero la red continúa creciendo hasta la actualidad. En 1991, el

[210] El activista Aron Swatz (1986-2013), defensor de la cultura libre de internet, es posteriormente reconocido como el hijo de internet. Fue brutalmente perseguido judicialmente por el MIT y posteriormente por el FBI, lo que desencadenó su trágico suicidio (más adelante veremos la persecución judicial y el asesinato por intimidación como armas de la guerra invisible).

británico Berners-Lee crea el WWW (protocolo HTTP y el HTML) y es reconocido como *Knight Commander* (Sir Berners-Lee) en 2014.

Figura 207

Comparación entre el modelo de referencia OSI y el protocolo TCP/IP.



Nota. (Fuente imagen: elaboración propia).

De forma simplificada, el funcionamiento de internet es el siguiente: el *host* que envía información (*PC*, servidor, equipo) divide el dato en partes más pequeñas. En dichos fragmentos se adiciona diferentes encabezados para identificar el remitente, el destinatario, un orden para rearmar la información, verificación de integridad, entre otros (similar a lo que puede ser el sobre de una carta). Los routers son equipos que se encargan de llevar el paquete a destino a partir de la dirección IP (poseen tablas de enrutamiento y protocolos de comunican para actualizarlas). Cuando el dato llega al destinatario, es rearmado. El protocolo define la estructura de la comunicación en un mutuo acuerdo previo entre el emisor y el receptor (Ej. vamos a hablar en español y hay que levantar la mano antes de iniciar la conversación). En caso de utilizar un protocolo orientado a la conexión (TCP) el remitente puede solicitar la retransmisión de paquetes faltantes (extraviados o corruptos). Por lo tanto, es adecuado para la transmisión de archivos que no pueden quedar incompletos. En caso de una transmisión tipo *streamming* (flujo), la velocidad es prioritaria sobre la integridad de los datos. Se utiliza el protocolo UDP que es más pequeño y no tiene control de flujo. Es adecuado para una charla de voz, donde es más importante la comunicación fluida que la calidad del audio.

Una analogía sería enviar mercadería a través de camiones desde una provincia a otra. Algunos camiones pueden tomar diferentes caminos, llegar en diferentes horarios o inclusive podrían tener algún desperfecto en el camino. Si tienen seguro (TCP) se puede reclamar el

reenvío de la mercadería extraviada. De lo contrario, se perdería una parte (UDP). Si bien existen innumerables protocolos y tecnologías de comunicación sobre diferentes medios físicos, conceptualmente el funcionamiento general es el descripto.

Ataques a los sistemas de información

La siguiente no pretende ser una clasificación rigurosa de todos los ataques existentes, sino más bien, una aproximación para quien no está familiarizado en la temática a tratar. Cabe aclarar que algunos ataques pueden estar en más de una categoría o ser una combinación de ellas y la siguiente es meramente una clasificación didáctica.

Vulnerabilidades y exploits.

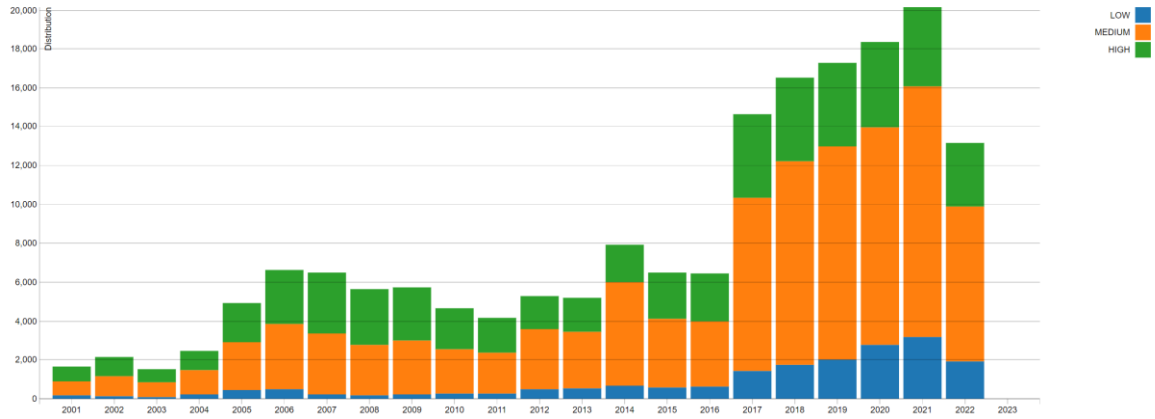
Según el NIST 800-30 revisión 1, una vulnerabilidad es una debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser aprovechada por una fuente de amenaza (NIST, 2012). Por definición podríamos encuadrar prácticamente todos los ataques en esta categoría, pero como ya se anticipó, separaremos algunos para facilitar la explicación de estos.

El Common Vulnerabilities and Exposures (CVE) es un sistema de referencia que identifica vulnerabilidades según un score de severidad. El mismo es mantenido por National Cybersecurity FFRDC (NCF) del NIST, operado por MITRE Corporation y financiado por el US National Cyber Security Division del US Department of Homeland Security. La National Vulnerability Database (NVD) registra las vulnerabilidades bajo el formato CVE-YEAR-ID y puede ser consultada por un atacante que haya realizado previamente inteligencia sobre un objetivo.

Tener presente que la cantidad de vulnerabilidades por producto refleja la calidad de desarrollo de software del vendedor, pero también hay que tener en cuenta que los productos más populares son los más investigados por su mayor interés, volumen de impacto, mejor paga por vulnerabilidad descubierta, mayor inversión, etcétera (ver figura 208 y 209).

Figura 208

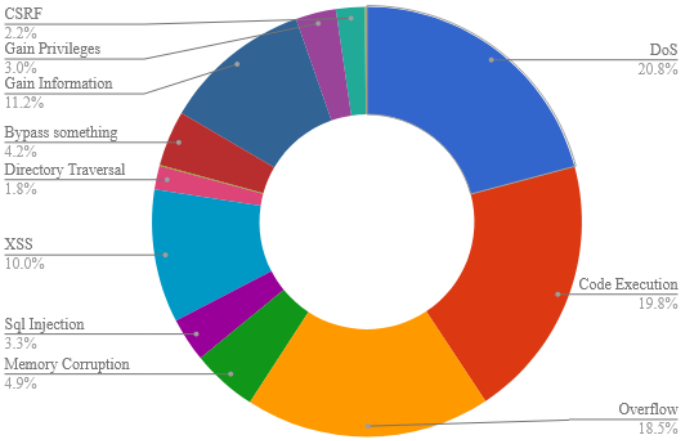
CVSS Severity Distribution over Time.



Nota. (fuente imagen: National Vulnerability Database, s.f.).

Figura 209

Gráfico de vulnerabilidades por tipo.



Nota. Datos de NVD durante 2017. (Fuente imagen: Techtalk GFI Software)

El Open Web Application Security Project (OWASP) es un proyecto abierto dedicado a la seguridad de aplicaciones web que también crea conciencia de los riesgos más importantes (OWASP TOP 10).

Cuando una vulnerabilidad es recién descubierta se denomina 0-Day (día cero). Aún no tiene solución dado que los desarrolladores recién la conocen. Por ello, pueden llegar a ser muy peligrosas y de alto interés. Diferentes actores, incluyendo estados naciones, compran vulnerabilidades 0-Day en mercados de la Deep Web o con empresas pantalla. La compra no tiene la finalidad de buscar una solución para una mejor sociedad, sino más bien incrementar su cyber arsenal y mantenerlas en secreto tanto tiempo como sea posible.

Cuando un atacante utiliza de forma deliberada una debilidad a su favor, se denomina *exploit*. En caso de utilizar vulnerabilidades recién descubiertas, estamos en presencia de u *0-Day Attack*.

En el momento que un estado nación detecta que otro estado tiene la misma capacidad de explotar una vulnerabilidad, deben sacrificar su herramienta y darla a conocer a fin de proteger su propia sociedad. Este es un delicado equilibro que deben mantener los servicios de inteligencia. Como remarca Buchanan (2020) preservar la vara de la seguridad lo suficientemente alta para que no puedan ingresar actores externos pero lo suficientemente baja para conservar el acceso ellos mismos.

Vulnerabilidades a nivel hardware.

El hardware también presenta vulnerabilidades y es propenso a ser explotado. A continuación, se mencionan algunos ejemplos de utilidad para los siguientes capítulos.

Si quisiéramos acceder desde un proceso a la memoria reservada (*address space*) del núcleo (*Kernel*) del Sistema Operativo (*OS*) o a la memoria de otro proceso, no podríamos. El mismo *OS* no lo permitiría ya que existe un aislamiento por razones obvias de seguridad

Spectre es una vulnerabilidad que afecta a los procesadores Intel y permite romper el aislamiento de memoria entre un proceso de usuario y el sistema Operativo. Por su parte, *Meltdown* es una vulnerabilidad que afecta a los procesadores Intel, AMD y ARM; y permite romper el aislamiento de memoria entre aplicaciones. La razón detrás de dichas vulnerabilidades es que las memorias caches incorporan un problema de seguridad conocido como *side-channel attack* del tipo *timming attack*, que junto con los algoritmos de ejecución especulativa del *CPU* (*speculative execution*), dieron lugar a *Spectre* y *Meltdown*

Debido a que el *CPU* es más rápida que las memorias, pasa gran parte del tiempo sin realizar operaciones y a la espera de los datos que debe operar. Por ello, se desarrolló la técnica de ejecución especulativa, en el cual el *CPU* asume una probabilidad de que cierto código pueda ejecutarse en los futuros ciclos.

Considere el siguiente ejemplo: Si (cierta condición es verdadera) {realizar X tareas}.

Antes que la CPU sepa el resultado de cierta condición (porque debe esperar los operadores de la memoria antes de verificarlos), ejecuta X tareas de forma anticipada. Si cierta condición finalmente resulta verdadera, entonces ya tiene disponible el resultado de X

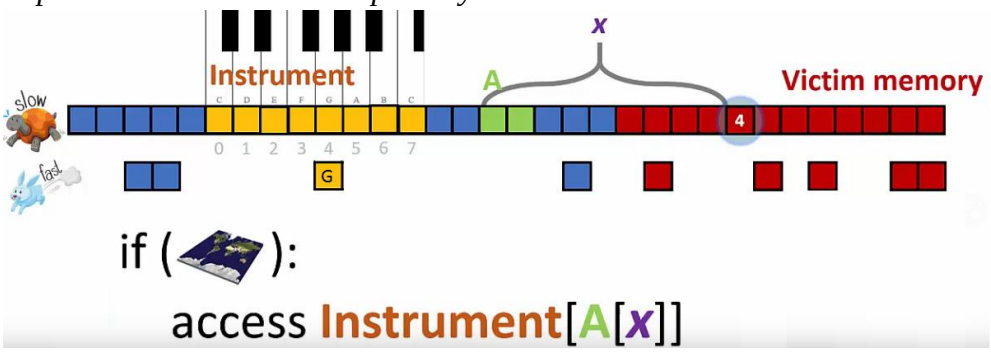
tareas en memoria cache. En caso de cierta condición resulte falsa, simplemente se descartan los resultados de X tareas como si nada hubiera sucedido. De esta forma, en promedio se logra un uso más efectivo del *CPU*. Este proceso es llamado *speculative execution*. El problema en dicha arquitectura es que la ejecución especulativa se realiza a nivel *CPU* previo a las validaciones de seguridad del *OS*. Además, en caso de descartar resultados, los mismos quedan disponibles en memoria cache y pueden ser accedidos mediante un ataque del tipo *Side Channel Attack*.

Para mayor detalle nos basaremos en una explicación del profesor Ymir (ver figura 210) de la universidad de Emory (2018): Si creamos un vector A y queremos acceder a una posición de memoria que excede el *Address Space* asignado para dicho proceso (llamemos A[X]), el Sistema Operativo arrojará un error (operación ilegal). Pero podemos acceder a dicha posición de forma especulativa para luego obtener el valor especulativo del cache mediante *timing attack*. Para ellos, creamos otro vector cuyo contenido conocemos y llamaremos Instrument. Además, nos aseguraremos de que Instrument no se almacene en cache (su acceso en memoria es lento). El resultado especulativo de A[X] traerá el valor que queremos acceder y no conocemos. En el ejemplo, el valor 4. Por lo tanto, Instrument [4] traerá el contenido de Instrument de la posición 4 (valor "G") de la memoria lenta a la memoria cache (rápida). Para finalizar el ataque se mide el tiempo de respuesta del acceso de cada posición de Instrument y podrá apreciarse una diferencia de tiempo significativa accediendo al valor G.

Repitiendo toda la operatoria para en diferentes posiciones X, nos permitirá acceder al contenido de la memoria que supuestamente no teníamos permitido.

Figura 210

Explotando vulnerabilidad Spectre y Meltdown.



Nota. (Fuente imagen: Ymir Vigfusson, 2018).

La vulnerabilidad mencionada fue posteriormente ampliada en otros ataques como ZombieLoad, RIDL[211] y Fallout[212] (Canella, Genkin, Giner, Gruss, Lipp, Minkin, Moghimi, Piessens, Schwarz, Sunar, Bulck, Yarom, 2019), (Schaik, Milburn, Österlund, Frigo, Maisuradze, Razavi, Bos, Giuffrida, 2019), (Schwarz, Lipp, Moghimi, Bulck, Stecklina, Prescher, Gruss, 2019). Pocos meses después, la firma Bitdefender encuentra una nueva vulnerabilidad de procesadores (*SWAPGS attack*) que permite acceder a la memoria del Kernel desde el modo usuario (sin privilegios elevados) mediante la ejecución especulativa de una instrucción SWAPGS[213] (Kumar, 2019).

Otra vulnerabilidad de interés que afecta a las memorias SDRAM[214] es *RowHammer*. Dichas memorias, en términos simplificados, almacenan bits mediante capacitores que deben energizarse con una frecuencia de refresco para que no pierdan su estado. Las celdas de datos conforman una matriz que a lo largo de los años han incrementado su densidad debido a los requerimientos de mayores capacidades. El acceso a la memoria se realiza de a filas (*rows*) y se ha demostrado que una gran cantidad de accesos simultáneos a una misma fila[215] durante una fracción de tiempo reducido tiene una probabilidad de afectar las filas aledañas, causando un *bit flip* (invierte el contenido de una celda de memoria) (ver figura 211). El nombre deriva a que proceso mencionado se asemeja a martillar (*hammer*) la fila accedida. Cambiar un bit de memoria podría parecer poca cosa, sin embargo, 1 bit puede ser la diferencia suficiente para un acceso privilegiado al sistema. En 2015, Project Zero de Google demostró una explotación de escalamiento de privilegios. En 2016, investigadores de VUSec Lab de la universidad de Vrije en Amsterdam presentan la variante Drammer[216] que permite ganar acceso root en smartphones Android (Der Veen, Fratantonio, Lindorfer, Gruss, Maurice, Vigna, Bos, Razavi, Giuffrida, 2016).

[211] Rogue In-Flight Data Load.
[212] CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2018-12130, CVE-2018-12126, CVE2018-12127, CVE-2019-11091.
[213] Instrucción del sistema con privilegios elevados. CVE-2019-1125.
[214] Dynamic Random Access Memory.
[215] Además del acceso a la fila, se realiza un flush del cache. Garantizando el acceso a la fila física en vez de la memoria cache.
[216] CVE-2016-6728.

Figura 211
Ejemplo en assembler de RowHammer.

```
1 codela:
2   mov (X), %eax
3   mov (Y), %ebx
4   clflush (X)
5   clflush (Y)
6   mfence
7   jmp codela
```

Nota. (Fuente imagen: Kim, et al, 2015).

Basados en los mismos principios, investigadores demostraron el ataque RAMBleed[217] donde extrajeron una clave RSA-2048 en OpenSSH 7.9 (Kwong, Genkin, Gruss, Yarom, 2020).

Un ataque de interés a mencionar son los *Fault injection attack*. Los fabricantes de chip diseñan sus productos para trabajar en ciertas condiciones de entorno (temperatura, rango de voltaje, frecuencia de reloj, entre otros). *Fault injection attack* es un ataque físico sobre un dispositivo que consiste en inyectar una falla deliberada a fin de modificar el comportamiento esperado del sistema. Estos ataques permiten un bypass de mecanismos de seguridad, cambios de comportamiento con intenciones maliciosas, extracción de llaves de cifrado, extracción de firmware para análisis de vulnerabilidades/búsqueda de *hardcoded passwords*, entre otros. Las técnicas usuales para producir estas fallas de hardware son la adulteración del voltaje (*voltage glitching*), la frecuencia del reloj (*clock glitching*), interferencia con láser (*laser injection*), campos electromagnéticos (*electromagnetic injection*), entre otros (Jha, 2020). Investigadores de la Universidad Técnica de Berlín y el Instituto Fraunhofer demostraron un ataque *voltage glitching* de sobre los procesadores AMD EPYC que vulnera la seguridad del cifrado de las máquinas virtuales. La inyección introduce una falla en el ROM Bootloader del Secure Procesor permitiendo un acceso total y acceso a las claves de cifrado (Buhren, Jacob, Thilo y Seifert, 2021).

Vulnerabilidades a nivel Sistema Operativo.

Tal como indica Tanenbaun (1993) existen 2 clases de software: los programas de aplicación que se enfocan en solucionar los problemas de los usuarios y los programas de

[217] CVE-2019-0174.

sistema que controlan el hardware del computador. El programa fundamental de los programas de sistemas es el Sistema Operativo; encargado de controlar los recursos del computador de presentar un nivel de abstracción o "máquina virtual" para los programadores/usuarios (ver figura 212).

Figura 212

Esquema sistema de cómputo.



Nota. Conformado por hardware, programas de sistema y de aplicación (Fuente imagen: Tanenbaum, 1993).

El Sistema Operativo es un software al igual las aplicaciones y por lo tanto también resulta propenso a desperfectos y vulnerabilidades. La diferencia radica en que la afectación/impacto en la explotación de una vulnerabilidad a nivel sistema, posiblemente sea mayor que a nivel aplicación. Según las circunstancias, la misma podría lograr privilegios elevados y un control total sobre el computador.

Un ejemplo reciente descubierto es la vulnerabilidad PwnKit (CVE-2021-4034) que afecta a todos los sistemas Linux. Permite elevación de privilegios Root con tan solo ejecutar un *exploit*. Se trata de una falla en la programación del componente Polkit, donde una función que espera argumentos nunca valida que estos puedan ser nulos. Al forzar dicha situación, el programa realiza un comportamiento no esperado, produciendo una lectura y una escritura *out-of-bounds*. Dado que la memoria sucesiva fuera de limite pertenece a la variable *environment*, dicho comportamiento es astutamente aprovechado por el atacante para introducir de forma insegura una *environment variable* que sumado a unos trucos adicionales termina ejecutando un binario en modo root (Goji, 2022; Wechsler, 2022).

Lo interesante a remarcar es que dicha vulnerabilidad lleva expuesta 12 años en todos los sistemas Linux del mundo. La pregunta de rigor es ¿pudo algún individuo/estado-nación

conocer y aprovechar dicha vulnerabilidad de forma secreta durante este tiempo? Responder específicamente esta pregunta no es de interés del presente trabajo sino más bien orientar al lector en un pensamiento crítico sobre la seguridad de las TIC y el futuro de la sociedad en relación con dicha temática.

Vulnerabilidades a nivel usuario (Social Engineering).

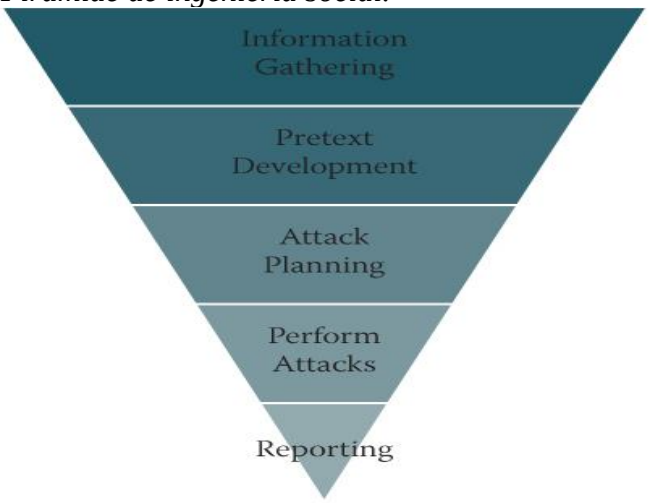
El 90% de los incidentes corresponden a vulnerabilidades humanas (Harris, 2019). Como nos ilustra Hadnagy:

> La ingeniería social es el acto de influenciar una persona a tomar una acción que puede o no ser de su mejor interés…. Un atacante malicioso puede usar disparadores emocionales, principios psicológicos y aplicar el arte/ciencia de la ingeniería social…La oxitocina es liberada en la sangre cuando sentimos que alguien confía en nosotros… la dopamina es un neurotransmisor producido por el cerebro en momentos de placer y felicidad. Mezclando la oxitocina y la dopamina se obtiene un cocktail de ingeniería social que puede abrir cualquier puerta que desees… cuando se disparan las emociones se piensa menos racionalmente y se responde rápidamente basado en dichas emociones, logrando una mayor tasa de éxito (Hadnagy, 2018, p. 5-9).

En la figura 213 puede apreciarse las fases de un ataque de ingeniería social que, como veremos más adelante, se asemeja mucho al *kill chain.* En la figura 214 se observa el sistema DISC (Direct, Influencing, Supporter, Concientious) que refleja los diferentes estilos de comunicación según cada persona. Adecuar al sujeto objetivo (receptor) en dicho sistema, permite al atacante (emisor) definir un estilo de comunicación más efectivo. Otro factor influyente en el éxito de una operación de ingeniería social es el entendimiento y adecuación de la cultura de la tribu de interés: vestimenta, forma de hablar, comportamiento esperable, etcétera. Por lo cual es nuevamente importante la inteligencia previa.

Figura 213

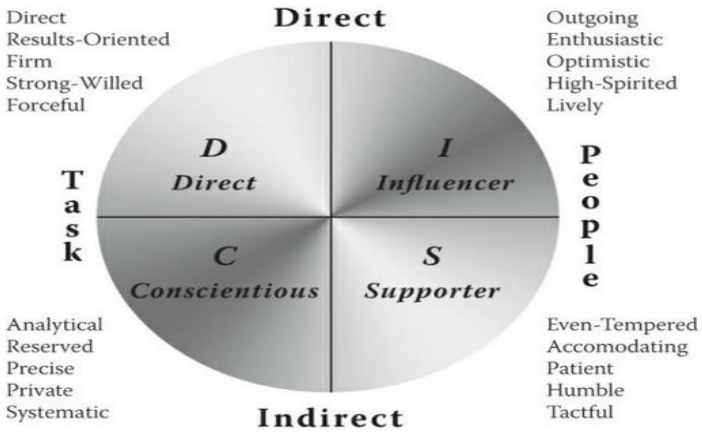
Pirámide de ingeniería social.



Nota. Desde la inteligencia hasta la planificación es donde toma más tiempo. Llevar a cabo el ataque es la resolución de lo plani*ficado (Fuente imagen: Hadnagy, 2018).*

Figura 214

DISC System (Marston, 1931).



Nota. Los cuadrantes marcan los diferentes estilos de comunicación *(Fuente imagen: Hadnagy, 2018).*

El objetivo de la ingeniería social es lograr que la víctima realice una acción mediante el engaño y la manipulación. Por ello, es importante el pretexto en la comunicación. Ej. personificar un técnico reparador de aire acondicionado y convencer al guardia de seguridad que permita el acceso físico a un centro de cómputos para luego efectuar otro tipo de ataques.

Según Kevin Mitnick, existen 3 métodos de engaño:

- Cuando el atacante va en contra de su interés para ganar la confianza (ej. indicar: "escribe tu contraseña, pero no me la digas porque no debes decírsela a nadie").

• Cuando el atacante advierta a la víctima de algo que el mismo atacante ha provocado, generando una mayor credibilidad en el ataque (ej. provocar que la víctima pierda conexión y decirle: “su red podría fallar”)

• Cuando el atacante ayuda a la víctima a resolver un problema, ganando su confianza y agradecimiento (ej. resolver el problema de conexión).

El atacante manipula a la víctima para que adopte un rol al cual luego le resulta difícil/incomodo de cambiar (ej. cuando la víctima asume una postura de ayudar, la misma se siente bien/útil y luego es difícil que se niegue a futuras peticiones). El atacante también busca ganar la simpatía con temas afines o gustos en común (aquí la inteligencia previa es útil) o inclusive realizar halagos/cumplidos. Otra alternativa es explotar el miedo a que algo malo está próximo a suceder, pero que puede evitarse si se siguen las indicaciones del atacante. Según los psicólogos hay 2 formas de pensamiento: sistémico o heurístico. Sistémico es cuando se piensa detenidamente de forma racional a fin de tomar una decisión, mientras que el pensamiento heurístico busca atajos para resolver rápidamente un problema (ej. Entregar información en función de quien afirma ser el solicitante en vez de analizar la clasificación de la información). El atacante aprovecha esta vulnerabilidad, generando presión y apuro sobre la víctima, para forzar que su pensamiento pase al modo heurístico, el cual es menos propenso a cuestionamientos/objeciones (ej. llamar 5 minutos antes de finalizar la jornada laboral) (Mitnick y Simon, 2001).

A continuación, mencionamos algunas vulnerabilidades vinculantes a la temática.

Vishing

Durante la pandemia del COVID se incrementó el cibercrimen. Un ataque con relación a la temática es el *Vishing* (voice + phishing) o engaño telefónico. Los atacantes crean cuentas falsas de bancos en Instagram y observan a la gente que empieza a seguir a los bancos reales. En ese momento aprovechan para contactar al cliente o que el cliente se contacte con ellos (*reverse vishing*). Una vez que entablan la conversación telefónicamente con el cliente, mediante técnicas de ingeniería social buscan blanquear el usuario de home banking y generar un token nuevo en el cajero para tomar el control de la cuenta del cliente.

En otro ataque similar, llaman a la víctima haciéndose pasar un empleado del gobierno, con el pretexto de la segunda dosis de la vacuna contra el COVID. Le indican que le enviaran

un código por WhatsApp y que debe indicar el mismo para confirmar el turno. Lo que realmente sucede cuando la víctima les pasa este código a los atacantes, es que logran el control total de WhatsApp. Una vez que logran la identidad robada, empiezan a pedir dinero a todos los contactos, alegando un problema grave y que necesita ayuda.

Phishing

Término utilizado específicamente para el engaño a través del correo electrónico. El envío de mail maliciosos que pretenden simular proceder de una fuente segura/confiable o simplemente buscan engañar al destinatario. Es como salir a pescar con una red y ver que sale. Habitualmente estos correos se envían de forma masiva por script a una lista de destinatario y tienen adjunto un *payload* (*malware*/*exploit*), un link de un sitio falso para robar credenciales (ej. homebanking), una amenaza de extorsión exigiendo el pago de dinero para evitar que expongan fotos/videos de la víctima en situaciones incomodas (que en realidad no poseen), el famoso cuento del tío o simplemente buscan obtener información de la víctima para un futuro ataque. Ej. Se distinguen fácilmente cuando solicitan cambiar la clave de un banco en el cual no utilizamos.

Spear Phishing

Término utilizado para un mail personalizado donde el atacante tiene información previa de la víctima y esto potencia su capacidad de éxito y poder de fuego (es como pescar con una lanza). Finalmente, el *Whalling* es similar, pero está dirigido a miembros de alto rango en una organización (es ir de pesca por una gran ballena).

Baiting

Consiste en infectar con un *malware* a un dispositivo como un pendrive y dejarlo tirado en una zona común (estacionamientos, escaleras, ascensores, etc.) a la espera que una víctima curiosa. En 2008 un servicio de inteligencia (presumiblemente ruso) colocó un pendrive infectado el estacionamiento de una base del *United States Department of Defense* (*DoD*) en medio oriente. Un empleado encontró el mismo y lo insertó en una notebook conectada con el *United States Central Command* (*USCENTCOM*), propagando así el *malware* Agent.btz por toda la red interna. El pentágono tardó 14 meses en poder remover

el gusano en la denominada operación Buckshot Yankee. Dicho acontecimiento propicio la creación del *United States Cyber Command* (*USCYBERCOM*) (Lynn, 2010).

Con relación a la temática. A continuación, puede observar dos herramientas de pentest (ver figura 215 y 216).

Figura 215
USB Rubber Ducky.



Nota. Pendrive que en realidad inyecta presiones de teclas a gran velocidad como si fuera un teclado (Fuente imagen: hak5, s.f.).

Figura 216
Bash Bunny II.



Nota. Plataforma de ataque automática USB con múltiples *payloads*. Incluye bluetooth trigger remoto (Fuente imagen: hak5, s.f.).

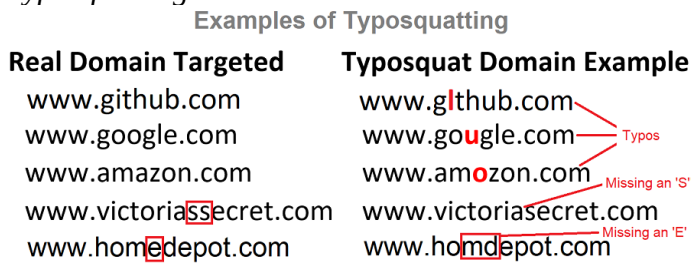
Typosquatting

El *Typosquatting* (homográfico) es una técnica que en ocasiones se utilizan en los ataques de *phishing*. Consiste en registrar un dominio que a simple vista parece ser el original, pero en realidad no lo es y se encuentra bajo el control del atacante (ver figura 217). Los atacantes inclusive pueden llegar a pagar anuncios en buscadores para que su sitio falso figure en los primeros resultados (técnica llamada *Black Hat SEO*[218]).

Eso fue lo que le ocurrió a la municipalidad de 25 de mayo en 2016 cuando el contador del municipio ingresó a un sitio falso del Banco Provincia desde Google. El sitio falso capturaba las credenciales y redireccionaba al sitio original para no llamar la atención (ver figura 218). El atacante hurtó 3.5 millones de pesos (Davidovsky, 2017).

Figura 217

Typosquatting attack.



Nota. (Fuente imagen: Stickley, Davis, 2019)

Figura 218

Ataque typosquatting sumado a un black hat SEO.



Nota. El sitio falso cambio una O por una S además de posicionarlo primero en las búsquedas de Google. Captura de pantalla que figura en el expediente judicial (Fuente: Davidovsky, 2017)

[218] Search Engine Optimisation

Comunicación no verbal

En lo que es un ataque de ingeniería social cara a cara, resulta fundamental comprender la comunicación no verbal. Esta herramienta, además de detectar mentiras, es utilizado para detectar emociones y adecuar la comunicación/pretexto a mejores resultados. En relación con el tema, Rulicki nos remarca:

> Darwin realizo una investigación en la que reunió datos provenientes de diferentes culturas, y también estudio a los bebes, pues entendió que en ellos la expresión de las emociones no estaba sujeta a los condicionamientos culturales. Sus hallazgos brindaron apoyo para su idea de que la expresión de ciertas emociones tenía una base hereditaria y era universal…. El Dr. Paul Ekman y sus colaboradores han investigado los significados emocionales de las expresiones faciales…se han determinado que las emociones básicas son siete: sorpresa, alegría, tristeza, amor, ira, disgusto y desprecio. Estas emociones se distinguen entre sí por cambios fisiológicos específicos, y por sus expresiones faciales prototípicas, asociadas a un mecanismo de desencadenamiento, automático e involuntario…. Dr. Ekman explica el fenómeno llamado emocionalidad secundaria, que consiste en sentir una determinada emoción por haber sentido otra previamente... Las emociones secundarias son indicadores privilegiados del perfil psicológico de un sujeto. (Rulicki, 2013, P 63 y 68).

Un abordaje más profundo en dicha temática excede el presente trabajo. Sin embargo, es importante mencionar su concepto y resaltar que los ataques no se limitan a cuestiones netamente técnicas de las TIC's. El factor humano y psicológico es relevante.

Vulnerabilidades a nivel comunicaciones.

DNS hijacking.

DNS hijacking o *poisoning* es un ataque que puede tomar diferentes formas (realizarse sobre el servidor DNS[219] o sobre la victima). El resultado final es el mismo. El atacante termina redirigiendo el tráfico de un dominio a una IP bajo su control para luego realizar diferentes ataques como ser captura de credenciales o instalación de *malware* entre otros.

Sniffing.

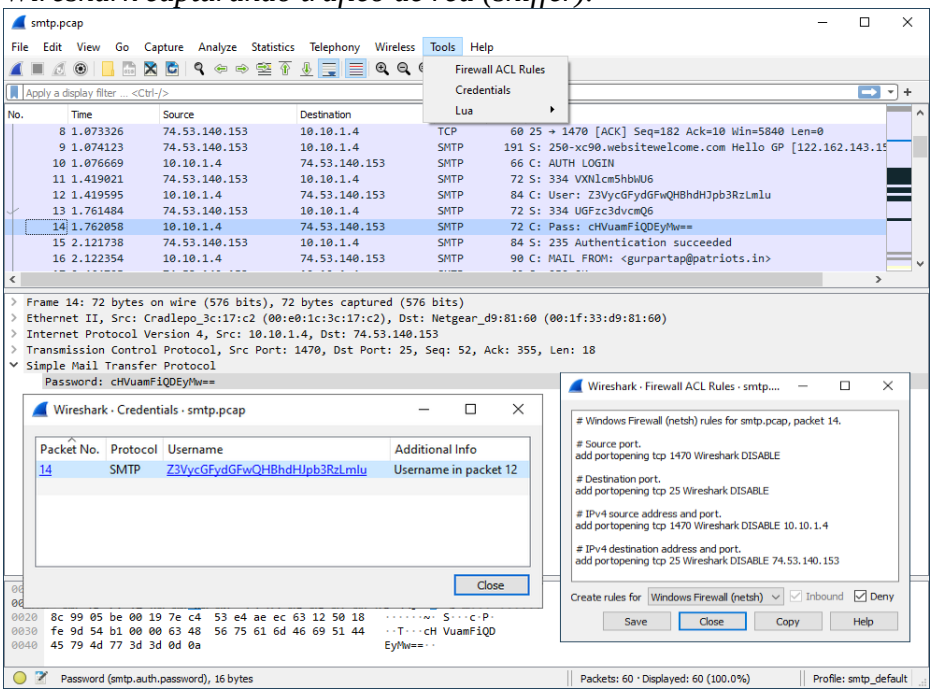
Sniffing (también llamado *eavesdropping*) es cuando un atacante escucha las comunicaciones afectando la confidencialidad de los datos in transit o in use.

[219]Domain Name System traduce los nombres de los dominios en direcciones de internet (IP).

Un ejemplo práctico es un analizador de trafico de red que consiste en colocar la placa de red en modo promiscuo y utilizar un software como Wireshark para ver todos los paquetes que pasan por la red. En una red segmentada se puede realizar un ataque previo para engañar al switch, por ejemplo, *VLAN Hopping*). Si los datos viajan sin cifrado (texto claro) es posible capturarlos, escuchar conversaciones VOIP u obtener credenciales de autenticación, entre otras (ver figura 219). Otra opción es utilizar un dispositivo para escuchar el tráfico en un cable, como ser un Lan tap (ver figura 220).

Figura 219

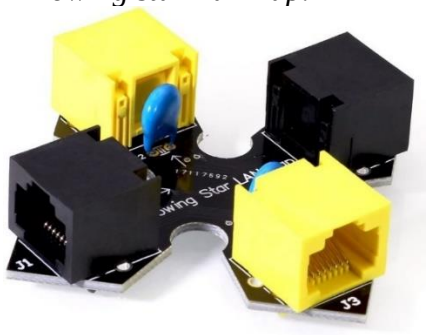
Wireshark capturando tráfico de red (sniffer).



Nota. En el mismo se puede apreciar la captura de una contraseña (Fuente: wireshark.org)

Figura 220

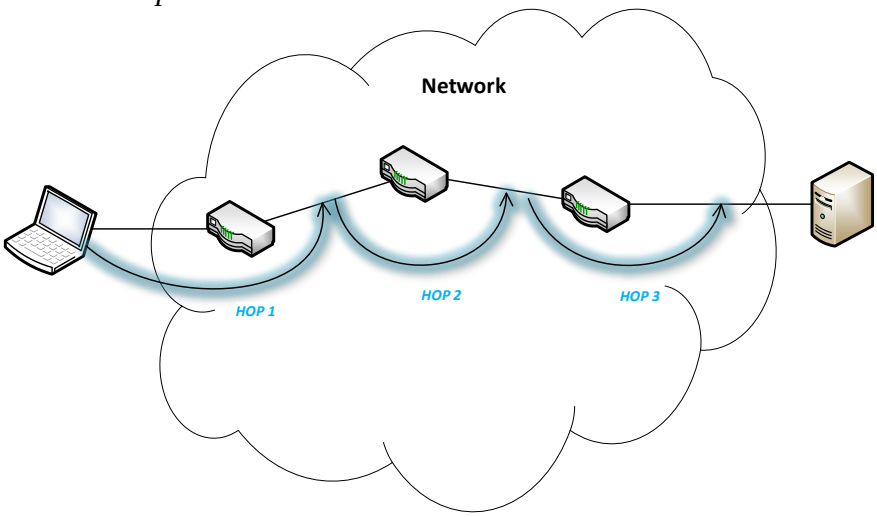
Throwing star Lan Tap.



Nota. Dispositivo para escucha del tráfico en un cable UTP (fuente imagen: Amazon, s.f.).

La naturaleza de la arquitectura de internet implica que el tráfico de datos debe pasa por diferentes equipos de red (*hop*) entre el origen y el destino (ver figura 221). Algunos proveedores de internet (*ISP*[220]) o gobiernos tienen analizadores de red, muchas veces bajo el pretexto de protección del ciudadano, lo que es un delito acorde a las leyes vigentes en nuestro país. Más adelante profundizaremos en dicho aspecto. Nota: el presente apartado le dedicaremos una mayor atención debido a su vinculación con la fase de *intel gathering (inteligencia)* del *Kill Chain* que estudiaremos en el siguiente capítulo.

Figura 221
Network Hops.



Nota. Para comunicarse, los datos deben pasar por los equipos de red intermediarios que podrían estar analizando el tráfico de red (Fuente imagen: elaboración propia).

Man in the middle (MITM).

Es cuando el atacante se coloca en el medio de la comunicación del objetivo. El atacante en tal condición puede no solo escuchar (*sniffing*), si no también modificar/adulterar los datos (*Tampering*) afectando tanto la confidencialidad como integridad. A continuación, algunos ejemplos.

El ataque *evil twin* consiste en montar un Access Point (AP) de WIFI falso que simula ser legítimo y forzar una desconexión del usuario con el AP legítimo, a la espera de que este se conecte al AP del atacante. Otra variante podría ser montar un WIFI de acceso público a la espera de que la víctima se conecte. Direccionar a sitios web del atacante permite robar

[220] Internet Service Provider

credenciales, explotar vulnerabilidades, instalar malware, etc. El ataque es sencillo de realizar con Kali[221] Linux o un Pineapple (ver figura 222).

Figura 222

Pineapple de Hack5.



Nota. Herramienta Red Team[222] de pentesting (Fuente Image: Hack5, s.f.)

Vulnerabilidades en la cadena de suministro

Drive by download / Watering hole attacks.

El ataque W*atering Hole* hace referencia a los depredadores que esperan a sus víctimas cuando van a tomar agua al estanque. En este caso, el atacante infecta un sitio web al cual es habitual la persona/grupo/organización objetivo. El termino habitualmente se utiliza como sinónimo de *Drive by Download* porque usualmente la persona no tiene más que visitar un sitio para que alguna vulnerabilidad instale algún tipo de *malware*.

En el caso de un *Supply Chain Attack* (ataque sobre la cadena de suministro) es un término un poco más amplio. En vez de atacar directamente al objetivo se intenta afectar a un proveedor de servicio o producto que menores medidas de seguridad. Es por eso por lo que algunas normas de seguridad apuntan a exigir ciertos estándares de seguridad a los proveedores. Como veremos posteriormente en algunos antecedentes de ataques, el

[221] Es una distribución de Linux dedicada al pentesting.
[222] Se denomina Red Team al equipo de personas que realizan un pentesting ofensivo, mientras que el Blue Team es el defensivo.

problema de la cadena de suministro conlleva riesgos altos y no fáciles de resolver, ya que nuestra seguridad en parte depende de la seguridad de un tercero.

Dentro del concepto de cadena de suministro podríamos incluir el denominado *Shadow code* que consiste en la utilización de código no verificado que podría contener vulnerabilidades o código malicioso. Tanto desarrolladores como profesionales usualmente utilizan código o herramientas de repositorios como Github sin verificar y esto implica un riesgo. Según Sharma (2021) investigadores descubrieron que un atacante infiltro paquetes en el repositorio PyPI de Python y que quienes lo instalaban descargaban un *malware* del tipo cryptominer.

Vulnerabilidades en la disponibilidad

Denial of service (DOS) attacks.

La denegación de servicio es un ataque que compromete la disponibilidad de un activo y es un concepto que puede abarcar diversas formas. Un ejemplo es el antiguo *ping of death* que malformaba un paquete ICMP[223] con un tamaño superior al esperado por el sistema operativo, produciendo que el mismo se congelara (*freeze*) debido a esta vulnerabilidad. Otro ejemplo similar es el *Teardrops/Fragmentation attack* que aprovechaba un bug de la implementación TCP/IP en algunos OS antiguos, al fragmentar deliberadamente paquetes que se superponían, causaba la inestabilidad de algunos sistemas.

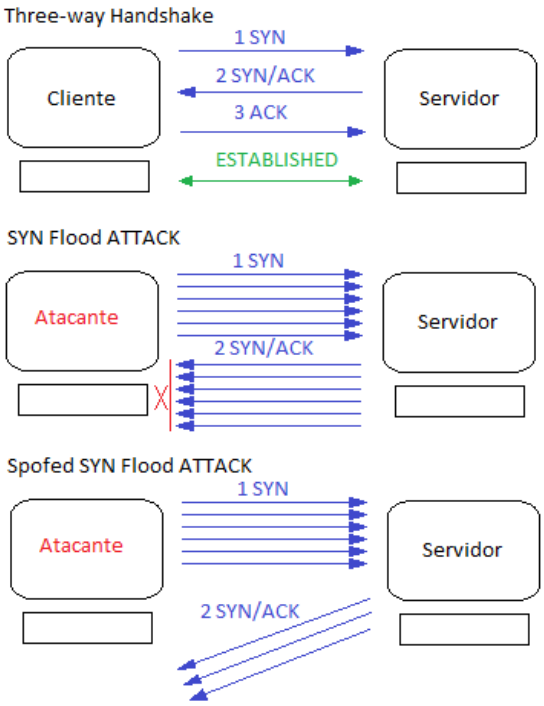
El Flood SYN es un ataque antiguo que hace abuso del handshake de 3 vías del protocolo TCP/IP (como se establecen las comunicaciones). Básicamente un acatante envía solicitudes de comunicación que nunca termina de establecer, llenando y desbordando el buffer de memoria del servidor. El atacante también puede hacer un *spoof* (falsificación) de la dirección de IP de origen para intentar ocultarse y/o que las respuestas a las peticiones realizadas se envíen reflejadas (*reflected*) a un tercero (ver figura 223). Cuando la respuesta a la víctima es superior a la petición del atacante se dice que hay una amplificación, dado de que con menor ancho de banda puede producir un ataque amplificado (ver figura 224).

Comúnmente también se utilizan ataques DOS con el protocolo UDP que no requiere del handshake de TCP.

[223] Es un tipo de protocolo de red.

Figura 223

Comparación entre el establecimiento de una conexión de 3 vías vs ataque SYN Flood.



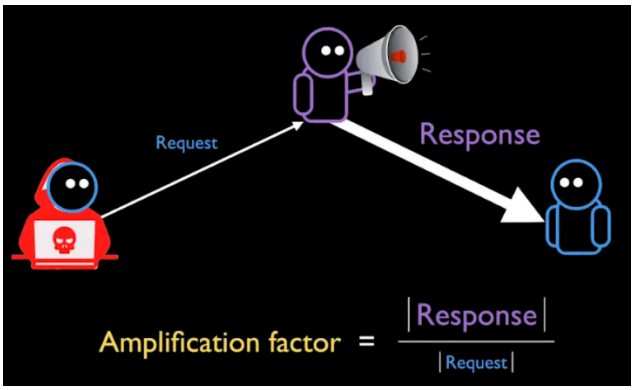
Nota. (Fuente imagen: elaboración propia).

En ataques del tipo *TCP reflected* solo podía aprovecharse la primera fase del 3 ways handshake dado que el atacante no podía conocer la secuencia generada por el servidor para completar el ACK (ver figura 225). Una reciente investigación demostró que no solo se puede aprovechar la segunda parte de la comunicación TCP abusando de *middleboxes* (como ser firewall, analizadores de contenido, etc.) (ver figura 226) sino que también es posible amplificar los ataques a de forma infinita explotando fallas en el diseño en los *middleboxes* o cuando los mismos se encuentran en loops[224] de enrutamientos. Con falla de diseños nos referimos a que cuando la víctima responde un RST (dado que desconoce que le están enviando) algunos middleboxes vuelven nuevamente a enviar la respuesta, quedando así en loops infinitos denominados *victim sustained deflection* (ver figura 227) (Bock, Alaraj, Fax, Hurley, Wustrow y Levin, 2021).

[224] Los routing loops suceden por una configuración inadecuada en los routers o por una falla en actualización de la tabla de enrutamiento. Ej. cuando un router no conocen como llegar a la red destino envía el paquete a otro router (ruta defecto) esperando que conozca la red. Si este, o un tercero, devuelven el paquete al primer router quedan en un loop hasta tanto se agote el TTL.

Figura 224

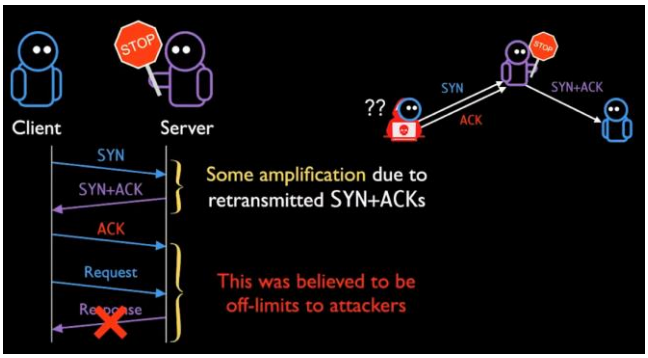
Amplification attack.



Nota. (Fuente imagen: Bock et al., 2021).

Figura 225

Reflected amplification attack.



Nota. (Fuente imagen: Bock et al., 2021).

Figura 226

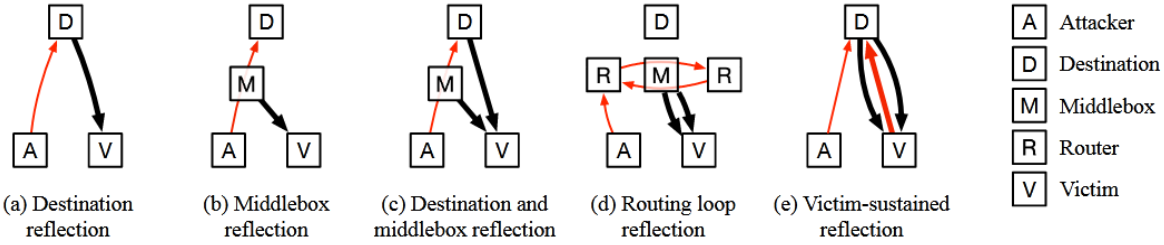
Weaponizing middleboxes.



Nota. (Fuente imagen: Bock et al., 2021)

Figura 227

Tipos de ataques investigados.



Nota. (Fuente imagen: Bock et al., 2021).

Distributed denial of service (DDOS) attacks.

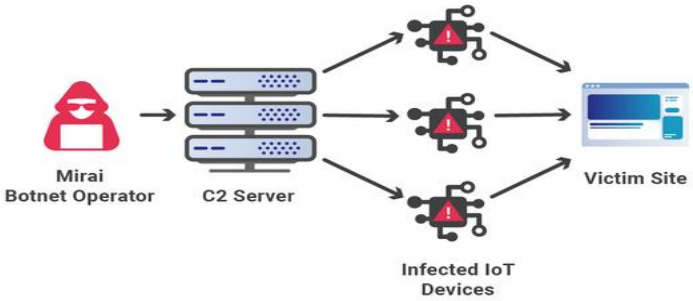
Un tipo especial de *DOS* de importancia es el *DDOS* (*distributed denial of service*). El mismo consiste en enviar una enorme cantidad de peticiones a fin de saturar (*flood*) la red o sistema objetivo. Para dicho ataque, previamente suele infectarse una gran cantidad de maquinar (*zombies*) que luego son controladas desde un C2C (*Command and Control*) con el objetivo de llevar el ataque en cuestión. Un ejemplo es el *malware* MIRAI que escaneaba dispositivos IOT (cámaras *IP*, *routers*) y los infectaba accediendo con el protocolo telnet y las credenciales por defecto, creando una gran *botnet.* Durante 2016 el *malware* MIRAI atacó, entre otros, al sitio web del periodista Brian Krebs y al *DNS provider* de Dyn. Recientemente Cloudflare reportó el ataque DDOS más grande hasta el momento (ver figura 228 y 229) de 17.2M de *RPS* (solicitudes HTTP por segundo) (Yoachimik, 2021).

Como medidas generales sobre la seguridad siempre es importante reforzar la seguridad física, tener sistemas redundantes de alta disponibilidad (*HA*), sitios de respaldo, contar con un BCP[225](*Business Continuity Plan*) y un DRP[226] *(Disaster Recovery Plan*), entre otros. Una contramedida habitual mencionada contra la denegación de servicio son las CDN[227] (*Content Distributed Network*).

[225] Plan de continuidad de negocio que define las acciones a tomar en caso de afectación a las operaciones.
[226] Plan que define las acciones necesarias para recuperar el centro de cómputos de un incidente.
[227] Redes donde los datos en vez de estar centralizados se encuentran distribuidos geográficamente en diferentes servidores.

Figura 228

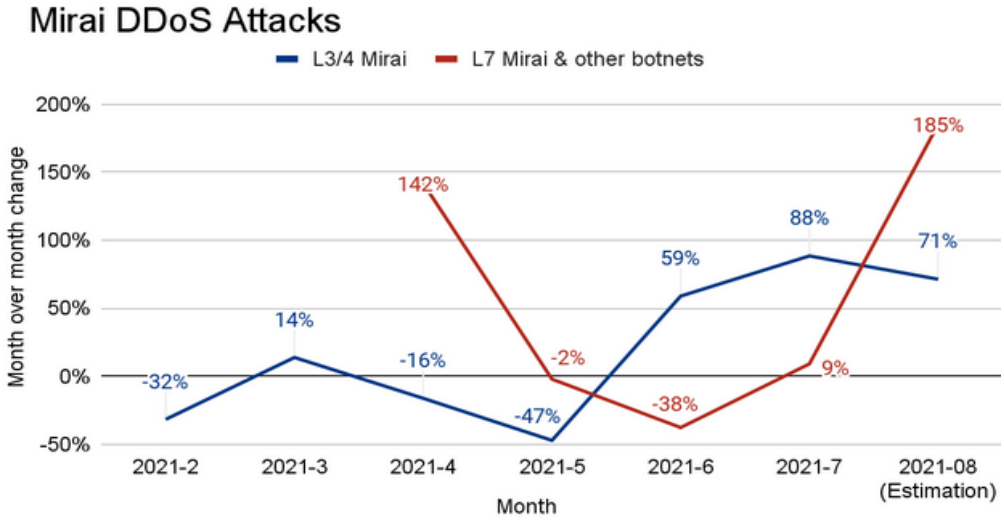
Ilustrativo de la arquitectura MIRAI.



Nota. (Fuente imagen: Yoachimik, 2021).

Figura 229

Grafica temporal de los ataques DDOS del tipo MIRAI.



Nota. (Fuente imagen: Yoachimik, 2021).

Jammers

Otro tipo de denegación de servicio es la técnica de guerra electrónica denomina *Jamming*, habitualmente utilizada para denegar los sistemas de comunicaciones. La misma consiste en saturar el espectro electromagnético dentro de un rango de frecuencias objetivos, denegando la utilización de dicho canal como medio de comunicación. Algunos ejemplos son inhabilitar una red de WIFI, interrumpir celulares durante un asalto o bloquear el cierre automático a distancia de un automóvil para ingresar al mismo/guardar el token para uso futuro (ver figura 230 y 231).

Figura 230

Jammer de comunicaciones portatil.



Nota. (Fuente imagen: jammer-shop.com)

Figura 231

Russian Krasukha-4.



Nota. Jammer de comunicaciones, low orbit satellites, drones y misiles (Fuente imagen: Clark, 2022)

Sabotaje

La seguridad física también tiene implicancias en la disponibilidad de un servicio (denegación de servicio). Algunos ejemplos son: robo de equipamiento, sabotaje del

suministro eléctrico, daño de un troncal de internet[228], implantación de un *kill switch* como el USBKill (ver figura 232), destrucción de equipamiento, etc.

Figura 232

USBKill.



Nota. Dispositivo USB remoto que deshabilita el hardware mediante una descarga eléctrica (Fuente imagen: USB Kill, s.f.)

Vulnerabilidades a nivel aplicación.

Como todo software, las aplicaciones presentan vulnerabilidades, en especial cuando los desarrollos se enfocan únicamente en la funcionalidad y dejan de lado la seguridad. Algunos aspectos que pueden atentar contra la seguridad son: no integrar al desarrollo al equipo de seguridad desde un comienzo, foco en reducir costos, cumplir con tiempos de lanzamiento, no realizar pruebas DAST/SAST[229], etc. Aun así, los mejores desarrollos son indefectiblemente propensos a presentar algún tipo de vulnerabilidad.

Como ejemplo de vulnerabilidad reciente tenemos el CVE-2022-29072 de 7-Zip que permite escalar privilegios debido a un desbordamiento de pila en la biblioteca 7z-dll dentro de la sección de ayuda del programa. La explotación de dicha vulnerabilidad permite la ejecución de una consola de comando a modo administrador (Kağan Çapar, 2022).

[228] Ejemplo los cables de fibra óptica en las Toninas que conectan a Argentina.
[229] Dynamic Application Security Test / Static Application Security Test

A continuación, se mencionan algunas vulnerabilidades sobre aplicaciones, no siendo estas las únicas.

Race condition/ TOCTOU attacks

Estos términos suelen utilizarse como sinónimos, aunque en realidad no son exactamente lo mismo.

Cuando el atacante logra manipular algo en el momento justo entre la ejecución de una tarea de verificación (TOC) y una de uso (TOU), puede obtener un resultado diferente al esperado. Este tipo de ataque se denomina TOCTOU[230]. Imagine un programa que verifica si el usuario puede leer un archivo contenido en un tipo de link antes de realizar la lectura. Si el atacante logra modificar la dirección del archivo en el momento justo, podría leer otro al cual no tiene acceso como por ejemplo password.

Cuando 2 o más procesos acceden a un recurso compartido sin un control de bloqueo y un atacante logra modificar el orden de ejecución esperado, el resultado podría resultar diferente. Esto se llama Race Condition. Imagine tener $200 en una cuenta bancaria, extraer $200 en un ATM y al mismo tiempo transferir los mismos $200 utilizando el homebaking en el smartphone. Si el sistema no estuviera correctamente diseñado, podría darse la situación que ambos procesos lean simultáneamente la disponibilidad de $200 y termines descontando los mismos, quedando finalmente la cuenta en $-200.

Algo similar demostró Homakov en 2015 al transferir el balance de una gift card de Starbucks a otra, utilizando 2 transacciones paralelas y simultáneas. Para el mismo utilizó el request “POST /step1?amount=1&from=wallet1&to=wallet2” y ejecutó la transacción con 2 navegadores a la vez en varias oportunidades hasta lograr el objetivo (ver figura 233) (Homakov, 2015).

Figura 233

Race condition sobre gift card de Starbucks.

```
# prepare transfer details in both sessions
curl starbucks/step1 -H «Cookie: session=session1» --data «amount=1&from=wallet1&to=wallet2»
curl starbucks/step1 -H «Cookie: session=session2» --data «amount=1&from=wallet1&to=wallet2»
# send $1 simultaneously from wallet1 to wallet2 using both sessions
curl starbucks/step2?confirm -H «Cookie: session=session1» & curl starbucks/step2?confirm -H «Cookie: session=session2» &
```

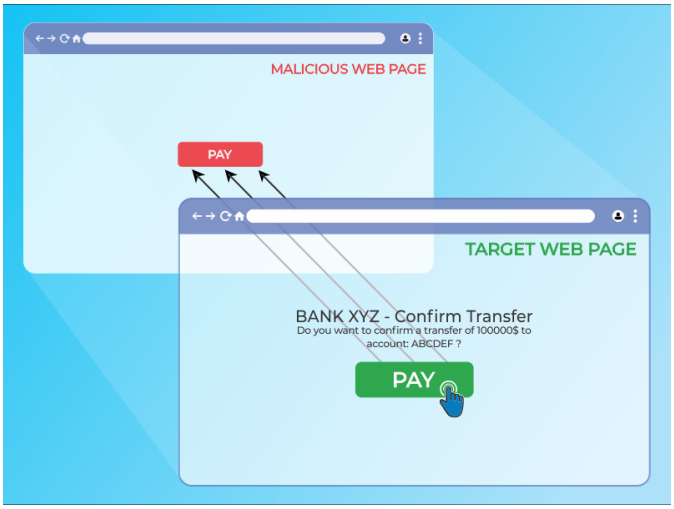
Nota. Pseudo código para transferir 2 veces el mismo balance. (Fuente Image: Homakov, 2015).

[230]Time Of Check – Time of Use.

Clickjaking

El *Clickjacking* es un término acuñado por Grossman y Hansen en 2008 (OWASP, s.f.). Es un ataque que consiste en engañar a la víctima, presentando un elemento invisible por arriba de otro (ver figura 234). La victima piensa estar interactuando con el sitio en pantalla cuando en realidad sus acciones se materializan sobre otro (usualmente un iframe invisible de HTML). Este ataque permite generar likes indeseados en redes sociales, visitar sitios web no solicitados, robo de credenciales, compras online involuntarias, descarga de *malware*, etc.

Figura 234
ClickJacking attack.



Nota. El termino fue acuñado por Grossman y Hansen en 2008 (Fuente imagen: OWASP, s.f.).

Use after free

Las aplicaciones que requieren de asignación dinámica de memoria (*HEAP*), utilizan punteros para referenciar las posiciones de memoria que utilizan para almacenar datos. En caso de que los datos sean eliminados y el puntero no sea adecuadamente actualizado, el mismo apuntara a un área de memoria que puede ser utilizada por un atacante (*dangling pointer*). Los resultados pueden ser desde un *crash* hasta la ejecución de código arbitrario.

Eso es exactamente lo que ocasionó la vulnerabilidad CVE-2022-0609 del navegador Chrome que aparentemente habría sido utilizada por 2 grupos de Corea del Norte en la Operación Dream Job y Operación AppleJeus. En el primer caso los objetivos fueron empleados de medios de comunicación, web hosting, registro de dominios y vendedores de

software. En el segundo caso los objetivos fueron Fintech y usuarios de criptomonedas. La campaña de ataque consistía en el envío de mail con oportunidades laborales y un link a sitios web falsos. Los sitios web contenían un *iframe* invisible que disparaba el *exploit* del navegador (Weidemann, 2022).

Directory traversal attack

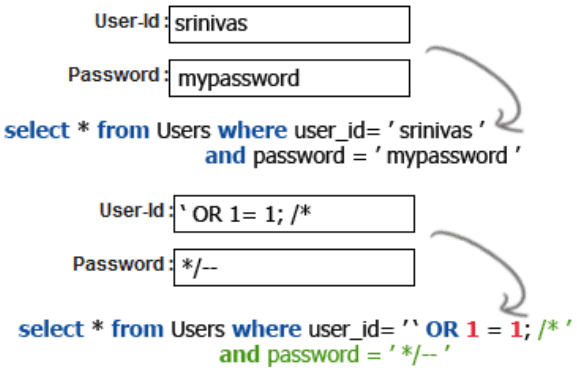
El *Directory traversal attack*; también llamado "./", *directory climbing* o *backtracking*; es una explotación de vulnerabilidad disponible cuando no se validan los inputs del usuario. Según CWE ™ [231]: "Muchas operaciones de archivos están destinadas a tener lugar dentro de un directorio restringido. Mediante el uso de elementos especiales como separadores ".." y "/", los atacantes pueden escapar fuera de la ubicación restringida para acceder a archivos o directorios que se encuentran en otras partes del sistema" (s.f.). Ej. Acceder a archivos de configuraciones de sistema o archivo de password. *Canonicalization Attack* puede utilizarse para evitar filtros de protección y consiste en utilizar formas canónicas alternativas. Ej. el equivalente (./) en Porcent/URI[232] encoding es (%2e%2e/).

SQL injection

SQL Injection es un ataque también relacionado con la falta de validación del input de usuario. Para su comprensión debemos explicar rápidamente el modelo cliente-servidor: En un esquema básico de 2 capas, existe una capa presentación llamada *Frontend* a la cual interactúa el usuario y una capa de acceso de datos llamada *Backend* que procesa las solicitudes del *Frontend*. Al no controlar adecuadamente las entradas del usuario, desde el cliente se podrían enviar solicitudes no deseadas a la base de datos, permitiendo descargar el contenido completo de la misma. Dicho de otra forma, el formulario de un sitio web espera una variable, como ser número de documento, mientras que el atacante abusa y eyecta código, modificando la lógica de consulta a la base de datos (ver figura 235).

[231]Common Weakness Enumeration de MITRE.
[232]Uniform Resource Identifier.

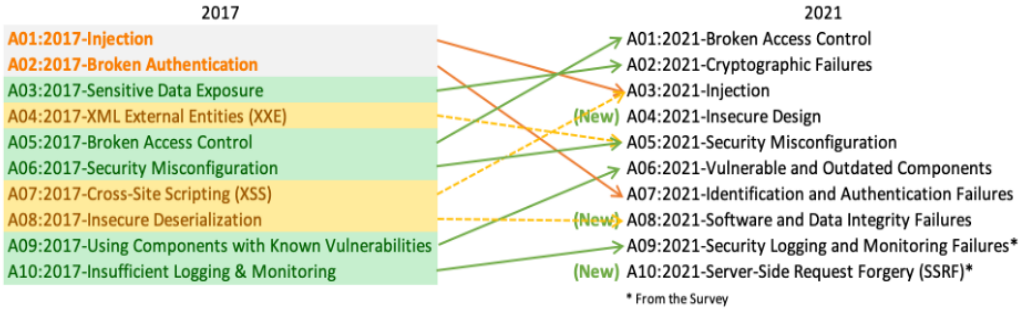
Figura 235
SQL Injection attack.



Nota. El carácter (`) finaliza el Sting esperado de entrada. Dado que la comparación de 1 con si mismo (1 = 1) es verdadero, lo será el OR acorde a la lógica booleana. El resto del código queda anulado dado el carácter de comentario (/*) (Fuente imagen: Tamada, 2008).

Resulta imposible mencionar todas las vulnerabilidades, dada la amplitud y diversidad de estas. Dado que muchas aplicaciones hoy en día son vía web, mencionamos a modo de cierre el Top 10 de vulnerabilidades OWASP (ver figura 236).

Figura 236
OWASP Top 10 Web Application Security Risks.



Nota. (Fuente imagen: OWASP, 2021).

Malware attacks.

Originalmente llamados virus, con el tiempo terminó definido como *malware*. Se trata de una pieza de software con finalidades maliciosas. Existen diferentes tipos de *malware* y su complejidad ha ido aumentando a lo largo de los años. Sus capacidades son sorprendentes, como así también, sus técnicas de ocultamiento y mecanismos para eludir a los antivirus.

Los primeros virus eran muy simples e incluso en muchos casos inofensivos. Hoy en día un *malware* puede ser muy complejo y sus capacidades ofensivas cuasi ilimitadas. Los

malware en la actualidad se asemejan más a un cohete de múltiples etapas, modular y con componentes que solo son un medio de transporte de una carga llamada *payload*.

Para ilustrar mencionamos el *malware* de inteligencia llamado Machete. Descripto en 2014 por Kaspersky, en 2017 por Cylance Team y en 2019 por Eset. Machete utiliza mecanismos de infección basado en ingeniería social, infectando a las víctimas con sitios web o con técnicas de *spear pishing* con archivos infectados de PowerPoint. En el caso de sitios web utiliza un código *snippets* en HTML (fragmentos de código raw dentro del sitio web). En el caso de *pishing*, los archivos (Hermosa XXX.pps.rar – Suntzu.rar – El arte de la guerra.rar – Hot brazilian XXX.rar) son en realidad un auto descomprimible que incluye un código en Python embebido, sumado al documento original como señuelo. Los autoejecutables (Zip o Rar) se generan con un software llamado Nullsoft Scriptable Install System (https://sourceforge.net/projects/nsis/) o el Self-extracting RAR executable (SFX). El primero de ellos permite fácilmente ofuscar el código utilizando compresión como Zlib, BZip2, LZMA. También se ha observado la utilización de hosting económicos (esy. ex) para almacenar los *payloads* a descargar por la víctima. Dicho de otra forma, la primera etapa es un ejecutable downloader que descarga el *payload* para una segunda etapa y así sucesivamente (ver figura 237 y 238). Para pasar el código de Python v2.7 a binario utilizan PY2EXE y durante la transferencia de archivos primero prueban la conectividad con un request HTTP (urllib) y luego utiliza un FTP con encriptación TLS (ftplib). Esta utilización de script compilados son una técnica para evitar la detección de antivirus. Además, se ha observado la utilización de un mecanismo de cifrado con AES CBS (posteriormente reemplazado por base64) previo al exfiltrado de datos al C2[233]. El mismo *malware* también ofusca algunas configuraciones propias mediante un XOR y partes del código Python mediante Pyobfuscate. Para garantizar la persistencia utiliza 2 mecanismos: una tarea programada (task scheduler) o un ejecutable durante el arranque del sistema. Algunas funcionalidades de este *malware* son:

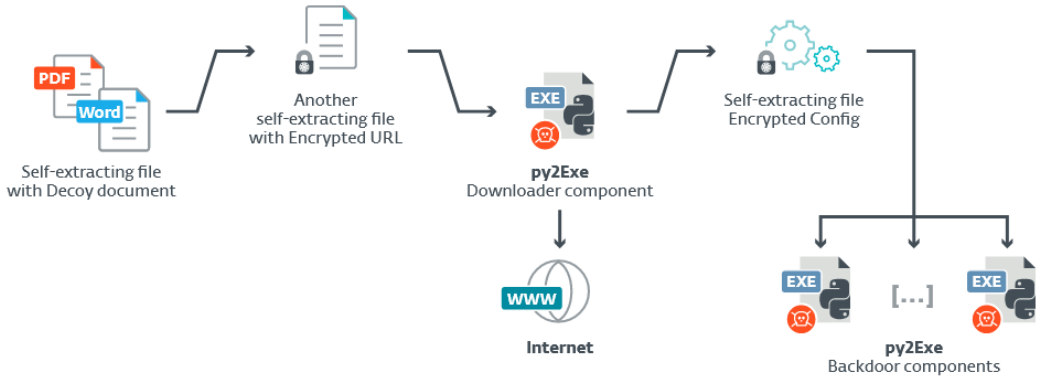
- *Keylogger* (captura de credenciales).
- Captura de audio desde el micrófono (espionaje).
- Captura de fotos desde webcam.

[233]Centro de control, Command and Control, C2C o simplemente C2.

- Captura de pantallas y geolocalización.
- Exfiltrado de datos en un servidor remoto.
- Copia de datos a pendrive (infección/persistencia).
- Captura de datos del *clipboard*.
- Auto actualización de sí mismo.
- Ejecución de otros binarios.

Figura 237

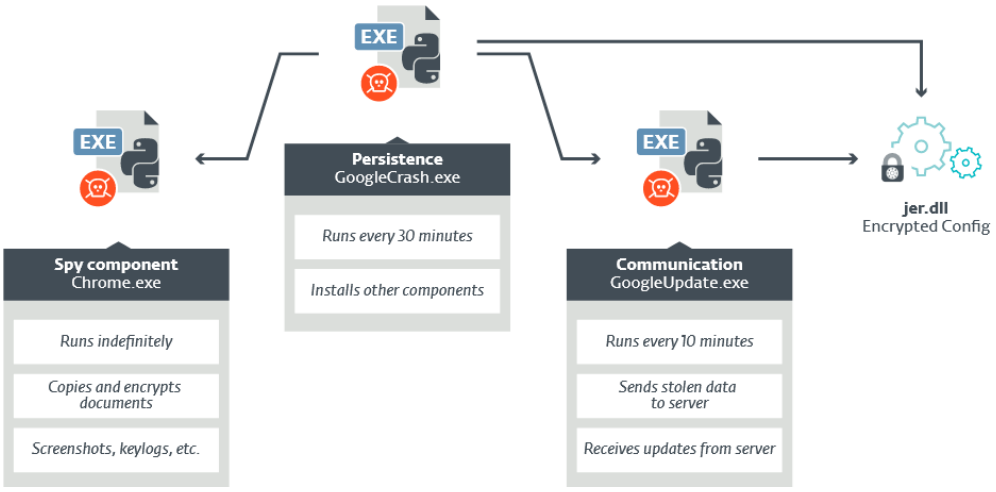
Componentes del malware Machete.



Nota. Multi etapas, similar al lanzamiento de un cohete. (Fuente Image: Eset, 2019).

Figura 238

Dropped executables.



Nota. Los nombres también buscan confundir con archivos genuinos. (Fuente Image: Eset, 2019).

No resulta imperioso entender la totalidad del *malware* mencionado, sino ilustrar al lector la complejidad y sus capacidades.

Existe una gran diversidad de *malware* basados una o múltiples funcionalidades. Para su comprensión planteamos convenientemente una clasificación básica a modo teórico de algunos tipos más importantes.

Virus

Originalmente llamados de esta manera ya que tenían un funcionamiento similar a un virus biológico. Consistía en una pieza de software incrustada dentro de otro programa benigno (como un parasito) y que al ejecutarse se reproducía infectando de la misma forma a otros archivos ejecutables. Von Neumann ya había teorizado en 1949 sobre el concepto de *self-reproducing autómatas* y es por ello por lo que es conocido como el padre de la virología informática (Filiol, 2005).

El primer virus conocido fue Creeper (1971) que infectaba las PDP-10 con OS Tenex en la red Arpanet. Fue Creado por Bob Thomas y su funcionalidad experimental era simplemente mostrar un mensaje en pantalla (“I'M THE CREEPER; CATCH ME IF YOU CAN”). Como respuesta, Ray Tomlinson crea la primera pieza de software del tipo antivirus llamada Reaper. Este fue el primer worm dado que se esparcía por la red a fin de eliminar todas las copias de Creeper.

Otro ejemplo temprano es el virus Elk Cloner. Creado en 1982 por Rich Skrenta cuando tenía 15 años. El virus infectaba el Boot sector de las Apple DOS 3.3 y mostrando en pantalla un poema. El virus se copiaba a todos los discos no infectados que se colocaban en la máquina.

Worm

También llamados gusanos, son piezas de software diseñadas para propagarse en los dispositivos de la red mediante la utilización de vulnerabilidades. La diferencia con el Virus es que no requiere un programa host donde alojarte.

El primer gusano maligno conocido fue el gusano de Morris (en referencia a su creador Robert Tappan Morris, hijo de un criptógrafo de la NSA). Data de 1988 y utilizaba diversas vulnerabilidades en el sendmail de unix, fingerd y accesos remotos de confianza sin

credenciales de autenticación en rexec/rsh. El gusano no estaba pensado para causar daño. Sin embargo, debido a una falla en su diseño, termino infectando a los equipos múltiples veces causando un consumo de recursos y finalmente una denegación de servicio. Debido al daño causado, estimado de varios millones de dólares, se crea el primer CERT (Computer Emergency Response Team).

Fileless

Son *malware* que residen en memoria RAM durante el proceso de infección y no requieren de un archivo físico en el disco, por lo cual desaparecen al reiniciar el dispositivo. Esto dificulta en gran medida el trabajo forense y la recolección de evidencias.

Macrovirus

Están programados en VBScript dentro de algún producto de office. Usualmente suelen tener el código ofuscado o descargan otros *payload* de internet. Similarmente, los scripts virus ejecutan código en Windows Script Host o JavaScripts.

Trojan Horse

En el poema Aeneid de Virgil, basado en la odisea de Homero, se menciona como los griegos construyeron un caballo de madera gigante donde ocultaron un grupo de guerreros en su interior. La finalidad era terminar con el asedio de la ciudad de Troya mediante el engaño de sus adversarios, quieren ingresaron el caballo a la ciudad tomándolo como un obsequio y terminaron siendo atacados durante la noche. En el caso de *malware* se refiere a un programa benigno que oculta una funcionalidad maligna. Por ejemplo, un software gratuito que puede descargarse desde internet y ser a la vista del usuario completamente útil y funcional. En el fondo, dicho programa puede contener un *backdoor*, keylogger, exfiltrar archivos, etc. Cuando el *malware* además permite el acceso remoto del atacante se denomina Remote Access Trojan (RAT).

Logic bomb

Software oculto en el sistema que es activado mediante algún evento disparador y cuya finalidad es la destrucción del sistema o archivos.

Botnet

Cuando el *malware* de este tipo infecta una maquina pasa a formar parte de una red de máquinas infectadas, como si fueran un ejército de zombies. Estas máquinas se contactan con un ordenador centralizado (ejemplo, mediante un canal de IRC) y se quedan a la espera de órdenes. El atacante al mando puede ordénales acciones. Lo más habitual suele ser realizar un ataque de DOS.

Rootkit

Se trata de una herramienta que se instala en un sistema comprometido (donde se obtuvo previamente privilegios elevados). Entre otras funcionalidades la herramienta permite el acceso remoto sin autenticación al atacante, captura de credenciales, sniffer de red, ocultamiento de huellas (log scrubber), exfiltración de archivos en canales ocultos (covert channels, ej. DNS request). Los rootkit habitualmente afectan al sistema de forma de poder ocultarse a los ojos de los administradores. Para lograrlo, por ejemplo, reemplazan los comandos “ls” o” find” a fin de no mostrar los archivos en los resultados en pantalla. Los más avanzados directamente se instalan a nivel Kernel del sistema, capturando y adulterando los resultados en pantalla (ej. ocultando procesos). El mecanismo por el cual modifican los resultados es una técnica de intercepción/adulteración de funciones o mensajes, denominada *hook*. En el caso de entornos Windows pueden instalarse de forma de *driver*. Recordemos que los drivers en la arquitectura Windows operan a nivel kernel mode, algo que le otorga flexibilidad, pero también un importante vector de ataque. Los rootkits también pueden estar persistentes a nivel firmware o a nivel hipervisor en caso de máquinas virtuales. Todo lo mencionado los hace sumamente poderosos, sigilosos (difícil de detectar) y complicado de remover.

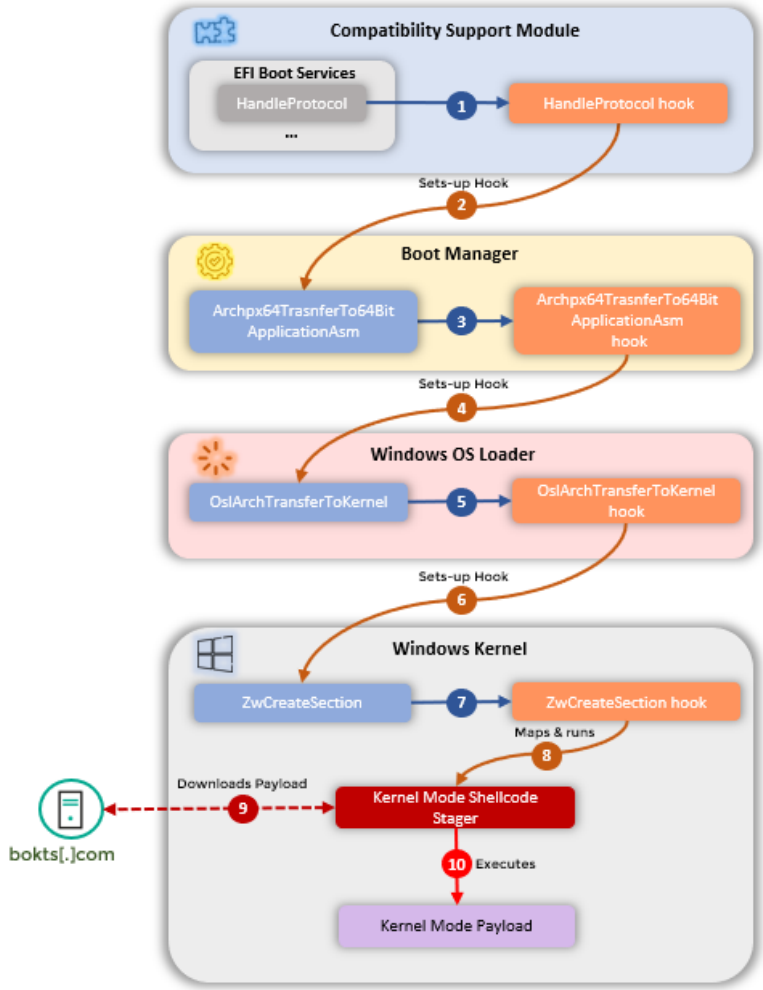
Bootkit

Malware que infectan el arranque del sistema (system startup). A modo ejemplo, investigadores de Kaspersky encontraron un *malware* (CosmicStrand) en motherboard ASUS y Gigabytes (H81 chipset). Posee capacidades de rootkit sigiloso y de infectar el firmware de los motherboards (bootkit), lo cual lo hace extremadamente peligroso. Persiste inclusive reinstalando el sistema operativo (Glazova, 2020).

La infección original a nivel UEFI[234] podría realizarse por un ataque de cadena de suministro o un *evil maid attack* (el nombre refiere dejar la computadora en un hotel donde puede ser manipulada por personal del hotel).

Utiliza una serie de hooks en puntos específicos del proceso de arranque (Hooks son modificaciones al flujo normal de ejecución (ver figura 239). El código se ejecuta durante el arranque, antes de iniciar el sistema operativo. Lo que permite el deploy de un implante a nivel kernel (Glazova, 2020).

Figura 239
Hooks utilizadas por CosmicStrand.



Nota. (Fuente imagen Glazova, 2020).

[234] Unified Extensible Firmware Interface, es el sucesor del BIOS. Encargado de inicializar el hardware e iniciar el proceso de inicio del sistema.

El *malware* espera 10 minutos y luego verifica el acceso a internet directamente a nivel kernetl I/O request packets (IRPs) evitando utilizar el Transport Device Interface de más alto nivel (sigilo). El *payload* se descarga de update.bokts.com

Las víctimas fueron de China, Vietnam, Irán and Rusia y la atribución se cree que son desarrolladores de habla china (Glazova, 2022)

Wiper

La funcionalidad es el borrado seguro de archivos (sobrescribiendo los archivos múltiples veces con información basura) a fin de que no puedan ser recuperados. La finalidad es causar daño a un sistema o adversario o también la de borrar evidencias de un ataque (usualmente realizado con otro *malware*).

Ransomware

Se trata de un tipo de *malware* que cifra el contenido de los archivos mediante una llave, quedando los mismos inutilizables. La finalidad usual es exigir el pago de crypto monedas a cambio de la llave para recuperar los archivos. No siempre los archivos son recuperables ya que han existido casos de que generan una llave aleatoria que es destruida en el proceso. Sin embargo, suele ser más lucrativo para los desarrolladores descifrar el contenido luego del pago extorsivo y demostrar su “transparencia” y “confiabilidad” a futuras víctimas.

Crypto minners

Cuando un sistema es infectado es utilizado para minar criptomonedas en favor del atacante. Usualmente operan cuando el sistema se encuentra inactivo a fin de no llamar la atención.

Backdoor

Las puertas traseras usualmente son elaboradas por los desarrolladores de software con la finalidad de realizar pruebas de este. Estas puertas permiten un acceso directo a funciones del sistema evitando controles de seguridad. Los desarrolladores pueden olvidar estas puertas y terminar en el software final en producción, también pueden dejarlo adrede o a

pedido de entidades gubernamentales en secreto. Además, existen *malware* que tienen justamente dicha funcionalidad de colocar una puerta trasera en un software o sistema.

Malware as a service

Es un tipo de arquitectura donde el desarrollador del *malware* no infecta las maquinas si no que ofrece el servicio y plataforma para que un tercero lleve a cabo los ataques. A cambio, el desarrollador obtiene un margen de recompensa (en caso de tratarse de un ransomware extorsivo) o un pago por el uso del servicio. De esta forma alguien sin conocimiento técnico puede adquirir una herramienta de ataque poderosa y elaborada. Inclusive utilizarla como insider desde dentro de una organización.

Rogue security malware

Se basa en un engaño del tipo scareware, donde se asusta al usuario indicando que su sistema está infectado por un *malware* y se ofrece una solución para descargar. Esta solución es en realidad el *malware* que el usuario nunca tuvo en primer lugar.

Spyware

Destinado a la adquisición de información sensible del usuario. Usualmente tienen la capacidad de exfiltración de archivos, captura de teclas, captura de pantalla, historial de navegación, etc. La información adquirida posteriormente es utilizada con fines delictivos, fraude, extorsiones u operaciones. Similar son los Adware, pero se encuentran enfocados únicamente a generar publicidad usualmente en forma de ventanas emergentes.

Exfiltration

Ampliando el concepto de spyware, la extracción de datos se denomina exfiltración y es una funcionalidad de algunos *malwares*. Usualmente para no ser detectados los datos son cifrados (ej. utilizando un XOR) y se utilizan canales encubiertos a fin de no llamar la atención y poder pasar los filtros de seguridad de red. Por ejemplo, el tráfico puede mimetizar una comunicación a un sitio web (TCP HTTP/HTTPS puerto 80, 443) o solicitudes de resolución de nombre de dominio (UDP ARP puerto 53).

Conceptos básicos de cifrado.

El siguiente apartado describe los conceptos básicos de cifrado a fin de facilitar la lectura de los posteriores capítulos.

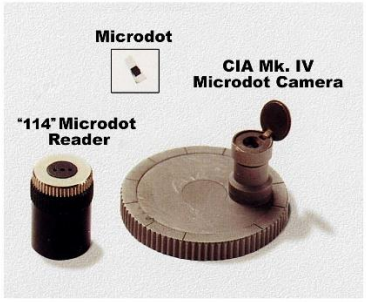
Esteganografía.

La *esteganografía* (del griego: escritura oculta) es una técnica para ocultar un mensaje dentro de otro. Según la obra "las historias" del historiador griego Herodoto (siglo V A.C.), el general Ateniense Histieo necesitaba enviar un mensaje a su yerno Aristágoras de Mileto para que se sublevara al padre de Jerjes. Para ello, afeito la cabeza de un esclavo, escribió un mensaje y espero a que creciera el pelo para enviarlo. El griego Eneas el táctico perforaba agujeros en algunas letras de un texto para ocultar otro mensaje. El científico italiano Giovanni Porta, utilizaba una tinta formada por alumbre y vinagre para escribir sobre un huevo duro que al ser pelado permitía leer el mensaje. Estos solo algunos de los tantos ejemplos de la antigüedad (Muller, 2006). La grilla de Cardan de 1550, desarrollada en la antigua China, tanto el receptor como el emisor tenían un papel con orificios en lugares aleatorios donde escribían el mensaje oculto, que al momento de quitar el papel se completaba con ideogramas. Durante el siglo 16 un matemático italiano reinvento el método conocido como la máscara de Cardan[235] (ver figura 240) (Katzenbeisser y Petitcolas, 2000). San Martin enviaba mensajes a sus seguidores en Lima, Perú; escondiendo los mensajes en un doble fondo de ollas de barro, colocaras durante su cocción (Podberezski, 2019).

En 1870, París se encontraba sitiada por la guerra Franco-Prusiana. René Dagron utilizó una técnica fotográfica de reducción para enviar una mayor cantidad de mensajes con las palomas mensajeras (Kipper, 2003). Posteriormente la técnica fue evolucionando y durante la primera y segunda guerra mundial, los alemanes utilizaron la técnica del micropunto para ocultar mensajes en los puntos de una carta (ver figura 241). Esta técnica no fue descubierta sino hasta 1941 por un doble agente.

[235] Una variante moderna, demuestra la utilización en imágenes junto a redes neuronales (Lui, Zhang, Ke, Lei, Zhang y Yang, 2018).

Figura 240
Microdots.



Nota. Cámara MK-VR de microdots (fuente imagen: White, 2015).

Cuando se utiliza la *esteganografía* para esconder un texto dentro de otro basado en ciertas reglas (ej. extraer la primera letra de cada palabra para obtener el mensaje oculto), se llama *concealment cipher* o *null cipher*.

Hoy en día, diferentes técnicas de *esteganografía* son utilizadas para esconder información dentro de archivos multimedia (imágenes/audio/video), como por ejemplo inyectar bits en la paleta de colores de manera invisible a los sentidos humanos. La finalidad puede ser tanto la privacidad/confidencialidad de una comunicación, como la exfiltración (hurto) imperceptible de información a través de un canal encubierto (*covert channel*). Los canales encubiertos también son ampliamente utilizados en el espionaje y son cuasi imposibles de descubrir (ejemplo, el emisor y el receptor acuerdan previamente que mencionar una palabra o N cantidad de veces durante una charla implica la orden de lanzar una operación; mientras que otra palabra o un numero N de veces diferentes implica su cancelación). Antiguamente los espías intercambian información mediante diferentes técnicas como dejar mensajes en ciertos lugares (*dead drop*), utilizar dispositivos de transmisiones rápidas/cortas e inclusive dispositivos extravagantes como transmitir a través del agua con una caña de pescar emisora y otra receptora, entre otros. Hoy en día las TIC ofrecen innumerables alternativas de comunicación. Ya mencionamos la técnica de utilizar los encabezados del protocolo TCP/IP para esconder datos. Internet dispone gran variedad de servicios de comunicación, inclusive, dentro de los video juegos. Como ejemplo de canal

encubierto podemos mencionar la investigación del FBI llamada Ghost Stories que culminó en 2010 con el arresto a varios agentes encubiertos rusos, de los cuales algunos transmitían información a través de una comunicación local WiFi cercana.

Book cipher.

Alrededor del año 1500, Jacobus Silvestri menciona el *book cipher* o *Ottendorf Cipher*, que consiste en que el emisor y el receptor acuerdan utilizar uno o varios libros en el cifrado (la llave es el libro propiamente dicho). El mensaje enviado consiste en una serie de 3 números que hacen referencia a un número de página, un numero de línea y la posición de la palabra a extraer. Traduciendo todas las series se logra obtener el mensaje en claro (Leighton and Matyas, 1985).

Criptografía.

La Criptografía (del griego: escritura secreta) es un arte cuyo objetivo es transformar (cifrar) un mensaje inteligible (*cleartext/plaintext*) en uno ininteligible (*ciphertext*), a fin de que un adversario no pueda violar la privacidad del mensaje.

Las técnicas de cifrado básicamente constan en 2 operaciones: *sustitución* y *permutación*. La *sustitución* consiste en cambiar una letra por otra. Cuando siempre se cambia las letras de la misma forma hablamos de *sustitución simple* o *mono alfabética*. Cuando las sustituciones de las letras más comunes tienen múltiples representaciones se llama sustitución homofónica y es utilizada para contrarrestar el análisis de frecuencia. En caso de que la sustitución cambie en función de una circunstancia, hablamos de sustitución *poli alfabética*. Algunos ejemplos de sustitución simple son el cifrado Atbash (que invierte el orden del alfabeto) o la cifra cesar (que desplaza las letras en 3 posiciones) (ver figura 242). El *nomenclator* es una variante de la sustitución que utiliza *codewords* (tablas de sustitución) y fue utilizado por el *Rossignols Great Cipher* durante el siglo XIV en Francia como así también por la logia Lautaro a la que pertenecía San Martín (ver figura 243).

Figura 241

Cifrado por sustitución simple.

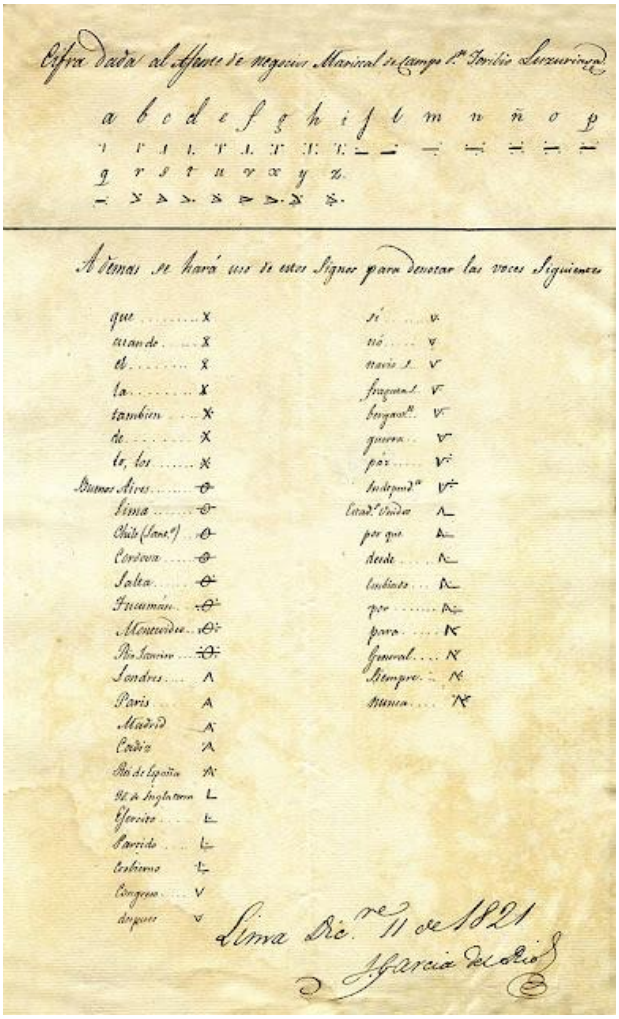
- **Standard Alphabet:**
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
- **Cryptographic Alphabet:**
  DEFGHIJKLMNOPQRSTUVWXYZABC

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA

Nota. En la parte superior: cifrado Cesar (desplazado 3 posiciones). Parte inferior cifrado Atbash (con alfabeto latino) en la parte inferior (Fuente imagen: Harris y Maimí, 2019).

Figura 242

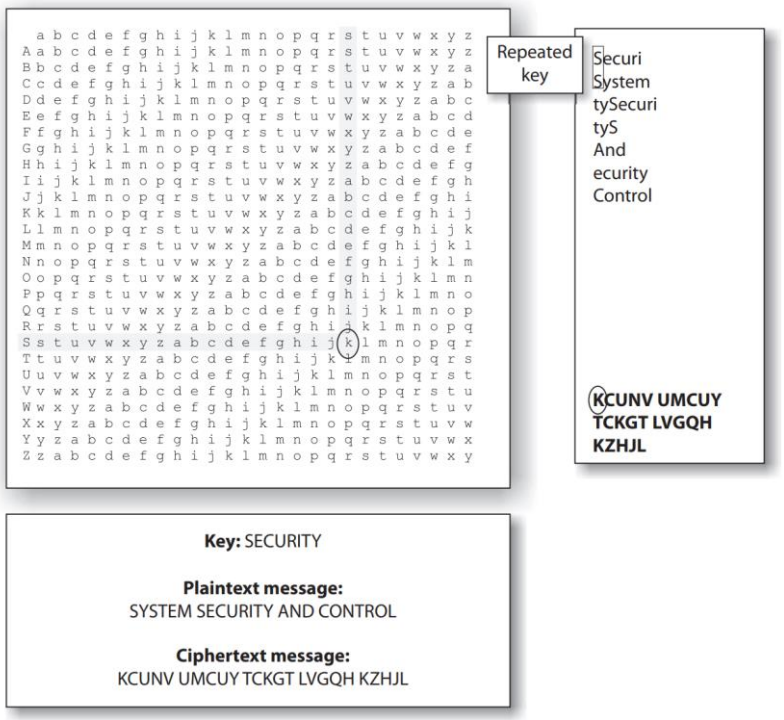
Ejemplo nomenclador.



Nota. *Claves secretas de la Logia Lautarina en 1821 (Archivo Nacional de Argentina como fue citado por Podberezski, 2019).*

Un ejemplo de sustitución *polialfabética* es el cifrado Vigénere (basado en Tritemio). El mismo consta de 26 alfabetos desplazados que conforman una matriz. Utilizando la clave como eje horizontal y el texto claro como eje vertical se realiza el cifrado (ver figura 244).

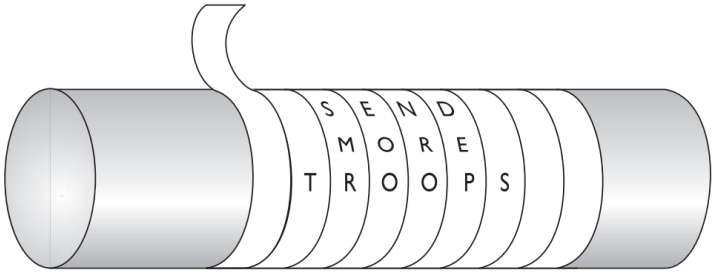
Figura 243
Vigenère square.



Nota. (Fuente imagen: Harris y Maimí, 2019).

La *permutación* consiste en cambiar del lugar la posición de las letras. Los espartanos utilizaban la escítala (vara de grosor variable) donde enrollaban una cinta de cuero y al desenrollarse perdía el sentido (ver figura 245).

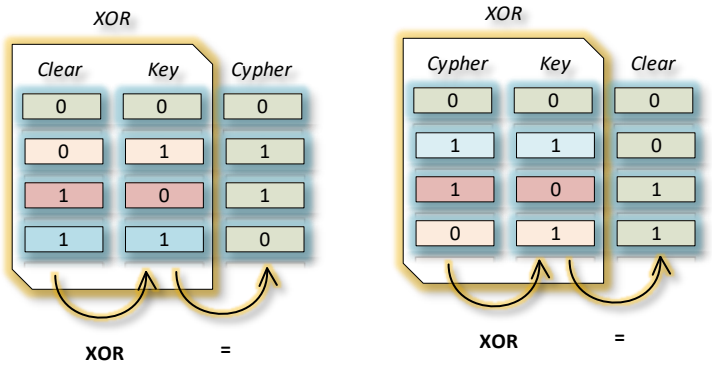
Figura 244
Scytale.



Nota. (Fuente imagen: Harris y Maimí, 2019).

El One-Time Pad, inventado por Gilbert Vernam en 1917, es considerado el cifrado perfecto. Requiere de un pad aleatorio de igual tamaño que el mensaje y una operación XOR (or exclusivo), dando como resultado el mensaje cifrado. El receptor, quien conoce el pad, aplica la misma operación para conseguir el texto claro (ver figura 246). La dificultad reside en que el emisor y el receptor previamente tienen que acordar y compartir una clave (pad). Además, debe garantizarse un pad genuinamente aleatorio, tan largo como el mensaje y ser utilizado por única vez. Asimismo, tanto la seguridad en la distribución del pad como la seguridad en el sitio del receptor/emisor son primordiales.

Figura 245
On Time Pad



Nota. El XOR tiene como propiedad volver al mismo resultado si se aplica 2 veces la misma operación (fuente imagen: elaboración propia).

El análisis de frecuencia es una técnica descripta por Al-Kindi (801-873) cuyo objetivo es romper el sistema de cifrados clásicos. Consiste en comparar la frecuencia de ocurrencia de ciertas letras en relación con el idioma del escrito y comprarlo contra el texto cifrado.

Según Shannon, para que un sistema sea resistente debe cumplir con el principio de *difusión* y *confusión*. La *difusión* implica que cambiar un bit en el texto claro, debería implicar la mayor cantidad de cambios en el texto cifrado. Horst Feistel describe similarmente el concepto como *Avalanche effect*. La *Confusión* conlleva a que la relación entre el texto cifrado y la clave debe ser lo más compleja posible.

Acorde al principio de Keckhoffs (1883), el único secreto en un sistema criptográfico debe ser la clave. El algoritmo de cifrado debe ser de conocimiento público. Personalmente no concuerdo con dicho principio ya que no necesariamente las vulnerabilidades

descubiertas serán puestas en consideración y podrían ser utilizadas en secreto para atacar el sistema de cifrado.

Criptografía moderna.

Gracias a los avances en la capacidad de cómputo de los computadores, la criptografía moderna se basa en esquemas complejos de cajas con funciones matemáticas que realizan operaciones de sustitución y transposición. La clave determina que cajas utilizar, con que parámetros deben ser usadas y en qué orden. Dicha complejidad previene los análisis de frecuencias

Los tipos de algoritmos criptográficos modernos son: *Symmetric* (*secret key*) y *Asymmetric* (*private/public key*). El primero utiliza una llave secreta tanto para el cifrado como para el descifrado mientras que el segundo usa un par de llaves (publica/privada).

La criptografía asimétrica se sustenta en ciertas funciones matemáticas simples de calcular en un sentido, aunque difíciles de computar en el sentido contrario. Estas funciones son denominadas *trapdoor functions* y el concepto fue presentado en 1976 por Diffie y Hellman. Dado que la criptografía asimétrica es más lenta que la simétrica, en las comunicaciones lo que usualmente sucede es que se establece la comunicación mediante un mecanismo asimétrico para posteriormente negociar una *clave de sesión* utilizada por un cifrado simétrico.

Public Key Infrastructure (PKI).

¿Cómo saber si una clave pública pertenece a la persona/sistema al que se quiere comunicar y no fue suplantada por un atacante? un sistema híbrido de *symmetric* y *asymmetric* que garantiza la confiabilidad, integridad y el no repudio es la *Public Key Instrastructure* (PKI). Cada entidad que participa en un esquema PKI tiene un certificado digital que contiene su clave pública. Estos certificados son creados y firmados por una tercera parte de confianza en común de los interlocutores llamada *Certificate authority* (CA). La *registration authority* (RA) es la encargada de verificar la identidad previa a la emisión del certificado digital (Harris y Maymí, 2019). La PKI es empleada hoy en día para validar la comunicación en sitios web, aplicaciones de mensajería, servidores de correo e incluso la

arquitectura X-ROAD utilizada por el e-Goverment (Estonia/Finlandia), entro otros ejemplos.

Es importante entender que quien tenga control de alguna PKI sobre internet, tiene un poder grande sobre la intercepción y manipulación de comunicaciones. De forma análoga, los root DNS[236] y los backbone de internet permiten llevar a cabo diferentes manipulaciones sobre las comunicaciones.

Vulnerabilidades a los sistemas criptográficos.

Los sistemas criptográficos también son vulnerables a ataques. El criptoanálisis el estudio de la criptografía con la finalidad de buscar las vulnerabilidades de los sistemas de cifrados. Es como la criptonita del cifrado.

Romper el sistema de cifrado implica obtener finalmente acceso a la información sensible (quebrando el principio de confidencialidad). La fortaleza del sistema criptográfico está determinada por el *work factor* (cantidad de recursos y tiempo) necesario para romper el mismo.

Algunas vulnerabilidades tienen que ver con el algoritmo de cifrado en sí mismo, mientras que otros están relacionados con una mala implementación o un uso inadecuado (ej. una mala generación de números pseudoaleatorios, utilizar la misma clave en 2 cifrados diferentes, firmar los mensajes siembre de la misma manera, etc.)

Las vulnerabilidades varían según el tipo de cifrado. Por ejemplo, los sistemas criptográficos tradicionales pueden explotarte mediante ataques de fuerza bruta, análisis de frecuencia, etc.; mientras que la criptografía moderna es más robusta y requiere de una gran cantidad de cómputo, factorización de números primos, explotar vulnerabilidades del propio sistema de cifrado, etc.

Sin embargo, la opción más simple es explotar las puntas del canal de comunicación (vulnerar al emisor/receptor) con algunas de todas las técnicas descriptas en el presente capitulo o afectar la cadena de suministro (sistemas de cifrado/hardware/generador de números aleatorios que contengan puertas traseras/vulnerabilidades). En los siguientes

[236] Es interesante observar quienes son los operadores actuales de los root DNS.

capítulos ampliaremos respecto de esta temática. Por lo pronto, podríamos afirmar que existen dos tipos de cifrados: los que ya han sido rotos y los que están por romperse.

Conceptos claves del capítulo.

A modo resumen, algunos conceptos importantes vistos en el presente capitulo son:

- Los pilares de la seguridad son la confidencialidad, la integridad y disponibilidad (+Safety). Usualmente el activo más valioso es la información a excepción de los entornos industriales donde la disponibilidad suele ser precedente.
- No existe la seguridad perfecta ni llave en mano. Eso se observa en el creciente número de leaks. La seguridad es la correcta gestión de los riesgos en un continuo y permanente ciclo de mejora continua.
- No esperar a confrontar los ataques. Además de las estrategias defensivas, buscar la disuasión y la prevención.
- La seguridad se aplica en capas redundantes y se tiende a entornos de confianza cero, donde todos los elementos deben ser verificados o entornos en maya donde cada dispositivo tiene su propia seguridad perimetral.
- El atacante tiene una ventaja estratégica sobre la defensa, un efecto sorpresa en la utilización de nuevas técnicas/herramientas/vulnerabilidades y usualmente un sinfín de posibilidades de intentos hasta lograr el objetivo deseado.
- La seguridad se rompe por el eslabón más débil de la cadena.
- La seguridad es inversamente proporcional al costo y a la facilidad de uso. Muchas veces se deja de lado la máxima seguridad en busca de un punto de equilibrio.
- Los sistemas son imperfectos y existen infinidad de vulnerabilidades descubiertas y por descubrir. Un atacante puede explotar las mismas en diferentes capas, ya sea a nivel hardware, sistema operativo, aplicación, protocolo/red o incluso a nivel usuario. Este último es usualmente citado como el eslabón más débil.
- Los *malware* fueron evolucionando y son cada vez más complejo y potentes.
- Los desarrolladores usualmente no se preocupan por la seguridad o dejan los productos inseguros por defecto, dando mayor preponderancia a la compatibilidad y funcionalidad. La reducción de costos o el time to market

también empuja a lanzar productos inseguros o que no cuentan con las pruebas de seguridad.

- Mientras que los criptógrafos estudian y desarrollan los sistemas criptográficos para garantizan la confidencialidad, los criptoanalistas buscan vulnerabilidades en dichos sistemas para romper el cifrado. Usualmente solo necesitan tiempo, inteligencia y capacidad de cómputo para lograr dicho fin. Es por ello por lo que existen 2 tipos de cifrados, los rotos y los que están por romperse.
- Quien tenga control sobre la PKI puede tener una ventaja estratégica superior sobre sus adversarios.

Apéndices adicionales:

La presente corresponde a la presentación original. La misma fue removida para dar conformidad a la corrección académica.

DISCLAMER: CHOOSE WISELY.
THIS IS A ONE WAY JOURNEY.

KEEP WALKING



[237]

OR KEEP READING

LAST CHANCE…
FASTEN YOUR SEATBELT

Dedicado a los futuros pioneros a quienes encomiendo la difícil tarea de cambiar al mundo del camino de la destrucción asegurada

[237] Autor OpenClipart-Vectors from https://pixabay.com/vectors/zombie-tv-man-stagger-156746/

Referencias bibliográficas

314th Airlift-Wing (s.f.). *Remembering a World War II commander - VIRIN: 100126-F-0000Z-003* [Photo]. Little Rock Air Force Base. Recuperado: https://www.littlerock.af.mil/News/Photos/igphoto/2000400098/

Ackerman E. (2011, Mar 4). AeroVironment's Nano Hummingbird Surveillance Bot Would Probably Fool You AeroVironment's surveillance robot looks, and performs, exactly like a real hummingbird. *IEEE Spectrum*. Recuperado: https://spectrum.ieee.org/aerovironments-nano-hummingbird-surveillance-bot-would-probably-fool-you

Adee S. (2009, Feb 10). Cyborg Moth Gets a New Radio Research reported this week advances the goal of turning insects into unmanned aerial vehicles. *IEEE Spectrum*. Recuperado: https://spectrum.ieee.org/cyborg-moth-gets-a-new-radio

Adwar C., Kelley M. (2014, Jul 21). Everything We Know About the Huge Spy Base in Cuba That Russia Is Reopening. *Insider*. Recuperado: https://www.businessinsider.com/the-spy-base-russia-may-reopen-in-lourdes-cuba-2014-7

AeroVironment (2011, Feb 17). Aerovironment develops world is first fully operational life-size hummingbird-like unmanned aircraft for DARPA. *AeroVironment*. Recuperado: https://investor.avinc.com/news-releases/news-release-details/aerovironment-develops-worlds-first-fully-operational-life-size

Aid M. (2013, Jun 10). Inside the NSA's Ultra-Secret China Hacking Group. *Foreign Policy*. Recuperado: https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/

Aid T., Burr W., Blanton T. (2010, Feb 12). Project Azorian: The CIA's Declassified History of the Glomar Explorer. *The National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/nukevault/ebb305/

Amazon (s.f.). *Throwing Star LAN Tap Network Packet Capture Mod Replica Monitoring Ethernet Communication Haker Tool* [Fotografía]. Amazon. Recuperado: https://www.amazon.in/Throwing-Network-Monitoring-Ethernet-Communication/dp/B077XY2TGD

Amer, K., Noujaim, J. (Directors) & Amer, K., White, G., Dreyfous, J., Korin, J. and Kos, P. (Producers). (2019). *The great hack* [Motion picture]. USA: The Othrs.

Amnesty International (2020, Sep 25). German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed. *Amnesty International*. Recuperado: https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

Andrew C., Mitrokhin V. (1999). *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. Basic Books. Recuperado: https://archive.org/details/TheSwordAndTheShield-TheMitrokhinArchiveAndTheSecretHistoryOfTheKGB/page/n1/mode/2up

Andrews W., Lindeman T. (2013, Aug 29). $52.6 billion The Black Budget. *The Washington Post*. Recuperado: https://www.washingtonpost.com/wp-srv/special/national/black-budget/

Angwin J., Savage C., Larson J., Moltke H., Poitras L., Risen J. (2015, Aug 15). Newly Disclosed N.S.A. Files Detail Partnerships with AT&T and Verizon. *New York Times*. Recuperado: https://www.nytimes.com/interactive/2015/08/15/us/documents.html

Appelbaum J., Blome N., Gude H., Neukirch R., Pfister R., Poitras L., Rosenbach M., Schindler J., Schmitz G., Stark H. (2013, Oct 27). The NSA's Secret Spy Hub in Berlin. *Spiegel Internacional*. Recuperado: https://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html

Appelbaum J., Blome N., Gude H., Neukirch R., Pfister R., Poitras L., Rosenbach M., Schindler J., Schmitz G., Stark H. (2013, Oct). Der unheimliche Freund. Der Spiger. Recuperado: https://cryptome.org/2013/10/nsa-cia-berlin-spy-nest.pdf

Appelbaum J., Gibson A., Guarnieri C., Müller-Maguhn A., Poitras L., Rosenbach M., Ryge L., Schmundt H., Sontheimer M. (2015, Jan 17). NSA Preps America for Future Battle. *Der Spiegel*. Recuperado: https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html

Appelbaum J., Horchert J., Stöcker C. (2013, Dic 29). Catalog Advertises NSA Toolbox. *Der Spiegel*. Recuperado: https://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html, https://web.archive.org/web/20140102051417/https://www.spiegel.de/international/world/a-941262.html

Arkin W. (2021, May 17). Exclusive: Inside the Military's Secret Undercover Army. *Newsweek*. Recuperado: https://www.newsweek.com/exclusive-inside-militarys-secret-undercover-army-1591881.

Army White Sands Missile Range photo (s.f.). Trinity Site. *National Park of White Sands*. Recuperado: https://www.nps.gov/whsa/learn/historyculture/trinity-site.htm

Ashur T., Luykx A. (2021). An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families. *In Security of Ubiquitous Computing Systems:* (pp. 63-78). Springer. Recuperado: https://doi.org/10.1007/978-3-030-10591-4_4

Aspriadis N, Takas E., Samaras A. (2019). "Country Reputation Assassination during the Greek Memorandum Re-Negotiations" in *Routledge handbook of character assassination and reputation management*, Chapter 17.

Auslen M. (2013, Jun 12). Google claims data given to NSA via secure FTP, by hand. *USA Today*. Recuperado: https://www.usatoday.com/story/money/business/2013/06/12/google-nsa-servers-secure-ftp/2416181/

Averre D. (2023, April 12). British and American Special Forces are inside Ukraine, leaked documents claim MoD denies suggestion that as many as 50 UK elite troops are operating in warzone against Putin's forces. *Daily mail*. Recuperado: https://www.dailymail.co.uk/news/article-11963787/British-American-special-forces-inside-Ukraine-leaked-documents-claim.html

Atomic Energy – United States Senate (1945, Nov. 27~30). Hearings before the Special Committee on Atomic Energy, United States Senate, Seventy-Ninth Congress, First Session, Part 1. Washington, D.C.: United States Government Printing Office. Recuperado: https://nsarchive.gwu.edu/document/28702-document-25-atomic-energy-hearings-special-committee-atomic-energy-united-states.

Avilés (2019, Oct). El caso Gladio: Una red militar clandestina en la Italia de la Guerra Fría. *Revista UNISCI / UNISCI Journal, Nº 51*. Recuperado: https://www.unisci.es/wp-content/uploads/2019/10/UNISCIDP51-5AVILESpdf-1.pdf

Bailin A., Halford J. (2012, Dec 19). Alan Turing pardon: we need a shift in legal position. *The Guardian*. Recuperado: https://www.theguardian.com/law/2012/dec/19/alan-turing-pardon-shift-legal-position

Bainin J. (1996, Feb 27). Egyptian jewish identities: Communitarianisms, nationalisms, nostalgias. *The Stanford Electronic Humanities Review, volume 5, issue 1*. Recuperado: https://web.archive.org/web/20140717143535/http://web.stanford.edu/group/SHR/5-1/text/beinin.html

Baldwin M. (2022, Mar 2). Did Britain sell Enigmas postwar? *Dr. Enigma*. Recuperado: https://drenigma.org/2022/03/02/did-britain-sell-enigmas-postwar/

Balerini Casal, E. (2018). La asesoría militar Argentina en Honduras. *Diálogos Revista Electrónica de Historia*, *19*(2), 198-231. https://doi.org/10.15517/dre.v19i2.31144

Ball J., Harding L., Garside J. (2013, Aug 2013). BT and Vodafone among telecoms companies passing details to GCHQ. *The Guardian*. Recuperado: https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.

Bamford J. (2012). The NSA Is Building the Country's Biggest Spy Center (Watch What You Say). *Wired*. Recuperado: https://www.wired.com/2012/03/ff-nsadatacenter/

Bandura A. (1999). Moral disengagement in the perpetration of inhumanities, *Personality and Social Psychology Review*, 3(3), p. 193-209.

Bandura A., Barbaranelli C., Caprara, G.V. y Pastorelli C. (1996). "Mechanisms of moral disengagement in the exercise of moral agency," *Journal of Personality and social psychology*, 71(2).

Barnes J., Cooper H., Schmitt E. (2022, May 4). U.S. Intelligence Is Helping Ukraine Kill Russian Generals, Officials Say. *The New York Times*. Recuperado: https://www.nytimes.com/2022/05/04/us/politics/russia-generals-killed-ukraine.html

Baumgartner K. (2014, Dec 4). Sony/Destover: mystery North Korean actor's destructive and past network activity. *Secure List*. Recuperado: https://securelist.com/operation-blockbuster-revealed/73914/

Baumgärtner M., Blome N., Gude H., Rosenbach M., Schindler J., Schmid F. (2015, Aprl 24). German Intelligence Under Fire for NSA Cooperation. *Spiegel International*. Recuperado: https://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html

Bauso M. (2020, Abr 9). A 40 años del Boicot a los Juegos Olímpicos de Moscú: la trama política y las pequeñas historias de los deportistas que no pudieron competir. *Infobae*. Recuperado: https://www.infobae.com/america/deportes/2020/04/09/a-40-anos-del-boicot-a-los-juegos-olimpicos-de-moscu-la-trama-politica-y-las-pequenas-historias-de-los-deportistas-que-no-pudieron-competir/

BBC News (2011, Dec 8). Iran shows film of captured US drone. *BBC News*. Recuperado: https://bbc.com/news/world-middle-east-16098562

BBC (2013, Jul 3). ¿Fue legal desviar el avión de Evo Morales? *BBC News Mundo*. Recuperado: https://www.bbc.com/mundo/noticias/2013/07/130703_bolivia_europa_derecho_internacional_espacio_aereo_men

Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. (2013, Jun 19). The Simon and Speck Families of Lightweight block cyphers. *National Security Agency*. Recuperado: https://eprint.iacr.org/2013/404.pdf

Beaumont P. (2021, Jun 11). Ex-Mossad chief signals Israel culpability for Iran attacks. *The Guardian*. Recuperado: https://www.theguardian.com/world/2021/jun/11/ex-mossad-chief-yossi-cohen-signals-israel-culpability-for-iran-attacks

Bergman R., Mazzetti M. (2023, Jun 15). The Battle for the World's Most Powerful Cyberweapon. *New York Times*. Recuperado: https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

Bergman M. (2001). The Deep Web: Surfacing Hidden Value. *Volume 7, Issue 1: Taking License, August 2001*. Recuperado: https://doi.org/10.3998/3336451.0007.104

Bencsáth B., Pék G., Buttyán L., Félegyházi M. (2011, Oct 14). Duqu: A Stuxnet-like malware found in the wild. *Laboratory of Cryptography and System Security*

(CrySyS). Recuperado: https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

Berish A. (s.f.). FDR and Polio. *National Archives - Franklin D. Roosevelt - Presidential Library Museum*. Recuperado: https://www.fdrlibrary.org/polio

Bergman R. (2022, Jul 22). El Mossad aclara nuevos datos sobre los ataques terroristas en Argentina en la década de 1990. The New York Times. Recuperado: https://www.nytimes.com/es/2022/07/22/espanol/argentina-mossad-amia-atentado.html

Bertram B. Magratten D. [The New York Times] (2014, Jan 7). *The Greatest Heist You've Never Heard Of | Retro Report | The New York Times* [Video]. Youtube. Recuperado: https://www.youtube.com/watch?v=KQk5cUMhI8k

Biddle P., England P., Peinado M., Willman B. (2003). The Darknet and the Future of Content Protection. *In: Feigenbaum, J. (eds) Digital Rights Management. DRM 2002. Lecture Notes in Computer Science, vol 2696*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-44993-5_10

Bischoff P. (2022, Jul 11). Surveillance camera statistics: which cities have the most CCTV cameras? *Comparitech*. Recuperado: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Black Hat (2020, Jan 8). Industroyer/Crashoverride: *Zero Things Cool about a Threat Group Targeting the Power Grid* [Video]. Youtube. Recuperado: https://www.youtube.com/watch?v=TH17hSH1PGQ

Blanton T. (2007, Junio 21). The CIA's Family Jewels: Agency Violated Charter for 25 Years, Wiretapped Journalists and Dissidents. *The National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB222/index.htm y https://nsarchive2.gwu.edu/NSAEBB/NSAEBB222/family_jewels_full_ocr.pdf

Bletchley Park Museum (s.f.). Outstations from the Park. Recuperado: https://www.mkheritage.org.uk/archive/bpt/Outstations/Outstations.html

Bock K., Alaraj A., Fax Y., Hurley K., Wustrow E., Levin D. (2021, Aug 11-13). *Weaponizing Middleboxes for TCP Reflected Amplification*. 30th USENIX Security Symposium. Recuperado: https://geneva.cs.umd.edu/papers/usenix-weaponizing-ddos.pdf

Boger M. (2009). *Operational Defenses through Weather Control in 2030* [Research]. Air Command and Staff College - Air University. Recuperado: https://apps.dtic.mil/sti/pdfs/ADA539515.pdf

Bogolyubova O. (2019). "Psychological traits of character assassinations: Studies in cyber-aggression." in *Routledge handbook of character assassination and reputation management*, Chapter 27.

Boyle D. (2022, April 20). REVEALED: US maritime surveillance plane was over Black Sea minutes before Russian flagship Moskva was 'hit by Ukrainian missiles. *Daily Mail*. Recuperado: https://www.dailymail.co.uk/news/article-10733677/Moskva-sinking-Did-supply-Kyiv-location-Black-Sea-flag-ship.html

Bozkurt A., Gilmour R., Stern D., Lal A. (2008, Jan 28). MEMS based bioelectronic neuromuscular interfaces for insect cyborg flight control. *2008 IEEE 21st International Conference on Micro Electromechanical Systems*. Recuperado: https://ieeexplore.ieee.org/document/4443617

Bozorgmehr S. (2012, Jan 18). Iranian company wants to send toy drone to Obama. *CNN Business*. Recuperado: https://edition.cnn.com/2012/01/18/world/meast/iran-drone-replicas/index.html

Bradner, E. (2014, December 10). CIA report's most shocking passages. *CNN*. Recuperado: https://edition.cnn.com/2014/12/09/politics/cia-reports-shocking-passages/

Brewster M., Burke A. (2022, March 4). Under a foreign flag: Canadian veterans explain why they are fighting for Ukraine. *CBC News*. Recuperado: https://www.cbc.ca/news/politics/ukraine-russia-putin-canadian-forces-1.6372259

Brewster T. (2015). These Ex-Israeli Surveillance Agents Hijack Your Browser to Profit from Ads. *Forbes*. Recuperado: https://www.forbes.com/sites/thomasbrewster/2015/06/09/from-israel-unit-8200-to-ad-men

Brewster T. (2016, Aug 25). Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones with a single text. *Forbes*. Recuperado: https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text

Brewster T. (2021, Nov 10). Exclusive: A Cyber Mercenary Is Hacking the Google and Telegram Accounts of Presidential Candidates, Journalists and Doctors. *Forbes*. Recuperado: https://www.forbes.com/sites/thomasbrewster/2021/11/10/rocket-hack-hacker-for-hire-targets-belrus-opposition-gmail-protonmail-and-telegram

Brewster T. (2021, Oct 14). Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find. *Forbes*. Recuperado: https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/

Bridi S., Greenwald G. (2013, Sep 08). NSA Documents Show United States Spied Brazilian Oil Giant. *Fantástico*. Recuperado: https://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html

Bridi S., Greenwald G. (2013, October 6). American and Canadian Spies target Brazilian Energy and Mining Ministry. *Fantástico*. Recuperado: https://g1.globo.com/fantastico/noticia/2013/10/american-and-canadian-spies-target-brazilian-energy-and-mining-ministry.html

British Embassy Oslo (2014, February 25). Sinking of DF Hydro 70th anniversary events in Norway. *GOV.UK*. Recuperado: https://www.gov.uk/government/news/sinking-of-df-hydro-70th-anniversary

Brooker G., Gomez J. (2013, November). Lev Termen's Great Seal Bug Analyzed. *IEEE Aerospace and Electronic Systems Magazine* (Volume: 28, Issue: 11. Recuperado: https://www.cryptomuseum.com/covert/bugs/thing/files/broker_gomez.pdf

Brose C. (2020). *The kill chain: Defending America in the future of high-tech warfare.* USA, NY: Hachette.

Brown J. (s.f.). Operation Ivy Bells. *Naval Order*. Recuperado: https://www.navalorder.org/national-history-day-winner-2021-operation-ivy-bells

Buchanan B. (2020). *The hacker and the state: cyber-attacks and the new normal of geopolitics.* UK, Cambridge: Harvard University Press.

Buckingham W. (1982). *The Air Force and Herbicides in Southeast Asia 1961-1971*. USA, Washington: Office of Air Force History - USAF - U.S. Government Printing

Office. Recuperado: https://media.defense.gov/2010/Sep/28/2001329797/-1/-1/0/operation_ranch_hand.pdf

Buhren R, Jacob N, Krachenfels T, Seifert J. (2021). One Glitch to Rule Them All: Fault Injection Attacks Against AMD's Secure Encrypted Virtualization *28th ACM Conference on Computer and Communications Security (CCS'21) in Seoul*. https://doi.org/10.48550/arXiv.2108.04575

Burns, T. (1990). *The Origins of the National Security Agency*. USA: United States Cryptologic History. National Security Agency. Recuperado: https://web.archive.org/web/20160322122158/https://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf

Burr W. (s.f.). Documents on the U.S. Atomic Energy Detection System [AEDS]. *The National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB7/nsaebb7.htm

Burr W., Evans M. (2001, Dec 6). Ford, Kissinger, and the Indonesian invasion, 1975-76. *The National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB62

Burrows S. (2005). "British propaganda and anti-Napoleonic feeling in the invasion crisis of 1803" en Lincoln, M. (ed.) *Nelson & Napoleon*. National Maritime Museum. UK: London.

Byrne C. (2001, Sep 11). Project: Acoustic Kitty. *The Guardian*. Recuperado: https://www.theguardian.com/world/2001/sep/11/worlddispatch

Byrne M. (2013, Aug 19). CIA Admits It Was behind Iran's Coup. *Foreign Policy Magazine*. Recuperado: https://foreignpolicy.com/2013/08/19/cia-admits-it-was-behind-irans-coup/

Cacciatore F. (2021). La Guerra fredda, il caso Gladio e l'intervento americano in Italia. *Nuova storia contemporanea, ISSN 1126-098X, Nº. 2 (maggio-agosto), 2021, págs. 69-88*.

Cámara Federal de Casación Penal (s.f.). CAUSA Nro. 15496 -SALA II-. Recuperado: https://www.mpf.gob.ar/wp-content/uploads/2016/03/56-20140423-Sala-II-Acosta-ESMA.pdf

Campbell D. (1999, Oct). Development of surveillance technology and risk of abuse of economic information. STOA Panel. Recuperado: https://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf

Campbell D. (2020, Aug 10). Spy in your server. *The Guardian*.

Campbell D. (2015, Aug 3). My life unmasking British eavesdroppers. *The Intercept*. Recuperado: https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/

Canella C., Genkin D., Giner L., Gruss D., Lipp M., Minkin M., Moghimi D., Piessens F., Schwarz M., Sunar B., Bulck J., Yarom Y. (2019). Fallout: Leaking Data on Meltdown-resistant CPUs. *ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom.* Recuperado: https://doi.org/10.1145/3319535.3363219

Çapar K. (2022). *CVE-2022-29072*. Github Repository. Recuperado: https://github.com/kagancapar/CVE-2022-29072

Carle M. (s.f.). The Mission Behind Operation Ivy Bells and How It Was Discovered. *Military.com*. Recuperado: https://www.military.com/history/operation-ivy-bells.html

Castro Olivas J. (2009). *Sociedades secretas y masonería en el proceso de emancipación peruano: La Logia Lautaro en el Perú*. [Tesis de Magíster en Historia]. Universidad Nacional Mayor de San Marco. Recuperado: http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/1369/Castro_oj.pdf

Cathcart B. (2006, May 25). Tube Alloys directorate. *Oxford Dictionary of National Biography*. Recuperado: https://doi.org/10.1093/ref:odnb/93791

Center for Arms Control and Non-Proliferation (2023, Jun 20). Fact Sheet: The Missing Tybee Bomb. Recuperado: https://armscontrolcenter.org/fact-sheet-the-missing-tybee-bomb/

Center for Strategic Communications and Information Security (2022, Feb 15). Увага: жодної загрози для коштів вкладників «Приватбанку» немає. *Ministry of Culture and Information Policy of Ukraine*. Recuperado:

https://spravdi.gov.ua/uvaga-zhodnoyi-zagrozy-dlya-koshtiv-vkladnykiv-pryvatbanku-nemaye/

Chancel, L., Piketty, T., Saez, E., Zucman, G. et al (2022). World Inequality Report 2022. *World Inequality Lab*. Recuperado: https://wir2022.wid.world/www-site/uploads/2022/03/0098-21_WIL_RIM_RAPPORT_A4.pdf

Chandler C., Bentley J. (1970, Jun). Forest fire as a military weapon. *U.S. Department of Agriculture - Forest Services*. Recuperado: https://apps.dtic.mil/sti/citations/AD0509724

Chandran J. (2020, Jan 3). Killing Soleimani: How was the operation carried out? *Gulf News*. Recuperado: https://gulfnews.com/world/mena/killing-soleimani-how-was-the-operation-carried-out-1.1578063347074

Channel 4 News [Channel 4 News]. (2018, Jun 6). *Former Cambridge Analytica CEO Alexander Nix faces MPs (full version)* [Video]. https://www.youtube.com/watch?v=weQ9E6e3aJo

Channel 4 News [Channel 4 News]. (2020, Sep 29). *The Great Hack's David Carroll finally sees his Cambridge Analytica data* [Video]. https://www.youtube.com/watch?v=5Swqc2NjEXM

Checkoway S., Cohney S., Garman C., Green M., Heninger N., Maskiewicz J., Rescorla E., Shacham E., Weinmann R. (2016). A Systematic Analysis of the Juniper Dual EC Incident. *Presented at CCS 2016 - the 23rd ACM Conference on Computer and Communications Security (October 24-28)*. Hofburg Palace Vienna, Austria. Recuperado: https://eprint.iacr.org/2016/376.pdf

Cherepanov (2017). WIN32/INDUSTROYER: A new threat for industrial control systems. *ESET*. Recuperado: https://cdn1.esetstatic.com/ESET/INT/Landing/2017/black-hat/WIN32_Industroyer-USLetter-WEB.pdf

Cherepanov (2017, Jun 12). Industroyer: la mayor amenaza para sistemas de control industrial desde Stuxnet. *We Live Security by Eset*. Recuperado: https://www.welivesecurity.com/la-es/2017/06/12/industroyer-amenaza-control-industrial/

Chien E. (2010, Nov 12). Stuxnet: A Breakthrough. *Symantec*. Recuperado: https://web.archive.org/web/20101115031013/http://www.symantec.com/connect/blogs/stuxnet-breakthrough

Chien E., Falliere N., Murchu L. (2010, Nov 12). W32.Stuxnet Dossier: Version 1.2. *Symantec*. Recuperado: https://web.archive.org/web/20101105203317/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Chomsky N. (1986). *What Uncle Sam really wants.* USA, California Berkeley: Odonian Press.

Chomsky N. (1997). *Media Control: The Spectacular Achievements of Propaganda*. USA, NY: Seven Stories Press.

CIA (s.f.) Artifacts Pigeon Camera [Fotografía]. *Central Intelligence Agency*. Recuperado: https://www.cia.gov/legacy/museum/artifact/pigeon-camera/

CIA (2001, Jan 8). Keeping secrets. *General CIA Records*. Recuperado: https://www.cia.gov/readingroom/docs/CIA-RDP80-01601R000300340071-7.pdf

CIA (2012, Feb 17). Ducking questions is an easy way out. *General CIA Records*. Recuperado: https://www.cia.gov/readingroom/document/cia-rdp91-00561r000100030079-2

CIA Historical Stuff (1971, Oct). *The history of SIGINT in the Central Intelligence Agency, 1947-70*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB506/docs/ciasignals_16.pdf

CIA Memorandum (1966, Jun 24). Maheu, Robert A. *Memorandum for Deputy Director of Central Intelligence*. Recuperado: https://nsarchive.gwu.edu/document/20836-6

CIA Museum (s.f.). Artifacts - Insectothopter. *Central Intelligence Agency*. Recuperado: https://www.cia.gov/legacy/museum/artifact/insectothopter/

CIA Museum (s.f.). Artifacts - Pigeon Camera. *Central Intelligence Agency*. Recuperado: https://www.cia.gov/legacy/museum/artifact/pigeon-camera/

Cimpanu C. (2017, April 14). Shadow Brokers Release New Files Revealing Windows Exploits, SWIFT Attacks. *Bleeping Computer*. Recuperado: bleepingcomputer.com/news/security/shadow-brokers-release-new-files-revealing-windows-exploits-swift-attacks/

Cimpanu C. (2017, Jun 8). Malware Uses Obscure Intel CPU Feature to Steal Data and Avoid Firewalls. *Bleeping Computer*. Recuperado: https://www.bleepingcomputer.com/news/security/malware-uses-obscure-intel-cpu-feature-to-steal-data-and-avoid-firewalls/

Cimpanu C. (2021, Oct. 18). Hacker steals government ID database for Argentina's entire population. *The Record*. Recuperado: https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/

Clark B. (2022, Jul 30). The fall and rise of Russian Electronic Warfare. *IEEE Spectrum*. Recuperado: https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

Clarke A. (1962). *Profiles of the future: an inquiry into the limits of the possible*. USA, NY: Bantam Books.

Clarke I., Sandberg O., Wiley B., Hong T.W. (2001). Freenet: A Distributed Anonymous Information Storage and Retrieval System. *In: Federrath, H. (eds) Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol 2009*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44702-4_4

Cole A. (2016, Oct 1). Open-Air Biowarfare Testing and the Evolution of Values. *Health Security, Vol. 14, No. 5*. Recuperado: https://doi.org/10.1089/hs.2016.0040

Col. Qiao L. y Col. Wang X. (1999). *Unrestricted Warface*. Beijing: China's people's liberation army.

Comisión Bicameral De Fiscalización De Los Organismos Y Actividades De Inteligencia (2021). Informe comisión bicameral de fiscalización de los organismos y actividades de inteligencia - espionaje ilegal 2016-2019. *Honorable Senado de la Nación Argentina*. recuperado: https://www4.hcdn.gob.ar/comisiones/especiales/cbinteligencia/Informe%20Comision%20Bicameral%20Inteligencia%202021-04-20.pdf

Committee on Homeland Security (2017, Oct 12). Empty threat or serious danger: assessing north Korea's risk to the homeland." *U.S. House of Representatives*. Recuperado: https://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-PryP-20171012.pdf

Committee on Veterans' Affairs (2002, Oct 9). Military Operations Aspects of Shad and Project 112. *House of Representatives*. Recuperado: https://www.health.mil/Reference-Center/Publications/2002/10/09/Military-Operations-Aspects-of-SHAD-and-Project-112

Computer History Museum (s.f.). Artifact Details. EDVAC Exhibit [Fotografía]. Recuperado: https://www.computerhistory.org/collections/catalog/102689071

Computer Museum of America (2020, Sept 18). Enigma Machine Exhibit Unveiled [Fotografía]. Recuperado: https://www.computermuseumofamerica.org/2020/09/18/enigma-machine-exhibit-unveiled/

CONADEP (1984). Nunca más: informe de la Comisión Nacional sobre la Desaparición de Personas. Recuperado: http://www.derechoshumanos.net/lesahumanidad/informes/argentina/informe-de-la-CONADEP-Nunca-mas-Indice.htm

Constantin L. (2015, Mar 9). Cyberespionage arsenal could be tied to French intelligence. *Computer World*. Recuperado: https://www.computerworld.com/article/2894379/cyberespionage-arsenal-could-be-tied-to-french-intelligence.html

Cooney M. (2015, Sep 22). CIA details agency's new digital and cyber espionage focus. *Network World*. Recuperado: https://www.networkworld.com/article/2985246/cia-details-agency-s-new-digital-and-cyber-espionage-focus.html

Copes J. (s.f.). HEXAGON KH-9 Reconnaissance Satellite [Fotografía]. National Museum of USA Air Force. Recuperado: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/195921/hexagon-kh-9-reconnaissance-satellite/hexagon-kh-9-reconnaissance-satellite/

Corbin J. (2019, Oct 2). Especial BBC | Jamal Khashoggi: qué dicen las grabaciones secretas del asesinato del periodista disidente en el consulado de Arabia Saudita. *BBC News*. Recuperado: https://bbc.com/mundo/noticias-internacional-49892850

Coulthart R. (2008, Jul 6). The Secret Test. *Sunday program*. Recuperado: https://web.archive.org/web/20080708071816/http://sunday.ninemsn.com.au/sunda

y/cover_stories/article_2503.asp vinculado: https://web.archive.org/web/20080721031009/http://sunday.ninemsn.com.au/sunday/feature_stories/article_2504.asp vinculado: https://web.archive.org/web/20080721031935/http://sunday.ninemsn.com.au/sunday/feature_stories/article_2505.asp

Cox J. (2017, Aprl 8). They are Back: The Shadow Brokers Release More Alleged Exploits. *Motherboard*. Recuperado: https://www.vice.com/en/article/5387an/theyre-back-the-shadow-brokers-release-more-alleged-exploits

Cox S. (2021, Jan 7). H-057-2: I-400 and Operation Cherry Blossoms at Night: Japanese Plan for Biological Warfare – September 1945. *Naval History and Heritage Command*. Recuperado: https://www.history.navy.mil/about-us/leadership/director/directors-corner/h-grams/h-gram-057/h-057-2.html

Crypto Museum (s.f.). Operation Rubicon: The secret purchase of Crypto AG by BND and CIA. *Crypto Museum*. Recuperado: el 21 junio 2022 de https://www.cryptomuseum.com/intel/cia/rubicon.htm

Crypto Museum (s.f.). The Thing: Great Seal Bug. *Crypto Museum*. Recuperado: el 17 octubre 2021 de https://www.cryptomuseum.com/covert/bugs/thing/index.htm

Crypto Museum (s.f.). Enigma: Enigma cipher machines. *Crypto Museum*. Recuperado: el 17 octubre 2021 de https://www.cryptomuseum.com/crypto/enigma/

Crypto Museum (s.f.). How does an Enigma machine work? *Crypto Museum*. Recuperado: https://www.cryptomuseum.com/crypto/enigma/working.htm

Crypto Museum (s.f.). Enigma wiring. *Crypto Museum*. Recuperado: https://www.cryptomuseum.com/crypto/enigma/wiring.htm

Crypto Museum (s.f.). SIGABA ECM II: Electric cipher machine (ECM) Mark II. *Crypto Museum*. Recuperado: el 17 octubre 2021 de https://www.cryptomuseum.com/crypto/usa/sigaba/index.htm

Crypto Museum (s.f.). Typex BID/08/02 /03: Wheel-based cipher machine. *Crypto Museum*. Recuperado: el 17 octubre 2021 de https://www.cryptomuseum.com/crypto/uk/typex/index.htm

C-SPAN [American History TV] (1975, Sep 16) Church Committee Hearings CIA William Colby 1975 [Video]. https://www.c-span.org/video/?409091-1/william-colby-church-committee-hearing

Cubeddu G. (2005). Nuclear weapons are immoral. *30Days in the Church and in the world's publications*. Recuperado: http://www.30giorni.it/articoli_id_9590_l3.htm

Culliford E. (2022, Feb 28). Facebook owner Meta will block access to Russia's RT, Sputnik in EU. *Reuters*. Recuperado: https://www.reuters.com/business/media-telecom/facebook-owner-meta-will-block-access-russias-rt-sputnik-eu-2022-02-28/

Cumming-Bruce N. (2020, Jul 9). The Killing of Qassim Suleimani Was Unlawful, Says U.N. Expert: The United States Provided No Evidence that Its Fatal January Drone Strike against General Suleimani Was in Response to an Imminent Threat, Said a United Nations Special Rapporteur. *New York Times*. Recuperado: https://www.nytimes.com/2020/07/09/world/middleeast/qassim-suleimani-killing-unlawful.html

Cunningham C. (2020). *Cyber warfare - Truth, tactics, and strategies.* UK, Birmingham: Packt Ltd.

Cylance (s.f.). Operation Cleaver. *Cylance*. Recuperado: https://web.archive.org/web/20150108041942/http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf

Daily Mail (2022, Sep. 29). *We will bring an end to it': Joe Biden warns Putin about Nord Stream 2 (February '22)* [Video]. Youtube. Recuperado: https://www.youtube.com/watch?v=B8BygV2kZBU

Danchev D. (2008, Aug 11). Coordinated Russia vs Georgia cyber-attack in progress. *ZDNET*. Recuperado: https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/

Daniels J. (2018, Feb 14). It is not just lizards in Iran - squirrels, cats, dolphins have also been tagged as ‘spies’ over the years. *CNBC*. Recuperado: https://www.cnbc.com/2018/02/14/its-not-just-lizards-in-iran--other-creatures-tagged-as-spies.html

Daugherty W. (2006). *Executive Secrets: Covert Action and the Presidency*. USA, Kentucky: The University press of Kentucky.

Davidovsky S. (2017, Aug 7). 25 de mayo: el pueblo al que le robaron $ 3,5 millones con un aviso en Google. *La nación*. Recuperado: https://www.lanacion.com.ar/tecnologia/25-de-mayo-el-pueblo-al-que-le-robaron-35-millones-con-un-aviso-en-google-nid2050082/

Davies H., Ganguly M. (2023, Aprl 11). Up to 50 UK special forces present in Ukraine this year, US leak suggests. *The Guardian*. Recuperado: https://www.theguardian.com/uk-news/2023/apr/11/up-to-50-uk-special-forces-present-in-ukraine-this-year-us-leak-suggests

Day D. (11 de Mar de 2013). The Lion and the Vortex. *The Space Review*. Recuperado: http://www.thespacereview.com/article/2258/1

De León P. (2015). *El Proyecto del misil Cóndor. Su origen, desarrollo y cancelación.* Universidad de San Andrés. Recuperado: https://repositorio.udesa.edu.ar/jspui/bitstream/10908/10945/1/%5BP%5D%5BW%5D%20T.%20D.%20His.%20Le%C3%B3n%2C%20Pablo%20Gabriel%20de.pdf

De León P. (2017). *El Proyecto del misil Cóndor. Su origen, desarrollo y cancelación.* Argentina, Buenos Aires: Lenguaje Claro.

De Miguel R. (2018, Septiembre 6). Reino Unido acusa a dos rusos del envenenamiento del exespía Skripal y su hija. *El País*. Recuperado: https://elpais.com/internacional/2018/09/05/actualidad/1536142407_528607.html

Defense Technical Information Center (1985, Sept 1). Operation HARDTACK - Project 8.2 - Thermal Radiation from High-Altitude Bursts. *AIR FORCE CAMBRIDGE RESEARCH LABS HANSCOM AFB MA*. Recuperado: https://apps.dtic.mil/sti/citations/ADA995390

Defense Technical Information Center (1962, Aug 1). STARFISH PRIME (Sanitized Version). *STANFORD RESEARCH INST MENLO PARK CA*. Recuperado: https://apps.dtic.mil/sti/citations/tr/ADA955694

Defence Select Committee (2006, Jan 20). Possible Constraints on future UK decision-making on any replacement for Trident. UK Parliament. Recuperado: https://publications.parliament.uk/pa/cm200506/cmselect/cmdfence/835/835m03.htm

Department of Defense (2003, Oct 30). *Information Operations Roadmap*. Recuperado: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/Information_Operations_Roadmap_30_October_2003.pdf

Department of State (s.f.). Foreign relations of the United States, 1952–1954, National Security Affairs, Volume II, Part 2: Memorandum by the Special Assistant to the Secretary of State for Atomic Energy Affairs (Arneson). *Office of the Historian*. Recuperado: https://history.state.gov/historicaldocuments/frus1952-54v02p2/d124

Department of State (s.f.). Oil Embargo, 1973–1974. *Office of the Historian*. Recuperado: https://history.state.gov/milestones/1969-1976/oil-embargo

Department of the Army (2005, April). *FM 3-05.30. Psychological Operations*. Recuperado: https://irp.fas.org/doddir/army/fm3-05-30.pdf

Department of the Army (2006). *FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations*. Recuperado: https://irp.fas.org/doddir/army/fm2-22-3.pdf

Department of the Army USA (1977, Feb 24). *U.S. Army activity in the U.S. Biological warfare programs*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB58/RNCBW_USABWP.pdf

Der Veen V., Fratantonio Y., Lindorfer M., Gruss D., Maurice C., Vigna G., Bos H., Razavi K., Giuffrida C. (2016). Drammer: Deterministic Rowhammer Attacks on Mobile Platforms. *CCS'16, October 24–28, 2016, Vienna, Austria*. Recuperado: http://dx.doi.org/10.1145/2976749.2978406

Designers for Palestine (2022, Mar 19). *When will Palestinians have the same right to self-defense that the US defends in #Ukraine?* [Facebook]. Recuperado: https://www.facebook.com/DesignersForPalestine/photos/a.728954683781943/5529107303766633/

Deutsche Welle [Documentales TC]. (2019, Jul 24). China La vigilancia absoluta DW Documental [Video]. https://www.youtube.com/watch?v=nl3bjvkJjT4

Dilanian K. (2020, Jan 3). Was it legal for Donald Trump to order the killing of a top Iranian general? *NBC News*. Recuperado: https://www.nbcnews.com/news/world/was-it-legal-donald-trump-order-killing-top-iranian-general-n1109961

Dilanian K., Kube C., Lee C. (2022, May 5). U.S. intel helped Ukraine sink Russian flagship Moskva, officials say. *NBC News*. Recuperado: https://www.nbcnews.com/politics/national-security/us-intel-helped-ukraine-sink-russian-flagship-moskva-officials-say-rcna27559

Director of National Intelligence (s.f.). *Five-eyes-banner.jpg* [Imagen]. Recuperado: https://www.dni.gov/files/ICIG/Images/five-eyes-banner.jpg

Director of National Intelligence (s.f.). Five Eyes Intelligence Oversight and Review Council (FIORC). *The National Counterintelligence and Security Center*. Recuperado: https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc

Dolak K. (2021, Feb 11). What Really Happened During the Deadly Raid at Black Panther Party Leader Fred Hampton's Home? *Oxygen True Crime*. Recuperado: https://www.oxygen.com/true-crime-buzz/what-really-happened-in-deadly-raid-on-fred-hamptons-home

Donnelly E. (2023, Jan 8). LNG fever: European firms sign mega-contracts as US shale gas imports boom. *Investigate Europe*. Recuperado: https://www.investigate-europe.eu/posts/lng-fever-mega-contracts-shale-gas-imports-us

Donoso F. (2017, Sep 22). DanderSpritz: *How the Equation Group's 2013 tools still pawn in 2017* [Video]. Conferencia Derbycon Legacy VII, Lousville, Kentucky, USA. Recuperado: https://www.youtube.com/watch?v=Zqw-T1YQKUQ&t=328s. Diapositivas: https://speakerdeck.com/francisck/danderspritz-how-the-equation-groups-2013-tools-still-pwn-in-2017

Dorfman Z., Naylor S. y Isikoff M. (2021, Sep 26). Kidnapping, assassination, and a London shoot-out: Inside the CIA's secret war plans against WikiLeaks. *Yahoo News*. Recuperado: https://news.yahoo.com/kidnapping-assassination-and-a-london-shoot-out-inside-the-ci-as-secret-war-plans-against-wiki-leaks-090057786.html

Dowson H. (s.f.). Declassified British Documents Reveal U.K. Support for Indonesian Invasion and Occupation of East Timor, Recognition of Denial of Self-Determination, 1975-1976. *The National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB174

Duffin A. (s.f.). 'Bat Bombs': WWII's Project X-Ray. *Warfare History Network.* Recuperado el 30 de junio del 2022 en: https://warfarehistorynetwork.com/bat-bombs-wwiis-project-x-ray/

Duffy D. (2017). *The secret Codebreakers of central Bureau*. UK, London: Scribe.

DW (2005, Aug 29). Identifican restos de monja francesa desaparecida en Argentina. *Deutsche Welle*. Recuperado: https://www.dw.com/es/identifican-restos-de-monja-francesa-desaparecida-en-argentina/a-1694461

DW News (2022, Sept 27). *Potential sabotage: What is behind the Nord Stream pipeline leaks? | DW News* [Vídeo]. Youtube. Recuperado: https://www.youtube.com/watch?v=ShXmPA21j-E

DW News (2023, Jul 23). *Who sabotaged the Nord Stream pipeline? | DW Analysis* [Video]. YouTube. Recuperado: https://www.youtube.com/watch?v=KqsX3jjQ2_U

ECA Group (s.f.). *Mini UAV for Image intelligence SIGINT / IMINT missions.* Recuperado: https://www.ecagroup.com/en/solutions/mini-uav-image-intelligence-sigint-imint-missions

Eck W. (1985). Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? Elsevier Science Publishers B.V. (North-Holland), Computers & Security 4, p269-286. Recuperado: http://www.tscm.com/vaneck85.pdf

Eisele I. (2022, March 1). Fact checks: Ukraine's 'Ghost of Kyiv' fighter pilot. *DW.* Recuperado: https://www.dw.com/en/fact-check-ukraines-ghost-of-kyiv-fighter-pilot/a-60951825

Ejército Argentino (1977). RC-9-1 Operaciones contra elementos subversivos. Argentina: Instituto Geográfico Militar. Recuperado: https://www.mpf.gob.ar/plan-condor/files/2018/12/16-1.pdf

El Machete (2014, Aug 20). Secure list by Kaspersky. Recuperado: https://securelist.com/el-machete/66108/

El Machete's Malware Attacks Cut Through LATAM (2017, Mar 22). BlackBerry Threat Vector Blog. Recuperado: https://blogs.blackberry.com/en/2017/03/el-machete-malware-attacks-cut-through-latam

Electronic Frontier Foundation (s.f.). Narus Surveillance Equipment Installed in Secret Room. *EFF*. Recuperado: https://www.eff.org/es/node/72381

Electronic Frontier Foundation (s.f.). NSA Spying. *EFF*. Recuperado: https://www.eff.org/nsa-spying.

Electronic Frontier Foundation (2015, Jan 23). Pay attention to that man behind the curtain: Discovering aliens on CNE infrastructure. *EFF*. Recuperado: https://www.eff.org/files/2015/01/23/20150117-speigel-csec_document_on_the_handling_of_existing_trojans_when_trojanizing_computers.pdf

Electronic Frontier Foundation (2014, Jun 23). 20140618-Dagbladet-RAMPART-A Overview. *EFF*. Recuperado: https://www.eff.org/files/2014/06/23/rampart-a_overview.pdf

Electrospaces (2013, Oct 31). How NSA targeted chancellor Merkel's mobile phone. *Electrospaces*. Recuperado: https://www.electrospaces.net/2013/10/how-nsa-targeted-chancellor-merkels.html

Electrospaces (2013, Jul 7). New insights into the PRISM program. *Electrospaces*. Recuperado: https://www.electrospaces.net/2013/07/new-insights-into-prism-program.html

Electrospaces (2014, Nov 29). INCENSER, or how NSA and GCHQ are tapping internet cables. *Electrospaces*. Recuperado: https://www.electrospaces.net/2014/11/incenser-or-how-nsa-and-gchq-are.html

Electrospaces (2014, Oct 15). The German operation Eikonal as part of NSA's RAMPART-A program. *Electrospaces*. Recuperado: https://www.electrospaces.net/2014/10/the-german-operation-eikonal-as-part-of.html

Electrospaces (2015, May 28). New details about the joint NSA-BND operation Eikonal. *Electrospaces*. Recuperado: https://www.electrospaces.net/2015/05/new-details-about-joint-nsa-bnd.html

Electrospaces (2016, Sep 22). Secret report reveals: German BND also uses XKEYSCORE for data collection. *Electrospaces*. Recuperado: https://www.electrospaces.net/2016/09/

Erskine R. (1999). The Holden agreement on naval Sigint: The first BRUSA? *Intelligence and National Security*, vol 14 number 2, pp.187-197.

Ermolov M., Goryachy M. [Black Hat]. (2020, Jan 8). *How to Hack a Turned-Off Computer or Running Unsigned Code in Intel Management Engine* [Video]. Youtube. Recuperado: https://www.youtube.com/watch?v=9fhNokIgBMU

Eset (2019, Jul). *ESET Research White papers. Machete just got sharpen. Venezuelan government institutions under attack. How spies managed to steal gigabytes of confidential data over the course of a year*. Recuperado: https://www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

Espinosa A. (2019, Sep 14). Arabia Saudí interrumpe la mitad de su producción de crudo tras un ataque con drones. *El País*. Recuperado: https://elpais.com/internacional/2019/09/14/actualidad/1568456455_053067.html

ESPN (2022, Feb 27). Federaciones que han apartado a Rusia de sus competiciones por invasión militar a Ucrania. Entertainment and Sports Programming Network. Recuperado: https://www.espn.com.ar/otros-deportes/nota/_/id/9998014/guerra-rusia-ucrania-eventos-deportivos-cancelados-federaciones-coi-fifa-fina-f1

European Commision (2022, Mar 2). Ukraine: EU agrees to exclude key Russian banks from SWIFT. *Directorate-General for Communication*. Recuperado: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1484

Swift (2022, Mar 20). An update to our message for the Swift Community. Recuperado: https://www.swift.com/about-us/discover-swift

EUR-Lex (2022, Feb 28). Document 32022R0336. Recuperado: http://data.europa.eu/eli/reg_impl/2022/336/oj

European Council (2023, Sep 14). EU restrictive measures against Russia over Ukraine (since 2014). *Council of the European Union*. Recuperado: https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/

European Court of Human Rights (2012, Dic 13). Case of EL-MASRI v. The Former Yugoslav Republic of Macedonia. Recuperado: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-115621%22]}

European Parliamentary Reserch Service (2014, Nov). The ECHELON Affair - The EP and the global interception system 1998 - 2002. European Parliament. Recuperado:

https://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf

European Space Agency (2020, Mar 30). Type of orbits. *ESA* Recuperado: https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits

Fassihi F. y Bergman R. (2022, May 25). Israel Tells U.S. It Killed Iranian Officer, Official Says. *The New York Times*. Recuperado: https://www.nytimes.com/2022/05/25/world/middleeast/iran-israel-killing-khodayee.html

Federal Bureau of Investigation (s.f.). John Winston Lennon. *FBI Records*. Recuperado: https://vault.fbi.gov/john-winston-lennon

Federal Bureau of Investigation (2014, Dec 19). Update on Sony Investigation. *FBI News*. Recuperado: https://www.fbi.gov/news/press-releases/update-on-sony-investigation

Fenton B. (2003, Sep 27). Macmillan backed Syria assassination plot. *The Guardian*. Recuperado: https://www.theguardian.com/politics/2003/sep/27/uk.syria1

Ferguson S. (2019, Jun 17). Xenotime Group Sets Sights on Electrical Power Plants. *Data Breach Today*. Recuperado: https://www.databreachtoday.com/xenotime-group-sets-sights-on-electrical-power-plants-a-12637

Fernández Y. (2016, Agosto 15). *Cuando una imagen oculta más información de lo que parece: qué es y cómo funciona la esteganografía*. Xataka. Recuperado: https://www.xataka.com/historia-tecnologica/cuando-una-imagen-oculta-mas-informacion-de-lo-que-parece-que-es-y-como-funciona-la-esteganografia

Filiol E. (2005). *Computer viruses: from theory to applications*. Germany, Berlin: Springer.

Finfisher (2014). Finfly ISP [Folleto]. *Wikileaks*. Recuperado: https://wikileaks.org/spyfiles4/documents/FinFly-ISP-Catalog.pdf

Finkle J. (2016, Dec 1). Shamoon virus returns in new Saudi attacks after 4-year hiatus. *Reuters*. Recuperado: https://www.reuters.com/article/cyber-saudi-shamoon-idUSL1N1DW05H

Finkle J. y Shalal-Esa A. (2011, May 27). Exclusive: Hackers breached U.S. defense contractors. *Reuters*. Recuperado: https://www.reuters.com/article/us-usa-defense-hackers-idUSTRE74Q6VY20110527

FireEye (2020, Dec 13). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor. *Mandiant*. Recuperado: https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

FireEye Intelligence (2018, Oct 23). TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. *Mandiant*. Recuperado: https://www.mandiant.com/resources/blog/triton-attribution-russian-government-owned-lab-most-likely-built-tools

Fischer L. (2012). *The Essential Gandhi: An Anthology of His Writings on His Life, Work, and Ideas*. USA, NY: Vintage.

Fisher M. (2013). Photos from Guantanamo's force-feeding facilities. *Washington Post*. Recuperado: https://www.washingtonpost.com/news/worldviews/wp/2013/05/10/photos-from-guantanamos-force-feeding-facilities/

Follorou J. (2016, Sep 3). Les Etats-Unis ont bien piraté l'Elysée en 2012. *Le Monde*. Recuperado: https://www.lemonde.fr/pixels/article/2016/09/03/les-etats-unis-ont-bien-pirate-l-elysee-en-2012_4991960_4408996.html

Follorou J., Untersinger M. (2014, May 19). La France suspectée de cyberespionnage. *Le Monde*. Recuperado: https://www.lemonde.fr/international/article/2014/03/21/la-france-suspectee-de-cyberattaque_4387232_3210.html

Follows, S. (2018). Who are the most prolific people working in Hollywood? Recuperado: https://stephenfollows.com/who-are-the-most-prolific-people-working-in-hollywood/

Folz N. (2022, Feb 23). Video von spektakulärem Unfall bei Saarstahl in Völklingen trendet im Netz. Saarbruecker Zeitung. Recuperado: https://www.saarbruecker-zeitung.de/saarland/saarbruecken/voelklingen/video-von-spektakulaerem-unfall-bei-saarstahl-trendet-auf-reddit-unternehmen-aeussert-sich_aid-66347689

Ford M. (2016). *El auge de los robots: La tecnología y la amenaza de un futuro sin empleo*. España, Barcelona: Paidós.

Foucault M. (1975). *Surveiller et punir*. France: Gallimard.

Foucault M. (1989). *Vigilar y castigar: nacimiento de la prisión*. Argentina, Buenos Aires: Siglo XXI.

Fox News (2015, Dec 20). NSA Director: China can damage US power grid. *Fox News*. Recuperado: https://www.foxnews.com/politics/nsadirector-china-can-damage-us-power-grid

Fürstenau M. (2021, Jul 02). Caso Assange: el testigo clave del FBI admite falso testimonio. *DW*. Recuperado: https://www.dw.com/es/caso-assange-el-testigo-clave-del-fbi-admite-falso-testimonio/a-58142641

Galeotti M. (2013, Feb 17). The 'Gerasimov Doctrine' and Russian Non-Linear War. *In Moscow's Shadows*. Recuperado: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Gafford R. (1958). The Operational Potential of Subliminal Perception. *Estudies in Intelligence*, vol. 2 Issue Spring. Recuperado: https://www.cia.gov/readingroom/docs/DOC_0000606555.pdf

Gallagher R., Moltke H. (2016, Nov 16). TITANPOINTE: The NSA's Spy Hub in New York, Hidden in Plain Sight. *The Intercept*. Recuperado: https://theintercept.com/2016/11/16/the-nsas-spy-hub-in-new-york-hidden-in-plain-sight/

Gallagher H. (1985). *FDR's Splendid Deception*. USA, NY: Dodd Mead.

Gallagher T. (2002). *Assault in Norway: Sabotaging the Nazi Nuclear Program*. USA, Guilford, Connecticut: Lyons Press.

Ganser D. (2004). *NATO's Secret Armies: Operation Gladio and Terrorism in Western Europe*. London, NY: Frank Cass.

Ganser D. (2007, Jan 24). The CIA in Western Europe and the abuse of human rights. *Intelligence and National Security Volume 21, 2006 - Issue 5*. Recuperado: https://doi.org/10.1080/02684520600957712

García A. (2021, Jun 8). Filtrada la mayor recopilación de contraseñas hackeadas de la historia. *Adslzone*. Recuperado: https://www.adslzone.net/noticias/seguridad/rockyou2021-filtracion-contrasenas/

Garmelo J. (1892). *Primer Homenaje a Colón*. Madrid: Museo Naval.

GCHQ (s.f.). Bletchley Park & WWII [Fotografía]. Recuperado: https://www.gchq.gov.uk/section/history/bletchley-park-and-wwii

Geist A., Gjerding S., Moltke H. (2014, Jun 19). NSA 'third party' partners tap the Internet backbone in global surveillance program. *Dagbladet Information*. Recuperado: https://www.information.dk/udland/2014/06/nsa-third-party-partners-tap-the-internet-backbone-in-global-surveillance-program

Gellman B., Poitras L. (2013, Jun 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *Washington Post*. Recuperado: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gellman B., Soltani A. (2013, Oct 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Recuperado: https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Gerstein J. (2020, Sep 2). Court rules NSA phone snooping illegal — after 7-year delay. *Político*. Recuperado: https://www.politico.com/news/2020/09/02/court-rules-nsa-phone-snooping-illegal-407727

Ghose T. (2018, Feb 13). No, Iran, Lizard 'Spies' Can't Detect Uranium. *Live Science*. Recuperado: https://www.livescience.com/61746-lizard-spies-skin-cannot-detect-radioactivity.html

Gibbs S. (2017, Dec 15). Triton: hackers take out safety systems in 'watershed' attack on energy plant. *The Guardian*. Recuperado: https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant

Glaser A. (2014, Jan 30). After NSA Backdoors, Security Experts Leave RSA for a Conference They Can Trust. *Electronic Frontier Foundation*. Recuperado: https://www.eff.org/deeplinks/2014/01/after-nsa-backdoors-security-experts-leave-rsa-conference-they-can-trust

Glazova J. (2022, Jul 29). CosmicStrand: un rootkit UEFI. *Kaspersky Daily*. Recuperado: https://www.kaspersky.es/blog/cosmicstrand-uefi-rootkit/27453/

Glüsing J., Poitras L., Rosenbach M., Stark H. (2013, Oct 20). NSA Accessed Mexican President's Email. *Spiegel*. Recuperado: https://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

Goldberg S. (2017, Jun22). Surveillance without Borders: The "Traffic Shaping" Loophole and Why It Matters. *The Century Foundation*. Recuperado: https://tcf.org/content/report/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters/

Goldman J. (2014, Dec 29). Cyber Attack Causes Physical Damage at German Iron Plant. *eSecurity Planet*. Recuperado: https://www.esecurityplanet.com/networks/cyber-attack-causes-physical-damage-at-german-iron-plant/

Gómez J. (2014, Septiembre 28). Michael Harari, oficial del Mossad. *El País*. Recuperado: https://elpais.com/internacional/2014/09/29/actualidad/1411942654_124862.html

Gorman S., Dreazen Y. y Cole A. (2009, Dec 17). Insurgents Hack U.S. Drones. *The Wall Street Journal*. Recuperado: https://www.wsj.com/articles/SB126102247889095011

Gostev A. (2012, May 28). The Flame: Questions and Answers. *Secure List*. Recuperado: https://securelist.com/the-flame-questions-and-answers/34344/

Graham B. (2004, Aprl 14). Pentagon Crash Scenario Was Rejected for Military Exercise. *Washington Post*. Recuperado: https://www.washingtonpost.com/archive/politics/2004/04/14/pentagon-crash-scenario-was-rejected-for-military-exercise/38cdf357-dcc6-487a-a3ab-7e8a063c3096/

Graham W. (2013, Dec 5). USA-247 reconnaissance satellite patch. *NASA Space Flight*. Recuperado: https://www.nasaspaceflight.com/2013/12/atlas-v-launch-nrol-39-vandenberg/

Greenberg A. (2015, Jun 24). With its French NSA Leak, Wikileaks if back. *Wired*. Recuperado: https://www.wired.com/2015/06/french-nsa-leak-wikileaks-back/

Greenberg A. (2015, Jul 21). Hackers Remotely Kill a Jeep on the Highway—With Me in I. *Wired*. Recuperado: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Greenberg A. (2017, Jun 12). 'Crash Override': The Malware That Took Down a Power Grid. *Wired*. Recuperado: https://www.wired.com/story/crash-override-malware/

Greenberg A. (2017, Jun 20). How an Entire Nation Became Russia's Test Lab for Cyberwar. *Wired*. Recuperado: https://www.wired.com/story/russian-hackers-attack-ukraine/

Greenberg A. (2019). *Sandworm: A new era of cyberwar and the hunt for the kremlin's most dangerous hackers.* USA, NY: Doubleday.

Greenberg A. (2019, April 10). A Peek into the Toolkit of the Dangerous Triton Hackers. *Wired*. Recuperado: https://www.wired.com/story/triton-hacker-toolkit-fireeye/

Greenwald G (2013, Jul 15). The crux of the NSA story in one phrase: 'collect it all'. *The Guardian*. Recuperado: https://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all

Greenwald G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. USA, New York: Metropolitan Books. (Documents: http://glenngreenwald.net/#BookDocuments)

Greenwald G. (2015, Feb 4). Western spy agencies secretly rely on hackers for intel and expertise. *The Intercept*. Recuperado: https://theintercept.com/2015/02/04/demonize-prosecute-hackers-nsa-gchq-rely-intel-expertise/

Gretchen V. (2004, Nov 19). WHO Gives a Cautious Green Light to Smallpox Experiments. *Science*. Recuperado: https://www.science.org/doi/10.1126/science.306.5700.1270a

Grez M. (2022, Mar 1). Estos son los deportes de los que Rusia ha sido suspendido. *CNN Español*. Recuperado: https://cnnespanol.cnn.com/2022/03/01/deportes-de-los-que-rusia-ha-sido-suspendido-trax/

Guarnieri C., Gallagher R. (2014, Nov 24). Secret malware in European Union Attack linked to US and British Intelligence. *The Intercept*. Recuperado: https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/

Gunter K. (s.f.). Nemesis 1, 2 (PAN, CLIO / P360). *Gunter's Space Page*. Recuperado el 1 septiembre del 2023 en https://space.skyrocket.de/doc_sdat/nemesis-1.htm

Hadnagy C. (2018). *Social engineering: The science of human hacking.* USA, Indianapolis: John Willey & Sons Inc.

Hak5 (s.f.). *Bash Bunny* [Fotografía]. Hack5. Recuperado: https://shop.hak5.org/products/bash-bunny

Hak5 (s.f.). *USB Rubber Duck* [Fotografía]. Hack5. Recuperado: https://shop.hak5.org/products/usb-rubber-ducky

Hak5 (s.f.). *WIFI Pineapple* [Fotografía]. Hack5. Recuperado: https://shop.hak5.org/products/wifi-pineapple

Han B. (2014). *Psicopolítica*. España, Barcelona: Herder Editorial, S.L.

Han B. (2014). *Sobre el poder*. España, Barcelona: Herder Editorial, S.L.

Harán J. (2019, May 13). Vulnerabilidad en WhatsApp permite instalar spyware en teléfonos con solo realizar una llamada. *We Live Security by Eset*. Recuperado: https://www.welivesecurity.com/la-es/2019/05/14/vulnerabilidad-whatsapp-permite-instalar-spyware-pegasus/

Harper L. (2013, Oct 11). The cat's out of the bag, so declassify it already. *Unredacted*. Recuperado: https://unredacted.com/2013/10/11/the-cats-out-of-the-bag-so-declassify-it-already/

Harris P. (2010). This article is more than 12 years old CIA's secret Iraq weapon revealed: a Saddam gay sex tape. *The Guardian*. Recuperado: https://www.theguardian.com/world/2010/may/26/cia-saddam-hussein-gay-sex-smear-plot

Harris S. y Maimí F. (2019). *CISSP® All in one* (8va edition). USA: McGraw Hill-Education.

Headquarters United States Air Force (1997, Jun 25). The Roswell report: case closed. *United States Air Force*. Recuperado: https://media.defense.gov/2010/Oct/27/2001330219/-1/-1/0/AFD-101027-030.pdf

Herling J., Wolfgang B. (2010, Oct 13). Advanced self-contained object removal for realizing real-time diminished reality in unconstrained environments. *2010 IEEE International Symposium on Mixed and Augmented Reality* p. 207-212.

Recuperado: https://www.researchgate.net/profile/Wolfgang-Broll-2/publication/224197761_Advanced_self-contained_object_removal_for_realizing_real-time_Diminished_Reality_in_unconstrained_environments/links/0c9605360f714d5261000000/Advanced-self-contained-object-removal-for-realizing-real-time-Diminished-Reality-in-unconstrained-environments.pdf

Hern A. (2018, Sun 28). Fitness tracking app Strava gives away location of secret US army bases. *The Guardian*. Recuperado: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Hernández Sampieri H. (2014). *Metodología de la investigación* (6ta edición). México, D.F.: McGraw Hill Education.

Higham N. (2015, Sep 30). Drawings of WW2 exploding chocolate bar bombs discovered. *BBC News*. Recuperado: https://www.bbc.com/news/av/uk-34399018

Hitchens C. (2001). *The Trial of Henry Kissinger*. USA: Verso.

Hogan M. (2013, Jun 24). Was Michael Hastings' Car Hacked? Richard Clarke Says It is Possible. *The Huffington Post*. Recuperado: https://www.huffpost.com/entry/michael-hastings-car-hacked_n_3492339huffpost

Hodfson Q. Shokh Y., Balk J. (2022). Many Hands in the cookie Jar. *RAND Corporation*. Recuperado: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1100/RRA1190-1/RAND_RRA1190-1.pdf

Hodge R. (2020, Aug 12). What is Kape Technologies? What you need to know about the parent company of CyberGhost VPN. *CNET*. Recuperado: https://www.cnet.com/tech/services-and-software/what-is-kape-technologies-what-you-need-to-know-about-the-parent-company-of-cyberghost-vpn/

Homakov E. (2015, May 21). Hacking Starbucks for unlimited coffee. *Sakurity*. Recuperado: http://sakurity.com/blog/2015/05/21/starbucks.html

Hosmer S. (1996). *Psychological Effects of U.S. Air Operations in four wars 1941-1991: Lessons for U.S. commanders*. United States, California: RAND. Recuperado: https://apps.dtic.mil/sti/pdfs/ADA307075.pdf

Howard M., Pincus J., Wing J. (2003). Measuring Relative Attack Surfaces. *School of Computer Science, Carnegie Mellon University*. Recuperado: https://www.cs.cmu.edu/~wing/publications/Howard-Wing03.pdf

Hu J., Li R., Tang C. (2017). A Real-time Inversion Attack on the GMR-2 Cipher Used in the Satellite Phones. *National University of Defense Technology, China.* Recuperado: https://eprint.iacr.org/2017/655.pdf

Huston G. (2020, Feb 12). At the bottom of the sea: a short history of submarine cables. *APNIC*. Recuperado: https://blog.apnic.net/2020/02/12/at-the-bottom-of-the-sea-a-short-history-of-submarine-cables/

Hutchins E., Cloppert M., Amin R. (2011, Jan). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Lockheed Martin*. Recuperado: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Illinger P. (2010, May 17). Wie entdeckt man gute Forscher? *Sueddeutsche Zeitung*. Recuperado: http://www.sueddeutsche.de/wissen/karl-heinz-beckurts-stiftung-wie-entdeckt-man-gute-forscher-1.352464

Informe Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia (2021). Espionaje ilegal 2016-2019. Argentina, BA: C.B.I. Recuperado: https://www4.hcdn.gob.ar/comisiones/especiales/cbinteligencia/Informe%20Comision%20Bicameral%20Inteligencia%202021-04-20.pdf

Ingreson G. (2012, Sep 24). Iranians Discovered a Fake Rock Spy Device, Which Exploded When They Tried to Move It. *Business Insider*. Recuperado: https://www.businessinsider.com/iranians-discover-a-fake-rock-spy-device-2012-9

Intel (2018, Jan 25). Intel® Active Management Technology (Intel® AMT) Technical Advisory. *Intel*. Recuperado: https://www.intel.com/content/dam/support/us/en/documents/technologies/amt_technical_advisory_usb_provisioning_non_nda.pdf

Intercept Monitoring systems (s.f.). Opto Acoustic Laser Microphone for Long Distance Audio Monitoring [Fotografía]. Recuperado el 1 de septiembre del 2022 en: https://www.intercept.ws/catalog/3710.html

International Olympic Committee (2023, Jun 27). Find Out Why South Africa Was Barred from the Olympics for 32 Years. Olympics games. Recuperado: https://olympics.com/en/news/why-south-africa-barred-from-the-olympics-apartheid

International Spy Museum (2018, March 28). From Russia with Love | A History of Poisonings. International Spy Museum Blog. Recuperado: https://blog.spymuseum.org/from-russia-with-love-a-history-of-poisonings/

Ipper G. (2003). *Investigator's Guide to Steganography*. USA, Florida: Auerbach.

Israel Military Intelligence: The Lavon Affair (s.f.). The library. https://www.jewishvirtuallibrary.org/jsource/History/lavon.html

Jacobsen A. (2014, Sept). Operation Paperclip: The Secret Intelligence Program to Bring Nazi Scientists to America - Reviewed by Jay Watkins. *Studies in Intelligence Vol. 58, No. 3*. Recuperado: https://www.cia.gov/static/Review-Operation-Paperclip.pdf

Jacobsen A. (2019). *Surprise, Kill, Vanish: The secret history of CIA paramilitary armies, operators, and assassins*. USA, NY: Little, Brown and company.

Jasper S. (2017). *Strategic cyber deterrence.* USA, NY: Rowman & Littlefield.

Jennings R. (2015, Jun 11). Hackers PWNED Kaspersky Lab servers for months -- Duqu 2.0 blamed on Israel. *ComputerWorld*. Recuperado: https://www.computerworld.com/article/2934593/duqu-2-0-kaspersky-israel-itbwcw.html

Jensen, K. (2014, Jun 19). Documentation: The Snowden files. *Dagbladet Information*. Recuperado: https://www.information.dk/databloggen/2014/06/documentation-the-snowden-files

JFCC Space photo (s.f.). Operators at the Joint Space Operations Center (JSpOC) at Vandenberg Air Force Base [Fotografía]. JFCC Space photo. Recuperado: https://media.defense.gov/2017/Apr/05/2001727285/-1/-1/0/140927-F-II211-204.JPG

Jha A. (2020). IoT Security - Part 20 (101 - Introduction to Fault Injection Attack (FI)). *Payatu*. Recuperado en: https://payatu.com/blog/asmita-jha/fault-injection-basics

Jogi B. (2022, Jan 25). PwnKit: Local Privilege Escalation Vulnerability Discovered in polkit's pkexec (CVE-2021-4034). *Qualys*. Recuperado en: https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

Johnson A. (2012, Jun 6). Flamer: Urgent Suicide. *Symantec*. Recuperado: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b17110bd-8387-4c38-b27e-7c875ca98021&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Johnson A. (2012, Aug 16). The Shamoon Attacks. *Symantec*. Recuperado: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=281521ea-2d18-4bf9-9e88-8b1dc41cfdb6

Johnson B., Caban D., Krotofil M., Scali D., Brubaker N., Glyer C. (2017, Dec 14). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. *Mediant*. Recuperado: https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton

Johnson S. (2004). *The Works of Samuel Johnson: The Adventurer and Idler*. EBook #12050. Recuperado: https://www.gutenberg.org/files/12050/12050-8.txt

Joint Chiefs of Staff (1962). *Justification for US Military Intervention in Cube (TS)*. Recuperado: https://nsarchive2.gwu.edu/news/20010430/

Joint Chiefs of Staff (1996, May 31). *Joint Publication 3-58: Joint Doctrine for Military Deception*. Recuperado: https://irp.fas.org/doddir/dod/jp3_58.pdf

Joint Chiefs of Staff (2003, Sep 5). *Joint Publication 3-53. Doctrine for Joint Psychological Operations*. Recuperado: https://irp.fas.org/doddir/dod/jp3_53.pdf / https://nsarchive2.gwu.edu/NSAEBB/NSAEBB177/02_psyop-jp-3-53.pdf

Joint Chiefs of Staff (2006, Jun 26). *Joint Publication 3-13-3.* Information *Security*. Recuperado: https://irp.fas.org/doddir/dod/jp3_13_3.pdf

Joint Chiefs of Staff (2012, Feb 8). *Joint Publication 3-13-1. Electronic Warfare*. Recuperado: https://irp.fas.org/doddir/dod/jp3-13-1.pdf

Joint Chiefs of Staff (2013, Jan 31). Joint Publication 3-60: *Joint Targeting*. Recuperado: https://www.justsecurity.org/wp-content/uploads/2015/06/Joint_Chiefs-Joint_Targeting_20130131.pdf

Joint Chiefs of Staff (2017, Feb 14). *Joint Publication 3-13.4. Military Deception*. Recuperado: https://irp.fas.org/doddir/dod/jp3_13_4.pdf

Joint Chiefs of Staff (2014, Nov 20). *Joint Publication 3-13. Information Operations*. Recuperado: https://irp.fas.org/doddir/dod/jp3_13.pdf

Joint Chiefs of Staff (2018, Jun 8). *Joint Publication 3-12. Cyberspace Operations*. Recuperado: https://irp.fas.org/doddir/dod/jp3_12.pdf

Joint Chiefs of Staff (2018, Oct 22). *Joint Publication 3-0. Joint Operations*. Recuperado: https://irp.fas.org/doddir/dod/jp3_0.pdf

Joint Chiefs of Staff (2020, Oct 26). *Joint Publication 3-14.* Space *Operations*. Recuperado: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14ch1.pdf

Joint Task Force Guantanamo (2003). *Guantanamo Standard Operating Procedures*. Recuperado: https://web.archive.org/web/20100114043336/http://www.dod.mil/pubs/foi/detainees/GITMO_MedicalSOPs.pdf

Jones N. (2010, Jul 16). Document Friday: The Poisonous Umbrella and the Assassination of Georgi Markov. *Unredacted*. Recuperado: https://unredacted.com/2010/07/16/document-friday-the-poisonous-umbrella-and-the-assassination-of-georgi-markov/

Jones, N. (2010, Aug 6). Document Friday: Sharks! (And the Military). *Unredacted*. https://unredacted.com/2010/08/06/document-friday-sharks-and-the-military/

Jones R. (2007). 1st Radio Broadcasting and Leaflet Group Conducts PSYWAR in Korea, Part II. *Veritas Journal of Army Special Operations History PB 31-05-2 Vol 3, No. 3, 2007*. Recuperado: https://arsof-history.org/articles/v3n3_ganders2_page_1.html

Joshi V. (2019, Apr 8). 'America's Hidden Stories' tackles CIA's alleged involvement in the Trans-Siberian Pipeline explosion of 1982. *Meaww*. Recuperado:

https://meaww.com/americas-hidden-stories-busting-myth-cia-involvement-trans-siberian-pipeline-explosion-1982

Kaiser J. (2014, Jul 8). Six vials of smallpox discovered in U.S. lab. *Science*. Recuperado: https://www.science.org/content/article/six-vials-smallpox-discovered-us-lab

Kan M. (2020, Jul 20). 7 VPN Services Found Recording User Logs, Despite 'No-Log' Pledge. *PC Mag*. Recuperado: https://www.pcmag.com/news/7-vpn-services-found-recording-user-logs-despite-no-log-pledge

Kaspersky (2012, Aug 9). Gauss: Nation-state cyber-surveillance meets banking Trojan. *Secure List*. Recuperado: https://securelist.com/gauss-nation-state-cyber-surveillance-meets-banking-trojan-54/33854/

Kaspersky (2018, Mar). Lazarus under the hood. *Kaspersky Lab*. Recuperado: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

Kaspersky Lab (2018, March). Gauss: Abnormal Distribution. *Kaspersky Lab Global Research and Analysis Team*. Recuperado: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134940/kaspersky-lab-gauss.pdf

Kaspersky Labs (2015, Feb 16). Equation Group: The Crown Creator of Cyber-Espionage. *Kaspersky*. Recuperado: https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage

Kaspersky Labs (2015, Feb 19). Equation Group: from Houston with love. *Secure List*. Recuperado: https://securelist.com/equation-group-from-houston-with-love/68877/

Kaspersky Labs (2018, Feb 19). Equation Group: Questions and answers. *Kaspersky*. Recuperado: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf

Katzenbeisser S., Petitcolas F. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. UK, London: Artech house.

Keizer G. (2012, May 29). Attacks on Iranian oil industry led to Flame malware find. *Computer World*. Recuperado:

https://www.computerworld.com/article/2727219/attacks-on-iranian-oil-industry-led-to-flame-malware-find.html

Keane D., Warner M. y Keefer E. (2007). *The Intelligence Community 1950–1955*. USA, Washington: US Government Printing Office. Recuperado: https://2001-2009.state.gov/documents/organization/96785.pdf

Kennerly D. (s.f.). *White House Photographs, December 6, 1975, Roll #A7504, frame 7* [Fotografía]. Wikipedia / Ford Library Museum. Recuperado: https://en.m.wikipedia.org/wiki/File:Kissinger,_Ford,_Suharto_and_Malik_%28cropped%29.jpg vinculado: https://www.fordlibrarymuseum.gov/library/whphotos/19751206whpo.pdf

Kettmann S. (2014, Mar 26). Soviets Burned by CIA Hackers? *Wired*. Recuperado: https://www.wired.com/2004/03/soviets-burned-by-cia-hackers/

Kiebler M. (2022, Nov 15). What is NATO and why was it created? *Deutsche Welle (DW)*. Recuperado: https://www.dw.com/en/what-is-nato-and-why-was-it-created/a-60688639

Kim Y., Ross D., Kim J., Fallin C., Lee J., Lee D., Wilkerson D., Lai K., Mutlu O. (2014, Jun 24). Flipping Bits in Memory without Accessing Them: An Experimental Study of DRAM Disturbance Errors. *ece.cmu.edu. IEEE*. Recuperado: http://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf

Kirill R. (2019, Nov 24). Gone in 67 hours. Operation Mount Hope III. *Top War*. Recuperado: https://en.topwar.ru/164945-ugnat-za-67-chasov-operacija-moun-hope-iii.html

Koppel T. (2015). *Lights Out*. USA, New York: Broadway Books.

Kornbluh P., Block S. (2020, Nov 3). Allende and Chile: 'Bring Him Down.' *National Security Archive*. Recuperado: https://nsarchive.gwu.edu/briefing-book/chile/2020-11-06/allende-inauguration-50th-anniversary

Kornbluh, P. (2021, Apl 16). As Castro Retires on 60th Anniversary of the Bay of Pigs, National Security Archive Posts Declassified Top-Secret CIA Cables, Reports from 1960. Agency Officials Willing to Pay Over $10,000 For 'Fatal Accident'. Another Assassination Plot against Fidel Castro Was Part of Bay of Pigs Invasion Strategy.

The National Security Archive. Recuperado: https://nsarchive.gwu.edu/briefing-book/cuba/2021-04-16/documents-cia-assassination-plot-targeted-raul-castro

Kornbluh, P. (s.f.). Transcript of Proceedings, "The Secretary's Staff Meeting – Friday, 3/26/76," Secret, [pages 19-23 relate to Argentina]. *National Security Archive*. Recuperado: https://nsarchive.gwu.edu/document/21563-document-2-staff-meeting-transcripts-secretary

Kornbluh, P. y Osorio C. (2020, Feb 11). Operation Condor Countries Used Crypto AG Devices Without Realizing the CIA Owned the Company, National Security Archive Documents Reveal. Encryption revelations raise questions about U.S. official knowledge of Argentina "dirty war" atrocities, Chile's Letelier assassination, Southern Cone military dictatorships. Swiss encryption company secretly owned by U.S. and German intelligence agencies, according to records obtained by the German public broadcaster, ZDF, and Washington Post. *The National Security Archive*. Recuperado: https://nsarchive.gwu.edu/briefing-book/chile-cyber-vault-intelligence-southern-cone/2020-02-11/cias-minerva-secret

Kumar M. (2019, Aug 6). SWAPGS Attack — New Speculative Execution Flaw Affects All Modern Intel CPUs. *The Hacker News.* Recuperado: https://thehackernews.com/2019/08/swapgs-speculative-execution.html

Kwong A., Genkin D., Gruss D., Yarom Y. (2020, May). RAMBleed: Reading Bits in Memory without Accessing Them. *In Proceedings of the 41st Annual IEEE Symposium on Security & Privacy, May 2020*.

Laborde A. (2023, May 26). The private meeting between Kissinger and Pinochet in Chile: 'We want to help.' *El País*. Recuperado: https://english.elpais.com/international/2023-05-26/the-private-meeting-between-kissinger-and-pinochet-in-chile-we-want-to-help.html

Lakhani N. (2021, Jul 18). Revealed: murdered journalist's number selected by Mexican NSO client. *The Guardian*. Recuperado: https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto

Lakshmanan R. (2020, Dec 16). New Evidence Suggests SolarWinds' Codebase Was Hacked to Inject Backdoor. *The Hacker News*. Recuperado: https://thehackernews.com/2020/12/new-evidence-suggests-solarwinds.html

Lakshmanan R. (2021, Jan 21). Here's How SolarWinds Hackers Stayed Undetected for Long Enough. *The Hacker News*. Recuperado: https://thehackernews.com/2021/01/heres-how-solarwinds-hackers-stayed.html

Landsberger H. (1958). *Hawthorne Revisited: A plea for an open city*. USA, New York: Cornell University.

Langner R. (2010, Sep 16). Stuxnet logbook, Sep 16, 2010, 1200 hours MESZ. *OT Base*. Recuperado: https://www.langner.com/2010/09/stuxnet-logbook-sep-16-2010-1200-hours-mesz/

Langner R. (2013). To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. *The Langner Group*. Recuperado: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Lathem N. (2001, March 1). Feds to offer FBI Mole Sing or Die deal. *New York Post*. Recuperado: https://nypost.com/2001/03/01/feds-to-offer-fbi-mole-sing-or-die-deal/

Lavieri o. (2020, Sep 26). Quedó expuesta la identidad de decenas de agentes y ex agentes de inteligencia por la difusión de un documento judicial. *Infobae*. Recuperado: https://www.infobae.com/politica/2020/09/26/quedo-expuesta-la-identidad-de-decenas-de-agentes-y-ex-agentes-de-inteligencia-por-la-difusion-de-un-documento-judicial/

Lee C., Kube C., Dilanian K. (2022, May 6). Biden told officials media reports about U.S. intel sharing with Ukraine are counterproductive. *NBC News*. Recuperado: https://www.nbcnews.com/politics/national-security/biden-told-officials-media-reports-us-intel-sharing-ukraine-are-counte-rcna27738

Lee D. (2019). Google admits error over hidden microphone. *BBC News*. Recuperado: https://www.bbc.com/news/technology-47303077

Lee D., Hong D., Sung J., Kim S., Hong S. (2021, Dec 30). Improved Ciphertext-Only Attack on GMR-1. *IEEE Access*. Recuperado: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9666909

Lee R. (2016, Jun 2). IRONGATE Malware - Thoughts and Lessons Learned for ICS/SCADA Defenders. *SANS Institute*. Recuperado: https://www.sans.org/blog/irongate-malware-thoughts-and-lessons-learned-for-ics-scada-defenders/

Leighton A. y Matyas M. (1985). The History of Book Ciphers. In: Blakley G.R., Chaum D. (eds) *Advances in Cryptology. CRYPTO 1984. Lecture Notes in Computer Science, vol. 196. Springer, Berlín, Heidelberg*. https://doi.org/10.1007/3-540-39568-7_11

Lejtman R. (2022, August 10). Exclusivo: el informe completo del Mossad sobre el ataque terrorista que Irán y Hezbollah ejecutaron contra la AMIA. *Infobae*. Recuperado: https://www.infobae.com/politica/2022/08/10/exclusivo-el-informe-completo-del-mossad-sobre-el-ataque-terrorista-que-iran-y-hezbollah-ejecutaron-contra-la-amia/

Lemish, M. (1999). *War Dogs: A History of Loyalty and Heroism*. USA, Washington: Brassey's.

Lendon B. (2014, May 12). Iran says it built copy of captured U.S. drone. *CNN Business*. Recuperado: https://edition.cnn.com/2014/05/12/world/meast/iran-u-s-drone-copy/index.html

Leyden J. (2018, Jun 11). Hackers target payment transfer system at Chile's biggest bank, 'take $10m'. *The Register*. Recuperado: https://www.theregister.com/2018/06/11/chile_bank_wiper_prelude_cyberheaist/

Linn W. (2010, Sep/Oct). Defending a New Domain. The Pentagon's Cyberstrategy. *ForeignAffairs*. Recuperado: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Lintott B. (2015). *Confidence Men: The Mediterranean Double-Cross System, 1941-45* [Degree of Doctor of Philosophy, University of Toronto]. Toronto Library. Recuperado: https://tspace.library.utoronto.ca/bitstream/1807/71018/1/Lintott_Brett_201511_PhD_thesis.pdf

Lipovsky R. (2014, Oct 14). CVE-2014-4114: Details in August BlackEnergy PowerPoint Campaigns. *We Live Security by ESET*. Recuperado:

https://www.welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns/

Lippman D. (2019, Dec 9). Israel accused of planting mysterious spy devices near the White House. *Político*. Recuperado: https://www.politico.com/story/2019/09/12/israel-white-house-spying-devices-1491351

Lockheed Martin (s.f.). *The Cyber Kill Chain®.* Cyber Kill Chain | Lockheed Martin. Recuperado: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Lowenthal M., Clark R. (2015). *The Five Disciplines of Intelligence Collection*. USA, Los Angeles: Sage.

Lui J., Zhang Z., Ke. Y., Lei Y., Zhang M., Yang X. (2018, Dec 8). Digital Cardan Grille: A Modern Approach for Information Hiding. *CSAI '18: Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence*. Pages 441–446. Recuperado: https://doi.org/10.1145/3297156.3297255

Lui R. (2022, Mar 31). US biggest spoiler of Ukraine situation, European security. *Global Times*. Recuperado: https://www.globaltimes.cn/page/202203/1257338.shtml

Lutgen D. (2019, Sep 1). ROCK ISLAND ARSENAL, Ill. – Soldier Sensors and Lasers (SSL), Rock Island Arsenal – Joint Manufacturing and Technology Center (RIA-JMTC), completed the first shipment of a new unmanned aerial system to the Warfighter [Fotografía]. *U.S. Army photo by Debralee Best/RIA-JMTC.* Recuperado: https://www.dvidshub.net/news/309396/ria-jmtc-peo-soldier-test-ship-new-aerial-reconnaissance-system

Ma A. (2018, Sep 5). Police release photos of the fake perfume bottle of nerve agent they say Russian intelligence used in a brazen assassination attempt. *Insider*. Recuperado: https://www.businessinsider.com/photos-of-fake-perfume-bottle-of-nerve-agent-used-in-skripal-poisoning-2018-9

Maass P., Poitras L. (2014, Oct 10). Core Secrets: NSA Saboteurs in China and Germany: NSA agents use “physical subversion” to infiltrate networks and devices, documents show. *The Intercept*. Recuperado: https://theintercept.com/2014/10/10/core-secrets/

Maas P. (2016, Jun 28). The Hunter - He Was a Hacker for the NSA and He Was Willing to Talk. I Was Willing to Listen. *The Intercept*. Recuperado: https://theintercept.com/2016/06/28/he-was-a-hacker-for-the-nsa-and-he-was-willing-to-talk-i-was-willing-to-listen/

Macaskill E., Dance G. (2013, Nov 1). NSA files decoded. *The Guardian*. Recuperado: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

Macleod A. (2022, Oct 31). Revealed: the former Israeli spies working in top jobs at Google, Facebook, and Microsoft. *Mint Press News*. Recuperado: https://www.mintpressnews.com/revealed-former-israeli-spies-working-top-jobs-google-facebook-amazon/282413/

Madhani A., Heath B., Kelly J. (2017, Mar 7). WikiLeaks: CIA hacking group 'UMBRAGE' stockpiled techniques from other hackers. *USA TODAY*. Recuperado: https://eu.usatoday.com/story/news/2017/03/07/wikileaks-cia-hacking-group-umbrage-stockpiled-techniques-other-hackers/98867462/

MAHER (2012, May 28). Following to investigations started since 2010, about Stuxnet and Duqu, Iran National CERT (MAHER) has done a technical survey during past several months. MAHER publishes information about the last found sample for the first time. *Irán National CERT*. Recuperado: https://web.archive.org/web/20121031161013/http://www.certcc.ir/index.php?name=news&file=article&sid=1894

Manners D. (2016, Oct 21). *The battle of the beams*. Electronicsweekly. Recuperado: https://www.electronicsweekly.com/blogs/mannerisms/yarns/the-battle-of-the-beams-2016-10/

Marczak B., Scott-Railton J. (2016, Aug 24). The million-dollar dissident nso group's iphone zero-days used against a UAE human rights defender. *Citizen Lab*. Recuperado: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Marczak B., Scott-Railton J., McKune S., Razzak B., Deibert R. (2018, Sept 18). Hide and seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries.

University of Toronto, The Citizen Lab. Recuperado: https://nsarchive.gwu.edu/document/27613-6-citizen-lab-report-pegasus-spyware

Marczak B., Scott-Railton J., McKune S., Razzak B., Al-Jizawi N., Anstis S., Berdan K., Deibert R. (2021, Sep 13). Forcedentry - NSO group imessage zero-click exploit captured in the wild. *Citizen Lab*. Recuperado: https://tspace.library.utoronto.ca/bitstream/1807/123970/1/Report%23143--forcedentry.pdf

Marquis-Boire M., Greenwald G., Lee M. (2015, Jul 1). XKEYSCORE NSA's Google for the World's Private Communications. *The Intercept*. Recuperado: https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

Marston W.M. (1931). *Integrative, Psychology: A Study of Unit Response*. Nature 128, 1025–1026 (1931). https://doi.org/10.1038/1281025c0

Martin A. (2015, Jul 20). The Ruskies are coming for you, NSA director tells City bankers. *The register*. Recuperado: https://www.theregister.com/2015/07/20/patriotic_russian_hackers_are_coming_for_you_exgchq_head_tells_stock_exchange/

Marxists Internet Archive (s.f.). Crear dos, tres, muchos vietnams. Mensaje a los pueblos del mundo a través de la Tricontinental (1967). Recuperado el 1 de septiembre del 2022 en: https://www.marxists.org/espanol/guevara/04_67.htm

Mascolo G., Leyendecker H., Goetz J. (2014, Oct 4). Code word Eikonal - the nightmare of the federal government. *Süddeutsche Zeitung*. Recuperado: https://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432

Mascolo G., Goetz J., Osten D. (2014, Oct 3). Codename "Eikonal". *Tagesschau*. Recuperado: https://web.archive.org/web/20150318052321/http://www.tagesschau.de/inland/bnd-nsa-datenweitergabe-101.html

Matthews D. (2014. Dic 9). 16 absolutely outrageous abuses detailed in the CIA torture report. *Vox*. Recuperado: https://www.vox.com/2014/12/9/7360823/cia-torture-roundup

Matthew M., Burr W. (2013, Sep 25). "Disreputable if Not Outright Illegal": The National Security Agency versus Martin Luther King, Muhammad Ali, Art Buchwald, Frank Church, et al. *The National Security Agency*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB441/

Mazzetti M. y Weisman J. (2014, Mar 11). Conflict Erupts in Public Rebuke on C.I.A. Inquiry. *The New York Times*. Recuperado: https://www.nytimes.com/2014/03/12/us/cia-accused-of-illegally-searching-computers-used-by-senate-committee.html

McCandless D., Evans T. (2022, Sep). World's Biggest Data Breaches & Hacks. *Information is beautiful*. Recuperado: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

McCartney R. (1986, Jul 10). Terrorist group kills executive near Munich. *Washington Post*. Recuperado: https://www.washingtonpost.com/archive/politics/1986/07/10/terrorist-group-kills-executive-near-munich/da623290-a2db-448f-ac1c-f18bda0da97f/

McKernan B. (2022, Feb 27). Ukraine appeals for foreign volunteers to join fight against Russia. *The Guardian*. Recuperado: https://www.theguardian.com/world/2022/feb/27/ukraine-appeals-for-foreign-volunteers-to-join-fight-against-russia

McLuhan M. (1962). *The Gutenberg Galaxy: The Making of Typographic Man*. Canada: University of Toronto press.

McNamara R. (2009, Oct. 21). Apocalypse Soon. *Foreign Policy*. Recuperado: https://foreignpolicy.com/2009/10/21/apocalypse-soon/

MCTR (s.f.). MTCR – MISSILE TECHNOLOGY CONTROL REGIME. *Government of Canada on behalf the partners of the Missile Technology Control Regime.* Recuperado: https://mtcr.info/mtcr/

MCTR (s.f.). Frequently asked questions (FAQS). *Government of Canada on behalf the partners of the Missile Technology Control Regime.* Recuperado: https://mtcr.info/frequently-asked-questions-faqs/

Mellgren D. (2000, Mar 1). Norway solves riddle of Mossad killing. *The Guardian*. Recuperado: https://www.theguardian.com/world/2000/mar/02/israel

Menn J. (2013, Dec 20). Exclusive: Secret contract tied NSA and security industry pioneer. *Reuters*. Recuperado: https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220

Merces F., Gelera B., Co M. (2018, Jun 07). KillDisk Variant Hits Latin American Finance Industry. *TrendMicro*. Recuperado: https://www.trendmicro.com/en_us/research/18/f/new-killdisk-variant-hits-latin-american-financial-organizations-again.html

MGT Cell Master (s.f.). Tactical IMSI Catcher Detector Grabber [Fotografía]. Recuperado el 1 de septiembre del 2022 en: https://www.mgteurope.com/mgt-europe-mgt-cell-master-tactical-imsi-catcher-detector-grabber/

Microsoft Cyber Defense Operations Center CDOC (2021, Jan 20). Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop. *Microsoft Threat Intelligence*. Recuperado: https://www.microsoft.com/en-us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Military Health System (s.f.). Project 112/SHAD. Military Health System and Defense Health Agency. Recuperado: https://www.health.mil/Military-Health-Topics/Health-Readiness/Environmental-Exposures/Project-112-SHAD

Military Health System (s.f.). Fact Sheets. *Military Health System and Defense Health Agency*. Recuperado: https://www.health.mil/Military-Health-Topics/Health-Readiness/Environmental-Exposures/Project-112-SHAD/Fact-Sheets

Milmo D. (2022, Feb 27). Anonymous: the hacker collective that has declared cyberwar in Russia. *The Guardian*. Recuperado: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

Miller C., Valasek C. (2015, Aug 10). Remote Exploitation of an Unaltered Passenger Vehicle. *DEFCON Conference 23, Aug 8, 2pm*. Recuperado: https://illmatics.com/Remote%20Car%20Hacking.pdf

Miller C., Valasek C. (2015, Aug 10). *DEF CON 23 - Charlie Miller & Chris Valasek - Remote Exploitation of an Unaltered Passenger Vehicle* [VIDEO]. Youtube. Recuperado: https://www.youtube.com/watch?v=OobLb1McxnI

Minnich R., Lim G., O'Leary R., Koch C., Chen X., Hudson T., Mirtchovski A., Verdun J., Giamarchi H. [The Linux Foundation]. (2007, Oct 27). *Replace Your Exploit-Ridden Firmware with Linux - Ronald Minnich, Google* [VIDEO]. Recuperado: https://www.youtube.com/watch?v=iffTJ1vPCSo

Minnich R., Lim G., O'Leary R., Koch C., Chen X., Hudson T., Mirtchovski A., Verdun J., Giamarchi H. (s.f.). *Replace your exploit-ridden firmware with a Linux kernel* [PowerPoint slides]. Embedded Linux Wiki. Recuperado: https://elinux.org/images/6/69/ELC_2FOCP_2FCEA_Oct._2017_NERF.pdf

Mirsky Y., Mahler T., Shelef I. y Elovici1 Y. (2019). *CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning*. 28th USENIX Security Symposium. Recuperado: https://arxiv.org/pdf/1901.03597.pdf

Mitnick K. y Simon L. (2021). *The art of deception: Controlling the human element of security*. USA, Indiana: Willey Publishing Inc.

MITRE (2017). CVE-2017-5689. *Common Vulnerabilities and Exposures*. The MITRE Corporation. Recuperado: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5689

MITRE ATT&CK Matrix Poster (2023, April). *23_MatrixFlags_48x24_v3* [Imagen]. The MITRE Corporation. Recuperado: https://attack.mitre.org/docs/attack_matrix_poster_2023_april.pdf

MITRE CWE (s.f.). *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')*. The MITRE Corporation. Recuperado el 17 de octubre de 2021 de: http://cwe.mitre.org/data/definitions/22.html

Mordechai G., Boris Z., Yuval E. (2020). ODINI: Escaping sensitive data from Faraday-Caged, Air-Gapped computers via magnetic fields. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 15, 2020*. Recuperado: https://ieeexplore.ieee.org/document/8820015

Molander R., Riddile A., Wilson P. (1996). Strategic Information Warfare: A New Face of War. *RAND*. Recuperado: https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf

Molina-Markham A., Shenoy P., Fu K., Cecchet E., Irwin D. (2010, Nov 2). *Private Memoirs of a Smart Meter*. Switzerland, Zurich: BuildSys 2010. Recuperado: https://lass.cs.umass.edu/papers/pdf/buildsys10.pdf

Moore C. (2015). "Moral disengagement," *Current Opinion in Psychology*, 6.

Mordechai G., Dima B., Yuval E. (2017, Sep.). aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR). arXiv:1709.05742 [cs.CR]. Recuperado: https://arxiv.org/ftp/arxiv/papers/1709/1709.05742.pdf

Moreno J. (2001). *Undue Risk – Secret state experiment on human*. New York and London: Routledge.

Morris V. (2015). Grading Gerasimov: Evaluating Russian Nonlinear War Through Modern Chinese Doctrine. *Small Wars Journal*, Sep 17, 2015. Recuperado: https://web.archive.org/web/20151217191006/http://smallwarsjournal.com/printpdf/30157

MrSmith (2016, Oct 31). Shadow Brokers leaks list of NSA targets and compromised servers. *CSO Online*. Recuperado: https://www.csoonline.com/article/3137065/shadow-brokers-leak-list-of-nsa-targets-and-compromised-servers.html

Mueller R. (2019, March). Report On the Investigation into Russian Interference in the 2016 Presidential Election. *U.S. Department of Justice*, Washington. Recuperado: https://www.justice.gov/archives/sco/file/1373816/download

Muller D. [Veritasium en español]. (2020, Dec 3). *La Lluvia Radiactiva que Intentaron Ocultar. Cómo Hizo Kodak para Descubrirla* [Video]. https://www.youtube.com/watch?v=I_Cz3oy-bCs

Mullin J. (2013, Aug 12). New US spy satellite features world-devouring octopus. *Ars Technica*. Recuperado: https://arstechnica.com/tech-policy/2013/12/new-us-spy-satellite-features-world-devouring-octopus/

Nakashima E. (2013, May 27). Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies. *Washington Post*. Recuperado:

https://www.washingtonpost.com/world/national-security/confidential-report-lists-usweapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html

Natalizio J. (s.f.). Hundimiento del crucero General Belgrano ¿un crimen de guerra? *Allá Ité - Universidad Nacional de Lanús*. Recuperado: http://revistaallaite.unla.edu.ar/52/hundimiento-del-crucero-general-belgrano-un-crimen-de-guerra-

Natalizio (2013, May 14). Entrevista a Pablo Baccaro. Abogado de los caídos en el Crucero General Belgrano. *Malvinas: "Memoria, Verdad y Soberanía"*. Recuperado: http://malvinas30mvs.blogspot.com/

National Archives (s.f.). Record Group 341: Records of Headquarters U.S. Air Force. *Project Mogul* [Video]. Recuperado: https://catalog.archives.gov/id/2789203

National Archives and Records Administration (1971). *Operation Red Hat: Men and a Mission* [Video]. Department of Defense. Department of the Army. U.S. Army Materiel Command. U.S. Army Munitions Command. Recuperado: https://archive.org/details/gov.archives.arc.3033306

National Security Archive (s.f.). Prisoner abuse: Patterns from the past. *National Security Archive Electronic Briefing Book No. 122*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB122/index.htm#kubark.

National Vulnerability Database (s.f.). CVSS Severity Distribution over Time. *NIST*. Recuperado: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

National Counterintelligence and security Center (2020, March 13). Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities. *Office of the Director of National Intelligence*. Recuperado: https://www.dni.gov/files/Governance/IC-Tech-Specs-for-Const-and-Mgmt-of-SCIFs-v15.pdf

National Museum of nuclear science & history (s.f.). Choices of the Manhattan project. *Atomic Heritage Foundation*. Recuperado: https://ahf.nuclearmuseum.org/voices/location/canada/

National Museum of nuclear science & history (s.f.). Alsos Mission. *Atomic Heritage Foundation*. Recuperado: https://ahf.nuclearmuseum.org/ahf/history/alsos-mission/

National Museum of nuclear science & history (s.f.). John von Neumann. *Atomic Heritage Foundation*. Recuperado: https://ahf.nuclearmuseum.org/ahf/profile/john-von-neumann/

National Museum of nuclear science & history (s.f.). Trinity Test -1945. *Atomic Heritage Foundation*. Recuperado: https://ahf.nuclearmuseum.org/ahf/history/trinity-test-1945/

National Museum of the United States Air Force (s.f.). Mikoyan-Gurevich MiG-15bis. *USAF*. Recuperado: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/196115/mikoyan-gurevich-mig-15bis/

National Museum of United States Air Force (s.f.). GAMBIT 3 KH-8 Reconnaissance Satellite [Imagen]. *USAF*. Recuperado: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/195922/gambit-3-kh-8-reconnaissance-satellite/

National Museum of USA Air Force (s.f.). 1962 - Operation Ranch Hand. *Air Force Historical Support Division*. Recuperado: https://www.afhistory.af.mil/FAQs/Fact-Sheets/Article/458998/1962-operation-ranch-hand/

National Security Archive (s.f.). FOXACID. Top Secret//Comint//Noforn. *National Security Archive - Cyber Vault Library*. Recuperado: https://nsarchive.gwu.edu/document/22069-document-01

National Security Archive (2010, Dec 15). Introduction to BADDECISION. Top Secret/Comint/Noforn, December 15, 2010. *National Security Archive - Cyber Vault Library*. Recuperado: https://nsarchive.gwu.edu/document/21985-document-05

National System for Geospatial Intelligence (2018, April). *Geospatial Intelligence (GEOINT) basic Doctrine*. Recuperado: https://irp.fas.org/agency/nga/doctrine-2018.pdf

Nelsson R. (2020, Sep 9). The poison-tipped umbrella: the death of Georgi Markov in 1978 – archive. *The Guardian*. Recuperado:

https://www.theguardian.com/world/from-the-archive-blog/2020/sep/09/georgi-markov-killed-poisoned-umbrella-london-1978

Nesbit J. (2017, Dec 8). Google's true origin partly lies in CIA and NSA research grants for mass surveillance. *Quartz*. Recuperado: https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance

New York Times [New York Times]. (2021, Sep 10). *How a U.S. Drone Strike Killed the Wrong Person in Afghanistan | Visual Investigations* [Video]. https://www.youtube.com/watch?v=ZtecNyXxb9A

NIST (2012). *Guide for Conducting Risk Assessments* (NIST 800-30 rev. 1). Recuperado: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Norton-Taylor R. (2022, Jan 3). UK deployed 31 nuclear weapons during Falklands war. *Declassified UK*. Recuperado https://declassifieduk.org/uk-deployed-31-nuclear-weapons-during-falklands-war/

Nouwens M. (2022, Dec. 7). China's Military Modernization: Will the People's Liberation Army complete its reforms? *Strategic International Institute for Strategic Studies*. Recuperado: https://www.iiss.org/sv/online-analysis/online-analysis/2022/12/strategic-survey-2022-chinas-military-modernisation/

NSA (s.f.). Amendment No. 4 to the Appendices to the UKUSA Agreement (Third Edition). National Security Agency/Central Security Service. Recuperado: https://media.defense.gov/2021/Jul/15/2002763729/-1/-1/0/NEW_UKUSA_AGREE_10MAY55.PDF

NSA (s.f.). British - US Communication Intelligence Agreement. National Security Agency/Central Security Service. Recuperado: https://media.defense.gov/2021/Jul/15/2002763709/-1/-1/0/AGREEMENT_OUTLINE_5MAR46.PDF

NSA (s.f.). UKUSA Agreement Release. National Security Agency/Central Security Service. Recuperado: https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/UKUSA/smdpage14704/

NSA (2013, Jun). Utah Data Center [Fotografía]. National Security Agency. Recuperado: https://nsa.gov1.info/utah-data-center/utah-data-center.html

O'Donnell S. (2011). *ArgenLeaks*. Argentina, Buenos Aires: Sudamericana.

O'Donnell S. (2014). *PolitiLeaks*. Argentina, Buenos Aires: Sudamericana.

OCCRP (s.f.). A World of Surveillance [The Pegasus Project]. *Organized Crime and Corruption Reporting Project*. Recuperado: https://cdn.occrp.org/projects/project-p/

Oltermann P. (2022, Jun 25). European politicians duped into deepfake video calls with mayor of Kyiv. *The Guardian*. Recuperado: https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko

Orgaz C. (2020, Dic 21). Por qué en 2020 se crearon más dólares que nunca (y qué consecuencias tendrá para las economías de América Latina). *BBC News*. Recuperado: https://www.bbc.com/mundo/noticias-america-latina-55315553

Orwell G. (1949). *Nineteen Eighty-Four*. UK, London: Secker & Warburg.

Osorio C. (2004, Aug 27). Kissinger to the Argentine generals in 1976: If there are things that have to be done, you should do them quickly. *National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB133/index.htm

Osorio C., Blanton T. (2002, Dec 8). US Declassified Documents: Argentine Junta Security Forces Killed, Disappeared Activists, Mothers and Nuns. *The National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB77/

Osorio C., Christiano S. y Maskell E. (2012, April 1). Reagan On the Falkland/Malvinas: "Give [] Maggie enough to carry on...". *National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB374/

Otterman M. (2007). *American Torture from the cold war to abu ghraib and beyond*. Australia: Melbourne university press.

Ouziel N. (2020, Jan 31). Top 7 IMSI Catcher Detection Solutions for 2020. *FirstPoint*. Recuperado: https://www.firstpoint-mg.com/blog/top-7-imsi-catcher-detection-solutions-2020/

OWASP (2021). *OWASP Top Ten*. Recuperado el 17 de octubre de 2021 en: https://owasp.org/www-project-top-ten/

OWASP (s.f.). *OWASP Web Security Testing Guide*. Recuperado el 17 de octubre de 2021 en: https://owasp.org/www-project-web-security-testing-guide/stable/

OWASP (s.f.). *Testing for Clickjacking*. Recuperado el 17 de octubre de 2021 en: https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/11-Client_Side_Testing/09-Testing_for_Clickjacking

Owen J. [@JaredOwen] (2021, Dec 11). How did the Enigma Machine work? [Vídeo]. *Youtube*. Recuperado: https://www.youtube.com/watch?v=ybkkiGtJmkM

Paganini P. (2012m Aug 30). Iran suspected of the attack on the Saudi Aramco. *Security Affairs*. Recuperado: https://securityaffairs.co/wordpress/8300/malware/iran-suspected-for-the-attack-on-the-saudi-aramco.html

Pangu Lab Technology (2022, Feb 23). The Bvp47 - a Top-tier Backdoor of US NSA Equation Group. *Pangu Lab Technology Co Ltd, Beijing Qi*. Recuperado: https://www.pangulab.cn/en/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/

Paresh D. (2022, Mar 11). YouTube blocks Russian state-funded media channels globally. *Reuters*. Recuperado: https://www.reuters.com/business/media-telecom/youtube-blocks-russian-state-funded-media-channels-globally-2022-03-11/

Parfitt T. (2010, nov. 26). Russian parliament admits guilt over Polish massacre. *The Guardian*. Recuperado: https://www.theguardian.com/world/2010/nov/26/russian-parliament-guilt-katyn-massacre

Pearson J. (2022, Feb 26). Ukraine launches 'IT army,' takes aim at Russian cyberspace. *Reuters*. Recuperado: https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/

Perlroth N. (2012, Agu 30). Software Meant to Fight Crime Is Used to Spy on Dissidents. *New York Times*. Recuperado: https://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html

Perlroth N., Shane S. (2017, Oct 10). How Israel Caught Russian Hackers Scouring the World for U.S. Secrets. *The New York Times*. Recuperado:

https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html

Peterson S., Faramarzi P. (2011, Dec 15). Exclusive: Iran hijacked US drone says Iranian engineer. *The Christian Science Monitor*. Recuperado: https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer

Pfeifer J. (2013, Jul). Fire as a Weapon in Terrorist Attacks. *Combating Terrorism Center, Vol 6, issue 7*. Recuperado: https://ctc.westpoint.edu/fire-as-a-weapon-in-terrorist-attacks/

Philosophy Talk (2015, Jul 9). Edward Snowden: The Ethics of Whistleblowing - Hero or Traitor? [Video]. *Youtube*. Recuperado: https://www.youtube.com/watch?v=57sPn6pQzUM

Pintos G. (2022, Feb 27). Cancelaciones en tiempos de guerra: artistas rusos pagan el precio de la invasión a Ucrania. *Infobae*. Recuperado: https://www.infobae.com/cultura/2022/02/27/cancelaciones-en-tiempos-de-guerra-artistas-rusos-pagan-el-precio-de-la-invasion-a-ucrania/

PKI Electronic Intelligence (s.f.). Catcher Detector Product number: PKI 1670 [Fotografía]. Recuperado el 1 de septiembre del 2022 en: https://pki-electronic.com/products/imsi-catcher/catcher-detector/

Plokhy S. (2017, Feb 7). The Man with the Poison Gun: Q&A with Serhii Plokhii. *Ukranian Research Institute of Harvard University*. Recuperado: https://huri.harvard.edu/news/man-poison-gun-qa-serhii-plokhii

Poder Judicial de la Nación (2008, Jun 3). Autos y Vistos número 18.967/03 del registro de este Juzgado Nacional en lo Criminaly Correccional Federal n° 12. *Centro de Estudios Legales y Sociales*. Recuperado: https://www.cels.org.ar/common/documentos/elevacion_juicio_testimonios_B.pdf

Podberezski V. (2019, August 16). El papel de la criptografía en las campañas del General San Martín en las guerras de independencia americanas. *Inside the trash can*. Recuperado: http://inside-the-trash-can.blogspot.com/2019/08/el-papel-de-la-criptografia-en-las.html

Pols P., (2017, Dec 7). Modeling Fancy Bear Cyber-attacks: Designing a Unified Kill Chain for analyzing, comparing, and defending against cyber-attacks. *Cyber Security Academy (CSA)*. Recuperado: https://studenttheses.universiteitleiden.nl/access/item%3A2666284/view

Pols P., (2023, Feb). The Unified Kill Chain v1.3. *Fox IT*. Recuperado: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

Poulsen K. (2013, Jun 27). WikiLeaks Volunteer Was a Paid Informant for the FBI. *Wired*. Recuperado: https://www.wired.com/2013/06/wikileaks-mole/

Prados J. (2006). *Safe for Democracy: The secret wars of the CIA*. USA, Chicago: Ivan R. Dee.

Prados J., Nichter L. (2020, Jun 25). Spying on Americans: Infamous 1970s White House Plan for Protest Surveillance Released. *National Security Archive*. Recuperado: https://nsarchive.gwu.edu/briefing-book/intelligence/2020-06-25/spying-americans-new-release-infamous-huston-plan

Pratkanis A. y Aeonson E. (2001). *Age of propaganda: The everyday use and abuse of persuasion*. New York: W.H. Freeman and Company.

Pratyusa M., Tan K., Maxion R., Wing J. (2007). An Approach to Measuring a System's Attack Surface. *School of Computer Science, Carnegie Mellon University*. Recuperado: https://www.cs.cmu.edu/~wing/publications/CMU-CS-07-146.pdf

Priest D. (2005, Dec 4). Wrongful Imprisonment: Anatomy of a CIA Mistake. *Washington Post*. Recuperado: https://www.washingtonpost.com/wp-dyn/content/article/2005/12/03/AR2005120301476_pf.html

Priest D. (2016, Jul 9). War reporter Marie Colvin was tracked, targeted, and killed by Assad's forces, family says. *Washington Post*. Recuperado: https://www.washingtonpost.com/world/national-security/war-reporter-marie-colvin-was-tracked-targeted-and-killed-by-assads-forces-family-says/2016/07/09/62968844-453a-11e6-88d0-6adee48be8bc_story.html

Priest D. (2021, Dec 21). A UAE agency put Pegasus spyware on phone of Jamal Khashoggi's wife months before his murder, new forensics show. *The Washington Post*. Recuperado: https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/

Pruchnicka A. (2023, Sep 25). U.S.-made Abrams tanks arrive in Ukraine - Zelenskiy. *Reuters*. Recuperado: https://www.reuters.com/world/europe/abrams-tanks-arrive-ukraine-zelenskiy-2023-09-25/

Rabkin, J., Basnett, G., Howker, E., Eastham, J. and Pett, H. [Channel 4 News]. (2020, Sep 28). *Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016* [Video]. https://www.youtube.com/watch?v=KIf5ELaOjOk

Rafferty A. (2017, Aprl 7). What Is a SCIF and Who Uses It? *NBC News*. Recuperado: https://www.nbcnews.com/politics/politics-news/what-scif-who-uses-it-n743991

Rankin, J. (2017, Nov 13). Catalan independence: EU experts detect rise in pro-Kremlin false claims. *The Guardian*. Recuperado: https://www.theguardian.com/world/2017/nov/13/catalan-independence-eu-experts-detect-rise-in-pro-kremlin-false-claims

Rapp N., Jenkins A. (2018, Jul 24). Chart: These 6 Companies Control Much of U.S. Media. *Fortune*. Recuperado: https://fortune.com/longform/media-company-ownership-consolidation/

Ratcliffe S. (2016). *Oxford Essential Quotations (4 ed)*. Oxford University Press. Reporte completo: https://www.pangulab.cn/files/The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group.en.pdf

Reinemann C. (s.f.). Receiving the digital stream from geostationary satellites. *Usradioguy*. Recuperado: https://usradioguy.com/goes-satellite-imagery-reception/

Richard F. (2020, Aug 13). The Horrible: American Strategic Options against Japan in 1945. *The National WWII Museum of New Orleans*. Recuperado: https://www.nationalww2museum.org/war/articles/american-strategic-options-against-japan-1945

Richelson J. (2005, Mar 11). The National Security Agency Declassified. *The National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB24/index.htm

Richelson J. (2006, Mar 21). U.S. Intelligence and the French Nuclear Weapons Program. *The National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB184/index.htm

Richelson J. (2012, Oct 4). Lifting the Veil on NRO Satellite Systems and Ground Stations - Documents Trace Effort to Declassify the Operations of America's Intelligence Satellite Agency. *The National Security Archive*. Recuperado: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB392/

Richelson J. (2013). The Area 51 File: Secret Aircraft and Soviet MiGs. *The National Security Archive*. Recuperado: https://nsarchive.gwu.edu/briefing-book/intelligence/2013-10-29/area-51-file-secret-aircraft-soviet-migs

Richelson J. (2015, Mar 20). The CIA and Signals Intelligence. *National Security Archive*. Recuperado: https://nsarchive.gwu.edu/briefing-book/cyber-vault-intelligence/2015-03-20/cia-and-signals-intelligence

Richelson J. (2015, Mar 20). Office of the National Counterintelligence Executive, Unauthorized Disclosures of Classified Information (Text Alternative), September 11, 2011. Unclassified. Extract. *National Security Archive*. Recuperado: https://nsarchive.gwu.edu/document/28400-document-42-office-national-counterintelligence-executive-unauthorized-disclosures

Risen J. (2000, April 16). SECRETS OF HISTORY: The C.I.A. in Iran -- A special report; How a Plot Convulsed Iran in '53 (and in '79). *The New York Times*. Recuperado: https://www.nytimes.com/2000/04/16/world/secrets-history-cia-iran-special-report-plot-convulsed-iran-53-79.html

Rob1blackops (2017, Jul 31). History of the US high-altitude SIGINT system. *SatelliteObservation*. Recuperado: https://satelliteobservation.net/2017/07/31/history-of-the-us-high-altitude-sigint-system/

Roberts A. (2010, Sep 19). MI6 Attacked Jewish Refugee Ships After WWII. *The Daily Beast*. Recuperado: https://www.thedailybeast.com/mi6-attacked-jewish-refugee-ships-after-wwii

Robertson H. (2022, Aug 13). Energy traders are making a killing exporting US natural gas to Europe as prices soar - with some single shipments bringing in $200 million, *Business Insider*. Recuperado:

https://markets.businessinsider.com/news/commodities/us-natural-gas-exports-europe-surge-energy-crisis-trader-profits-2022-8

Robertson J., Riley M. (2018, Oct 4). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg*. Recuperado: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Robin H. (2015, February 24). "James Vicary: Experiment & Overview." *Study.com*. Recuperado: https://study.com/academy/lesson/james-vicary-experiment-lesson-quiz.html.

Roccia T. (2018, Nov 8). Triton Malware Spearheads Latest Attacks on Industrial Systems. *McAfee*. Recuperado: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/

Rockett K. (2019, Sep 14). Declassified CIA documents show secret use of photographer spy-pigeons in Cold War. *Mirror*. Recuperado: https://www.mirror.co.uk/news/weird-news/declassified-cia-documents-show-secret-20065285

Rojas J. [Armapedia]. (2022, April 11). El SAC: La Unidad más SECRETA de la CIA [Video]. https://www. https://www.youtube.com/watch?v=sVyJrcE9nQg

Rose W. (1981, March). An Evaluation of entomological warfare as a potential danger to the United States and European NATO Nations (u). *U.S. Army*. Recuperado: https://www.thesmokinggun.com/file/attack-killer-mosquitoes-0

Rossi E. [Cronologias]. (2021, Nov 8). *Cronología de medios de comunicación en Argentina* [Video]. Recuperado: https://www.youtube.com/watch?v=NuqM64EiHxo

RT (2022, April 30). Moscú: Varias generaciones de ucranianos van a costear las armas enviadas por EE.UU. *RT Actualidad*. Recuperado: https://actualidad.rt.com/actualidad/428467-moscu-generaciones-ucranianos-van-pagar

RT Stuff (2014, May 21). High-level hooligan: Chinese media vents spleen over US cybercrime charges. *RT News*. Recuperado: https://www.rt.com/news/160388-china-us-cybersecurity-hacking/

Ruiz J. (2022, Feb 25). Suspendido el Gran Premio de Rusia de Fórmula 1. *Marca*. Recuperado: https://www.marca.com/motor/formula1/2022/02/25/6218c91b22601d017e8b45be.html

Rulicki S. (2013). *Las caras de la mentira (y de la verdad)*. Argentina, CABA: Margen izquierdo.

Ruppe D. (2006, Jan 7). U.S. Military Wanted to Provoke War with Cuba. *ABC News*. Recuperado: https://abcnews.go.com/US/story?id=92662

Ryan D. (2000, Nov 3). Contingency planning Pentagon MASCAL exercise. *Military District of Washington*. Recuperado: https://web.archive.org/web/20010111100400/http://www.dcmilitary.com/army/pentagram/5_44/local_news/2852-1.html

S.N. (2001, Nov 21). An Eye for an Eye. *CBS News*. Recuperado: https://web.archive.org/web/20070206033135/https://www.cbsnews.com/stories/2001/11/20/60II/main318655.shtml

S.N. (2011, Aug 31). Extraordinary rendition: a backstory: Used since the Reagan era, extraordinary rendition was stepped up after 9/11 to extract intelligence from suspected terrorists. *TheGuardian*. Recuperado: https://www.theguardian.com/world/2011/aug/31/extraordinary-rendition-backstory

S.N. (2012, April 5). Jean Gerard Leigh. *The Telegraph*. Recuperado: https://www.telegraph.co.uk/news/obituaries/military-obituaries/9189418/Jean-Gerard-Leigh.html

S.N. (2013, Sep 5). The animals mistaken for spies. *BBC*. Recuperado: https://www.bbc.com/news/blogs-magazine-monitor-23962379

S.N. (2017, aprl). DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis. *@zerosum0x0 blogspot*. Recuperado: https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html

S.N. (2020, Apr 11). Truth Is the First Casualty in War. *Quoteinvestigator*. Recuperado: https://quoteinvestigator.com/2020/04/11/casualty/

S.N. (2020, Oct 5). La AFI filtró los datos de 12 agentes activos en el exterior. *TN Noticias*. Recuperado: https://tn.com.ar/politica/la-afi-filtro-los-datos-de-12-agentes-activos-en-el-exterior/2020/10/05/HV2YHMLZIJBIBNEBWEVJ4X5EME_story/

S.N. (2020, Oct 24). 42 ADMITTED False Flag Attacks. *Washington's Blog*. Recuperado: https://washingtonsblog.com/42-admitted-false-flag-attacks/

S.N. (2021, Sep 3). Los informes que implican a los servicios secretos rusos con la fallida declaración de independencia de Cataluña de 2017. *Infobae*. Recuperado: https://www.infobae.com/espana/2021/09/03/los-informes-que-implican-a-los-servicios-secretos-rusos-con-la-fallida-declaracion-de-independencia-de-cataluna-de-2017/

S.N. (2022, May 22). Iran: Revolutionary Guard colonel killed by motorbike gunmen in Tehran. *The Guardian*. Recuperado: https://www.theguardian.com/world/2022/may/22/iran-revolutionary-guard-colonel-killed-by-motorbike-gunmen-in-tehran

S.N. (2022, Mar 2). Polémica en Italia: una universidad quiso prohibir textos de Dostoievski por ser ruso. *Telam*. Recuperado: https://www.telam.com.ar/notas/202203/585027-dostoievski-prohido-universidad-italia-por-ruso.html

S.N. [Lord Draugr] (2021, Jun 7). Lo que no te cuentan los Youtubers de las VPN [Video]. Youtube. Recuperado: https://www.youtube.com/watch?v=CBwZ5RLrKWM

Sacquety J. (2022, Mar). Triumph in the Desert - Recovering a Cold War Prize. *U.S. Army Special Operations History Office*. Recuperado: https://arsof-history.org/articles/21dec_triumph_in_the_desert_page_1.html

Sagaian N. (s.f.). Henry Kissinger at the 1978 World Cup Videla's guest of honour. *Papelitos*. Recuperado: https://papelitos.com.ar/nota/henry-kissinger-en-el-mundial-78

Salces D. (2021, Dic 21). Se confirma que Pegasus se empleó para espiar a Jamal Khashoggi. *My computer*. Recuperado: https://www.muycomputer.com/2021/12/21/pegasus-mujer-jamal-khashoggi/

Samoilenko S., Icks M., Keohane J., Shiraev E. (2020). *Routledge handbook of character assassination and reputation management*. USA, New York: Routledge.

Samoilenko, S. (2016). Character assassination. In C. Carroll (Ed.), *The SAGE Encyclopedia of Corporate Reputation*. (Vol. 1, pp. 115-118). Thousand Oaks, CA: SAGE.

Sanger D., Perlroth N. (2019, Jun 15). U.S. Escalates Online Attacks on Russia's Power Grid. *New York Times*. Recuperado: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

Sato H., Berry C., Peeri Y., Baghoomian E., Casey B., Lavella G., VandenBrooks J., Harrison J., Maharbiz M. (2009, Oct 5). Remote radio control of insect flight. *Frontiers in Integrative Neuroscience Volume 3, Article 24*. Recuperado: https://www.frontiersin.org/articles/10.3389/neuro.07.024.2009/full

Savoia C. (2015). *Espiados: Como controla el gobierno a todos los argentinos. Infiltrados, espías y escuchas. La guerra por la información clandestina*. Argentina, CABA: Planeta®.

Sayer P. (2016, Sep 8). Yes, U.S. did hack Elysée Palace in 2012, French ex-spy says. *Computer World*. Recuperado: https://www.computerworld.com/article/3118322/yes-us-did-hack-elyse-palace-in-2012-french-ex-spy-says.html

Sharma R. (2023, Jun 11). Captured US Stealth Drone, Reversed-Engineered by Iran, Could Help Russia in Gaining Air Superiority Over Ukraine. *EurAsian Times*. Recuperado: https://www.eurasiantimes.com/us-stealth-drone-reversed-engineered-by-iran-to-help/

Sharp G. (1973). *The Politics of Nonviolent Action* (3 volumes). USA: Porter Sargent.

Singleton C., Moore S., McMillen D. (2021, Mar 10). Top 10 cybersecurity vulnerabilities of 2020. *Security Intelligence*. Recuperado: https://securityintelligence.com/posts/top-10-cybersecurity-vulnerabilities-2020/

Schaik S., Milburn A., Österlund S., Frigo P., Maisuradze G., Razavi K., Bos H., Giuffrida G., (2019). RIDL: Rogue In-Flight Data Load. Recuperado: https://mdsattacks.com/files/ridl.pdf

Schmitt M. (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. UK, Cambridge: Cambridge University Press.

Schneier B. (2013, Oct 7). How the NSA Attacks Tor/Firefox Users with QUANTUM and FOXACID. *Schneier on Security*. Recuperado: https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html

Schultz D., Schultz S. (2011). *A history of modern psychology (10 edition)*. USA, California: Wadsworth, Cengage Learning.

Schwarz M., Lipp M., Moghimi D., Bulck J., Stecklina J., Prescher T., Gruss D. (2019). ZombieLoad: Cross-Privilege-Boundary Data Sampling. *ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom*. Recuperado: https://doi.org/10.1145/3319535.3354252

Sciaroni M. (2016, Dec). Satélites Norteamericanos sobre las Islas Malvinas. *ESGN Nº 62*. Recuperado: http://www.cefadigital.edu.ar/bitstream/1847939/713/1/5_Rev_62_Satelites_norteamericanos_sobre_las_islas_malvinas_w5.pdf

Scislowska M., Olsen J., Keyton D. (2022, Sept 27). Blasts precede Baltic pipeline leaks, sabotage seen likely. *AP News*. Recuperado: https://apnews.com/article/russia-ukraine-germany-berlin-00232df3f4b4bc89afd47d4707724e33

Sciutto J., Rizzo J. (2016, nov. 29). War in space: Kamikazes, kidnapper satellites and lasers. *CNN*. Recuperado: https://edition.cnn.com/2016/11/29/politics/space-war-lasers-satellites-russia-china/index.html

Sciutto J. (2019). *The shadow war: Inside Russia's and China's secret operations to defeat America*. USA, NY: Harper Collins.

Scott T. (2022, Mar 26). Anonymous leaked 28 GB of information from the Central Bank of Russia. *Global Happening*. Recuperado: https://globalhappenings.com/technology/135080.html

Seoane, M. (2006, Mar 24). Los secretos de la guerra sucia continental de la dictadura. *Clarín*.

SecureList (2021, Oct 6). FinSpy: nuevos hallazgos. *Secure List by Kaspersky*. Recuperado: https://securelist.lat/finspy-unseen-findings/95636/

Select Committee on Intelligence and Committee on Human Resources (1977, Aug 3). Joint Hearing before the Select committee on intelligence and the subcommittee on health and scientific research of the committee on human resources. United States Senate. Recuperado: https://www.intelligence.senate.gov/sites/default/files/hearings/95mkultra.pdf

Senate Select Committee on intelligence (2014, Dec 3). Committee study of the central intelligence agency detention and interrogation program. United States Senate. Recuperado: https://documents.latimes.com/committee-study-central-intelligence-agencys-detention-and-interrogation-program/

Shaik A. (2017). Practical Attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems. *Internet Society*. Recuperado: http://dx.doi.org/10.14722/ndss.2016.23236

Sharma A. (2021, Jun 21). Sonatype Catches New PyPI Cryptomining Malware. *Sonatype*. Recuperado: https://blog.sonatype.com/sonatype-catches-new-pypi-cryptomining-malware-via-automated-detection

Shearer J. (2010, Jul 13). W32.Stuxnet. *Symantec*. Recuperado: https://web.archive.org/web/20191223000908/https://www.symantec.com/security-center/writeup/2010-071400-3123-99/

Sherzad T. and Ukrainskiy A. (2021, Nov 11). Spystone: Voronezh Academy has developed a new way to track the enemy. *Zvezda news*. Recuperado: https://tvzvezda.ru/news/202111261748-YvgtU.html

Shields N. (2018, Jun 8). Criminal Complaint. *United States Department of Justice*. Recuperado: https://www.justice.gov/opa/press-release/file/1092091/download

Shoghi Communications (s.f.). Tactical Thuraya Monitoring System (SCL-5030P) [Fotografía]. Recuperado el 1 de septiembre del 2022 en: https://www.shoghicom.com/tactical-thuraya-monitoring.php

Shoghi Communications (s.f.). Unified Satellite Phone Monitoring System (SCL-1625TII) [Fotografía]. Recuperado el 1 de septiembre del 2022 en: https://www.shoghicom.com/unified-satellite-phone-monitoring-system.php

Shoshin P. (2019, Jul 15). FinSpy: Un spyware commercial. *Kaspersky Daily*. Recuperado: https://www.kaspersky.es/blog/finspy-commercial-spyware/18869/

Sidell F., Takafushi E., Franz D. (1997). Overview: Defense against the Effects of Chemical and Biological Warfare Agents (From Medical Aspects of Chemical and Biological Warfare. *Medical Department of the Army*. Recuperado: https://www.ojp.gov/ncjrs/virtual-library/abstracts/overview-defense-against-effects-chemical-and-biological-warfare

Siemens AG (2011, Jul 8). Siemens pays tribute to Karl Heinz Beckurts and Eckhard Groppler. *Siemens Press*. Recuperado: https://press.siemens.com/global/en/pressrelease/siemens-pays-tribute-karl-heinz-beckurts-and-eckhard-groppler

Signals Defense (s.f.). SIGNALS DEFENSE SD 2500/2510 [Fotografía]. Recuperado el 1 de septiembre del 2022 en: https://www.signalsdefense.com/rf-window-films/2500-2510/

Simpson B., Venkatasubramanian V. (2019). U.S. sought to preserve close ties to Indonesian military as it terrorized East Timor in runup to 1999 independence referendum. *The National Security Archive*. Recuperado: https://nsarchive.gwu.edu/briefing-book/indonesia/2019-08-28/us-sought-preserve-close-ties-indonesian-military-it-terrorized-east-timor-runup-1999-independence

Sims J. (1997, Jan). The BRUSA Agreement of May 17, 1943. *Cryptologia*, Vol 21 number 1, pp. 30-38.

Singh M. (2020, Aug 7). Trump bans US transactions with Chinese-owned TikTok and WeChat. *The Guardian*. Recuperado: https://www.theguardian.com/technology/2020/aug/06/us-senate-tiktok-ban

Sislin, J. D. (2019). Underappreciated, Underrepresented: Thoughts on Teaching MASINT. *American Intelligence Journal, 36(2)*, 28–39. https://www.jstor.org/stable/27066370

Sontag S., Drew C. (1998). *Blind Man's Bluff: The Untold Story of American Submarine Espionage*. USA, New York: Public Affairs.

Sontheimer M. (2017, Mar 7). CIA Spies May Also Operate in Frankfurt. *Der Spiegel*. Recuperado: https://www.spiegel.de/international/world/wikileaks-data-dump-on-cia-spying-vault-7-a-1137740.html

Soshnikov A., Reiter S. (2019, Julio 19). Москит, Надежда, Наутилус: хакеры раскрыли суть проектов тайного подрядчика ФСБ. *BBC News*. Recuperado: https://www.bbc.com/russian/features-49050982

Sotnek I. (2019). Stingrays and IMSI-Catchers. *National Security Archive*. Recuperado: https://nsarchive.gwu.edu/news/cyber-vault/2019-11-15/stingrays-imsi-catchers

Spiegel Staff (2013, Sep 20). Britain's GCHQ Hacked Belgian Telecoms Firm. Spiegel International. Recuperado: https://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

Spiegel Staff (2013, Dic 29). Documents Reveal Top NSA Hacking Unit. *Der Spiegel*. Recuperado: https://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

Spiegel Staff (2013, Dec 30). How the Intelligence Service Cracks Internet Hubs.*Der Spiegel*. Recuperado: https://www.spiegel.de/fotostrecke/photo-gallery-how-the-intelligence-service-cracks-internet-hubs-fotostrecke-105336.html

Spy Museum (s.f.). Pigeon Camera. *Spy Museum*. Recuperado el 30 Jun del 2022 en: https://www.spymuseum.org/exhibition-experiences/about-the-collection/collection-highlights/pigeon-camera

Spy Museum (s.f.). Bulgarian Umbrella (replica) [Fotografía]. *Spy Museum*. Recuperado: https://www.spymuseum.org/exhibition-experiences/about-the-collection/collection-highlights/bulgarian-umbrella-replica/

Statement of director of CIA before Subcommittee on health and scientific research senate committee on human resources (1977, Sep 21). Recuperado: https://www.cia.gov/readingroom/docs/CIA-RDP99-00498R000300020007-3.pdf

Stebner B. (2013, Jun 19). Michael Hastings conspiracy theories: Web goes wild after NSA, CIA reporter killed in crash. *New York Daily News*. Recuperado: https://www.nydailynews.com/news/national/conspiracy-theories-abound-michael-hastings-death-article-1.1377392

Stevens R. (2019, Nov 8). In Cold War Berlin, the Americans had a tunnel, but the Soviets had a mole. *Washington Post*. Recuperado: https://www.washingtonpost.com/outlook/in-cold-war-berlin-the-americans-had-a-

tunnel-but-the-soviets-had-a-mole/2019/11/08/d7fa0328-b714-11e9-a091-6a96e67d9cce_story.html

Stewart W. (2013, Dec 3). Revealed: Stalin's kamikaze canines who were trained to blow themselves up as anti-tank dogs. *Dailymail*. Recuperado: https://www.dailymail.co.uk/news/article-2517413/The-kamikaze-canines-blew-destroy-Nazi-tanks-WWII-photographs-reveal-Stalins-dogs-war-explosives-strapped-them.html

Stickley J., Davis T. (2019, Sep 25). Typosquatting Is Quickly Rising, How to Protect Yourself. *SOS Daily News*. Recuperado: https://www.sosdailynews.com/?articleid=%20F154B01155AFF572D218E6301EBFEAF1

Stokes J. (2024, Feb. 1). Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition. *Center for a new American Security*. Recuperado: https://www.cnas.org/publications/congressional-testimony/military-artificial-intelligence-the-peoples-liberation-army-and-u-s-china-strategic-competition

Stollznow K. (2014, Aug 7). Eavesdropping: etymology, meaning, and some creepy little statues. Karen Stollznow. Recuperado: https://web.archive.org/web/20190329192339/http://karenstollznow.com/eavesdropping/

Stone O. (Director). (2016). *Snowden* [Movie]. Endgame Entertainment.

Stonecypher M. (2019, Oct 27). X-37B breaks record, lands after 780 days in orbit [Fotografía]. U.S. Air Force photo. Recuperado: https://www.afspc.af.mil/News/Photos/igphoto/2002204566/

Stonecypher M. (2010, Dec 3). X-37B at Vandenberg Air Force base [Fotografía]. U.S. Air Force photo. Recuperado: https://www.afspc.af.mil/News/Photos/igphoto/2000302656/

Strom B., Battaglia J., Kemmerer M., Kupersanin W., Miller D., Wampler C., Whitley S., Wolf S. (2017, Jun). Finding Cyber Threats with ATT&CK™-Based Analytics. *Mitre*. Recuperado: https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att&ck-based-analytics.pdf

Strom B., Applebaum A., Miller D., Nickels K., Pennington A., Thomas C. (2020). MITRE ATT&CK®: Design and philosophy. *Mitre*. Recuperado: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Stuckless N. y Goranson R. (1992). The vengeance scale: Development of a measure of attitudes toward revenge. *Journal of social behavior & Personality*, 7(1).

Stupp C. (2019, Aug 20). Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. *The Wall Street Journal*. Recuperado: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Sun W. (512 B.C.). *The Art of War (孫子兵法)*. China.

Symantec (2014). Security response: Dragonfly. *Symantec*. Recuperado: https://scadahacker.com/files/havex/Symantec%20-%20Security%20Response%20-%20Dragonfly%20v1.0.pdf

Symantec Security Response (2014). Regin: Top-tier espionage tool enables stealthy surveillance. *Symantec*. Recuperado: https://web.archive.org/web/20150312190049/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf

Symantec Security Response (2017, Dec 14). Triton: New Malware Threatens Industrial Safety Systems. *Symantec Enterprise Blogs / Threat Intelligence*. Recuperado: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/triton-malware-ics

Szoldra P. (2013, Dec 7). US Spy Agency Boasts 'Nothing Is Beyond Our Reach' With New Logo. *Insider*. Recuperado: https://www.businessinsider.com/nrol-39-logo-nothing-beyond-our-reach-2013-12

Tagliabue J. (2986, Jul 26). Car bomb hits a West German company involved in STAR WARS. *The New York Times*. Recuperado: https://www.nytimes.com/1986/07/26/world/car-bomb-hits-a-west-german-company-involved-in-star-wars.html

Tamada S. (2008). Hack your Own Web Project? SQL Injection. *9lessons*. Recuperado el 17 de octubre de 2021 en: https://www.9lessons.info/2008/12/sql-injection.html

Tech Minds [Tech Minds]. (2020, Jul 9). *Eavesdropping Video Monitors with TempestSDR RTL-SDR* [Video]. https://www.youtube.com/watch?v=QjqpKtGNbQo

TELAM (2022, Mar 2). La "guerra económica" contra Moscú avanza sin pausa. *Télam digital*. Recuperado: https://www.telam.com.ar/notas/202203/585090-rusia-sanciones-economia.html

Tanenbaum S. (2017, Nov 7). An Open Letter to Intel. *Department of Computer Science - Vrije Universiteit - Andrew S. Tanenbaum's Home Page*. Recuperado: https://www.cs.vu.nl/~ast/intel/

Terragno R. (1998). *Maitland & San Martín*. Argentina, BA: Universidad Nacional de Quilmes. Recuperado: https://web.archive.org/web/20081010105149/http://www.terragno.org.ar/pdfs/Maitland%26San%20Martin%203a%20ed.pdf

The Avalon Project (s.f.). The Quebec Conference - Agreement Relating to Atomic Energy. *Yale Law School: Lillian Goldman Law Library*. Recuperado: https://avalon.law.yale.edu/wwii/q003.asp

The Avalon Project (s.f.). Nuremberg Trial Proceedings Volume 2: NINTH DAY Friday, 30 November 1945 Morning Session. *Yale Law School: Lillian Goldman Law Library*. Recuperado: https://avalon.law.yale.edu/imt/11-30-45.asp

The Intercept (2016, Sep 6). Menwith collection assets. Recuperado: https://theintercept.com/document/2016/09/06/menwith-collection-assets/

The Ministry of Defence of the Russian Federation (2017). Krasukha-4 [Fotografía]. Wikimedia Commons. Recuperado: https://commons.wikimedia.org/wiki/File:1RL257E_Krasukha-4.jpg

The most vulnerable players of 2017 (2018, March 29). Techtalk. Recuperado: https://techtalk.gfi.com/the-most-vulnerable-players-of-2017/

The National Archives (s.f.). Records of the Directorate of Tube Alloys and related bodies. *The National Archives*. Recuperado: https://discovery.nationalarchives.gov.uk/details/r/C1182

The New Voice of Ukraine [@NewVoiceUkraine] (2022, Feb 28). *Time, the return of history* [Tweet].Twitter, @NewVoiceUkraine. Recuperado: https://twitter.com/NewVoiceUkraine/status/1498197285569810432

The New Zealand Herald (2017, Mar 7). WikiLeaks 'Vault 7' dump reignites conspiracy theories surrounding death of Michael Hastings. *The New Zealand Herald*. Recuperado: https://www.nzherald.co.nz/world/wikileaks-vault-7-dump-reignites-conspiracy-theories-surrounding-death-of-michael-hastings/ELBKFNH3PH425JDXXT44ZAND2Y/

Thomas E. (2019, May 8). HamasCyberHQ.exe has been removed—but what does that actually mean? *Australian Strategic Policy Institute: The Strategist*. Recuperado: https://www.aspistrategist.org.au/hamascyberhq-exe-has-been-removed-but-what-does-that-actually-mean/

Thorndike E. (1898). “Some Experiments on Animal Intelligence". *Science, Vol. VII, 818-824.*

Tidy J. (2022, Jan 14). Ukraine cyber-attack: Russia to blame for hack, says Kyiv. *BBC News*. Recuperado: https://www.bbc.com/news/world-europe-59992531

Tiefenbrun S. (2010). *Semiotic Definition of Lawfare*. Vol 43 Case W. Res. J. Int'l L. 29. Recuperado: https://scholarlycommons.law.case.edu/jil/vol43/iss1/3/

Tirpak J. (2000, Jul 1). Find, Fix, Track, Target, Engage, Assess. *Air force magazine*. Recuperado: https://www.airforcemag.com/article/0700find/

Tobei W. (2012). Nuclear scientists as assassination targets. *Bulletin of the Atomic Scientists, Volume: 68* (issue), p61-69. Recuperado: https://doi.org/10.1177/0096340211433019

Topping A. and Elder M. (2012, Jan 19). Britain admits 'fake rock' plot to spy on Russians. The Guardian. Recuperado: https://www.theguardian.com/world/2012/jan/19/fake-rock-plot-spy-russians

Tor Project (s.f.). History. Recuperado: https://www.torproject.org/about/history/

Toussaint E. (2018). *Sistema Deuda*. Argentina, Buenos Aires: Metrópolis.

Toussaint E. (2020, Apr 9). World Bank and IMF support to dictatorships. *CADTM*. Recuperado: https://www.cadtm.org/World-Bank-and-IMF-support-to-dictatorships

Toussaint E. [RFI español]. (2017, Dec 10). Eric Toussaint "La Deuda" editorial LLL, Paris 2017 [Video]. Recuperado: https://www.youtube.com/watch?v=wkMg69LUXBE

Tree O. (2011, May 5). Did U.S. forces use secret stealth helicopters in bin Laden raid? *Dailymail*. Recuperado: https://www.dailymail.co.uk/news/article-1383482/Osama-Bin-Laden-dead-Did-US-forces-use-stealth-helicopters-raid.html

TrendMicro (2018, Jul 16). The Aurora Power Grid Vulnerability and the BlackEnergy Trojan. *TrendMicro*. Recuperado: https://blog.trendmicro.com/the-aurora-power-grid-vulnerabilityand-the-blackenergy-trojan/

Trevithick J. Rogoway T. (2022, Apr 13). Russia's Black Sea Flagship Moskva Has Exploded Off Ukraine (Updated). *The Warzone*. Recuperado: https://www.thedrive.com/the-war-zone/russias-black-sea-flagship-has-exploded-off-ukraine

Hacquebord F. (2021, Nov 10). The Far-Reaching Attacks of the Void Balaur Cybermercenary Group. *TrendMicro*. Recuperado: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-far-reaching-attacks-of-the-void-balaur-cybermercenary-group

Hacquebord F. (2021, Nov 10). Void Balaur: Tracking a Cybermercenary's Activities. *TrendMicro*. Recuperado: https://documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pdf

The Rothschild Archive (s.f.). The Laurence Fish Collection (Counter-sabotage Devices Drawings). Rothschild Family Papers. Recuperado: https://guide-to-the-archive.rothschildarchive.org/rothschild-family-collection/depts/named-collections/the-laurence-fish-collection-counter-sabotage-devices-drawings

The White House (2022, March 02). Notice on the Continuation of the National Emergency with Respect to Ukraine. Recuperado: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/02/notice-on-the-continuation-of-the-national-emergency-with-respect-to-ukraine-2/

True Crime Magazine [True Crime Magazine]. (2016, Jun 20). *Subliminal Message to the BTK Killer Aired on TV* [Video]. https://www.youtube.com/watch?v=qLVjFji_tu8

Tweedie J. (2019, Jul 17). Secret locations of US nuclear weapons hidden in Europe are revealed in NATO document. *Dailymail*. Recuperado:

https://www.dailymail.co.uk/news/article-7257223/Secret-locations-nuclear-weapons-hidden-Europe-revealed-NATO-document.html

UK Government (2013, Dec 24). Royal pardon for WW2 code-breaker Dr Alan Turing. Recuperado: https://www.gov.uk/government/news/royal-pardon-for-ww2-code-breaker-dr-alan-turing

U.S. Air Force (s.f.). Trinity: World's first nuclear test. *Air Force Nuclear Weapons Center*. Recuperado: https://www.afnwc.af.mil/About-Us/History/Trinity-Nuclear-Test/

U.S. Army (1960, Dec). Outdoor Mosquito Bit~Ng Activity Studies, Project Bellwether-I, BW 459 (U). *Chemical Corps Research and Development Command*. Recuperado: https://apps.dtic.mil/sti/pdfs/AD0596046.pdf

U.S. Army Chemical Corps Historical Office (1960, Jan). Summary of major events and Problems - United States Army Chemical Corps (U). *Army Chemical Center, Maryland*. Recuperado: https://www.osti.gov/opennet/servlets/purl/16006843-5BAfk6/16006843.pdf

U.S. Defense Department (s.f.). Broken Arrows: Nuclear Weapons Accidents. *Atomic Archive*. Recuperado: https://www.atomicarchive.com/almanac/broken-arrows/index.html

U.S. Department of Commerce (2021, Nov 3). Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities. *Office of Public Affairs*. Recuperado: https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

U.S. Department of Defense (s.f.). Ukraine Events Timeline. Recuperado: https://www.defense.gov/Spotlights/Support-for-Ukraine/Timeline/

U.S. Department of Defense (2019, Feb 19). Contracts For Feb. 19, 2019. Recuperado: https://www.defense.gov/News/Contracts/Contract/Article/1760766/

U.S. Department of Defense (2020, Jan 2). Statement by the Department of Defense. Recuperado: https://www.defense.gov/News/Releases/Release/Article/2049534/statement-by-the-department-of-defense/

U.S. Department of Defense (1993, Feb 9). Management of Measurement and Signature Intelligence (MASINT) Instruction ADA272866. Recuperado: https://apps.dtic.mil/sti/pdfs/ADA272866.pdf

U.S. Department of energy (s.f.). The Manhattan Project of interactive History: Einstein's letter (1939). *U.S. Department of Energy - Office of History and Heritage Resources*. Recuperado: https://www.osti.gov/opennet/manhattan-project-history/Events/1939-1942/einstein_letter.htm

U.S. Department of Justice (2003, Aug 1). A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen - Unclassified Executive Summar. *Office of the Inspector General*. Recuperado: https://oig.justice.gov/reports/review-fbis-performance-deterring-detecting-and-investigating-espionage-activities-robert

U.S. Department of Justice (2009, Jul 10). Report on the President's Surveillance Program (unclassified), prepared by the Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of. *Office of the Inspector General*. Recuperado: https://oig.justice.gov/reports/report-presidents-surveillance-program-unclassified-prepared-offices-inspectors-general

U.S. Department of State (2017, April 18). Working tape - 3 - Side A/Side B. Recuperado: https://nsarchive.gwu.edu/document/22850-document-5-u-s-embassy-argentina-audio

U.S. Department of State (s.f.). What is a special military operation? *Bureau of Global Public Affairs*. Recuperado: https://stories.state.gov/what-is-a-special-military-operation/

U.S. Department of State (2023, Sep 14). Imposing Further Sanctions in Response to Russia's Illegal War Against Ukraine. *The Secretary of State*. Recuperado: https://www.state.gov/imposing-further-sanctions-in-response-to-russias-illegal-war-against-ukraine-2/

U.S. Department of Veterans Affairs (s.f.). Edgewood/Aberdeen Experiments. *United States Federal Government*. Recuperado: https://www.publichealth.va.gov/exposures/edgewood-aberdeen/index.asp

U.S. Energy Information Administration (2023, Mar 22). Europe was the main destination for U.S. LNG exports in 2022. *EIA*. Recuperado: https://www.eia.gov/todayinenergy/detail.php?id=55920#:~:text=Europe%20became%20the%20primary%20destination,U.S.%20LNG%20exports%20to%20Europe

U.S.-China Economic and Security Review Commission (2011, Nov). 2011 Report to Congress of the U.S.-CHINA Economic and Security Review Commission. USA, Washington: U.S. Government Printing Office. Recuperado: https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

UFI-AMIA (2022). Informe de la UFI-AMIA sobre el estado de la investigación por el atentado a la Asociación Mutual Israelí Argentina. *Ministerio Publico Fiscal - Procuración General de la Nación - República Argentina*. Recuperado: https://www.mpf.gob.ar/ufiamia/files/2022/07/Informe-de-la-UFI-AMIA-sobre-el-estado-de-la-investigaci%C3%B3n-por-el-atentado-a-la-Asociaci%C3%B3n-Mutual-Israel%C3%AD-Argentina.pdf

Ukraine / Україна [@Ukraine] (2022, Feb 24). *Illustration* [Tweet]. Twitter. Recuperado: https://twitter.com/Ukraine/status/1496716168920547331

Ulrich A. (2005, Jun 5). Hitler's Drugged Soldiers. *Spiegel International*. Recuperado: https://www.spiegel.de/international/the-nazi-death-machine-hitler-s-drugged-soldiers-a-354606.html

Une University of New England (s.f.). Codes and codebreaking: Modern era. Recuperado el 1 septiembre de 2022 en https://www.une.edu.au/info-for/visitors/museums/museum-of-antiquities/exhibitions-and-programs/codebreaker-challenge/enigma

United Launch Alliance [@unitedlaunchalliance] (2013, Dec 6). *Atlas V NROL-39 Launch Highlights* [Video]. Youtube. Recuperado: https://www.youtube.com/watch?v=pobAggvJlOQ&list=UUnrGPRKAg1PgvuSHrRIl3jg

United States Senate (1975, Nov 20). Alleged assassination plots involving foreign leaders. Recuperado: https://web.archive.org/web/20130921171400/http://www.intelligence.senate.gov/pdfs94th/94465.pdf

United States Senate (1976, aprl 23). *Supplementary detailed staff reports on intelligence activities and the rights of Americans - Book III - Final Report of the Select Committee to Study Governmental operations with respect to Intelligence activities*. USA, Washington: US Government printing office. Recuperado: https://www.intelligence.senate.gov/sites/default/files/94755_III.pdfU.S. Air Force (1946, march). Photograph of Hiroshima after Atomic Bombing [Fotografía]. *National Archives Catalog*. Recuperado: https://catalog.archives.gov/id/148728174

U.S. Air Force (1947). Atomic bomb damage in Nagasaki, Japan. (U.S. Air Force Number C58584AC) [Fotografía]. National Archives Catalog. Recuperado: https://catalog.archives.gov/id/204836597

U.S. Congress (2022, Sep 5). S.3522. *Ukraine Democracy Defense Lend-Lease Act of 2022*. Recuperado: https://www.congress.gov/bill/117th-congress/senate-bill/3522/text

U.S. Department of Justice (2018, Sep 25). Former NSA Employee Sentenced to Prison for Willful Retention of Classified National Defense Information. *Department of Justice Office of Public Affairs*. Recuperado: https://www.justice.gov/opa/pr/former-nsa-employee-sentenced-prison-willful-retention-classified-national-defense

U.S. Navy (s.f.). Victory in Europe: Germany's Surrender and Aftermath April–July 1945. *Naval history and Heritage command*. Recuperado: https://www.history.navy.mil/browse-by-topic/wars-conflicts-and-operations/world-war-ii/1945/ve-day/ve-day-aftermath.html

U.S. Navy (s.f.). Victory in the Pacific: Japan's Surrender and Aftermath. *Naval history and Heritage command*. Recuperado: https://www.history.navy.mil/browse-by-topic/wars-conflicts-and-operations/world-war-ii/1945/victory-in-pacific.html

U.S. Department of State (s.f.). The Olympic Boycott, 1980. *U.S. Department of State*. Recuperado: https://2001-2009.state.gov/r/pa/ho/time/qfp/104481.htm

USB Kill (s.f.). *USBKill V4.0* [Fotografía]. Recuperado el 1 de septiembre de 2021 en: https://usbkill.com/

USAF (S.F.). Chapter V: Satellite Systems. *Los Angeles Air Force Base*. Recuperado: https://www.losangeles.spaceforce.mil/Portals/16/documents/AFD-060912-025.pdf

Usenix [USENIX]. (2021, Sep 3). USENIX Security '21 - Weaponizing Middleboxes for TCP Reflected Amplification [Video]. https://www.youtube.com/watch?v=O4Vs_g--5d4

Vague S. (2022). Second army in the world... *ArtStation*. Recuperado: https://www.artstation.com/artwork/8wO45G

Vavra S. (2019, Jul 19). Former NSA contractor sentenced to 9 years for theft of government info. *Cybercoop*. Recuperado: https://www.cyberscoop.com/hal-martin-sentence-nsa-shadow-brokers/

Vega S. (2020). Hollywood y el Pentágono. La producción cultural propagandística del departamento de defensa de Estados Unidos. *Vivat Academia, Nº150*, 81-102. Recuperado: https://dialnet.unirioja.es/servlet/articulo?codigo=7480173

Vincent J. (2021, Aprl 30). 'Deepfake' that supposedly fooled European politicians was just a look-alike, say pranksters. *The Verge*. Recuperado: https://www.theverge.com/2021/4/30/22407264/deepfake-european-polticians-leonid-volkov-vovan-lexus

Vinculando: https://wikileaks.org/nsa-france/

Vinculante: https://www.archives.gov/files/research/jfk/releases/104-10213-10101.pdf

Vivek S., Yanni D., Yunker P. y Silverberg J. (2019, Jul 30). Cyberphysical risks of hacked internet-connected vehicles. *American Physical Society*. Doi: https://doi.org/10.1103/PhysRevE.100.012316

Vlahos M. (2019). *"Men Will Come": A History of the 314th Troop Carrier Group 1942-1945*. USA, NY: Merriam Press.

Von Clausewitz, C. (1832). *Vom Kriege* (on war). Berlin: Dümmlers Verlag.

Von Hein M. (2023, sept 23). Sabotaje de Nord Stream: muchas especulaciones, pocos hechos. *Deutsche Welle*. Recuperado: https://www.dw.com/es/el-sabotaje-de-nord-stream-muchas-especulaciones-pocas-certezas/a-66902816

Wallace R. y Melton K. (2008). *Spycraft: The Secret History of the CIA's Spytechs, from Communism to al-Qaeda*. USA: Dutton Adult.

Walton G. (2001, Jan 1). China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China. *International Centre*

for Human Rights and Democratic Development. Recuperado: https://ora.ox.ac.uk/objects/uuid:084840ac-b192-407b-ab6c-f8f810310369/download_file?file_format=application%2Fpdf&safe_filename=CGS_ENG.pdf&type_of_work=Book

Wechsler H. (2022, Jan 27). CVE-2021-4034: A Walkthrough of Pwnkit – the Latest Linux Privileges Escalation Vulnerability. *WhiteSource*. Recuperado en: https://www.whitesourcesoftware.com/resources/blog/polkit-pkexec-vulnerability-cve-2021-4034/

Weidemann A. (2022, Mar 24). Countering threats from North Korea. *Google Threat Analysis Group*. Recuperado: https://blog.google/threat-analysis-group/countering-threats-north-korea/

Weinberg A. (2021, Jan 19). A step-by-step guide to Silent SMS Attacks and Security. *FirstPoint*. Recuperado: https://www.firstpoint-mg.com/blog/step-by-step-silent-sms-attacks/

Weiss G. (1996). The Farewell Dossier: Duping the Soviets. *CIA, Studies in Intelligence*. Recuperado: https://www.cia.gov/static/887689795bd91ed08ca926a2f6278ee4/The-Farewell-Dossier.pdf

Westwick P. (2010, Oct 21). The International History of the Strategic Defense Initiative: American Influence and Economic Competition in the Late Cold War. *Centaurus, Vol. 52, Issue 4, November 2010, Pages 338-351*. Recuperado: https://onlinelibrary.wiley.com/doi/10.1111/j.1600-0498.2010.00197.x

Wheelis M., Rózsa L., Dando M. (2006). *Deadly Cultures: Biological Weapons since 1945*. USA: Harvard university press.

White G. (2014, Nov 20). Spy cable revealed: how telecoms firm worked with GCHQ. *Channel 4*. Recuperado: https://www.channel4.com/news/spy-cable-revealed-how-telecoms-firm-worked-with-gchq.

White T. (2015, Jul 8). A peek into the new Spy! exhibit coming to Rivercenter Mall. *MYSA*. Recuperado: https://www.mysanantonio.com/news/local/slideshow/A-peek-into-the-new-Spy-exhibit-coming-to-113038.php

Wikileaks (2010, Dec 1). *Hamburg police track polonium trail*. Recuperado: https://web.archive.org/web/20140414012414/http://wikileaks.org/cable/2006/12/06HAMBURG85.html

Wikileaks (2017, Mar 7). Vault 7: CIA Hacking Tools Revealed. *WikiLeaks*. Recuperado: https://wikileaks.org/ciav7p1/

Wikileaks (2018, April 3). RFQ19AR2018Q0017. *US Embassy Shopping List*. Recuperado: https://web.archive.org/web/20211130113431/https://shoppinglist.wikileaks.org/docs/ar_RFQ19AR2018Q0017

William F., Heather A., Harriet M. (2007). Long-Term Health Effects of Participation in Project SHAD (Shipboard Hazard and Defense). *Institute Of Medicine of The National Academies*. Recuperado: https://doi.org/10.17226/11900

Wilson J. (2020, Oct 3). Spain: judge probes Catalan separatism links with Russia. *AP News*. Recuperado: https://apnews.com/article/police-spain-barcelona-2fc97ed44c9cf8d6ac62bcd71b2bcc20

Williams D. (2012, Jan 19). Tinker, Tailor, Soldier... stone: We DID use 'plastic rock' to spy on Russia, admits UK. *Dailymail*. Recuperado: https://www.dailymail.co.uk/news/article-2088575/Tinker-Tailor-Soldier--rock-We-used-hidden-device-spy-Russia-admits-UK.html

Wintonick P., Achbar M. (1992). *Manufacturing Consent: Noam Chomsky and the Media* [Documental]. Necessary Illusions Productions Inc, National Film Board of Canada, Téléfilm Canada.

Wired Staff (2006, May 17). AT&T Whistle-Blower's Evidence. *Wired*. Recuperado: https://www.wired.com/2006/05/att-whistle-blowers-evidence/

Woodward A. (2022, Mar 10). Canadian sniper from famed regiment joins Ukraine's foreign legion: 'I have to help.' *Independent*. Recuperado: https://www.independent.co.uk/news/world/americas/canadian-sniper-ukraine-wali-b2032523.html

World Health Organization (s.f.). Smallpox: WHO response. Recuperado: https://www.who.int/health-topics/smallpox#tab=tab_3

Ymir V. [Ymir Vigfusson]. (2018, Jan 6). *Spectre and Meltdown attacks explained understandably* [Video]. https://www.youtube.com/watch?v=mgAN4w7LH2o

Yoachimik O. (2021, Aug 19). Cloudflare thwarts 17.2M rps DDoS attack — the largest ever reported. *The Cloudflare Blog*. Recuperado: https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/

Young C. (2017, May 18). Shining Light on the Shadow Brokers. *Tripwire*. Recuperado: https://www.tripwire.com/state-of-security/shining-light-shadow-brokers

Zach P. (2022, Mar 2). Double standard on refugees. *ToonPool*. Recuperado: https://www.toonpool.com/cartoons/Double%20standard%20on%20refugees_401569

Zetter K. (2012, Aug 30). Qatari Gas Company Hit with Virus in Wave of Attacks on Energy Companies. *Wired*. Recuperado: https://www.wired.com/2012/08/hack-attack-strikes-rasgas/

Zetter K., Modderkolk H. (2019, Sep 2). Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran. *Yahoo news*. Recuperado: https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html

Zhu Y. (2022, May 11). True colors of U.S. in Russia-Ukraine conflict: Root cause of divisions between the two countries. *People's Daily Online*. Recuperado: http://en.people.cn/n3/2022/0511/c90000-10095080.html

Zuboff S. (2019). *The age of surveillance capitalism: The fight for the human future at the new frontier of power*. USA, NY: Public Affairs.