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

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

TRABAJO FINAL DE MAESTRÍA

CONFORMACIÓN DE EQUIPOS MULTIDISCIPLINARIOS PARA CIBERSEGURIDAD Y CIBERDEFENSA

(UN APORTE A LA POLÍTICA Y ESTRATEGIA DE CIBERSEGURIDAD NACIONAL)

AUTOR: LIC. JUAN CARLOS GUERRA

DIRECTOR: MG. ING. ANÍBAL LUIS INTINI

JULIO 2021

i. RESUMEN

El presente Trabajo Final de Maestría se encuadra, en forma genérica, en el rol de la Ciberseguridad y la Ciberdefensa en los conflictos modernos. Dentro de este marco, se presentará un análisis de las particularidades de estos conflictos, su complejidad y la rápida mutación de sus características distintivas, siempre a la luz del rol cada vez más destacado de las operaciones cibernéticas.

El enfoque multidimensional y multidisciplinario de los conflictos que utilizan y enfrentan amenazas de carácter híbrido, conlleva la necesidad de contar con grupos de expertos sectoriales en grado de desempañarse eficientemente en el análisis de sistemas complejos, la determinación de sus actores, sus interrelaciones, los puntos de poder y debilidad, las estructuras de apoyo, etc. Esto proporcionará al decisor un mapa completo y realista de la situación y de las variables que serán afectadas. En el espacio cibernético, la necesidad de análisis sistémico es también válida y para ello es necesario conformar grupos específicos multidisciplinarios debidamente capacitados para desempeñarse en el llamado 5to dominio.

La precedente propuesta, requiere de una política de Estado que diseñe y conduzca un proceso formativo que asegure la capacitación y adiestramiento continuo de recursos humanos.

El desarrollo de este trabajo comprende un análisis de las características de los conflictos modernos y su vinculación directa con las ciberoperaciones; de los equipos multidisciplinarios necesarios a ser creados y su liderazgo; de las áreas de capacitación comunes de sus miembros en relación a la oferta académica actual; y finalmente del indispensable adiestramiento continuo para mantener e incrementar las capacidades alcanzadas y consolidar los equipos.

Para materializar la propuesta expuesta precedentemente, se desarrollará un trabajo de investigación del tipo metodológico, precedido por una etapa de investigación exploratoria y descriptiva, con un enfoque de análisis cualitativo y de proceso deductivo.

ii. ÍNDICE GENERAL

iii. ÍNDICE DE FIGURAS

Capítulo I: Introducción

Situación (marco de referencia):

Los conflictos actuales a los que se enfrentan los Estados son de naturaleza dinámica y compleja. Se verifica una permanentemente exposición a amenazas y acciones de carácter híbrido que afectan a diferentes organismos de gobierno y/o estructuras críticas nacionales. El carácter híbrido de este entorno, es a su vez transversal en muchos sentidos. No reconoce límites entre las esferas de incumbencia de seguridad y defensa. Se desarrolla en todos los espacios o dominios de conflicto (terrestre, aéreo, marítimo, espacial y ciberespacial), lo que lo convierte en "multidimensional". Sus acciones se planifican y ejecutan en todos los niveles de conducción (estratégico, operacional y táctico). No discrimina objetivos públicos o privados. A menudo, su origen no es abiertamente conocido, individuos, grupos independientes, empresas privadas o los mismos Estados los promueven y/o financian sus acciones.

En este complejo contexto, las operaciones en el ciberespacio se afirman como una herramienta fundamental en los conflictos híbridos.

Esta realidad impone un análisis omnicomprensivo de los problemas que excede al tradicional enfoque de pensamiento lineal. Adicionalmente, debe tenerse en cuenta que la correcta preparación para afrontar contingencias nace en la anticipación estratégica y en la acertada adopción de las medidas preventivas y disuasivas que se prescriban.

En virtud de ello, es imperiosa la determinación de políticas y estrategias de ciberseguridad nacional que contemplen integralmente todo el potencial nacional, sus estructuras críticas y todas las aristas que presentan los conflictos modernos.

Problema evidenciado:

Dentro de la situación general en materia de Ciberdefensa y Ciberseguridad, la formación es un eslabón importante de la cadena. Como tal, una debilidad o vulnerabilidad en un eslabón, repercute en la fortaleza misma de toda la cadena.

En la actualidad, existen estructuras estatales y privadas que atienden esta problemática reclutando personal formado de modo independiente. Cada uno de ellos, mayormente de formación técnica de base, accede a cursos y estudios de posgrado según sus propias inquietudes o necesidades (personales o del empleador). En su trabajo de campo, Guillermo Rutz verifica que "respecto a los criterios curriculares, podemos decir que la mayoría de los casos analizados surgen de experiencias profesionales previas o de carreras en

seguridad informática" (2020, pág. 41) y respecto de la actualización curricular, su studio destaca que "(…) Todos comentan que la propia realidad y práctica va actualizando la curricula" (2020, pág. 57).

Sin embargo, no existe un proceso formal planificado de capacitación integral de sus miembros que garantice la adquisición de conocimientos comunes homogéneos para desempeñarse dentro de equipos multidisciplinarios con objetivos compartidos. Adicionalmente la oferta formativa a nivel local e internacional es muy variada, respondiendo a distintos niveles de capacitación con preponderancia de áreas eminentemente técnicas.

Propuesta de solución:

La simple convocatoria de estos expertos, no asegura por sí sola un verdadero efecto sinérgico. Es necesario entonces, diseñar un itinerario formativo con este fin específico y luego una metodología de adiestramiento que permita mantener e incrementar las capacidades necesarias.

La constitución de equipos multidisciplinarios (propuestos en el Cap III), no se agota en la mera selección de expertos y su convocatoria oportuna a modo de *staff ad hoc* para el análisis y/o resolución de un problema. La sinergia deseable de trabajo en equipo se logra, entre otras cosas, con la formación común en determinadas áreas convergentes, el liderazgo adecuado y la práctica constante.

En virtud de ello, el propósito de este trabajo se orienta a proponer un itinerario concreto para la selección, formación y adiestramiento de recursos humanos para la conformación de equipos multidisciplinarios en el área de Ciberseguridad y Ciberdefensa en los niveles estratégico nacional y sectorial.

Consecuentemente, se vincula con la posibilidad cierta de su incorporación en estructuras del Estado, tales como la Secretaría de Asuntos Estratégicos o la Secretaría de Innovación Pública (Dirección Nacional de Ciberseguridad). Dentro del Ministerio de Seguridad de la Nación, en la Dirección de Investigaciones del Ciberdelito o en la Dirección Nacional de Inteligencia Criminal. En Ministerio de Defensa, en la Subsecretaría de Ciberdefensa, en la Dirección Nacional de Inteligencia Estratégica Militar y eventualmente en el Comando Conjunto de Ciberdefensa.

Capítulo II: Los conflictos modernos y el ciberespacio

Sección I. Las particularidades de los conflictos modernos[1].

¿Por qué es necesario un enfoque multidimensional y multidisciplinario?

A fin de orientar la lectura de esta sección, se debe advertir que la finalidad de la misma se circunscribe a una descripción de los principales postulados teóricos vigentes que sintetizan las formas de la guerra o conflictos actuales, por lo tanto, un análisis profundo de las particularidades del conflicto moderno es, sin duda, un planteo ambicioso que excede los límites de este trabajo de investigación. Sin embargo, es necesario un abordaje inicial polemológico actualizado para dar un verdadero marco teórico de referencia al desarrollo de acciones en el ciberespacio.

Los conflictos (como concepto superior y abarcativo de la guerra), contienen numerosas facetas, con cambios de ritmos y preponderancia de los instrumentos de poder disponibles. Del mismo modo, las operaciones en el ciberespacio no se limitan al plano estrictamente militar, pero los límites en materia de Ciberseguridad y lo que conocemos como Ciberdefensa no sólo son difusos en este dominio, sino que además se retroalimentan, se complementan y hasta se encubren para aumentar el grado de confusión creado ex profeso[2].

Actualmente, es posible encontrar en desarrollo y ejecución, un variado número de teorías y doctrinas militares que, respondiendo a criterios y cosmovisiones propias, surgen para intentar ordenar el pensamiento y estructurar el caos de los conflictos modernos de manera asequible para quienes tienen responsabilidad de conducción.

Tanto en occidente como en oriente, expertos civiles y militares han dado a luz expresiones como guerra de 4ta o 5ta generación, guerra híbrida, guerra irrestricta, guerra asimétrica, guerra civil molecular y guerra no lineal, entre otras. Entrados ya en el Siglo XXI, nadie discute la naturaleza social del fenómeno de la guerra, excediendo el plano puramente militar que reduce el concepto y sesga el pensamiento lineal. Ahora bien, estas teorías /

[1] A continuación se mencionarán tipologías de conflictos que no se condicen necesariamente con la doctrina vigente en nuestro país, pero es necesario conocer las características propias de los mismos, ya que su interpretación y el estudio de su desarrollo nos permiten ampliar nuestra visión de cómo se plantean los mismos y su incidencia en materia de Ciberoperaciones.

[2] Si bien no es punto central del presente trabajo, cabe mencionar que cada país estructura las interrelaciones y precedencias en materia de seguridad y defensa de modo diferente. La República Argentina marca taxativamente un límite en las áreas de responsabilidad de Defensa (Ley 23.5554 Defensa Nacional, 1988) y de Seguridad (Ley 24.059 Seguridad Interior, 1992). Más aún, en materia de inteligencia, el sistema queda definido por la Ley 25.520 (Ley de Inteligencia Nacional, 2001). Esto repercute lógicamente en el tratamiento de acciones u operaciones en el ciberespacio, los cuales requieren de un alto grado de coordinación para lograr la eficiencia deseada.

doctrinas emergentes concuerdan en este punto inicial y recurren a citar otros conceptos como omnicomprensión, multidimensionalidad, alternancia de prioridades de instrumentos de poder, sistemas dominantes a afectar / proteger, etc. Esto ya previene a cualquier analista sobre la complejidad del entramado de factores de los conflictos modernos y la necesidad de una mente avezada en lo que se denomina pensamiento complejo no-lineal.

Los conflictos modernos en la cosmovisión occidental.

La guerra híbrida.

En 2005, dos oficiales del Cuerpo de Infantería de Marina de los Estados Unidos exponen su teoría llamada "Guerra híbrida" (Mattis & Frank, 2005), la cual resulta de gran interés en los círculos militares estadounidenses al punto de convertirse posteriormente en doctrina militar. Este concepto ha ido evolucionando y actualizándose hasta nuestros días. Originalmente el sustento práctico de estos postulados los encontramos ya en la experiencia israelí en las operaciones llevadas a cabo contra milicias de Hezbolah en el sur del Líbano en 2006. Dada su premonitoria y verificada conceptualización, llama inmediatamente la atención de la comunidad intelectual militar.

Sus principales postulados pueden resumirse en los análisis de especialistas que desarrollaron trabajos que combinan la idea original y posteriores publicaciones que abonan el concepto híbrido y multifacético de este tipo de conflictos.

El propio "Hoffman señala que el principio de la guerra convencional no ha perdido vigencia, que Clausewitz tampoco ha perdido notoriedad (las guerras interestatales siguen estando allí), pero sugiere desechar el paradigma que asocia el concepto de las Guerras Interestatales con Ejércitos Convencionales, Guerras entre actores no estatales o con actores no estatales con fuerzas irregulares, pues lo que avizora Hoffman es el advenimiento de una fusión de formas, de organizaciones, de procedimientos convencionales y no convencionales en un mismo espacio de batalla" (Tepedino, Guerra irrestricta, guerra civil molecular y guerra híbrida: tres modos de hacer la guerra en el S. XXI, 2017).

En la misma intención de caracterizar la complejidad omnidireccional, al analizar los trabajos de Hoffman, se afirma que:

> (…) el concepto de guerra híbrida busca fusionar la letalidad del conflicto estatal con el fervor salvaje y fanático de la guerra irregular. El término híbrido captura tanto su organización como sus medios. Las organizaciones pueden tener una estructura política jerárquica, junto con células centralizadas o unidades tácticas en red. En lo que respecta a los medios, estos son híbridos en cuanto a su tipo y a su aplicación. Es decir,

> pueden recurrir tanto al uso de sistemas de comando encriptados, misiles tierra–aire portátiles, así como a emboscadas, ciberataques, dispositivos explosivos improvisados y/o asesinatos. En su aplicación, estas guerras incluyen desde "las capacidades convencionales, las formaciones y tácticas irregulares, actos terroristas, incluyendo coerción y violencia indiscriminada, y desorden criminal". Entonces, las guerras híbridas serían, según Hoffman, las llamadas guerras irregulares, que en esta nueva era serán cada vez más comunes, pero con "mayor velocidad y letalidad que en el pasado debido en parte a la difusión de la tecnología militar avanzada. (Eissa, 2010).

En términos prácticos y viendo lo sucedido en conflictos contemporáneos, observamos que los responsables de dirigirlos intentan con mayor énfasis una mejor comprensión de los conceptos ya vistos de multidimensionalidad y multimedios. Cuenta de ello dan las incursiones estadounidenses en Irak y Afganistán, la cuasi pasividad europea ante la desintegración de Libia, la injerencia de EE.UU y en segundo plano de la OTAN en la fragmentación y virulencia del conflicto étnico-religioso-geopolítico de Siria. Convengamos que los resultados a la fecha no son los esperados por las fuerzas occidentales empeñadas en distinto grado en estos conflictos, pero es claro que la dimensión social, cultural y religiosa son más importante, en términos absolutos, que la dimensión estrictamente militar. Como prueba de ello podemos mencionar el grado de atención de las coaliciones occidentales al manejo de la información, los esfuerzos por contrarrestar la propaganda (inicialmente muy efectiva) de ISIS en redes sociales, la necesidad de no provocar ni caer en provocación de fundamentalistas islámicos que coaccionan para lograr la inclusión directa de Israel en la confrontación, el sostenimiento del frente interno doméstico y su apoyo al esfuerzo militar, las consecuencias de la alternancia de gobiernos democráticos y su postura dogmática particular frente a los conflictos armados, el necesario equilibrio de poder y participación de los miembros de la OTAN al enfrentar distintos escenarios simultáneos con distinto grado de interés / afectación.

En su análisis de la incursión estadounidense en Irak en 2003, cuando el General David Petraeus concibió su estrategia de contrainsurgencia:

> (…) la planificó en esos términos habida cuenta que la batalla en el plano social e info-comunicacional atesora la misma importancia que la batalla militar. En síntesis, esa visión de efectos en distintos ámbitos militares y no militares debe ser sincronizada agregándoles la dimensión temporal y también asimétrica, la asimetría que tradicionalmente era buscada en el plano militar, ahora debe ser procurada en las

> dimensiones no militares del teatro de operaciones. (Tepedino, Guerra irrestricta, guerra civil molecular y guerra híbrida: tres modos de hacer la guerra en el S. XXI, 2017).

La guerra civil molecular.

Para abordar este tema debe hacerse un esfuerzo particular en la afirmación de una mirada multidimensional de los conflictos modernos. Una crisis o guerra intestina en un estado puede ser sólo eso, pero no en pocas ocasiones será un frente de batalla más en un esquema estratégico mayor que enfrenta a ese estado con otro o con intereses no estatales altamente involucrados. Cobra especial atención el concepto de guerras proxy e intervencionismo oculto.

En 1994, el escritor y sociólogo germano Enzensberger, redactó una publicación, en ella prefigura un mundo pos-guerra fría con numerosos conflictos locales y/o regionales en formato de guerras civiles, al punto de afirmar que:

> (…) la guerra civil molecular ha estallado en las metrópolis a escala mundial. Ruanda, Kosovo, Sarajevo, Srebrenica, Timor Oriental, Grozny, Puerto Príncipe, ninguno de ellos se caracterizó por factores ideológicos, sino más bien se ha tratado de conflictos con detonantes étnicos, culturales y religiosos, así como la proliferación de zonas urbanas disputadas y bajo el control de la criminalidad organizada que subroga la ausencia estatal por desidia o abulia. (Enzensberger, 1994).

Los focos de guerra civil molecular del presente son muy diferentes a las guerras civiles del pasado ya que se destaca "(…) la naturaleza autista de los perpetradores y su incapacidad de distinguir entre destrucción y auto-destrucción. En las guerras civiles de hoy ya no existe la necesidad de legitimar las acciones. La violencia se ha liberado de la ideología" (Enzensberger, 1994). Nada tienen que ver con los dogmáticos combatientes nazis o comunistas de la 2da Guerra Mundial, ni con los latinoamericanos de la década del 70', o sus contemporáneos palestinos. El motor idealista (equivocado o no) que los impulsaba, operaba como justificativo de sus acciones. Los vándalos actuales carecen de sentido del honor o valor, su impulso es la ira reaccionaria y la insatisfacción crónica. Enzensberger los cataloga de seres autistas y sin convicciones. Incluso llega a poner en tela de juicio las verdaderas motivaciones de cabecillas de movimientos radicalizados islámicos de los que duda de su verdadera y profunda convicción anclada en postulados religiosos.

En relación con esta teoría que intenta explicar los furiosos y crecientes movimientos internos actuales, es de particular interés del presente trabajo, estudiar la posibilidad de su

instrumentación manipulada por parte de actores externos. Una dimensión más donde las líneas de fuerza se atan con hilos invisibles, pero los efectos son concretos y visibles.

Europa es un caso particular en este sentido. La inmigración clandestina proveniente del Magreb-islámico, los musulmanes de medio oriente y los balcánicos, conforman hoy un entramado social complejo, que lejos de haberse asimilado a las formas comunes europeas occidentales, las desafían desde adentro y abusan de las garantías del sistema normativo para atacar su estilo de vida.

En Latinoamérica, las bandas armadas de Centroamérica (como las Maras salvadoreñas), los otrora grupos armados de liberación de los 60'y 70' devenidos en socios de grupos narcotraficantes y los carteles propiamente, son subconjuntos de focos de guerra civil al oeste del Atlántico.

Como se puede observar, una cosa son las motivaciones reales de los líderes impulsores de estos grupos, pero otra muy distinta es el motor que anima a sus integrantes, como se dijera anteriormente, lejos de convicciones políticas dogmáticas o verdaderamente religiosas.

El abordaje de los conflictos modernos desde la cosmovisión occidental.

Luego de la 2da Guerra Mundial, la naturaleza de los conflictos muta hacia un involucramiento creciente de actores no militares, fundamentalmente en las denominadas guerras de liberación registradas en el sudeste asiático y el África subsahariana. Los componentes sociales, político-ideológicos, religiosos, económicos y diplomáticos emergen como factores trascendentes, haciendo que la simplificación del ambiente estratégico y operacional con sesgos de una solución exclusivamente militar, fracasen rotundamente[3].

La lección aprendida deriva en una visión omnicomprensiva del conflicto, que las doctrinas occidentales (OTAN / UE) adoptan para un mejor entendimiento de la naturaleza del problema, la identificación de actores y factores de poder, el juego de relaciones y los estados iniciales y finales de situación. Esto impone un análisis sistémico de la situación y la concurrencia de especialistas que profundicen en los diferentes dominios e instrumentos de poder que inciden en el conflicto[4].

Las situaciones de crisis complejas son consecuencia de factores de desequilibrio dentro del sistema principal en los que tiene lugar la interacción cotidiana de ciertos dominios

[3] Como referencia obligada se cita los casos de la intervención estadounidense en Vietnam y aquella de la ex-URSS en Afganistán.

[4] Conceptos contenidos en NATO Comprehensive Approach.

sistémicos. Estos dominios son: el de la política, el militar, el económico, el social, el de infraestructura y el informativo. Las condiciones en uno o más de estos dominios pueden verse afectadas e influenciadas por el empleo (normalmente combinado) de los instrumentos de poder que poseen los estados nacionales y las alianzas intervinientes. Dichos instrumentos son: militares, políticos, económicos y civiles.[5]

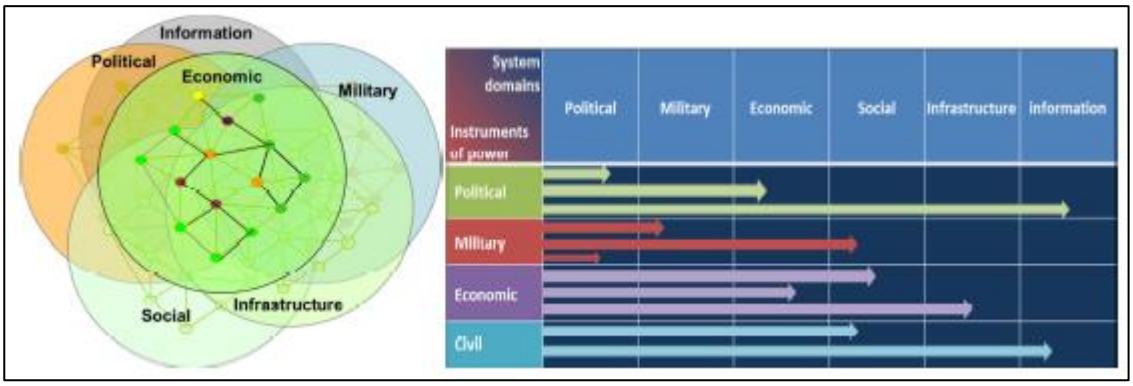


Figura 1: Esquema de aproximación omnicomprensiva. Ilustración a modo de ejemplo no asociada a un caso concreto. (ISSMI, 2015, pág. 20).

Luego del análisis sistémico de base, se diseña el marco general de la estrategia de nivel político donde se emplean todos los instrumentos a disposición, se fija el objetivo general y los objetivos sectoriales, las líneas de acción de cada uno y los efectos parciales a lograr, a fin de concurrir en el estado final deseado que resuelva el conflicto por equilibrio del sistema inicialmente analizado.

[5] La doctrina básica para la Acción Militar Conjunta argentina identifica los "Factores de Poder Nacional" los cuales pueden dividirse en dos grupos en función de su aplicabilidad y origen: "nacional" (geografía, recursos y población) y "social" (económico, político, militar, psicológico e informativo). Para el logro de los objetivos, el Gobierno de la Nación dispone de seis factores de poder: diplomático, político, económico, social, militar y científico-tecnológico que son la forma en que se desagregan para su análisis y tratamiento. (PC-00-01, 2018, pág. 10)

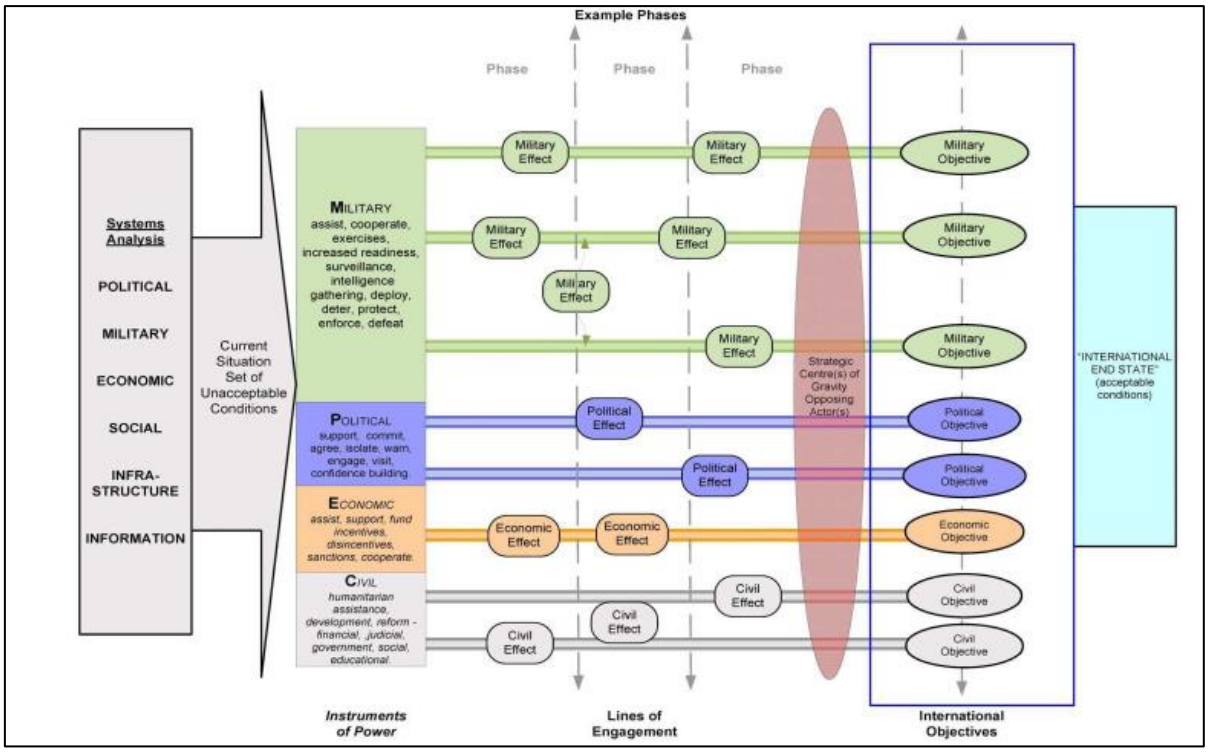


Figura 2: Esquema de diseño estratégico. Ilustración a modo de ejemplo no asociada a un caso concreto (ISSMI, 2015, pág. 27)

Los conflictos modernos en la cosmovisión oriental (China). La guerra irrestricta.

Esta es ya una doctrina militar desarrollada e implementada por el EPL - Ejército Popular de Liberación de China (como se conocen sus Fuerzas Armadas) [6]. Para aproximarnos a sus postulados, es necesario entender primeramente la imposibilidad de leer sus páginas sin cambiar nuestros filtros mentales occidentales. Conceptos tales como el valor de la vida, la trascendencia, el tiempo, las magnitudes en juego y los sistemas políticos que rigen los destinos de China son desde el origen, muy diferentes a los nuestros. Por ende, una lectura despojada de este preaviso equivaldría a una mera traducción literal de expresiones idiomáticas de una lengua extranjera la cual no reflejaría la cultura.

En principio, los Coroneles Qiao Liang y Wang Xiangsui adhieren a los postulados que amplifican los dominios de los conflictos actuales trascendiendo en puro ámbito militar. Bajo esta premisa, S. Tedepino (2017) enfatiza que "barrenar todo tipo de reglas es uno de los principios rectores de la Guerra Irrestricta, un conflicto que se mueve en tres dimensiones, una dimensión militar, otra dimensión transmilitar y una dimensión no militar".

[6] Esta doctrina se apoya en los postulados de los Coroneles Qiao Liang y Wang Xiangsui del EPL de China publicados en 1999 en "*Unrestricted Warfare – Thoughts on War and Strategy in a Global Era*".
Nota: la versión estadounidense publicada en 2002 se titula "*Unrestricted warfare - china's master plan to destroy America*".

MILITAR	TRANSMILITAR	NO MILITAR
1- Guerra Atómica	1- Guerra de Proxys	1- Guerra Ecológica
2- Guerra Biológica	2- Guerra Diplomática	2- Guerra Financiera
3- Guerra Convencional	3- Guerra de Redes	3- Guerra Idiomática
4- Guerra Internacional	4- Cyberwar and Netwar	4- Guerra Mediática
5- Guerra Electrónica	5- Guerra de Inteligencia	5- Guerra de Ayuda Econ.
6- Guerra Espacial	6- Guerra Psicológica	6- Guerra Tecnológica
7- Guerra Política	7- Guerra de Contrabando	7- Guerra Regulatoria
8- Guerra de Guerrillas	8- Guerra Psicotrópica	8- Guerra de Sanciones
9- Guerra Terrorista	9- Guerra Táctica	9- Guerra Información
10- Guerra QBN	10- Guerra Virtual	10- Guerra Ideológica

Figura 3: Esquema descriptivo de la combinación de dimensiones (Tepedino, Guerra irrestricta, guerra civil molecular y guerra híbrida: tres modos de hacer la guerra en el S. XXI, 2017, pág. 6).

El Coronel Qiao Liang dio una entrevista a un medio chino en 1999 donde expresa categóricamente que "(…) la primera regla de la guerra irrestricta es que no existen reglas, no hay nada prohibido" (Liang & Wang, 1999, pág. 2). La posición de los autores chinos respecto de las reglas, se enmarca en el preconcepto de asimetría en el enfrentamiento, por lo tanto observan que los países fuertes no aplican el mismo esquema contra países débiles "(…) las naciones fuertes hacen las reglas mientras que las que están creciendo rompen y explotan algunas. (...) los Estados Unidos rompen y hacen otras reglas nuevas cuando estas no se ajustan a sus propósitos, pero tienen que observar sus propias reglas o el resto del mundo no confiaría en ellos (Liang & Wang, 1999).

En relación a los métodos, esta doctrina propone combinar cualquier medio a disposición para atacar a su oponente: "(…) acciones de hackers en la red, ataques contra instituciones financieras, terrorismo, empleo de medios de comunicación, operaciones de combate urbano, etc" (Liang & Wang, 1999).

Esta multitud de medios y métodos hacen de los conflictos modernos un ambiente multidireccional, de acciones transversales y fundamentalmente desbordantes del mero empleo militar, por ello se afirma el concepto de ir más allá de los límites.

S. Tepedino (2017, pág. 9 a 12) teoriza en su trabajo, agrupando 4 niveles de combinaciones posibles:

> Combinaciones Supranacionales: cuando la Seguridad Nacional está amenazada por actores reales, potenciales o contingentes, la respuesta no implica seleccionar los medios para afrontar militarmente a otras naciones, sino más bien se trataría de una cuestión de difuminar la crisis mediante el empleo de "combinaciones supranacionales" que se revelan como un aspecto esencial de la guerra irrestricta.

Combinaciones de Supradominio: la gran conjugación de tecnologías propias de la Era de la Información es el impulso para que los dominios políticos, económicos, culturales, militares, diplomáticos y teológicos se yuxtapongan, incluso el campo de los Derechos Humanos. Esto implica la combinación de campos de batalla, cada dominio puede posicionarse como el dominio principal de la guerra futura, un ejemplo fructífero de tal combinación fue la Guerra del Golfo Pérsico donde hubo una combinación de Guerra Convencional + Guerra Diplomática + Sanciones de Guerra + Guerra Informativa + Guerra Psicológica + Guerra de Inteligencia.

Combinaciones de Supramedios: Implica la combinación de todos los medios disponibles, es decir, militares y no militares para llevar a cabo operaciones. Las combinaciones supramedios adquirirán preponderancia en todo el S. XXI.

Combinaciones de Supraniveles: Lo que la Guerra Irrestricta busca romper son las reglas de escalonamiento y progreso gradual secuencial por niveles de los enfrentamientos armados, en la lógica del Ejército Popular de Liberación, el nivel de acumulación hasta llegar al cruce de espadas es contraproducente. La guerra tiene otras connotaciones que superan cualquier escala de medida.

Los conflictos modernos en la cosmovisión rusa. La guerra no-lineal o doctrina Gerasimov[7].

En 2013, Gerasimov publicó un trabajo intelectual titulado "El valor de la ciencia está en la capacidad de prever lo que sucederá en el futuro" (Gerasimov, 2016). En el mismo detalla su visión sobre las características multidimensionales de los conflictos modernos, lo que se puede verificar en algunas acciones contemporáneas atribuibles a intereses directos del Kremlin.

De este artículo es posible extraer algunas afirmaciones que describen tal doctrina y la cosmovisión rusa de los conflictos modernos.

"Las «mismas leyes de guerra» han cambiado. El papel que desempeñan los medios no militares para lograr metas políticas y estratégicas ha aumentado y, en muchos casos, ha superado el poder de la fuerza de las armas en cuanto a su eficacia" (2016, pág. 48).

Haciendo un análisis de las lecciones de la denominada "Primavera Árabe", Gerasimov afirma que:

[7] La doctrina Gerasimov (Rusky Nelineynoy Voyne o Guerra No Lineal Rusa), lleva el nombre de su creador, el General Valery Gerasimov Jefe del Estado Mayor General de las Fuerzas Armadas de la Federación Rusa.

> El enfoque de los métodos usados en el conflicto ha cambiado la dirección del uso general de medidas políticas, económicas, de información, humanitaria y demás medidas no militares; usadas en coordinación con el potencial de protesta de la población. Todo esto se complementa con medios militares de carácter oculto, incluyendo llevar a cabo acciones de conflicto informativo y acciones de fuerzas de operaciones especiales. El uso abierto de las fuerzas - a menudo, bajo el pretexto de mantenimiento de la paz y regulación de crisis - sólo ha sido empleado en un determinado momento, sobre todo para el logro del éxito final en el conflicto. (2016, pág. 48).

Más adelante, observando la nueva dinámica de los procesos en los llamados niveles de conducción militares, asegura que todo ha cambiado:

> Los enfrentamientos directos de grandes formaciones de fuerzas en el nivel estratégico y operacional se están convirtiendo gradualmente en cosa del pasado. Las acciones sin contacto a larga distancia contra el enemigo se están convirtiendo en los medios principales para lograr las metas de combate y operacionales. La derrota de los objetivos enemigos se lleva a cabo a través de todo su territorio. Las diferencias que existen entre los niveles estratégicos, operacionales y tácticos, así como entre las operaciones ofensivas y defensivas están siendo eliminadas. (2016, pág. 49).

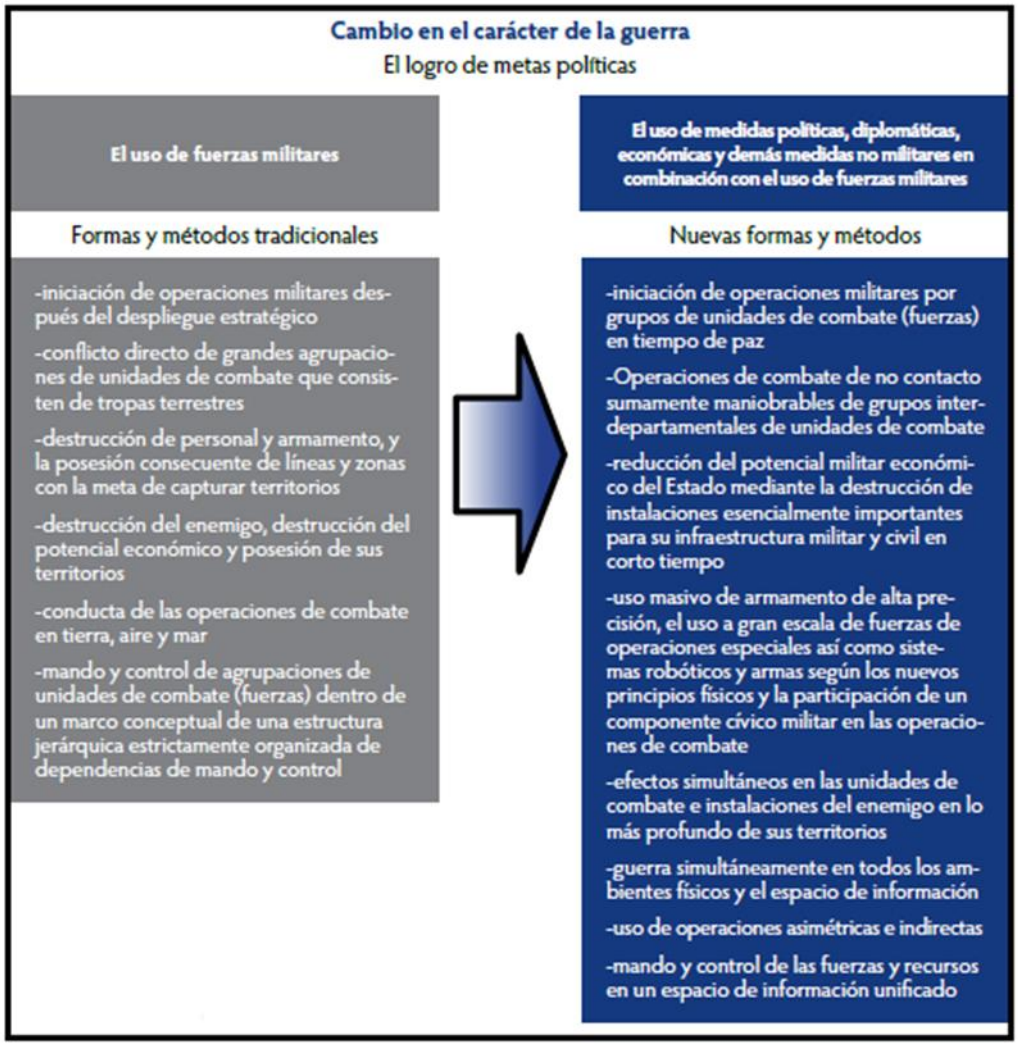


Figura 4: Diseño gráfico del artículo (Gerasimov, 2016, pág. 49)

Según de S. Tepedino (2019), el artículo es la formulación más vívida de la estrategia moderna rusa. La visión de una guerra total que coloca a la política y a la guerra dentro del mismo rango de acciones. Dentro de esta categoría se concentran métodos técnicos, tácticos y estratégicos, tales como:

- ✓ Subcontratación de Fuerzas Militares.
- ✓ Creación de movimientos insurgentes.
- ✓ Revolución de Colores.
- ✓ Ciberguerra.
- ✓ Hacktivismo.
- ✓ Guerra de información (Operaciones de Información).
- ✓ Operaciones de injerencia (en los asuntos internos de otras naciones).
- ✓ Operaciones psicológicas.
- ✓ Medidas activas.
- ✓ Maskirovka (encubrimiento) y desinformación.
- ✓ Guerra Centrada en Redes (Netwar).
- ✓ Operaciones financieras.

✓ Operaciones con armamentos de alta tecnología (incursión aérea rusa en Siria).

Gerasimov resume el abanico de opciones combinadas y sincronizadas de medios militares y no militares en eje con los estadios del conflicto y el papel que cada uno de ellos juega en ese entramado único.

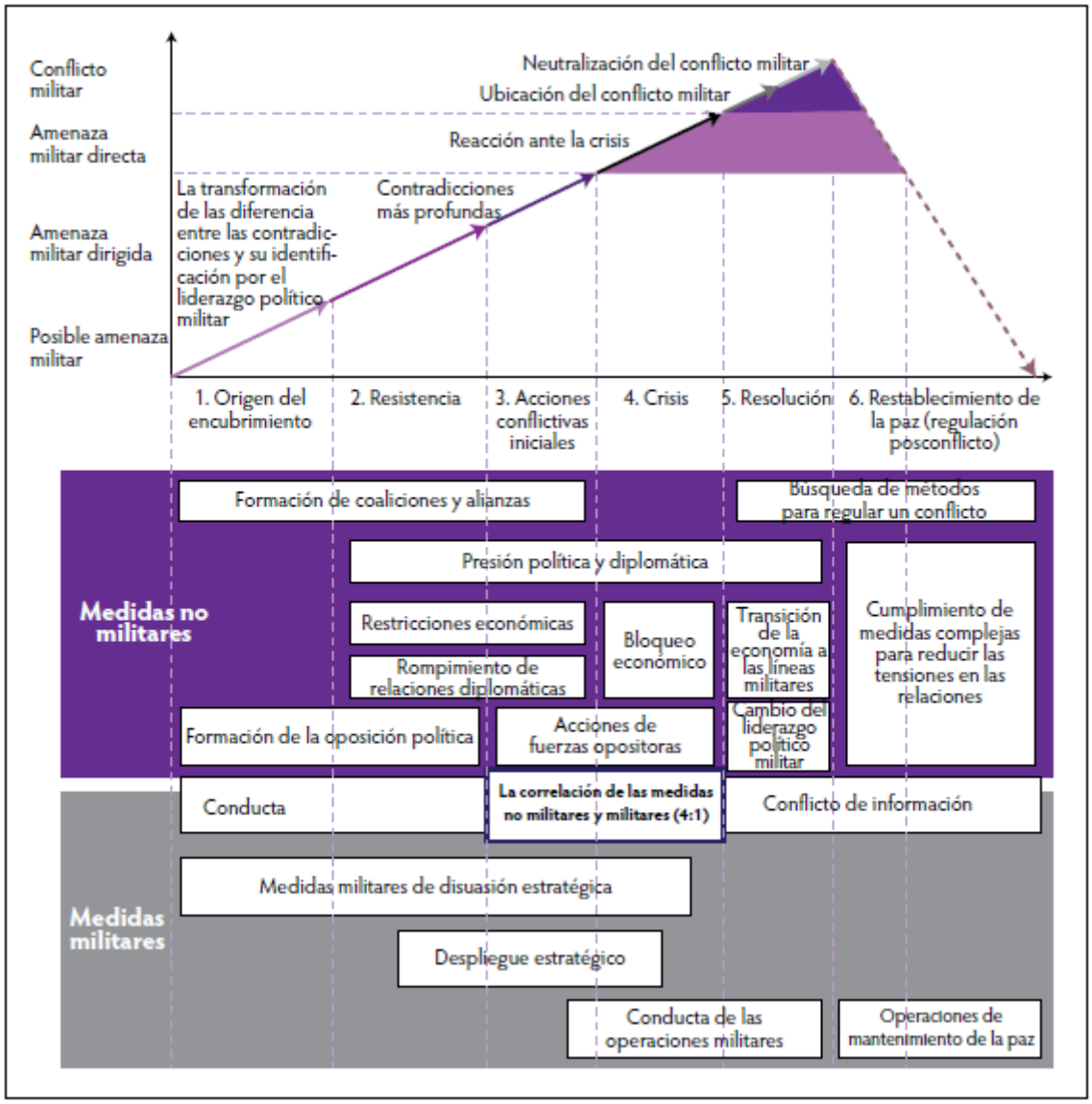


Figura 5: Diseño gráfico del artículo (Gerasimov, 2016, pág. 53)

Ahora bien, no son pocos los analistas que identifican la aplicación de la doctrina Gerasimov en los sucesos ocurridos en Ucrania en 2014 y la anexión de Crimea (Collom Piell, 2018) (Makotczenko, 2019). La combinación sincronizada de operaciones de fuerzas irregulares, fuerzas especiales encubiertas, ciberataques, operaciones de desinformación, financiamiento económico e insurrección civil, pueden dar cuenta de ello.

Del mismo modo, recaen fuertes sospechas sobre la injerencia rusa en las elecciones presidenciales estadounidenses de 2016 que culminan con el ascenso al poder de Donald Trump[8]. En ambos casos resuenan las afirmaciones de Gerasimov: "El espacio de la información ofrece amplias oportunidades asimétricas para reducir el potencial de combate del enemigo" (2016, pág. 51).

Habiendo expuesto las principales ideas rectoras de las teorías / doctrinas militares contemporáneas, es posible establecer un patrón común en cuanto a la multidimensionalidad del conflicto y los métodos empleados para su resolución. La preponderancia exclusiva de métodos y medios militares se ve superada por la combinación sincronizada de métodos y medios no militares y según la cosmovisión de cada actor, se ve incluso venida a menos en un plano complementario. Otra característica común es la apelación al ciberespacio y las acciones que en él se desarrollan como de importancia cada vez más gravitante.

Debemos tener en cuenta, que no estudiamos estos conceptos teóricos para aplicarlos sobre nuestro pensamiento como producto final importado[9], sino como un modo de entender cómo los aplican los actores que detentan el poder y aquellos que buscan hacerse fuertes en las posibilidades de la asimetría, viendo en ella no solamente una posición débil, sino la exigencia de encontrar creativamente soluciones alternativas en escenarios donde la misma sea equiparada. Uno de ellos es el ciberespacio.

Sección II. El ciberespacio en los conflictos modernos.

El desarrollo de esta sección intenta vincular las características singulares del ciberespacio, y las acciones en él desarrolladas, con los conceptos precedentes sobre las particularidades distintivas de los conflictos modernos. La irrupción de esta dimensión, no sólo es relativamente reciente, sino que lo es de modo permanente de cara al futuro.

El ciberespacio, un dominio particular.

Se han vertido un sinnúmero de expresiones para definir qué es el ciberespacio y cuál es su lugar dentro de los dominios tradicionales donde se desarrollan los conflictos. A los fines de este trabajo, es innecesario, abonar un concepto más a la discusión sintáctica y semántica en torno a la palabra ciberespacio, sin embargo es menester resumir sus características y comprender las acciones reales en él y aquellas potenciales en un futuro aparentemente sin fronteras.

[8] En Argentina se ha vinculado a Cambridge Analytica con trabajos locales antes de las elecciones de 2015. URL: https://www.lanacion.com.ar/politica/cambridge-analytica-hizo-trabajos-pro-antes-campana-nid2289827/
[9] Sin perder de vista las particularidades de los ámbitos de injerencia de seguridad y defensa en nuestro país.

De Vergara y Trama (2017) realizan una síntesis de las definiciones existentes en ámbitos académicos y militares las cuales coinciden en mayor o menor grado en afirmaciones tales como:

> El Espacio cibernético es lo que se denomina un Global Common, entendiendo por tal aquel entorno en los que ninguna persona o estado puede tener su propiedad o control exclusivo pero que son básicos para el desenvolvimiento de la vida de las personas y de las colectividades. Son Global Commons el mar, el espacio extraterrestre, el espacio electromagnético y por supuesto el espacio cibernético que, sin embargo, posee una serie de características diferenciales del resto de los espacios. Feliú, Ortega (Feliu Ortega, 2012, pág. 42).

Otra cualidad relevante que suele señalarse del ciberespacio es su carácter virtual. Sin embargo, este dominio artificial creado por el hombre no es intangible al 100%. A similitud con el espacio electromagnético, cuenta con elementos concretos que interconectan lo virtual con lo real. En este sentido podemos citar a los dispositivos de hardware sobre los que corren o se almacenan millones de bits que contienen virtualmente lo que denominamos dato. En línea con ello se expresa el Dr. Roberto Uzal (Uzal, 2013) quien conceptualiza al ciberespacio como "la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan".

Este dominio, por lo tanto se soporta tanto en el mundo real físico como en el virtual. Este detalle no es menor, ya que las acciones en el ciberespacio podrán ser ejecutadas en cualquiera de ellos. Por derivación, se plantea una cuestión de límites sobre los cuales reclaman para sí dominio y exclusividad aquellos que intentan ejercer el poder. ¿Qué será entonces un ataque físico a un servidor esencial de una infraestructura crítica del oponente?. Es aquí donde es conveniente no imponer límites teóricos que dividen y no aportan una solución al problema. En reemplazo del concepto de límites, es necesario trascender a un concepto de frontera. Por analogía del término geográfico, los puntos de anclaje físicos del ciberespacio en el mundo real, deberían ser considerados duales y su acción como integradora, tal como las actividades que desarrollan los seres humanos en zonas fronterizas que vinculan a unos y otros en intereses comunes para bien común. Las responsabilidades son compartidas y yuxtapuestas.

Describiendo la naturaleza del ciberespacio, la doctrina estadounidense (US JP 3-12, 2018, págs. I-2) lo ubica como parte del ambiente de información, y dependiente de los dominios físicos de tierra, aire, mar y espacial. Por consiguiente las operaciones en el

ciberespacio dependen de infraestructura de IT y de los datos que residen y se transmiten a través de estos componentes para permitir operaciones militares en un dominio hecho por el hombre.

El siguiente cuadro exhibe la multiplicidad de agencias que la doctrina estadounidense involucra en la planificación y ejecución de operaciones en el ciberespacio.

United States Code (USC)	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland security	Department of Homeland Security	Security of US cyberspace
Title 10	*Armed Forces*	National defense	Department of Defense	Man, train, and equip US forces for military operations in cyberspace
Title 18 Title 28	*Crimes and Criminal Procedure* *Judiciary and Judicial Procedure*	Law enforcement	Department of Justice	Crime prevention, apprehension, and prosecution of criminals operating in cyberspace
Title 32	*National Guard*	National defense and civil support training and operations, in the US	State Army National Guard, State Air National Guard	Domestic consequence management (if activated for federal service, the National Guard is integrated into the Title 10, USC), *Armed Forces*
Title 40	*Public Buildings, Property, and Works*	Chief Information Officer roles and responsibilities	All Federal departments and agencies	Establish and enforce standards for acquisition and security of information technologies
Title 44	*Public Printing and Documents*	Defines basic agency responsibilities and authorities for information security policy	All Federal departments and agencies	The foundation for what we now call cybersecurity activities, as outlined in Department of Defense Instruction, 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations*.
Title 50	*War and National Defense*	A broad spectrum of military, foreign intelligence, and counterintelligence activities	Commands, Services, and agencies under the Department of Defense and intelligence community agencies aligned under the Office of the Director of National Intelligence	Secure US interests by conducting military and foreign intelligence operations in cyberspace

Figura 6: US Code (US JP 3-12, 2018, págs. III-2).

A modo de síntesis, se recurre a la didáctica explicación de la doctrina estadounidense que propone una visión, el ciberespacio en capas, la física, la lógica y la social, cada una de las cuales representa un nivel en el cual se podrán conducir operaciones cibernéticas.

La capa física es el medio por donde transitan los datos. El componente geográfico es la ubicación, ya sea en tierra, en el aire, el mar o el espacio, donde se encuentran los elementos de las redes. Los componentes físicos comprenden el hardware y la infraestructura (los cables, los sistemas wireless, los enlaces electromagnéticos, los satelitales y los ópticos), que apoyan a las redes y a los conectores físicos (cables, radio frecuencia, routers, switches, servers y computadoras).

La capa lógica consiste en aquellos elementos de la red que se relacionan unos con otros de manera que se abstraen de la red física, es decir, la forma o las relaciones no están vinculadas a un individuo, ruta de acceso específica o nodo. Un ejemplo simple es cualquier sitio web que está alojado en los servidores en múltiples ubicaciones físicas donde se puede acceder a todo el contenido a través de un localizador URL.

La capa social, de las ciber-personas, consiste en las personas que se encuentran en un determinado momento presentes en la red. Una sola ciber-persona puede tener varios usuarios. En consecuencia, la atribución de responsabilidad en el espacio cibernético es difícil. (US JP 3-12, 2018, págs. I-3)

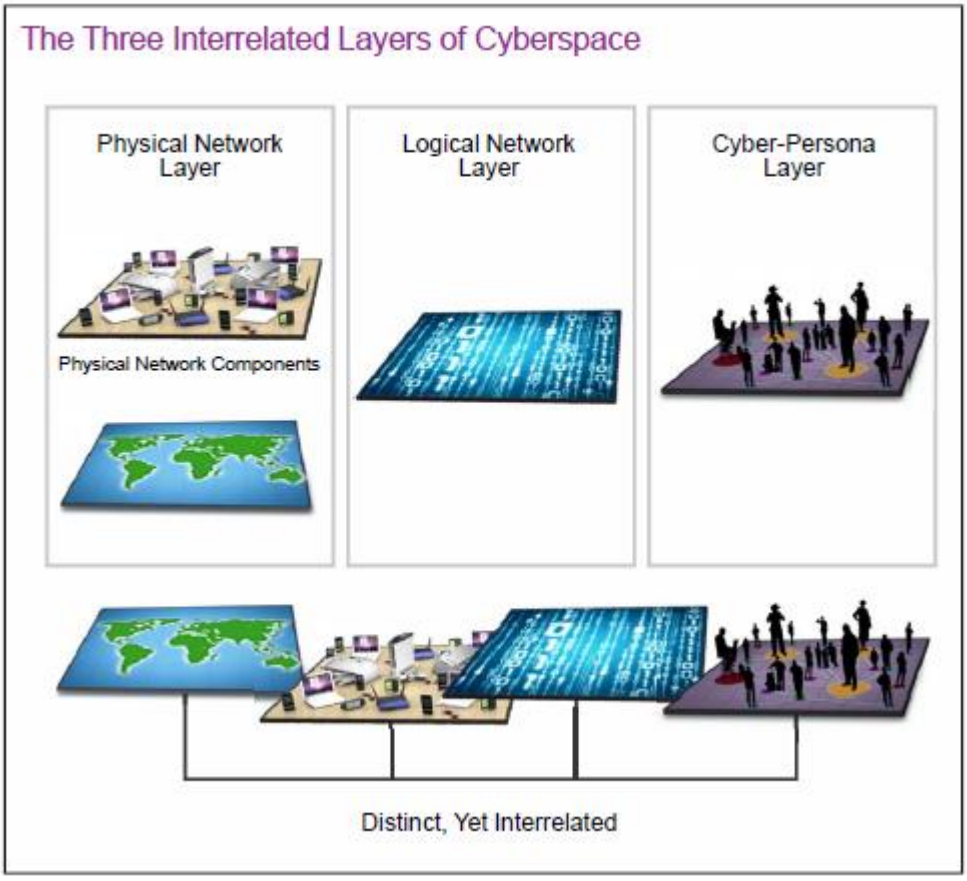


Figura 7: El ciberespacio en capas (US JP 3-12, 2018, págs. I-3)

Esto último es una característica propia del ciberespacio, el problema de la atribución[10]. Respecto de la posibilidad cierta de definir la atribución de una acción en este ambiente, existen opiniones encontradas, desde quienes la descartan completamente, hasta quienes sostienen su posibilidad concreta. Este punto no debe ser considerado aisladamente, ya que sus consecuencias derivan en un problema de orden práctico: la posibilidad o no de

[10] Capacidad de determinar fehacientemente (con prueba científica) la autoría de una acción.

recurrir a acciones de represalia con mayor o menor sustento legal[11]. Este es uno de los mayores escollos con los que tropieza la legitimidad y la legalidad a la hora de accionar en el ciberespacio. Asimismo, el problema de la atribución crea a su vez una zona gris donde aquellos agresores que no se rigen por análogos valores, encuentran un terreno fértil en estructuras autoimpuestas por los defensores que serán aprovechadas en su propia contra.

Por todo lo expresado, este nuevo espacio artificial y compuesto (real + virtual) requiere de un tratamiento particular que no puede ser automáticamente equiparado con las leyes que rigen los otros dominios físicos considerados.

Esquematizando ciertas afirmaciones definitorias de las características del ciberespacio, José Casar Corredera (Casar Corredera, 2012) enuncia una serie de diferenciales del resto de los espacios.

- El espacio cibernético es un entorno único, en el que el atacante puede estar en cualquier parte del globo.
- En la defensa intervienen muchos factores, y no sólo elementos estatales sino también privados. Se exige pues una estrecha coordinación entre todos ellos.
- La confrontación en el espacio cibernético presenta frecuentemente las características de un conflicto asimétrico; y es frecuentemente anónimo y clandestino.
- Permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema y, a menudo, sin delatarse.
- Permite también ejercer el chantaje; pero, al mismo, tiempo, la defensa puede utilizarlo para la disuasión.
- Evoluciona rápidamente siguiendo la evolución tecnológica de las TIC.

Operaciones en el ciberespacio.

Habiendo explorado las características distintivas del ciberespacio como dominio en el cual se llevan adelante acciones propias de su naturaleza y desde el cual se proyectan sobre los llamados dominios tradicionales, es necesario ahora describir cuales son algunas de estas acciones y su lugar dentro de las esferas de responsabilidad de cada instrumento de poder.

[11] Es el caso de aplicación o no del Art 51 de la Carta de las Naciones Unidas: “Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales”.

Las acciones en este dominio pueden ser aisladas, con fines en sí mismas y perpetradas por individuos con distintas motivaciones. En esta categoría podríamos agrupar lo que comúnmente denominamos ciberdelitos, acciones cibernéticas llevadas a cabo por hackers con finalidad delictiva, auto-test de capacidades o motivos religiosos / dogmáticos / políticos.

Si consideramos esas acciones (aparentemente aisladas) en conjunto con otras acciones enfocadas hacia un objetivo y con algún grado de coordinación o sincronización de sus efectos, podríamos encontrarnos en presencia de una operación cibernética.

Así, el prefijo "ciber" podría ser (y de hecho es) empleado para casi cualquier acto que involucre origen o vector dentro del dominio cibernético. Ciber Terrorismo, Ciber Espionaje, Ciber Crimen, Ciber Agresiones, Ciber Guerra, Ciber Lavado de Activos, son sólo algunos ejemplos.

A este esfuerzo de segmentación y definiciones catalogables, se suma el problema ya mencionado de la ciber atribución (incluyendo la disquisición más fina sobre su origen puramente estatal, individual, mixto, público, privado, etc.), y luego el esfuerzo de acertar en el objetivo perseguido (aparente y real) del o de los perpetradores y sus superiores (responsables materiales e intelectuales de los hechos).

Estas operaciones pueden ser desarrolladas a su vez dentro de cualquier instrumento de poder considerado (político, militar, económico, etc). Incluso pueden coordinar acciones o sincronizar efectos entre ellos si existe una entidad superior que los nuclea y dirige.

Un simple ataque cibernético a un banco podría ser tanto un acto delictivo de uno o más individuos con intenciones criminales puras, como una acción (coordinada con otras) de un grupo financiero independiente (o proxy de un estado) para provocar la degradación o colapso financiero en una entidad o país determinado. Este a su vez, puede ser el objetivo final de esa operación en ámbito financiero, o se podría enmarcar en un conjunto de operaciones con efectos sincronizados con otros instrumentos en más de una dimensión con una finalidad ulterior más importante[12].

Es aquí donde la discusión sobre límites y fronteras recobra valor. Las acciones y/u operaciones con intenciones variadas y sobre objetivos diversos, serán normalmente esquivas a su catalogación y se servirán de esta dicotomía intelectual que causa parálisis operativa. Las zonas grises de nuestros sistemas legales, de defensa / seguridad, de jurisdicción política, económica, etc., son sin dudas el ámbito donde correrán los sendero de estas actividades.

[12] Desde el punto de vista nacional, esta complejidad sólo incrementa la magnitud del problema. Debemos recordar que la ciberdefensa y ciberseguridad tienen competencias distintas, y debieran actuar de manera conjunta y coordinada.

Para añadir mayor dificultad al entramado de las acciones en el ciberespacio, no se restringen solamente a la sustracción de datos útiles, el espionajes estatal / industrial o la afectación de sistemas digitales de defensa u operaciones financieras. Existen también operaciones de información (De Vergara & Trama, 2017, pág. 48) para hacer equivocar al enemigo en sus decisiones, y operaciones de redes y sistemas de redes para alterar el funcionamiento de los sistemas cibernéticos en los que los algoritmos reemplazan a la decisión del hombre.

Operaciones en el ciberespacio dentro del instrumento militar.

¿Guerra Cibernética u Operaciones Militares Cibernéticas? Existe también aquí una discusión teórica de definiciones las cuales no arriban a una conclusión determinante. Sin embargo, su tratamiento en el ámbito militar no es una cuestión menor. Si se quiere actuar ajustado a derecho en el plano internacional (o las circunstancias lo obligan), no podemos olvidar los límites que impone la invocación del Artículo 51 de la Carta de Las Naciones Unidas al cual ya se ha hecho referencia.

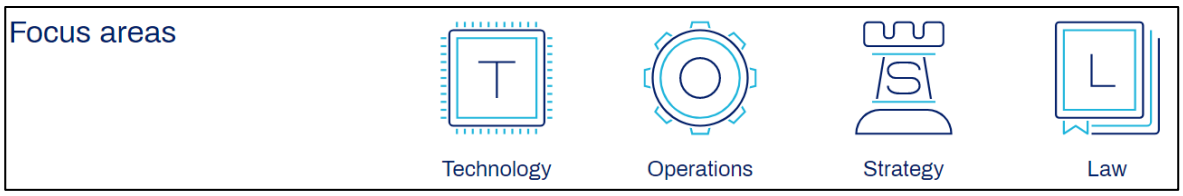
De Vergara y Trama (2017, pág. 42) abordan esta problemática y se preguntan: ¿cuál es la validez del concepto de agresión expresado en la Resolución ONU 3314/74 titulada Definición de la agresión? ¿Cuál de toda esta muestra de incidentes cibernéticos pueden ser considerados por los analistas vernáculos como “agresiones militares estatales externas” que afectan específicamente el ámbito de la Defensa Nacional? ¿Puede ser considerado como un ataque el acceder a una computadora (o sistema de cómputos) sin autorización, o excediendo el nivel de acceso autorizado y, por medio de esa conducta, obtener información?. En conclusión, ¿los trataremos como actos delictivos o acciones de guerra?

Adentrándonos más aún en el ámbito militar, los conflictos de nuestra era son indiscutiblemente de carácter conjunto[13]. Asociando las Fuerzas que se crean para actuar en cada dominio referido (Ejército - tierra / Fuerza Aérea – aire / Armada – mar / Fuerza Espacial – espacio (en el caso de las FFAA estadounidenses), el ciberespacio es considerado de modo diferente por cada país. Sin embargo, en la mayoría de las Fuerzas Armadas se han creado Comandos de Ciberdefensa Conjuntos que coordinan las actividades propias en el ciberespacio de los Comandos de Ciberdefensa de cada Fuerza y tienen una fuerte injerencia

[13] Definición que expresa el empleo coordinado de fuerzas terrestres, navales y/o aéreas. Para ser identificadas como conjuntas según la doctrina militar argentina deben empeñarse al menos 2 de las 3 Fuerzas consideradas.

a nivel nacional como el USCYBERCOM[14]. Aun así, hay Comandos de Ciberdefensa que se restringen exclusivamente a proteger la infraestructura crítica militar de sus Fuerzas Armadas y otros a los que se les ha confiado trascender el ámbito puramente castrense y atender infraestructuras criticas nacionales asignadas.

Existen también organismos multinacionales como el NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE, s.f.). Este centro, con sede en Tallin (Estonia), es en esencia una entidad cuya misión es apoyar a países miembros y a la OTAN con un enfoque interdisciplinario en el campo de la investigación, el entrenamiento y los ejercicios de ciberdefensa que cubren las áreas de tecnología, estrategia, operaciones y derecho.



El corazón del CCDCOE es un grupo heterogeneo de expertos de 25 naciones: Austria, Bélgica, Bulgaria, la República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Italia, Letonia, Lituania, los Países Bajos, Noruega, Polonia, Portugal, Rumania, Eslovaquia, España, Suecia, Turquía, Reino Unido y Estados Unidos. El mismo reúne a investigadores, analistas y educadores de las Fuerzas Armadas, del gobierno, de la academia y de la industria.

La apreciación del Escenario Global y Regional de la República Argentina (DPDN, Directiva de Política de Defensa Nacional, 2018) nos brinda el enfoque particular de nuestro país sobre esta materia al señalar que:

> Las amenazas cibernéticas sofisticadas provienen de organizaciones militares y agencias de inteligencia de otros Estados. Si bien los gobiernos tecnológicamente avanzados explotan sus ventajas comparativas con relación al resto de los países, el despliegue de operaciones disruptivas en el ciberespacio también está al alcance de las naciones menos desarrolladas. El abordaje de esta problemática desde la perspectiva de la Defensa Nacional requiere adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional y de aquellas que sean designadas para su preservación, independientemente del origen de la agresión.

[14] USCYBERCOM es un organismo dependiente del Departamento de Defensa a través del Comando Estratégico (USSTRATCOM). Desde su fundación, el Comandante del USCYBERCOM es a su vez el Director de la Agencia Nacional de Seguridad (NSA). Misión: *The Commander, USCYBERCOM, has the mission to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners*. https://www.cybercom.mil/

Más adelante, en el apartado *"Utilización del ciberespacio con fines militares",* se encuadra al ciberespacio dentro del esquema de la política de defensa nacional entendiendo que "(…) la consolidación del ciberespacio como un ambiente operacional militar configura una amenaza de interés estratégico para la Defensa Nacional" y por lo tanto, "(…) la REPÚBLICA ARGENTINA debe adecuar sus organizaciones militares al impacto que emerge de estos nuevos riesgos. La política de Ciberdefensa debe orientarse a la reducción gradual de las vulnerabilidades que emergen de la informatización de los activos estratégicos de interés para la Defensa Nacional. Esta tarea debe contemplar la cooperación con otras áreas del Estado que tengan responsabilidad en la política de Ciberseguridad nacional".

No obstante los distintos organismos que se crean para abordar el problema de la Ciberdefensa, es lógico reconocer que están concebidos a la luz de las leyes locales y su posición respecto de las relaciones internacionales, sus usos y costumbres y lo que dicta el Derecho Internacional Público.

En el caso de los EEUU, el cual incluye una Fuerza Espacial para desempeñarse exclusivamente en este domino, entiende que:

> Las operaciones en el ciberespacio utilizan enlaces y nodos ubicados en los dominios físicos y realizan funciones lógicas para crear efectos primero en el ciberespacio y luego, según sea necesario, en los dominios físicos. Acciones en el ciberespacio, a través de efectos en cascada cuidadosamente controlados, pueden permitir la libertad de acción para actividades en los dominios físicos. Asimismo, actividades en los dominios físicos pueden crear efectos en y a través del ciberespacio al afectar el espectro electromagnético o la infraestructura física. La relación entre el espacio (como dominio particular) y el ciberespacio es única, ya que prácticamente todas las operaciones espaciales dependen del ciberespacio, y una porción crítica del ancho de banda del ciberespacio sólo se puede proporcionar a través de operaciones espaciales, que proporcionan una opción de conectividad global clave para las operaciones en el ciberespacio. (US JP 3-12, 2018, págs. I-2).

En el empleo concreto del dominio cibernético, cada estado distingue categorías de operaciones cibernéticas y desarrolla estructuras y capacidades acordes para ello.

En general, tal como sostiene Héctor Gómez Arriaga (Gomez Arriagada, 2013), las ciberoperaciones deberían entenderse como un instrumento más para la solución de problemas militares en su amplio espectro y, por lo mismo, implican eventualmente enfrentar a un antagonista. Pueden, por tanto, ser defensivas cuando buscan detectar, neutralizar y mitigar el impacto de un ataque; o bien, ser ofensivas cuando se utilizan para obtener inteligencia a

través del espacio cibernético o para negar su empleo. Es decir, las ciberoperaciones implican intencionalidad, voluntades contrapuestas y el enfrentamiento en el espacio cibernético con fines militares, elementos clave que permiten distinguir las ciberoperaciones de otras actividades como la seguridad informática o las operaciones de información.

Los mismos autores resumen la categorización de distintos países exponiendo similitudes y diferencias (De Vergara & Trama, 2017, págs. 48-58):

Para Francia, las operaciones en el espacio cibernético incluyen acciones defensivas (lucha informática defensiva "LID"), las acciones de exploración (u exploración informática, "IE") y las acciones ofensivas (o lucha informática ofensiva, "LIO"). Todas ellas son conducidas por la cadena de comando operacional de defensa cibernética.

Para el Reino Unido, las operaciones cibernéticas son la planificación y sincronización de actividades en y a través del espacio cibernético para permitir la libertad de maniobra y, de esa manera, alcanzar los objetivos militares. Pueden categorizarse en cuatro funciones distintas: las operaciones cibernéticas defensivas (DCO); las operaciones cibernéticas ofensivas (OCO); las operaciones de ciberinteligencia, vigilancia y reconocimiento (IVR); y las operaciones cibernéticas de preparación operacional del ambiente.

Según la doctrina brasileña, las ofensivas comprenden las acciones para interrumpir, negar, degradar, corromper o destruir informaciones o sistemas de computación almacenados en dispositivos o redes de computadoras o de comunicaciones del oponente. Las de protección son aquellas que se llevan a cabo de manera permanente con la finalidad de neutralizar los ataques o la exploración cibernética contra las computadoras o redes de computadoras y de comunicaciones propias e incrementan las acciones de seguridad y defensa en una situación de crisis o conflicto.

Para los Estados Unidos de América, tomando como base lo establecido por el USCYBERCOM, las operaciones cibernéticas constan de tres líneas diferentes: operaciones de red del Departamento de Defensa, operaciones de espacio cibernético defensivas y operaciones de espacio cibernético ofensivas. El área de operaciones de red del Departamento de Defensa (DoDIN) incorpora actividades para diseñar, construir, configurar, asegurar, operar y mantener, así como sostener redes del Departamento de Defensa con el fin de crear y preservar la seguridad de la información en las redes de información de dicho Departamento. El área de operaciones defensivas en el espacio cibernético (DCO) consiste en operaciones pasivas y activas en el espacio cibernético que pretenden preservar la capacidad de utilizar el espacio cibernético y proteger datos, redes y capacidades centradas en redes. El área de

operaciones ofensivas (OCO) incorpora todas las operaciones realizadas para proyectar el poder contra adversarios en o a través del espacio cibernético.

Englobando características asociativas de los dominios en estudio se verifica que, en el espacio cibernético, pueden apreciarse efectos tanto en el nivel estratégico, como en el operacional y en el táctico, lo que no ocurre en el dominio espacial. Asimismo, en el espacio cibernético convergen actores civiles internos e internacionales, comerciales y gubernamentales, los que van a influenciar sobre las operaciones cibernéticas militares. Luego, tal como ocurre con los dominios territoriales, habrá que preocuparse del fratricidio, de los no combatientes, de los daños colaterales, de la proporcionalidad, de la discriminación y de las reglas de empeñamiento (De Vergara & Trama, 2017, pág. 31).

Sintetizando los conceptos analizados sobre las particularidades de las teorías y doctrinas militares que describen (y profetizan) la naturaleza y modos de los conflictos modernos con las características del llamado 5to dominio, podemos señalar que:

Las teorías y doctrinas militares actuales consideran la esencia multidimensional de los conflictos modernos y afirman el carácter fundamental de la irrupción de las operaciones en el ciberespacio[15], algunas con un sesgo más defensivo y otras dual. Sin embargo, hay cierta coincidencia en la omnipresencia de estas acciones en todas las etapas del conflicto y su factibilidad de alternancia de prioridad al momento de empeñarse junto con otras opciones (militares y no militares).

Los estados estructuran sus organizaciones y desarrollan capacidades coherentemente con su doctrina y visión del conflicto y por derivación conducen abierta o secretamente operaciones cibernéticas en todos los niveles de conducción (Estratégico Nacional y Militar, Operacional y Táctico)[16].

El problema de la atribución, sumado al marco legal internacional vigente que regula los conflictos armados en los dominios tradicionales, complejiza enormemente la conducción de las ciberoperaciones ya sean de carácter ofensivo, defensivo o exploratorio.

---

[15] DPDN 2018. *El papel de los recursos cibernéticos se juega tanto en el ámbito civil como militar, público como privado. Con identidad y fuerza propia, el ciberespacio es un componente que atraviesa todos los instrumentos de poder y aporta significativamente a la solución del conflicto. Por lo expresado, no puede soslayarse su inclusión en el abordaje omnicomprensivo ya citado, desde el análisis inicial hasta la determinación de los objetivos estratégicos y operacionales para el estado de situación final deseado.*

[16] S. Tepedino, *La doctrina Gerasimov,* op. cit., *El uso de alta tecnología (no sólo en armamentos militares) y de instrumentos para guerras de mediana y alta intensidad como la Cyberwar, y la estructuración de mecanismos de ataque centrados en redes para guerras de baja intensidad, como es el caso de la Netwar, adquieren una relevancia vital para la Doctrina Gerasimov, por lo que el Estado Mayor Ruso puso el lente en la creación de divisiones encargadas en Operaciones de Ciberguerra, y Operaciones de Información.*

Las zonas grises que crean los límites autoimpuestos y la falta de legislación en esta materia son y serán aprovechadas recurrentemente por quienes no se avengan a respetar normas consuetudinarias y se sientan avalados por razones de asimetría[17].

En resumen, esta complejidad no lineal y multidimensional descripta en todas las afirmaciones anteriores, previene de la necesidad de abordar la problemática desde una mirada omnicomprensiva. No deberíamos intentar encasillar, catalogar o normar absolutamente todo. Las claves son flexibilidad, trabajo inter-agencial, estándares reales de confianza mutua y una entidad superior que observe y dirija el conjunto de actividades.

Todas estas expresiones de buena voluntad sólo podrán ser concretas si disponemos de antemano de equipos multidisciplinarios de expertos debidamente preparados y que trabajen eficientemente coordinados.

[17] S. Tepedino, *Guerra irrestricta, guerra civil molecular y guerra híbrida: tres modos de hacer la guerra en el S. XXI*, op. cit.. p 7. El autor concluye que *"…los chinos comprendieron que nunca podrían prevalecer sobre Estados Unidos en el campo de la alta tecnología, sólo podrían salir airosos disponiendo de fuerzas de baja tecnología y han preparado a su poderoso ejército con regimientos de hackers y crackers".*

Capítulo III. Los equipos multidisciplinarios.

Este capítulo tiene como finalidad identificar las áreas de competencias afines a la problemática de la Ciberdefensa en el nivel estratégico (ya sea nacional o sectorial) para la conformación de equipos multidisciplinarios y las particularidades de liderazgo de los mismos.

Sección I. Identificación áreas de conocimiento afines para selección de expertos sectoriales.

Partiendo de las conclusiones parciales del Capítulo II, es necesario identificar cuáles son esas áreas de capacidades que puedan aportar a la construcción del abordaje omnicomprensivo y a la concreción de una verdadera "conciencia situacional"[18] en el ciberespacio.

Para Conti y Surdu (Conti, 2009, pág. 17), "la guerra cibernética requiere no sólo de habilidades técnicas, sino también de habilidades para solucionar problemas de creatividad, para actuar de manera equilibrada bajo presión y de pensamiento crítico".

Como se señalara anteriormente, la multidimensionalidad de los conflictos modernos abarca esferas muy disímiles de la vida cotidiana de cualquier sociedad. En el mismo sentido, se afirmaba que la opción de empelo del poder militar puro no es siempre la más deseada si se cuenta con un verdadero abanico de herramientas para actuar. Operaciones de lawfare, financieras, guerra de información (sobre un muy variado espectro de público blanco y objetivos), espionaje y/o sabotaje industrial (civil y militar), alteración o manipulación de datos del área de salud, agricultura o sistemas electorales, son sólo algunos ejemplos. Todos ellos son posibles de ser afectados en mayor o menor medida con operaciones dentro y desde el dominio del ciberespacio.

Una consideración más en este mismo sentido hacen Paul Christopher y otros (Christopher, Paul - Porche II, Isaac - Axelbandt, Eliot), al expresar que:

[18] Conciencia Situacional: Cyberspace situational awareness is the requisite current and predictive knowledge of cyberspace and the operational environment (OE) upon which cyberspace operations (CO) depend, including all factors affecting friendly and adversary cyberspace forces. A commander continually assesses the OE through a combination of staff element and other reporting; personal observation; intelligence, to include threat warning; and representations of various activities occurring in the OE using a common operational picture (COP). (US JP 3-12, 2018, págs. IV-5)

"(…) el adiestramiento de los que hoy en día se denominan "ciberguerreros" va mucho más allá de "adquirir habilidades". Algunos de ellos no sólo poseen conocimientos sobre idiomas informáticos, sino que también se capacitan en idiomas extranjeros.

Más aún, los Comandos de Ciberdefensa suelen incluir (o tener acceso regular) a personal con una buena comprensión de los matices culturales, la dinámica humana y las estrategias de influencia y persuasión. La guerra cibernética no siempre se trata de ceros y unos; también puede implicar la intrusión de contenidos en las redes de los adversarios, un contenido distinto al del código de la computadora que está diseñada para tener un impacto en el dominio cognitivo".

Más aún, Lucy Tsado (2019) en su trabajo sobre la necesidad de un enfoque desde lo gerencial[19], no sólo refuerza el carácter multidisciplinario de los recursos humanos (técnicos y no técnicos) (2019, pág. 1), sino que además resalta la ventana de oportunidad de las instituciones académicas para la formación de especialistas que no han sido tenidos en cuenta inicialmente en el proceso selectivo. Su postura se basa en la inclusión curricular de estas áreas de interés las cuales responden a perfiles previamente identificados (2019, pág. 5 & 9) que las instituciones estatales, si bien reconocen, pero no se abocan a capacitar.

La selección de personal no se circunscribe únicamente al ámbito público, por el contrario, necesariamente debe integrar al ámbito privado[20].

Los recursos humanos que se requieren para afrontar estas amenazas deben estar debidamente calificados y entrenados en cada área identificada como blanco potencial y ser capaces a su vez de trabajar de modo integrado en el dominio del ciberespacio. Separando los operadores técnicos a cargo de las razonables tareas de seguridad informática, los especialistas a reclutar deben pertenecen inicialmente a las áreas sensibles identificadas por la conducción superior como parte de la infraestructura crítica a ser protegida. Cada país lo analiza y proyecta en función de su percepción sobre fortalezas / debilidades y amenazas en el contexto regional y global. Una pista de ello se puede encontrar en documentos oficiales como Estrategias y

[19] The need for a top-driven approach. In the 2015 survey, a clear majority of Information Security (IS) respondents (90 percent) stated that communication skills were vital for IS experts to be successful at their jobs. Other areas of knowledge identified as important were regulatory policy (71 percent), security policy formulation and application (70 percent), leadership skills (69 percent), and business management skills (53 percent). In 2013, ISC2's top executives issued a report titled *A View from the Top: The (ISC)2 Global Information Security Workforce Study CXO Report*, in which 74 percent of respondents stated that they spent most of their time on governance, risk management, and compliance. (Tsado, 2019, pág. 4)

[20] *U.S. Cyber Command needs nontraditional personnel authorities, particularly to facilitate the recruitment of highly skilled personnel from the private sector*. The Other Quiet Professionals - Lessons for Future Cyber Forces from the Evolution of Special Forces.

Políticas de Ciberseguridad, y para el plano específico de la defensa, en las Directivas de Defensa Nacional y en el Libro Blanco de la Defensa Nacional, entre otros.

Abordando esta temática desde la óptica nacional, se observa en la Estrategia Nacional de Ciberseguridad desde su párrafo introductorio, una coincidencia en la mutidimensionalidad del ciberespacio.

> "La Estrategia Nacional de Ciberseguridad, establecida por el Poder Ejecutivo Nacional con el consenso del conjunto de la sociedad en forma multidisciplinaria y multisectorial, sienta los principios básicos y desarrolla los objetivos fundamentales que permitirán fijar las previsiones nacionales en materia de protección del Ciberespacio. Más adelante explicita el amplio campo de desarrollo y entidades abarcativas, […] estas acciones se llevarán a cabo sobre la base de la coordinación y cooperación entre la Administración Pública Nacional, otros poderes nacionales, las administraciones y poderes de las jurisdicciones provinciales y de la Ciudad Autónoma de Buenos Aires, municipales, el sector privado, las organizaciones no gubernamentales y las entidades académicas". (Resol 829/19 - Anexo I - Estrategia Nacional de Ciberseguridad, 2019).[21]

Una primera conclusión nos lleva a inferir que estas entidades mencionadas deberán contar con personal especializado en capacidad de intervenir en estos estudios y la aplicación de tales acciones.

Del mismo modo, la Estrategia Nacional de Ciberseguridad visualiza un escenario con actividades multidependientes signadas por su vinculación con el mundo virtual, […] la realidad exhibe que servicios esenciales para la vida de las personas y para la economía, como la energía, el agua, el transporte, las comunicaciones y los servicios financieros, entre otros, tienen en la actualidad una fuerte dependencia de las redes informáticas. Su protección es extremadamente compleja, entre otras razones, porque implica la coordinación de esfuerzos de múltiples actores públicos y privados (Resol 829/19 - Anexo I - Estrategia Nacional de Ciberseguridad, 2019). De allí deriva una especificación primaria de especialistas sectoriales que se intenta identificar en esta sección.

Por su parte la Secretaría de Modernización, al tipificar las infraestructuras críticas señala que:

> Son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social,

[21] Para el análisis de esta problemática, debe tenerse en cuenta que los organismo de Ciberseguridad y Ciberdefensa nacionales tiene roles y funciones específicos y que los aspectos que impacten en amabas esferas requieren coordinación en todos los niveles para su tratamiento.

la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.

Las Infraestructuras Críticas de Información son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas. (Resol 1523/19, 2019).

En función de ello se fijaron los "criterios de identificación de infraestructuras críticas según el impacto sobre la vida humana, la economía, el medio ambiente, el ejercicio de los derechos humanos y de las libertades individuales, lo público o social, en el ejercicio de las funciones del estado, en la soberanía nacional y en el mantenimiento de la integridad territorial nacional" (Resol 1523/19, 2019).

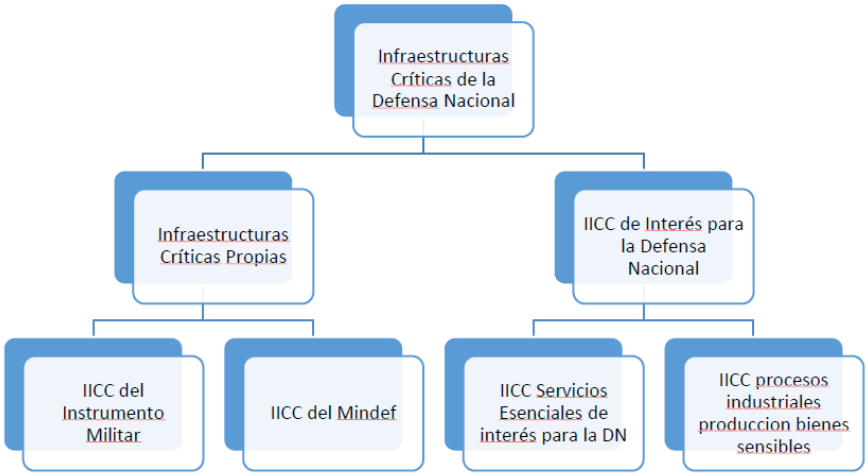
Derivado de estas definiciones, el documento ha identificado los siguientes sectores de interés primario:

• Energía.
• Tecnologías de Información y Comunicaciones.
• Transportes.
• Recursos Hídricos.
• Salud.
• Alimentación.
• Finanzas.
• Nuclear.
• Químico.
• Espacio.
• Estado.

Analizando otras realidades, (Flores, 2015) destaca que España por ejemplo, a través de la sanción de la Ley 8/2011 de Protección de Infraestructuras Críticas (LPIC) y el posterior Real Decreto 704/2011 difundió el Reglamento de Protección de las Infraestructuras Críticas que, "entre otras disposiciones, creó la Comisión Nacional para la Protección de las Infraestructuras Críticas a las que clasificó en doce sectores estratégicos, a saber: Administración, alimentación, energía, espacio, sistema Financiero y Tributario, agua, industria Nuclear , industria Química, instalaciones de Investigación, salud, tecnologías de la Información y las Comunicaciones, transporte, etc" (pág. 14).

Comparativamente, las áreas identificadas son lógicamente similares y de indiscutida importancia.

En el área específica de la Ciberdefensa argentina, la infraestructura crítica es definida como aquellas infraestructuras estratégicas cuyo "funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto en la capacidad operacional del Instrumento Militar en el ciberespacio y/o en la prestación de los servicios esenciales así como la producción de bienes de interés para la Defensa" (Resol 1380/19 - Anexo 4 - Política de Ciberdefensa, 2019)[22].



IICC DE INTERÉS PARA LA DEFENSA NACIONAL	***Infraestructuras TO soporte de los Servicios Esenciales***	- Energética - Nuclear	CSIRT - MINDEF
	Infraestructuras TO soporte de procesos industriales de fabricación de bienes sensibles	- Explosivos - Moderadores de fisión en reactores nucleares - Con capacidad de producir daños masivos al medioambiente	CSIRT - MINDEF
IICC DEL SISTEMA DE DEFENSA	***Infraestructuras TO y TI del Instrumento Militar y Mindef***	No disponible	No disponible

Figura 8 y 9: Relación entre los diferentes grupos de infraestructuras críticas (Resol 1380/19 - Anexo 4 - Política de Ciberdefensa, 2019). Ver nota de pie de página N° 22.

Como puede observarse, las infraestructuras críticas de interés para la Defensa Nacional requieren de especialistas, además del personal profesional militar, abocados a los

[22] Nota: esta norma se encuentra actualmente derogada y la política de Ciberdefensa en reelaboración, no obstante ello, su contenido se presenta en el marco de conceptos teóricos afines al presente trabajo.

servicios esenciales de interés (como en las áreas de energía) y a los procesos industriales de producción de bienes sensibles (como por ejemplo: combustibles, armamento, munición y explosivos, vehículos, aeronaves, etc.).[23]

Analizando los documentos directrices de la política de defensa argentina, cabe aclarar que respecto al ámbito de injerencia de la defensa, ya la DPDN (2014) entendía que:

> Si bien las acciones de ciberguerra poseen su origen en el ámbito virtual de las redes de comunicación y sistemas informáticos, sus efectos impactan sobre el mundo físico, pudiendo afectar, por ejemplo, el tráfico aéreo y terrestre, el control de las infraestructuras críticas, el abastecimiento energético y de agua potable, entre otros.
>
> Dentro de la amplia gama de operaciones cibernéticas, sólo una porción de éstas afectan específicamente el ámbito de la Defensa Nacional. En efecto, en materia de Ciberdefensa existen dificultades fácticas manifiestas para determinar a priori y ab initio si la afectación se trata de una agresión militar estatal externa. Por tal motivo, resulta necesario establecer dicha calificación a posteriori actuando como respuesta inmediata el Sistema de Defensa únicamente en aquellos casos que se persiguieron objetivos bajo protección de dicho sistema, es decir que poseen la intención de alterar e impedir el funcionamiento de sus capacidades.

Independientemente de esta disquisición sobre los alcances que incumben a las infraestructuras críticas del sistema de defensa y aquellas de "interés" para este, cabe preguntarnos como Flores:

> ¿toda infraestructura catalogada como crítica para el funcionamiento del Estado no debería estar protegida por el Sistema de Defensa?.
>
> Ante un eventual ciberataque, ¿podrá el Sistema de Defensa argentino identificar que la agresión pueda ser de carácter militar estatal externa?; parecería difícil y quizás lo más peligroso seria el tiempo de respuesta que el mismo puede requerir hasta tanto se lo califique como tal. En los casos mencionados (ataques a Estonia y a Georgia) es sabido que pese al apoyo internacional que recibieron estos países, los efectos fueron significativos para todo el Estado. (2015, pág. 13).

Por su parte, la DPDN (2018), entiende que "la necesidad de resguardar la soberanía e independencia de la República Argentina, la integridad territorial, la capacidad de autodeterminación, la protección de la vida y la libertad de sus habitantes ante agresiones de

[23] Una vez más es necesario advertir que dada la legislación vigente en materia de seguridad y defensa en la república Argentina, las IICC determinadas deberán ser asignadas a una u otra esfera y la coordinación de ambas debe ser potenciada con protocolos ágiles para reaccionar ante ataques que involucren a más de una de ellas.

origen externo constituyen una función permanente del Sistema de Defensa Nacional*"*. Esta expresión omite ex profeso el carácter de origen "estatal" externo de las amenazas a enfrentar con el Instrumento Militar, ampliando enormemente su área de injerencia. Esta visión se desarrolla más en concordancia con escenarios en los que se perciben amenazas híbridas como se explicitara en el capítulo II del presente trabajo.

Es más, en el mismo documento observa que:

> Las potencias regionales y globales han modernizado sus estrategias de defensa y sus fuerzas armadas. Esta actualización exhibe la creciente integración entre formas tradicionales y no tradicionales de agresión e influencia. Estas últimas refieren a acciones no militares dirigidas a desestabilizar a la población y los gobiernos de las naciones adversarias. Los beligerantes combinan instrumentos políticos, diplomáticos, informativos, ciberespaciales, militares y económicos. La diseminación masiva de información falsa y el reemplazo de las tropas regulares por organizaciones irregulares o empresas militares privadas configuran algunas de las tendencias propias de la última década. Algunos Estados apelan a estas tácticas para promover sus intereses en regiones ajenas a sus espacios soberanos. Como corolario, los conflictos armados actuales ocurren crecientemente por debajo del umbral de la violencia militar directa y en los márgenes del derecho internacional. (DPDN, 2018).

A partir de esta cosmovisión más amplia de la Defensa Nacional, la DPDN 2018 encuadra al ciberespacio, como ámbito de interés en un marco de interdependencia tecnológica, obliga a atender los fenómenos que se desarrollan en él, incluyendo los riesgos asociados a la militarización del ciberespacio. En este contexto, enfatiza la dualidad de origen de las amenazas tanto estatales como de actores no estatales, los cuales están desarrollando medios cibernéticos para explotar las vulnerabilidades inherentes a los sistemas de comando, control, comunicaciones, inteligencia, vigilancia y reconocimiento. Incluso abarca al terrorismo, el cual explota el ciberespacio para reclutar miembros, recaudar fondos y difundir su propaganda.

Además, entiende que:

> Las amenazas cibernéticas sofisticadas provienen de organizaciones militares y agencias de inteligencia de otros Estados. Si bien los gobiernos tecnológicamente avanzados explotan sus ventajas comparativas con relación al resto de los países, el despliegue de operaciones disruptivas en el ciberespacio también está al alcance de las naciones menos desarrolladas. El abordaje de esta problemática desde la perspectiva de la Defensa Nacional requiere adoptar medidas y acciones tendientes a resguardar la

> seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional y de aquellas que sean designadas para su preservación, independientemente del origen de la agresión. (DPDN, 2018, pág. 9).

La misma ambigüedad encontramos al analizar el llamado "Libro Blanco de la Defensa". Estos documentos abundan en expresiones que amplían o restringen el ámbito de injerencia de la defensa nacional y por derivación de empeño del Instrumento Militar. No obstante ello, las amenazas en o desde el ciberespacio son tenidas en cuenta y reclaman ser igualmente atendibles.

Este aspecto particular en la cambiante cosmovisión nacional de separación estricta entre las esferas de defensa / seguridad y los alcances de aplicación del Instrumento Militar, no es objeto de análisis de este capítulo; sin embargo, dada las particularidades mencionadas anteriormente del ciberespacio y las acciones que en él y desde él se realizan, la interacción y necesaria integración de ambas esferas es absolutamente imperativa.

Analizando las dos últimas ediciones de las DPDN y la última edición del Libro Blanco de la Defensa, emerge la necesidad de disponer en el tratamiento de amenazas en el ciberespacio a nivel estratégico nacional y militar, no sólo de personal militar, sino también de expertos en seguridad, en economía y finanzas (nacional e internacional), en relaciones internacionales e ingenieros especializados en explotación de recursos naturales, tales como minerales, gas, petróleo, energía nuclear, agua, etc., entendiendo a estos como recursos estratégicos.

Tanto en un marco conceptual como en otro, la necesidad de contar con expertos sectoriales para abordar las amenazas en el ciberespacio es evidente.

Considerando las organizaciones existentes en el ámbito nacional, estas no escapan a las consecuencias derivadas de los cambios de administración del poder ejecutivo y sus diferencias conceptuales e ideológicas. Desde fines de 2017 el máximo órgano nacional en materia de empleo y seguridad en el ciberespacio era el Comité de Ciberseguridad (Comité de Ciberseguridad), el cual se componía de representantes de los Ministerios de Modernización, Seguridad y Defensa. Posteriormente, en el año 2019, se decretó una ampliación del Comité (Decreto 480/19) incorporando a otras áreas de interés como el Ministerio de Relaciones Exteriores y Culto (por su necesaria vinculación con la cooperación internacional y el análisis de escenarios regionales y globales), y el Ministerios de Justicia y Derechos humanos (por incumbencia en el marco normativo nacional).

Esta organización, destaca singularmente la necesidad de contar con profesionales expertos en:

- ✓ Ingeniería (informáticos, en telecomunicaciones, electrónicos, industriales, etc).
- ✓ Seguridad (personal de Fuerzas de Seguridad, Fuerzas Policiales y civiles con experiencia en la materia).
- ✓ Defensa (personal de las FFAA y civiles con experiencia en la materia).
- ✓ Relaciones Internacionales.
- ✓ Abogacía, especializados en Derecho Público (Penal, Internacional, Financiero y Tributario, Público y Constitucional); y Derecho Privado (Comercial e Internacional).

El Art 3 (Decreto-480, 2019) establece que "los órganos integrantes del Comité de Ciberseguridad, designarán DOS (2) funcionarios de sus respectivas áreas que los representarán ante el mencionado Comité".

Actualmente, producto de la reestructuración del Estado, la Secretaría de Modernización ha sido disuelta, y se infiere que las tareas del Comité de Ciberseguridad fueron asumidas por la Dirección Nacional de Ciberseguridad [24], la cual desarrolla estrategias y mecanismos para la protección de la información y los servicios del Estado Nacional y sus ciudadanos y coordina la gestión de incidentes a nivel nacional.

A modo de conclusión parcial, es evidente la necesidad de contar con profesionales militares y de seguridad, políticos; especialistas en recursos naturales (fundamentalmente energía), y en redes sociales, en áreas de salud y sistemas hospitalarios y sociólogos; personal experto en procesos industriales, del ámbito financiero y económico; en sistemas de transporte, comunicaciones (terrestres y satelitales); y para el marco normativo, juristas de diversas ramas del derecho y especialistas en relaciones internacionales. El presente listado no pretende ser excluyente ni taxativo, sino una aproximación al carácter multidisciplinario del dominio ciberespacial.

¿Dónde podría / debería trabajar este personal?

Dicho personal podría ser empleado para trabajar coordinadamente en estructuras de nivel estratégico nacional, tales como:

- Secretaría de Asuntos Estratégicos de la Nación.
- Secretaría de Innovación Pública:
  - Dirección Nacional de Ciberseguridad.

[24] Esta entidad depende de la Jefatura de Gabinete de Ministros / Secretaría de Innovación Pública https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad - Abril 2020.

Estas entidades son el ámbito donde se desarrollan las políticas y estrategias de más alto nivel nacional, incluidas las referentes al uso del ciberespacio.

En lo específico, la Dirección Nacional de Ciberseguridad es el espacio institucional donde la conformación de equipos multidisciplinarios propuesto encontraría su máximo potencial.

En virtud de lo establecido por el Decreto 577/2017, basta recordar que se ha encomendado al Comité de Ciberseguridad (entidad predecesora de la Dirección), la elaboración de la Estrategia Nacional de Ciberseguridad, y que en el párrafo introductorio de la misma, explícitamente menciona "ser establecida por el Poder Ejecutivo Nacional con el consenso del conjunto de la sociedad en forma multidisciplinaria y multisectorial, la cual sienta los principios básicos y desarrolla los objetivos fundamentales que permitirán fijar las previsiones nacionales en materia de protección del Ciberespacio" (Modernización, 2019).

En los ámbitos sectoriales, sería útil su participación en entidades afines que a su vez formen parte del Comité de Ciberseguridad o podrían ser citados para la conformación de equipos *ah-hoc*.[25]

- Ministerio de Defensa:
  - Secretaría de Estrategia y Asuntos Militares:
    Subsecretaría de Ciberdefensa.
  - Dirección Nacional de Inteligencia Estratégico Militar.
  - Estado Mayor Conjunto de las Fuerzas Armadas - Comando Conjunto de Ciberdefensa:
- Ministerio de Seguridad:
  - Dirección de Investigaciones del Ciberdelito.
  - Dirección Nacional de Inteligencia Criminal.
- Agencia Federal de Inteligencia.
- Ministerio de Ciencia, Tecnología e Innovación.
- Ministerio de Desarrollo Productivo:
  - Secretaría de Energía.
  - Secretaría de Comercio.
- Ministerio de Relaciones Exteriores y Culto.
- Ministerio de Transporte.

[25] Los roles y competencias de cada caso son definidos por la legislación vigente respetando la separación de esferas de seguridad y defensa. Dado el grado de dependencia alcanzado de los sistemas informáticos y las IICC determinadas en cada ámbito, es necesaria la presencia de expertos en ciberseguridad y ciberdefensa con capacidad de trabajo específico en su área y en tareas grupales multidisciplinarias cuando sea requerido.

- Ministerio de Economía.
- Ministerio de Justicia y Derechos Humanos.
- Ministerio de Salud.

En el ámbito público y privado, en empresas y entes reguladores de servicios esenciales, en el área académica y en industrias asociadas a desarrollos tecnológicos.

Todos estos expertos seguramente tendrán mucho que aportar, pero no debemos perder de vista que, de cara a las amenazas híbridas y complejas del Siglo XXI y a la probabilidad de ocurrencia de una escalada a conflicto bélico, "en última instancia, guerra cibernética es lo que en el mundo real se cree que es. Al final del día, es el Presidente quien tiene que decidir si se trata de guerra u otra cosa. La norma es ambigua. Decidir cuándo algo es un acto de guerra no es automático, es siempre un tema de juicio" Singer & Friedman (Singer, 2014, pág. 67).

Sección II. El liderazgo de equipos multidisciplinarios.

Esta sección aborda conceptos relacionados con el liderazgo de equipos multidisciplinarios de nivel estratégico y operacional dentro de entidades como la Dirección Nacional de Ciberseguridad, el Comité Nacional de Ciberseguridad, la Secretaría de Ciberdefensa (Min Def) / Comando Conjunto de Ciberdefensa u otras de similar magnitud.

Las organizaciones involucradas en la dirección de tareas de Ciberseguridad y Ciberdefensa, requieren de personal con habilidades particulares que podríamos catalogar de "no tradicionales"[26], a su vez el personal designado para liderar estos grupos deberá reunir ciertas características que le permitan llevar adelante trabajos multidisciplinarios en escenarios complejos. Obviamente el perfil de quien tendrá la responsabilidad de gerenciar este tipo de organizaciones, debe poseer consolidados conocimientos generales de las áreas de desempeño de sus miembros y una reconocida experiencia en al menos una de ellas.

A decir de Galeiras-Vázquez:

> […] la tarea de administrar un equipo multidisciplinar profesional pasa por fomentar el aprendizaje. Tradicionalmente, el estatus estaba en lo que uno sabía acerca de algo. Esto requiere coraje y puede ser difícil para un experto admitir con franqueza que podrían ser mejores en lo que hacen si supieran más. Pero está asistido por las normas de la profesión, que requieren una formación continua por parte de sus miembros. Hay

[26] The Other Quiet Professionals - Lessons for Future Cyber Forces from the Evolution of Special Forces. Recommendations. https://www.rand.org/pubs/research_reports/RR780.html

que permitir la innovación y la creatividad en todos los niveles del equipo. En este sentido, es lo opuesto a aislar y limitar el comportamiento profesional con políticas proteccionistas. Planificar escenarios ayuda a prepararse, y la simulación ha mostrado ser una herramienta útil para enseñar nuevos conocimientos, habilidades y comportamientos en un ambiente libre de estrés y eventos adversos. (Liderar un grupo multidisciplinar, 2017).

El jefe de equipo, previamente formado y con experiencia en los aspectos comunes citados precedentemente, deberá poseer características / habilidades distintivas, tales como:

- Conocimiento de la "Alta Gerencia Estatal". Su experiencia en esta área es requerida para coordinar estrategias y actividades propias de la esencia transversal del dominio del ciberespacio. Asimismo, capacidad para vincularse con el ámbito privado (industrial, financiero, telecomunicaciones, etc.).
- Dominio y experiencia en sistemas de planeamiento de nivel estratégico. La participación del equipo en trabajos tendientes a la resolución de problemas en curso o de carácter anticipatorio, conlleva necesariamente esta habilidad para integrar el planeamiento propio dentro del marco superior.

  Dentro del ámbito específico de la Ciberdefensa, la capacidad de planeamiento estratégico / operacional es imprescindible ya que la integración efectiva con operaciones en los dominios físicos requiere la participación activa de planificadores y operadores de Ciberdefensa en cada fase de operaciones conjuntas. Los límites físicos y lógicos dentro de los que fuerzas conjuntas ejecutan ciberoperaciones, y las prioridades y restricciones sobre su uso, también deben ser identificados por el Comandante en coordinación con otros departamentos y agencias de nivel nacional. En particular, la creación de efectos en el ciberespacio con anclaje en territorio extranjero puede tener el potencial para impactar otros esfuerzos de niveles paralelos o superiores. Donde existe el potencial para tal impacto, la política nacional requiere la coordinación del Ministerio de Defensa con socios interinstitucionales. (US JP 3-12, 2018, págs. I-8).
- La característica de indefinida del ámbito geográfico del ciberespacio requiere de una capacidad omnicomprensiva en las tareas de análisis de escenarios globales / regionales. A esto acude complementariamente la formación previa en habilidades de inteligencia estratégica.
- Obviamente, se requiere de un perfil técnico básico en relación a las áreas de telecomunicaciones e informática, particularmente enfocado a seguridad de las mismas.

Sin embargo, cabe destacar que en este nivel, la sola excelencia en el área técnica no garantiza las cualidades de liderazgo requeridas para esta tarea.

- Vínculos académicos. Esto es especialmente importante por la injerencia en el diseño de itinerarios formativos de los aspirantes a conformar el equipo y para facilitar el permanente proceso de actualización de sus miembros. En el mismo sentido, la comunidad académica suele ser en sí misma, una suerte de *Think tank* que retroalimenta las tareas de análisis concurrentes.
- Experiencia con organizaciones pares a nivel internacional. Los lazos reales creados con expertos en Ciberseguridad y Ciberdefensa son absolutamente necesarios para interactuar en escenarios globales. Consecuentemente, esto requiere de habilidades idiomáticas avanzadas.
- La heterogeneidad del equipo, es un desafío adicional (Carpenter & Mendoza, 2017). La comunicación puede ser más difícil debido a la variación en el lenguaje, expectativas culturales, valores y presunciones, por ende la resolución de problemas es más compleja.

La deseable sinergia resultante del trabajo en equipo, deviene de su forma de trabajar y del liderazgo de su jefe. Esta cualidad intangible requiere de experiencia previa y dotes individuales para potenciar las capacidades de los miembros del equipo. Existen cursos de capacitación orientados a mejorar estas habilidades, pero la personalidad y el ascendente profesional del jefe de equipo son factores indiscutibles para la elección del mismo.

Capítulo IV. La formación común de los equipos multidisciplinarios.

Sección I. El proceso formativo común.

La Estrategia Nacional de Ciberseguridad, al definir su 2do objetivo, expresa la necesidad de "capacitación y educación en el uso seguro del Ciberespacio, entendido ello como el proceso de formación y adquisición de conocimientos, aptitudes y habilidades necesarias para un uso seguro del Ciberespacio. Para ello será necesario:

- Promover la formación de profesionales, técnicos e investigadores.
- Desarrollar talleres y ejercicios, tanto gubernamentales como con los sectores privados y el sector civil.
- Fortalecer la capacitación en técnicas de prevención, detección, respuesta y resiliencia ante incidentes.
- Incrementar las actividades transversales de formación en el sector académico". (Modernización, 2019).

En el marco del presente trabajo, se sugiere una visión más amplia de la necesidad de capacitación de personal, no sólo dirigida al "uso seguro del Ciberespacio", sino además, a la formación integral del personal profesional que debe actuar en el mismo.

Ya se ha detallado, en el capítulo precedente, la variedad de especialistas sectoriales involucrados, contando con su capacitación específica de base. Sin embargo, para su desempeño eficiente en áreas dirigenciales y de coordinación de entidades de incumbencia en el ciberespacio, es menester que estos sean provistos de habilidades complementarias comunes.

Desde luego se requiere de una formación común en las particularidades del ciberespacio y en forma directa en todo lo relacionado con la Ciberseguridad y Ciberdefensa. Rutz se expresa coincidente con esta idea al señalar que "es muy importante que haya un entendimiento común sobre el ciberespacio y los conceptos que sobre el mismo se abordan, discuten y enseñan" (Rutz, 2020, pág. 58).

Este ámbito de conocimiento excede en gran medida las nociones de seguridad informática aplicables a cualquier nivel. No se trata de una capacitación de carácter meramente técnico-operativo, sino de conocimientos interdisciplinarios como los provistos en la Maestría en Ciberdefensa y Ciberseguridad de la UBA. Ellos abarcan aspectos del

ciberespacio tan disímiles como lo normativo, las operaciones militares cibernéticas, el ciberterrorismo, consecuencias en política global, derivaciones en terreno criminal nacional y transnacional, estructuras estatales y privadas vinculadas, análisis de infraestructuras críticas y riesgos asociados, escenarios, análisis de riesgos y amenazas, e incluso un mínimo de conocimientos técnicos necesarios para quienes provienen de una formación de base no asociada a la TICs.

Ahora bien, según la investigación de Rutz, la realidad local evidencia un vacío respecto de estas definiciones:

> […] en el caso argentino, si existen definiciones de roles y modelos formativos para perfiles de recursos humanos en el área de ciberdefensa, no llegaron al conocimiento de las universidades o instancias académicas para su implementación. Esta situación local determina el estado de madurez política, académica e institucional de la cuestión, lo cual justifica la necesidad de abordajes académicos, políticos y prácticos-profesionales en función de pensar y definir necesidades, roles y modelos formativos. (Rutz, 2020, pág. 62).

Complementariamente, la necesidad de análisis y prospectiva del entorno volátil y cambiante del ciberespacio, requiere de nociones comunes en inteligencia estratégica y operacional. Esto permitirá integrar eficazmente las capacidades individuales de cada experto del equipo, enfocadas con una visión común dentro del ámbito del ciberespacio lograda en la etapa de formación anterior. Cada uno de ellos operará en su ámbito particular, pero deben ser capaces de interrelacionar los indicios de diferentes campos que le son ajenos y poder integrarlos en la compleja trama que tejen las amenazas híbridas, según sus características ya detalladas[27].

Superadas estas etapas, es necesario que los especialistas dispongan de un sistema común para el planeamiento según el nivel de trabajo en el cual se enmarca su tarea (ver Cap IV – Sec IV). Las metodologías para la toma de decisiones son herramientas útiles para que los mismos sean capaces de reconocerse a sí mismos en las etapas de asesoramiento y asistencia del planeamiento, y su particular incidencia en cada paso del proceso. Es importante dominar técnicas de análisis en entornos de crisis y el delineamiento de opciones de respuestas

[27] La capacidad mencionada, de carácter obviamente subjetivo, se podrá verificar en la participación de ejercicios diseñados específicamente a tal fin que permitan al especialista identificar esos datos, interrelacionarlos con otros y dar un producto resultante acorde (método propio del ciclo de inteligencia). La preparación y conducción de ejercicios se desarrolla en el Cap V del presente trabajo.
Asimismo, tal integración potencia el trabajo conjunto y coordinado de especialistas de las áreas de seguridad y defensa los cuales tienen funciones y responsabilidades específicas.

preventivas y reactivas. Esta habilidad en particular, ayudará a concretar más particularmente el valor del rol a cumplir de cada experto en una estructura mayor con objetivos concatenados desde el nivel estratégico nacional hasta el nivel sectorial al cual sirvan.

¿Cómo y dónde formarlos?

En nuestro país, al igual que en otros, existe una institución pública dedicada a elaborar políticas y a dirigir programas de capacitación, el Instituto Nacional de la Administración Pública (INAP) que desde 1973 atiende esta temática. En su plataforma digital[28] expone que "[…] La propuesta formativa del INAP, se organiza articulando los lineamientos estratégicos de la gestión gubernamental con las demandas que surgen de las innovaciones en los campos profesionales, de los requerimientos en la actualización de competencias de los/las trabajadores/as, de sus derechos para el avance en sus trayectorias públicas y de las políticas y proyectos que las organizaciones públicas gestionan".

Dentro de su campo de actividades, el instituto diseña, planifica e implementa actividades de formación específicas para los/las agentes que ocupan mandos medios, ejercen funciones ejecutivas o equivalentes y se encuentran a cargo de las principales políticas públicas.

Aun así, el INAP no detenta el monopolio de la formación para desempeñarse en el área pública. Otras instituciones ofrecen programas que capacitan personal para distintas ramas de gestión y pueden o no estar coordinadas con el INAP[29]. Independientemente del modo de institucionalización, la estrategia que se presenta como más adecuada, apunta a la formación continua o profesional (Bonifacio, 2009, pág. 342), la cual otorga mayor relevancia al enfoque centrado en competencias, ya sea atendiendo a competencias preexistentes para mantenerlas; desarrollando nuevas competencias para la realización de un proyecto de cambio a mediano plazo, o atendiendo a requerimientos de determinadas profesiones que emergen debido a la evolución del entorno socio-técnico. La otra discusión gira en torno al alcance de la institución sobre su potestad para, además de capacitar, seleccionar personal previo al acceso del desempeño efectivo en la función (2009, pág. 343). En tal sentido, experiencias

[28] El INAP ofrece actividades de capacitación para los/las trabajadores/as del Estado, en todos niveles, desde el ingreso y durante el desarrollo de sus trayectorias públicas, con el fin de fomentar su participación y recuperar sus conocimientos, en línea con los desafíos estratégicos del Gobierno. https://www.argentina.gob.ar/jefatura/gestion-y-empleo-publico/inap/cursos

[29] Un ejemplo de ello es el Programa Virtual de Formación para la Alta Gerencia Pública Latinoamericana de la Universidad Austral, la cual otorga créditos del INAP para los agentes públicos que quieran aplicarlos a la carrera. https://www.austral.edu.ar/derecho/programas/programa-virtual-de-formacion-para-la-alta-gerencia-publica-latinoamericana/

previas del INAP como el programa de Formación de Administradores Gubernamentales (PROFAG) pueden ser un ejemplo interesante para adecuar al proceso de formación y selección de profesionales.

En la actualidad, a nivel nacional e internacional, existen instituciones públicas y privadas dedicadas a la capacitación de profesionales en áreas de Ciberseguridad y Ciberdefensa, inteligencia y procesos de toma de decisiones, las cuales serán presentadas en el desarrollo de las secciones subsiguientes.

Sección II. La formación común en Ciberseguridad y Ciberdefensa.

Para abordar este apartado, es menester precisar el objetivo perseguido al plantear la necesidad de dotar a los expertos sectoriales de "una formación común en Ciberseguridad y Ciberdefensa". En consecuencia, es imprescindible en primera instancia, recordar que el presente trabajo apunta a la conformación de equipos multidisciplinarios que se desempañarán en el nivel gerencial de organismos e instituciones relacionadas con la Ciberseguridad y la Ciberdefensa. Estos equipos tendrán la responsabilidad de elaborar políticas y estrategias de alcance nacional, vinculadas por un lado con áreas públicas y privadas subordinadas y por el otro, con entidades equivalentes en el plano internacional. Por lo tanto, la primera advertencia recae en diferenciar esta propuesta de la formación específicamente técnica que busca capacitar a los operadores de áreas de las TICs e incluso a sus gerentes / líderes.

Los conocimientos básicos a proveer a los expertos de diversas especialidades, podrían agruparse conceptualmente en cuatro áreas, a saber:

1. **Área de conocimientos técnicos mínimos**. Dada la amplitud de origen de los especialistas identificados (especialmente de aquellos que provienen de ciencias "blandas"), es necesario un conocimiento básico de aspectos técnicos para un correcto desenvolvimiento en el ambiente del ciberespacio. Dentro del mismo, la interrelación con el área puramente técnica es indispensable y requiere del dominio general de sus principios de funcionamiento y su terminología particular. Algunos tópicos esenciales a incluir podrán ser:
   a. Fundamentos de TICs.
   b. Programación (paradigmas y lenguajes).
   c. Análisis de malware.
   d. Criptografía.
   e. Inteligencia artificial.

f. Ingeniería reversa.
g. Back-tracing.
h. Forensia informática.
i. Diseño de software seguro y Seguridad en el desarrollo de software (involucra etapas de análisis, implementación, testing de penetración y despliegue seguro).
j. Tecnologías exponenciales: vulnerabilidades y riesgos.
k. Principios de computación cuántica.

2. **Área de conocimientos orientados al gerenciamiento**. El trabajo en equipo dentro de estructuras de nivel nacional y/o sectorial, requiere de conocimientos y habilidades básicas para el desarrollo de la deseada sinergia resultante. Materias comunes de gerenciamiento de equipos y proyectos sirven a tal propósito:
   a. Teoría organizacional y Psicología organizacional.
   b. Gobernanza y fundamento de management en Ciberseguridad.
   c. Gerenciamiento de proyectos.
   d. Determinación de infraestructuras críticas y análisis de riesgos. Este conocimiento se orienta a que los especialistas sean capaces de analizar la estructura de sus propias organizaciones y sistemas, entender sus vulnerabilidades y las opciones de protección disponibles para protegerlas. Luego, es indispensable un ejercicio de entendimiento más amplio para poder identificar la interrelación de infraestructuras críticas particulares con el funcionamiento macro de sistemas mayores.
   e. Innovación y emprendedurismso.
   f. Liderazgo de equipos multidisciplinarios.
3. **Área de conocimientos de entorno general**. El ámbito y las características particulares del ciberespacio (ya detallados en el Capítulo II), hacen necesario que los especialistas comprendan y asimilen la realidad multifacética donde deben operar. Se pretende iniciarlos en el conocimiento de distintas áreas convergentes en la problemática de la Ciberseguridad y la Ciberdefensa:
   a. Hacking Ético[30].

[30] Hacking ético es una forma de referirse al acto de una persona, o mejor conocido como hacker, que utiliza sus conocimientos de informática y seguridad para encontrar vulnerabilidades o fallas de seguridad en el sistema, con el objetivo de reportarlas en la organización para que se tomen todas las medidas necesarias que posibilite prevenir una catástrofe cibernética, como el robo de información.Es necesario conocer la actividad y modos de operación de aquellos que operan.
URL: https://www.iniseg.es/blog/ciberseguridad/que-es-el-hacking-etico/

b. Evolución del plexo legal relativo al ciberespacio. Su vinculación con el llamado *lawfare*, los problemas de aplicación en el ámbito local e internacional, el problema de la jurisdicción y los vacíos legales.
c. Metodologías y organizaciones de respuesta a incidentes. Funcionamiento de CSIRTs / CERTs, NOCs y SOCs. Diferencias y capacidades de cada uno de ellos. Cómo operan y se integran.
d. Estructuras nacionales de Ciberdefensa y Ciberseguridad (comparativo con entidades internacionales).
e. Los conflictos modernos, la Ciberseguridad y la Ciberdefensa (características de los conflictos modernos de naturaleza híbrida, organizaciones militares de Ciberdefensa y estudio de casos). Campañas de desinformación o manipulación.

   Este tópico en particular debe desarrollarse con una visión integradora de escenarios regionales e internacionales y muy particularmente con acento en el carácter híbrido de las amenazas reales y potenciales. Es aquí donde cada especialista comprende su rol dentro del equipo, al poder identificar su área de dominio en el complejo esquema del ciberespacio y fundamentalmente su interrelación con otras áreas paralelas. Es importante analizar cómo operan los grupos locales y extranjeros de manera coordinada o aislada sobre la infraestructura crítica, cuál es el rol de las ciberoperaciones en un conflicto híbrido con y sin ejercicio de la violencia armada, el valor de la inteligencia estratégica y la capacidad anticipatoria necesaria para impedir o mitigar los efectos adversos.

4. **Área aplicativa**. Esta área complementaria busca un acercamiento eminentemente práctico con las organizaciones y entidades vinculadas con la Ciberseguridad y la Ciberdefensa. El contacto personal y la participación en actividades afines será, además de un incentivo, una gran oportunidad para presentar campos concretos de desempeño profesional multidisciplinario.
   a. Visitas a centros de respuesta a incidentes, a empresas de seguridad informática, a entidades de telecomunicaciones, etc.
   b. Participación en ejercicios académicos de planeamiento militar con injerencia del componente cibernético.

A continuación, se analizarán con fines eminentemente prácticos, algunas ofertas educativas nacionales y extranjeras que pueden resultar de utilidad para este fin.

La Universidad de Buenos Aires (Facultad de Ciencias Económicas - Escuela de Negocios y Administración Pública) dicta la Maestría en Ciberdefensa y Ciberseguridad (UBA, Posgrado FCE). La misma está orientada a capacitar y formar a agentes gubernamentales y a ejecutivos empresariales en el diseño e implementación de Sistemas de Detección de Ciber-intrusiones; en el desarrollo de software seguro; en la detección de la circulación de malware en las redes teleinformáticas; en la preservación de la Infraestructura Crítica y en técnicas de "backtracing".

La Universidad de la Defensa Nacional, a través de la Facultad de Ingeniería del Ejército, presenta la Maestría en Ciberdefensa (FIE). Esta propuesta educativa, articulada con la Especialización en Criptografía y Seguridad teleinformática (de la misma facultad), profundiza los contenidos agrupados en el área de base técnica, al mismo tiempo que incluye en su plan de estudios, algunas temáticas del entrono general propuesto como introducción a la Ciberdefensa y su Comando y Control.

En ámbito regional, la Escuela Superior de Guerra "General Rafael Reyes Prieto" (Colombia) presenta la Maestría en Ciberdefensa y Ciberseguridad (ESG-Col). El perfil de egreso planteado y su plan de estudio, abarcan casi todos los aspectos relevantes propuestos en este trabajo para la formación básica común de especialistas multidisciplinarios, incluyendo tópicos de la Seguridad y Defensa Nacional, el Concepto Operacional y la Prospectiva en Ciberseguridad y Ciberdefensa. Por su parte la Universidad Mayor (Chile) dicta el Magíster de Ingeniería en Seguridad de la Información (UM). El plan de estudios abarca igualmente muchos de los contenidos señalados en el análisis de formación común pero no incluye aspectos relacionados con el entorno general amplio del ciberespacio al que pretende orientar la propuesta del presente trabajo, al excluir implícitamente el rol de la Ciberseguridad / Ciberdefensa en los conflictos modernos.

La Universidad Tecnológica de Tallin (Estonia) dicta una carrera de grado denominada Cyber Security Engineering (TECH), la cual, si bien define un perfil de egreso preponderantemente técnico, incluye aspectos comunes que han sido señalados dentro del abanico de conocimientos de formación general tratados en este capítulo.

Existe también un grado de capacitación complementaria en el marco de las llamadas "diplomaturas", las cuales en ámbito académico universitario ofrecen estudios orientados, por lo general, hacia la Seguridad Informática, aunque su titulación invoque a un concepto más amplio como es la Ciberseguridad. Ejemplo de ello son las diplomaturas en Ciberseguridad

ofrecidas localmente por la Universidad de Palermo (UP), la Universidad de la Cámara Argentina de Comercio y Servicios (CAECE) o la Universidad del CEMA (UCEMA).

Un caso distinto, lo conforma el Programa Avanzado en Introducción a la Ciberdefensa y la Ciberseguridad de la Escuela Superior de Guerra Conjunta de Argentina (ESGC-Arg, PAICyC). Si bien la misma es una capacitación de corta duración (comparada con una maestría), su objetivo revela una concepción amplia del entorno del ciberespacio: El curso constituye una introducción general a la Ciberdefensa y la Ciberseguridad mostrando que las mismas requieren enfoques interdisciplinarios y multidisciplinarios. Se destaca que la Ciberdefensa y Ciberseguridad requieren de profesionales con las formaciones de grado más diversas.

Otro aspecto destacable de esta casa de estudios lo constituye el establecimiento del Observatorio Argentino del Ciberespacio (OAC), cuyo objetivo general busca establecer y generar una estructura estable y multidisciplinar, orientada específicamente al estudio y difusión de los estudios, informes y reportes relativos que hacen a la Ciberdefensa y Ciberseguridad y su estado de actualización a nivel nacional e internacional. Esta suerte de Think Tank específico es sin dudas una entidad de capital importancia para los especialistas debidamente formados a los que se pretende acceder. Independientemente de su afectación laboral concreta, la pertenencia al mismo retroalimenta el sistema de conocimiento permanente. El Observatorio trabaja conjuntamente con todos los elementos que hacen al componente militar, y además, con Universidades, Administraciones, Empresas, Fundaciones y Organizaciones sensibles que también hacen a la Defensa Nacional, como por ejemplo Consejos Profesionales, Centros de Estudio relacionados o vinculados con este ámbito temático.

Sección III. La formación común en Inteligencia.

Esta sección detalla la necesidad de dominar las técnicas básicas del análisis de inteligencia en los niveles Estratégico Nacional y Sectorial. Esto permitirá integrar eficazmente las capacidades individuales de cada experto del equipo, enfocadas con una visión común dentro del ámbito del ciberespacio lograda en la etapa de formación anterior[31]. Se apunta a que el experto sepa qué observar de la situación, qué buscar, cómo hacerlo y cómo procesar esa información recopilada para servir al equipo como un todo.

[31] Los especialistas formados para trabajos multidisciplinarios deben conocer acabadamente los ámbitos de responsabilidad y competencia definidos en materia de inteligencia en las esferas de seguridad y defensa. Base de ellos es estudio de la Ley 25.520 (Ley de Inteligencia Nacional, 2001).

La gerencia de alto nivel debe batallar permanentemente con el balance de tres áreas que a veces se muestran complementarias y otras de modo suplementario, estas son: la gestión de información, la inteligencia y la toma de decisiones. Las características propias de la llamada "era de la información" complejizan enormemente esta tarea. "Si consideramos que la información y su análisis son los elementos fundamentales del proceso de toma de decisiones, contar con herramientas metodológicas para lidiar con esta situación es sumamente necesario. La necesidad de contar con información acorde a las necesidades se da tanto en la órbita pública como privada, en todos los ámbitos de desarrollo de una sociedad" (UCA, Curso de Posgrado en Inteligencia Estratégica).

No es posible conducir una organización en un entorno volátil, incierto, complejo y ambiguo sin información, y es la inteligencia quien provee dicha información.[33]

El escenario de amenazas híbridas descripto como marco teórico para el desarrollo de este trabajo, añade una dimensión aún más compleja a la que se expone el decisor. En este sentido, el Teniente Coronel Lucas Martín (2019), resalta que […] "las amenazas son transversales y nos afectan a todos y se trabaja de forma coordinada. Se contrarresta con un esfuerzo desmedido en el campo de inteligencia, la única forma de atajar estas amenazas. La labor de inteligencia tiene que identificar puntos blandos, debilidades, económicas y sociales".

Esta afirmación sirve tanto para analizar un sistema propio y defenderlo, como para analizar un sistema externo al cual se quisiera potencialmente afectar.

La inteligencia estratégica[35]. Para definir la expresión, se recurre al trabajo de Joao Aguirre (Sciencedirect, 2015), quien lo aborda desde un enfoque administrativo, argumentando que […] "de manera integral la inteligencia estratégica es entendida como una forma de generar, filtrar y organizar la información estructurada para que permita tomar decisiones estratégicas en una organización". Aunque advierte asimismo que "es un concepto tradicionalmente empleado en contextos militares, de defensa e incluso como «secreto gubernamental», existen tímidas aplicaciones de índole académica y administrativa".

[33] Si bien esta es una definición genérica, el proceso de planeamiento estratégico nacional (en el ámbito de defensa), recurre al método de planeamiento por capacidades el cual define posibles escenarios de acción que buscan dar mayor previsibilidad a la tarea. No obstante ello, es la inteligencia quien con su actividad minimiza esta incertidumbre omnipresente.

[35] Para aplicación de estos conceptos es necesario reconocer los límites funcionales de las actividades de inteligencia en áreas de seguridad y defensa acordes a la legislación nacional vigente. Leyes 23.554, 24.059 y 25.5520)

El mismo autor propone un esquema general de desarrollo desde un enfoque cronológico donde la inteligencia producida sirve a fines particulares y luego se integra en un sistema mayor completo.

La vigilancia tecnológica (Aguirre, 2015, pág. 104). Es un sistema organizacional, conformado por un conjunto de métodos, herramientas, recursos tecnológicos y humanos, con capacidades altamente diferenciadas para seleccionar, filtrar, procesar, evaluar, almacenar y difundir información del pasado, transformándola en conocimiento para la toma de decisiones estratégicas. De esta manera se concluye que la vigilancia tecnológica es un proceso que analiza la información cronológica del pasado.[37]

La inteligencia competitiva (Aguirre, 2015, pág. 104). Es un sistema organizacional de referenciación del estado actual de la compañía, clientes, competidores, proveedores y todos los agentes relacionados en la cadena de valor, identificando variables económicas, sociales, tecnológicas, de mercado, de competencia y laborales, con el fin conocer el entorno dinámico y cambiante de la actualidad.

La inteligencia prospectiva (Aguirre, 2015, pág. 105). El uso de herramientas de prospectiva se ha convertido en un aspecto fundamental para el planeamiento estratégico, para generar visiones compartidas de futuro, orientar políticas de largo plazo y tomar decisiones estratégicas en el presente, dadas las condiciones y las posibilidades locales, nacionales y globales. Además, también se debe comprender como un proceso de análisis de escenarios futuros de la organización, en función del mercado, de los agentes de directa relación, de las metas y del entorno social, con la finalidad de orientar estrategias de largo plazo.

[37] Debe hacerse hincapié en

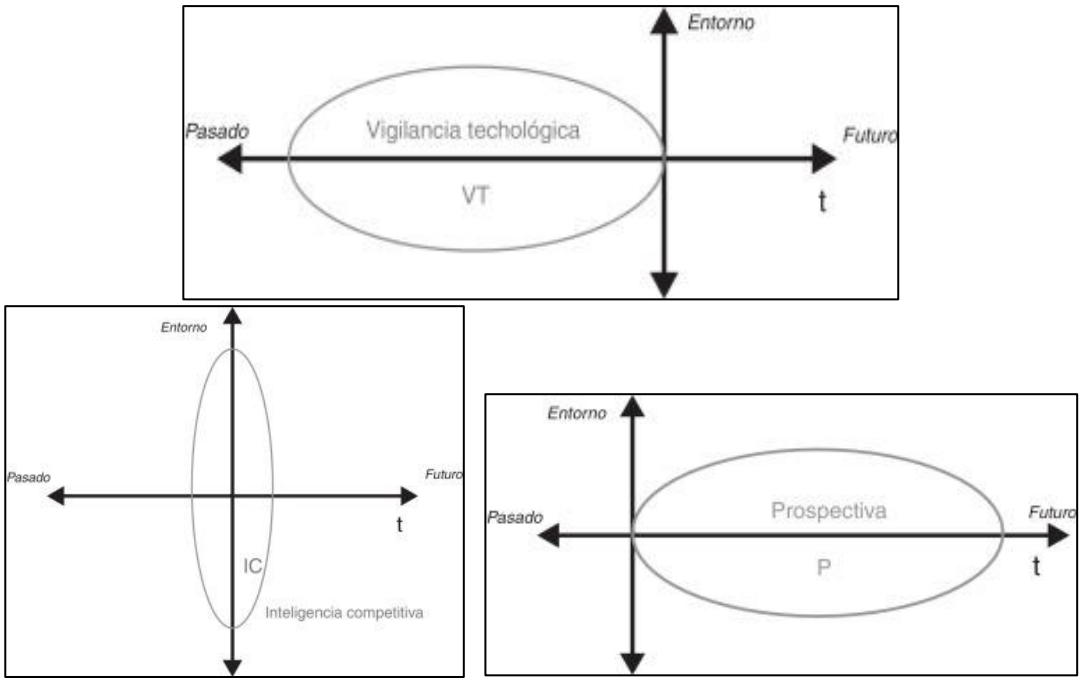


Figura 10: Vigilancia tecnológica, competitiva y prospectiva desde un enfoque cronológico (Aguirre, 2015, pág. 106)

Desde esta conceptualización genérica, se pretende que los especialistas, en términos concretos de formación, sean instruidos en conceptos básicos del área de inteligencia, como por ejemplo:

- La información como dato y la inteligencia como proceso.
- Niveles y tipos de inteligencia.
- El ciclo de inteligencia.
- Las fuentes y los medios de reunión de inteligencia. Conceptos generales, técnicas particulares y sistema de valoración.
- Los riesgos de la infoxicación.
- El planeamiento y la ejecución de la actividad de inteligencia.
- La evaluación del uso de la información. El concepto de necesidad de saber.
- Ética profesional.
- Bases legales de la actividad.
- Organizaciones de inteligencia (nacionales e internacionales).

La Ciberinteligencia. Luego de esta etapa básica genérica y pasando a un enfoque más particularizado, es importante la asimilación del concepto de ciberinteligencia. Entendiendo a esta como una aplicación concreta de la actividad en el ciberespacio. La ciberinteligencia “es una actividad de obtención y análisis de información cuyo objetivo es identificar, rastrear y

predecir capacidades, intenciones y actividades de actores hostiles en el ciberespacio" (LISA-Institute, Curso-Certificado de Experto en Ciberinteligencia)**.**[40]

Aquí convergen temáticas ya enunciadas en la descripción del entorno de amenazas híbridas, donde deben ser aplicados los conocimientos sobre Cibercrimen, Ciberterrorismo, Hacktivismo, Ciberespionaje, y otras actividades posibles de ser ejercidas dentro y desde el ciberespacio con la finalidad de "conocer sus características para mitigar su impacto y mejorar así la toma de decisiones en el ámbito de la Ciberseguridad. Las empresas e instituciones contratan a profesionales con conocimientos en Ciberinteligencia para prevenir ciberataques, averiguar información de sus atacantes y tomar decisiones que reduzcan el impacto de los mismos" (LISA-Institute, Curso-Certificado de Experto en Ciberinteligencia).

La intención de una formación básica en Inteligencia Estratégica de los expertos sectoriales, no pretende en modo alguno escalar al desarrollo de especialistas en grado de desempeñar actividades por fuera del análisis de fuentes abiertas. Para información específica que requiera de especialistas en inteligencia, se debe recurrir naturalmente a las instituciones creadas y capacitadas a tal fin.

Dado el enorme desarrollo actual de las fuentes de información, aquellas de carácter abierto son igualmente complejas y sobreabundantes. Para ser eficaces en la tarea de buscar información pertinente y de calidad, existen técnicas específicamente diseñadas a tal fin. Las llamadas OSINT (Open Source Intelligence).

¿Cuáles son las ventajas del OSINT? "Permiten acelerar y mejorar la obtención de datos e información en fuentes abiertas (principalmente internet) sobre personas, empresas e instituciones clave, contribuyendo así a una mejor toma de decisiones a nivel operativo, táctico y estratégico" (LISA-Institute, Curso de Experto en OSINT).

Esta técnica debe tener en cuenta algunos conocimientos asociados, los cuales suelen ser cubiertos por la oferta formativa que se dedica a su difusión:

- Búsqueda anónima de datos e información sobre personas, empresas e instituciones.
- Límites jurídicos de la actividad.
- Seguridad propia durante las tareas de investigación.
- Fuentes de exploración, internet, Deep Web y Dark Web.
- Ciberinteligencia y Análisis de Redes Sociales (Técnicas ARS)
- Realización y representación en Informes

[40] En el caso de nuestro país, es importante diferenciar las actividades propias dentro del ámbito de la Inteligencia Criminal de aquellos asociados a la esfera de la Inteligencia Estratégica Nacional.

La Contrainteligencia. La contracara de la actividad de inteligencia, son las medidas adoptadas por individuos y organizaciones a fin de protegerse de la actividad hostil de terceros, a esto llamamos Contrainteligencia. Las técnicas aplicadas y los organismos especializados serán consecuentemente empleados para protegerse de las actividades de inteligencia y su denominación es coherente con este sentido: Actividades de contra inteligencia; Contra-espionaje; Contra-sabotaje; Agencias de Contrainteligencia y Operaciones de Contrainteligencia son algunos ejemplos. Operativamente se pretende que el personal debidamente capacitado esté en condiciones de ejecutar una correcta apreciación de contrainteligencia y participar en el diseño de un estudio seguridad de instalaciones y sistemas críticos.

La Inteligencia, la Defensa Nacional y la Ciberdefensa.

Nuestro plexo normativo tiene una visión particular de la inteligencia sobre las esferas de responsabilidad en relación a la Defensa y la Seguridad, la cual no puede ser soslayada en el abordaje de este apartado.

La DPDN (2014, pág. Cap III) considera Inteligencia Estratégica Militar "al nivel de la inteligencia que se refiere al conocimiento de las capacidades y debilidades del potencial militar de los países que interesen desde el punto de vista de la Defensa Nacional, así como del ambiente geográfico de las áreas estratégicas operacionales determinadas por el Planeamiento de la Defensa Nacional y, más específicamente, por su contribuyente Planeamiento Estratégico Militar. Posteriormente especifica que: [---] en materia de Inteligencia Estratégica Militar el MINISTERIO DE DEFENSA deberá contribuir a la "alerta temprana estratégica" a través de la provisión oportuna de la inteligencia estratégica militar necesaria, a los efectos de prevenir una potencial agresión estatal militar externa."

Esta función primaria de la Inteligencia en general, plasmada aquí en particular para la Inteligencia Estratégico Militar, no puede prescindir de uno de las más novedosas e importantes fuentes de obtención actuales, el Ciberespacio y del más especializado medio de obtención, la Ciberinteligencia.

La DPDN (2018, pág. Cap I), se explaya un poco más sobre el particular y explicita su visión indicando que:

> Las amenazas cibernéticas sofisticadas provienen de organizaciones militares y agencias de inteligencia de otros Estados. Si bien los gobiernos tecnológicamente avanzados explotan sus ventajas comparativas con relación al resto de los países, el despliegue de operaciones disruptivas en el ciberespacio también está al alcance de las

> naciones menos desarrolladas. El abordaje de esta problemática desde la perspectiva de la Defensa Nacional requiere adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional y de aquellas que sean designadas para su preservación, independientemente del origen de la agresión.

Es evidente una vez más, que las visones de los documentos citados expresan diferencias sustanciales sobre los ámbitos de Seguridad y Defensa que se trasladan también a la esfera del Ciberespacio. No obstante ello, es una realidad que desde la óptica del potencial agresor puede ser usufructuada a su favor.

> No todos los países tienen esta diferenciación tan marcada. En el caso de los EE.UU., (…) el general Keith Alexander fue designado Director de la NSA (Agencia Nacional de Seguridad) y, a su vez, Comandante del CYBERCOM. Este criterio fue objetado por algunos, mientras otros vieron esta dualidad como algo natural al considerar que ambas organizaciones poseen responsabilidades afines. Las críticas se fundamentaron, principalmente, en la preocupación que en algunos provoca el desdibujamiento de los límites entre lo interno y externo, como el que se produjo en los EE.UU. como consecuencia del ataque del 11 de septiembre de 2001 (Flores, 2015).

En línea con este concepto, la doctrina estadounidense establece que "(…) las organizaciones de inteligencia a nivel nacional llevan a cabo actividades de inteligencia en, a través y sobre el ciberespacio en respuesta a las prioridades nacionales de inteligencia. Esta inteligencia puede apoyar la planificación y preparación de un comandante militar" (US JP 3-12, 2018, págs. II-9).

En el plano puramente militar, los sistemas de comunicaciones y de toma de decisiones están cada vez más integrados a sistemas informáticos y sus raíces profundamente afincadas en el Ciberespacio. Esta afirmación, cobra mayor relevancia en los niveles Estratégico Militar y Operacional (aunque es válida en términos generales en el nivel Táctico). Las tareas de inteligencia y en particular las actividades de Ciberinteligencia militar, apuntan a preservar la libertad de acción de los propios Comandantes en el uso del Ciberespacio (en tiempos de paz y guerra) y al mismo tiempo a proveer de información certera y oportuna para el entendimiento del ambiente operacional donde se deba operar. Asimismo, analiza las fortalezas y debilidades del enemigo dentro del ciberespacio, sus capacidades para desarrollar ciberoperaciones (reales y potenciales) y la determinación del centro de gravedad de sus sistemas que puedan ser potencialmente afectados (aspecto que será ampliado en el Capítulo VI).

La oferta formativa especializada.

Tanto en el ámbito local como en el internacional, existe un nutrido abanico de instituciones y programas que brindan capacitación en el campo de la Inteligencia Estratégica y/o de la Ciberinteligencia.

La Universidad de Buenos Aires (UBA), presenta la Especialización en Inteligencia Estratégica y Crimen Organizado. La misma está orientada al análisis, asesoramiento y difusión especializada de información calificada transformada en inteligencia. Integra estudios de los sistemas institucionales y políticos del Estado y de la seguridad y defensa de la Nación. Se trata de generar capacidades para intervenir en el análisis y gestión de inteligencia en organizaciones públicas y privadas.

La Universidad Católica Argentina (UCA) dicta un curso de Posgrado: Inteligencia Estratégica y la Universidad Nacional de La Plata (UNLP) desarrolla una Maestría en Inteligencia Estratégica Nacional. Los planes de estudio están orientados a aquellos profesionales que analizan información y aportan al proceso de toma de decisiones en cualquier organización, aplicando herramientas del proceso estratégico para generar y/o identificar estrategias propias y de terceros. En el caso de la maestría de la UNLP, es particularmente interesante la formación integral de los especialistas, el abordaje de conceptos de Defensa Nacional, planeamiento, visión estratégica mundial y política exterior argentina. Asimismo propone el desarrollo de habilidades sobre operativos de inteligencia, contrainteligencia y tratamiento de conflictos de baja intensidad. También se instruyen en informática, criptología e idiomas.

La Universidad de la Defensa Nacional, a través del Instituto de Inteligencia de las FFAA (IIFA), presenta la Especialización en Análisis de Inteligencia Estratégica. El posgrado se centra en formar especialistas en análisis de inteligencia estratégica y gestión de la información, para asesorar y asistir en la producción de conocimiento - inteligencia, tanto en el ámbito de la Defensa Nacional como a la Alta Dirección en el ámbito privado. Es útil a la formación perseguida para los especialistas, la capacidad para interpretar y ejercitar la aplicación práctica de la doctrina de inteligencia, con énfasis en el planeamiento a nivel estratégico militar, como así también la habilidad para poder aplicar metodologías de análisis de información, a fin de proyectar conclusiones con fundamento sistémico.

La Universidad Francisco de Vitoria - Campus Internacional de Ciberseguridad (España) (UFV). dicta una Maestría en Ciberinteligencia. El objetivo fundamental es formar a un profesional que pueda ejercer como Analista de Ciberinteligencia, aplicando al ciclo de

inteligencia, herramientas y procesos de investigación de fuentes abiertas (como OSINT (Open-Source Intelligence) / SOCMINT (Social Media Intelligence)), y análisis de la Deep Web.

LISA Institute del Reino de España (LISA-Institute), ofrece un curso de experto en Ciberinteligencia. El mismo está dirigido a personal dedicado a la Ciberseguridad, a la protección de activos y a la investigación de ciberamenazas. Vincula directamente la esfera de inteligencia con la ciberseguridad, proponiendo capacitación para analizar información sobre ciberseguridad, ciberterrorismo, cibercrimen y hacktivismo, y el manejo de metodologías para obtener y producir inteligencia sobre riesgos y ciberriesgos.

Sección IV. La formación común en metodología de la toma de decisiones.

¿Para qué sirve planificar?

Tanto en el ámbito civil como militar, público como privado, las organizaciones e instituciones enfrentan problemas diversos en escenarios cada vez más complejos donde reina como factor común la incertidumbre. Contar con una metodología de planificación es fundamental para el proceso de toma de decisiones.

El planeamiento es el conjunto de actividades destinadas a establecer objetivos, determinar políticas o modos de acción y preparar los planes correspondientes.

La aplicación de un método en la solución del problema estará basado en “el proceso lógico que sigue el pensamiento al enfrentar una situación de incertidumbre y, consecuentemente, en los principios que fundamentan la lógica cartesiana. Dichas características se basarán en el análisis y síntesis, la analogía, la deducción, la inducción y la flexibilidad, todo ello para asegurar la recurrencia del proceso” (ROD-71-01-I, 1998, pág. 63 a 65).

Su aplicación separa lo racional de lo irracional y evita el desgaste que significa la práctica del proceso prueba-error-prueba. Su empleo fortalecerá la capacidad de raciocinio, disminuyendo el peligro de aceptar conclusiones por razones emocionales, intuitivas o instintivas, y pondrá de manifiesto la falacia de llegar a deducciones preestablecidas, basadas en la tradición o en el hábito. La práctica en el análisis y apreciación de factores y circunstancias, facultará para tomar decisiones lo más racionales y correctas posibles, aspecto básico e imprescindible cuando el tiempo es una exigencia.

El Planeamiento en general, su estructura.

En términos generales, la actividad de planeamiento comprenderá (ROD-71-01-I, 1998, pág. 17):

a. La identificación y definición de problemas.

   Este paso es de radical importancia en el proceso. Quienes pasen por alto esta instancia o la aborden de forma poco profunda, corren riesgo de intentar dar solución al problema equivocado o de no entender el valor de la concatenación de objetivos en un proceso jerárquico, cayendo en una suerte de pensamiento egocéntrico.

b. La reunión, organización y procesamiento de información.

   En auxilio del desarrollo de este paso, se plasmarán las destrezas adquiridas en la formación de análisis y proceso de inteligencia. Es tan importante saber que buscar, como registrarlo, procesarlo y exponerlo al equipo con certeza y oportunidad.

c. La apreciación de situaciones.

   Las mismas destrezas de análisis de inteligencia coadyuvan en el análisis de escenarios complejos, ya sean locales, regionales o globales. Es importante observar e identificar las variables que afectan y sostienen a los sistemas en estudio, su interrelación e interdependencia, sus puntos fuertes y vulnerables, las entidades y personalidades involucradas y/o decisores, la interpretación de sus aparentes objetivos, etc.

d. La formulación de proposiciones.

   Habiendo identificado correctamente el problema a resolver, interpretado la propia misión en relación a los objetivos de la entidad superior a la cual se sirve, habiendo reunido, procesado y compartido la información disponible y habiéndose analizado el contexto con una mirada omnicomprensiva, es en este paso, donde se formulan las posibles soluciones al problema.

   Tales propuestas de solución pasan por un proceso de validación y comparación para ser presentadas luego al decisor junto con las conclusiones y recomendaciones asociadas.

   Los posibles modos de acción a tomarse deben ser expuestos a un proceso de validación sobre su aptitud para alcanzar el objetivo, la factibilidad de hacerlo y una consideración sobre la relación costo beneficio de su aplicación.

   Una vez validados, esos modos de acción (los que superaran la prueba) deben ser comparados para seleccionar el mejor de ellos. Esta actividad debe ser correctamente planificada, consensuada en forma y fondo y ejecutada con profesionalismo, ya que los sesgos mentales y las ideas preconcebidas atentarán contra la excelencia del resultado.

e. El desarrollo de la resolución.

Se presentan al decisor todas las opciones validadas consideradas junto a sus conclusiones y el asesoramiento sobre cuál de ellas es mejor para alcanzar el objetivo. En última instancia, el equipo asesora y es el decisor quien carga sobre sus hombros con la responsabilidad de resolverse sobre el modo de acción a ser adoptado y ejecutado.

f. La preparación de planes y órdenes.

Esta etapa comprende la coordinación de planes cooperantes y la sincronización espacio-temporal de los efectos a realizar. Metodológicamente se elaboran matrices de sincronización para visualizar mejor el esquema y posteriormente facilitar su control durante el desarrollo de las acciones.

Este proceso mental esquemático es solamente una guía metodológica. Cada organización debe adaptar este esquema a su cultura organizacional y sus procesos de funcionamiento, sin embargo, los pasos secuenciados son comunes en líneas generales a toda metodología adoptada.

Los niveles de la guerra y de conducción.

En esta instancia, es necesario recordar que el marco teórico de referencia del presente trabajo (detallado en el Capítulo II), describe una situación de conflicto particularmente vinculado a amenazas híbridas, donde las Ciberoperaciones juegan un rol cada vez más relevante.

La división en niveles de conducción (ROB-00-01, 2015, págs. I-2), que abarcan todo el espectro del conflicto, permite un análisis metodológico de los hechos que se suceden en una guerra, para poder encontrarles una secuencia lógica de razonamiento. La doctrina militar argentina reconoce tres niveles de la guerra y cuatro niveles de conducción.

NIVELES DE GUERRA	NIVELES DE CONDUCCIÓN	RECURSOS	FINALIDAD
ESTRATÉGICO	*Estratégico general o nacional o Gran Estrategia.*	*Todos los medios del Poder Nacional.*	*El estado final político.*
	Estratégico militar.	*Todos los medios militares del Poder Nacional y, eventualmente, aquellos otros provenientes del Poder Nacional.*	*El estado final militar.*
OPERACIONAL	*Operacional.*	*Los asignados a los comandantes de nivel operacinal.*	*El estado final operacional.*
TÁCTICO	*Táctico.*	*Los medios que se emplean en una operación militar.*	*Obtener los puntos decisivos y los objetivos de acuerdo con el plan de campaña.*

Figura 11: Relaciones entre los niveles de la guerra, los niveles de conducción, recursos y finalidad (ROB-00-01, 2015)

Esta división metodológica se basa en la relación medios/fines y su consecuencia causa/efecto. No se relacionan estrictamente con los niveles de comando, sino con los llamados niveles de la conducción. Cada nivel implica un problema de distinta naturaleza e involucra una lógica de razonamiento particular.

El Nivel Estratégico Nacional es el responsable de conducir el potencial nacional para alcanzar los objetivos políticos establecidos. Su propósito es dirigir en forma coherente y articulada todos los instrumentos del Poder Nacional. La estrategia nacional impondrá restricciones y límites a los componentes del poder que sean empleados.

Tanto en tiempos de paz como en tiempos de guerra, los conflictos se desarrollan inevitablemente por oposición de dos o más voluntades orientadas a objetivos contrapuestos. El Nivel Estratégico Nacional debe prever y actuar conforme al grado de amenaza que estas voluntades opuestas representen, a su propia visión y objetivos. Para ello evalúa constantemente su entorno, las amenazas reales y potenciales, sus aliados y oponentes y todo a la luz de sus propios recursos, fortalezas y debilidades.

El punto de partida que orienta la tarea en materia de ciberoperaciones es lo determinado en la Estrategia Nacional de Ciberseguridad vigente, la cual señala que:

> El ciberespacio es un elemento esencial en la vida de las personas y las organizaciones no habiendo aspecto del desarrollo social que no esté alcanzado por este fenómeno. Consciente de esta realidad, establece los principios esenciales y los objetivos centrales de la nación en torno a su proyecto para la protección del ciberespacio

> En tal sentido, el documento enumera ocho objetivos centrales desde donde se desplegarán planes de acción vinculados a la generación de un marco normativo acorde; al desarrollo y la articulación de capacidades de respuesta a incidentes de seguridad a gran escala; a la protección de infraestructuras críticas que habilitan la prestación de servicios esenciales para la sociedad y la economía; a la integración con otros países y a la creación de una cultura de Ciberseguridad, a partir de la cual las personas aprovechen los beneficios de las nuevas tecnologías, minimizando los riesgos devenidos de su utilización. (Resol 829/19 - Anexo I - Estrategia Nacional de Ciberseguridad, 2019).

La Dirección Nacional de Ciberseguridad, como máximo órgano en la materia, debe contar a su vez con su propio y particularizado método de planeamiento, incluyendo una mirada omnicomprensiva sobre todos los factores del poder nacional. En la paz, el planeamiento derivado de esta directriz, servirá para delinear más eficientemente las políticas y estrategias que, en materia de Ciberseguridad, deben ser adoptadas para proteger las infraestructuras críticas de la nación y sus sistemas principales. Cada sector del potencial nacional (económico, industrial, político, social, científico, militar, etc.) tendrá su propio sistema de apoyo para toma de decisiones de utilidad en las organizaciones que los materializan. Los expertos sectoriales reclutados, deben necesariamente dominar las metodologías de planeamiento de su área y utilizar sus conclusiones para los trabajos de conjunto al trabajar en equipo en el nivel de conducción estratégico nacional dentro del área de la Ciberseguridad.

El Planeamiento en el Nivel Estratégico Militar.

La ya citada Estrategia Nacional de Ciberseguridad, observa las amenazas en relación al ciberespacio desde una posición preventiva, con énfasis en la implementación de acciones coordinadas más propias del ámbito de la seguridad informática. La Ciberseguridad es así dirigida a la prevención de ataques contra la propia infraestructura y las acciones reactivas se prevén sólo a nivel de restauración de sistemas críticos.

Independientemente de lo expuesto, cuando los conflictos en desarrollo o en ciernes se proyectan en modo de afectar los intereses vitales de la nación, se comienza a transitar en la esfera de la defensa nacional. Esta premisa abarca del mismo modo, a las acciones que se desarrollan en y desde el ciberespacio. Es un concepto difícil de ser delimitado y corresponde al poder político hacerlo. Sin embargo la realidad de los acontecimientos se impondrá en algún momento donde las evidencias hagan necesaria esta definición política concreta. Ahora bien,

el sistema de defensa nacional como tal, debe estar preparado de antemano para enfrentar tales amenazas. No puede ni debe comenzar la tarea con el conflicto en desarrollo.

El planeamiento es la herramienta que permite a de cada nivel de conducción, desde la paz y en la guerra, trabajar sobre los escenarios futuros, esbozar líneas de acción y objetivos intermedios a ser alcanzados por cada factor de fuerza considerado. Por lo tanto, la Ciberdefensa, partiendo de la orientación del Nivel Estratégico Militar direccionado por el poder político del Nivel Estratégico Nacional, debe desarrollar constantemente ejercicios de planeamiento con equipos multidisciplinarios capaces de generar eficazmente resultados concretos cooperantes con la consecución de los objetivos del sistema de defensa nacional.

Las organizaciones del factor de poder militar tienen estructurado su propio sistema de planeamiento en sus distintos niveles (Estratégico Militar, Operacional y Táctico). El Nivel Estratégico Militar, reglamenta su propio sistema de planeamiento en la doctrina conjunta elaborada a tal fin (PC-10-04, 2018).

Desde su apartado introductorio, la Publicación Conjunta "Procedimientos para el Planeamiento Estratégico Militar" (PC-20-09, 2018) especifica que el Presidente de la Nación, en su carácter de Comandante en Jefe de las Fuerzas Armadas, establece los objetivos para la Defensa Nacional:

- Durante tiempos de paz, dispone la vigilancia de los escenarios pasibles de evolucionar hacia situaciones de crisis, mediante la dirección y control de las acciones concurrentes y la aprobación de los planes de contingencia.
- Durante situaciones de crisis, fijar los objetivos estratégicos militares / misiones que contribuyan a alcanzar los objetivos políticos en juego y graduar la ejecución de acciones para el control, de escaladas.
- Durante tiempos de guerra, asegurar que las fuerzas militares obtengan los objetivos estratégicos militares / misiones que permitan alcanzar los objetivos políticos perseguidos.

El punto de partida para el planeamiento de este nivel es la Directiva Política de Defensa Nacional, la cual emana del Nivel Estratégico Nacional como directriz del proceso.

Como se ha expuesto en el Capítulo III, la DPDN considera seriamente el ámbito del ciberespacio y su interrelación con los dominios terrestre, aéreo y naval. Sin embargo, cabe recordar que no existe en la estructura nacional una Fuerza Armada particular para este dominio.

El Planeamiento en el Nivel Operacional (PC-20-01, 2015)**.**

Este nivel es considerado esencialmente conjunto, ya que operan normalmente más de una de Fuerza. Es un nivel de planeamiento y ejecución. Su planeamiento puede tratar sobre contingencias o eventos a prever (planeamiento deliberado) o bien de crisis.

El Nivel Operacional es el que lleva la teoría del Nivel Estratégico a la práctica del Nivel Táctico. El resultado será una Campaña u Operación militar de magnitud las que se concretarán en enfrentamientos en el nivel Táctico.

El llamado "arte operacional" es la forma creativa en que se combinan elementos del "diseño operacional" a través de la estructuración eficiente de acciones tácticas en espacio, tiempo y propósito, con un balance de riesgo y oportunidad, para crear condiciones necesarias afines al logro de objetivos del propio nivel o del nivel superior.

En el Nivel Operacional resultará de suma importancia armonizar la disponibilidad de recursos para alcanzar fines, e implicará el uso creativo de esos recursos para diseñar caminos o métodos para alcanzarlos.

Los elementos del diseño operacional considerados son: el Estado Final Deseado, el Centro de Gravedad, los Puntos Decisivos, las Líneas de Operaciones, el Momento y el Ritmo.

Es necesario recordar que las ciberoperaciones están presentes transversalmente en todos los niveles y como se expresara anteriormente, no reconocen límites entre ellos ni sus organizaciones. Es este quizás el aspecto más relevante y complejo que daría forma a un proceso de planeamiento específico de Ciberdefensa.

Una mirada sobre las Ciberoperaciones en el Nivel Estratégico Militar y Operacional.

Coincidiendo con De Vergara y Trama (2017, pág. 168), las actividades cibernéticas ejecutadas por las fuerzas militares se llevan a cabo en todos los tipos de conflicto, durante todas las fases de las operaciones militares y en todos los niveles de la guerra. Sin embargo cabe señalar que esta sentencia debe ajustarse a nuestro plexo normativo el cual confiere la prerrogativa del uso de la fuerza al componente militar durante el desarrollo de operaciones militares. No obstante, las amenazas externas pueden provenir incluso de agentes no estatales / militares. Como Gómez Arriaga, tendremos en cuenta aquellas amenazas que "implican intencionalidad, voluntades contrapuestas y el enfrentamiento en el espacio cibernético con fines militares, elementos claves que permiten distinguir las ciberoperaciones de otras

actividades como la seguridad informática o las operaciones de información" (Gomez Arriagada, 2013, pág. 362)[59]

Los mismos autores señalas además, que:

> "*en el mundo sobran ejemplos de ataques cibernéticos de nivel estratégico militar mediante los cuales se habrían manipulado redes de energía eléctrica llevándolas a un blackout, como podría haber sido el que impactó a millones de brasileros en 2005 y 2007, o las que permitirían la apertura de las compuertas de represas o provocar accidentes de ferrocarril. Puede crearse un caos con la simple inserción de un troyano, a través de malware en un sistema militar de comando y control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento (C4ISR) o en un sistema SCADA de una empresa de energía eléctrica"*. (2017, pág. 170)

Vemos aquí la complejidad de las amenazas híbridas, que hábilmente pueden coordinar acciones y sincronizar efectos en el campo puramente militar y fuera de este, como la afectación de otros sistemas esenciales del estado (provisión de agua, servicios sanitarios, financieros, etc).

Las operaciones ofensivas en el ciberespacio, básicamente tendrán por objeto afectar los tres pilares de la seguridad informática: confidencialidad, integridad y disponibilidad. Dependiendo del efecto final a alcanzar, la selección del objetivo será precisada en su modalidad, alcance, oportunidad y duración.

Es importante recordar que la mera disponibilidad de capacidad ofensiva no implica una postura estratégica ofensiva, sino la capacidad de reacción y por ende un factor de disuasión importante. De otro modo, considerar estratégicamente sólo el desarrollo de capacidades puramente defensivas, implicaría una debilidad manifiesta. Adicionalmente, el desarrollo de técnicas ofensivas potencia las capacidades defensivas propias.

Las actividades ofensivas, van precedidas de otras de carácter exploratorio del sistema a afectar, ya que es condición *sine qua non* concretar el acceso al mismo y descifrar sus debilidades y vulnerabilidades. Esta etapa está íntimamente relacionada con las actividades de inteligencia desarrolladas dentro y fuera del ciberespacio que normalmente involucran a distintos medios y fuentes de obtención.

[59] No obstante, debemos recordar que en el caso de nuestro país se considerará como una cuestión de Ciberdefensa sólo si el objetivo afectado es propio del Sistema de Defensa Nacional y si su origen es atribuible a una Fuerza Militar externa. Caso contrario es un asunto de Ciberseguridad.

Luego se desarrolla la intrusión propiamente dicha. La misma se llevará a cabo desde un vínculo de conectividad en red (a los sistemas conectados) o por intrusión física (a los sistemas aislados de la red).

Finalmente se suceden las tareas que previamente se especificaron en la etapa de planeamiento respecto del objetivo a alcanzar en cuanto a la afectación de alguno de la confidencialidad, integridad o disponibilidad del sistema blanco.

Como puede apreciarse, los efectos de un ataque cibernético pueden tener efectos en cualquiera de los niveles considerados. Es por ello que un Comandante Operacional que eventualmente tenga delegada facultades de ejecución de este tipo de actividades estará muy condicionado por el nivel superior en cuanto a sus objetivos y el alcance de sus acciones. Traspasar estos límites puede potenciar rápidamente una situación de escalada no deseada por el Nivel Estratégico Militar y/o Nacional.

Otro aspecto, ya mencionado en el Capítulo II, que viene a ser considerado es la dependencia y conexión de las ciberoperaciones con aquellas planificadas y ejecutadas en el mundo físico. Las mismas se complementan y se coordinan con acciones militares tradicionales, fundamentalmente en el gran marco de la denominada guerra híbrida.

Tanto en la doctrina de Brasil, como la de los Estados Unidos o la del Reino Unido, "se establece que las operaciones que se lleven a cabo en el espacio cibernético deben ser consideradas como un complemento de las operaciones militares tradicionales, pues al mismo tiempo que pueden afectar la dirección, el planeamiento y la ejecución de las operaciones militares, también pueden producir efectos sobre los sistemas de comando y control de armas o sobre la población, a través del uso de la web con propósitos de propaganda y acción disuasoria o trasmitiendo información falsa" (De Vergara & Trama, 2017, pág. 166)

En este nivel se suele citar como ejemplo las acciones mixtas ejecutadas presuntamente por Rusia en el conflicto de Crimea y el este de Ucrania, el cual combinaba perfectamente acciones de ciberoperaciones, guerra de la información, fuerzas especiales, milicias locales y diplomacia hacia un solo objetivo estratégico.

Planeamiento de las Ciberoperaciones.

Habiendo visto las generalidades de las metodologías de toma de decisión y escrutado algunos aspectos puntuales del desarrollo de las ciberoperaciones en los distintos niveles de la guerra y de conducción. Es posible ahora, dirigir la atención hacia el planeamiento específico de las ciberoperaciones.

Un aspecto a considerar es el de los niveles. El planeamiento de ciberoperaciones en el nivel Estratégico Militar responde a dar opciones de efectos a ser producidos en el ciberespacio contribuyentes a la consecución de los objetivos superiores. Adicionalmente, debería reservarse el planeamiento y ejecución de acciones ofensivas a este nivel superior. Desde la paz, el sistema de planeamiento de este nivel (al menos en nuestra doctrina) considera las capacidades a ser desarrolladas para enfrentar las contingencias posibles en los escenarios retenidos o las deducidas de un análisis de incertidumbre.

El planeamiento de nivel Operacional (como nivel traductor) se centra en la determinación de cadena de efectos (objetivos intermedios secuenciados y/o simultáneos) y las acciones concretas que los materializarán.

Consideraciones particulares respecto de la identificación y definición de problemas.

Atentos a esta situación desbordante de incertidumbre y carente de límites de responsabilidades definibles y excluyentes, el planeamiento de Ciberdefensa debe expandir su visión en la etapa de "identificación y definición de problemas". En este estadio inicial del proceso donde se define el problema, se analiza en detalle la propia misión y se listan las tareas impuestas y deducidas. Para ello, el personal abocado al planeamiento debe tener en cuenta algunos aspectos:

El dominio del ciberespacio es relativamente nuevo aún en el ámbito militar, por lo tanto se requiere de un tiempo de madurez y asimilación por parte de los conductores civiles y militares de la defensa. Esta realidad se expone para comprender que no siempre se sabe que misión concreta puede ser encomendada a la Ciberdefensa, o incluso que esta no sea tenida en cuenta más que en relación a la protección de los propios sistemas, fundamentalmente aquellos de Comando y Control.

Esto conlleva un esfuerzo adicional del área de ciberoperaciones para descifrar la propia misión derivada y muy particularmente las llamadas "tareas deducidas".

Consideraciones particulares respecto de la reunión, organización y procesamiento de información.

La búsqueda y el análisis de información, son y deben ser actividades permanentes para actualizar la carta de situación del entorno considerado. De Vergara y Trama coinciden que:

> Hoy en día, la información e inteligencia sobre los sistemas de comunicación y las redes eléctricas del enemigo, sus medios de transporte y obras públicas de infraestructura y estructura incluso social, instituciones y actores políticos pueden y

> deben ser, cuando sea posible, recogidos, analizados, difundidos y explotados. En este sentido, no se debe esperar ninguna posibilidad de conflicto, sino transformarse en actividades rutinarias de prevención. Es por tal razón que las funciones de inteligencia y comunicaciones deben integrarse más estrechamente con las operaciones del ciberespacio. (2017, pág. 182).

Las actividades de inteligencia no se limitan aquí a la Ciberinteligencia. Ya se ha expresado que, dada la naturaleza del espacio cibernético, se requiere de la fusión de todos los medios y fuentes de obtención disponibles.

Consideraciones particulares respecto de la apreciación de situaciones.

> En el espacio cibernético, el área de interés que debe analizarse no está limitada por fronteras nacionales o naturales. Por ello, normalmente incluye ciber-personas, estructuras y actividades sobre las que el comandante es capaz de influir o que están bajo el control del adversario y podrían llegar a obstaculizar o impedir el cumplimiento de la misión. El área de interés es global por naturaleza, pero para limitar su alcance se pueden evaluar ciertos factores que podrían ser clave en el espacio cibernético. (De Vergara & Trama, 2017, pág. 184).

Otras restricciones de carácter político y jurídico presionan con igual fuerza sobre los límites del área de interés, fundamentalmente por la característica de las capas física, lógica y social que integran el ciberespacio.

En este punto y en concreto, en el planeamiento de Ciberoperaciones de Nivel Operacional es necesario tener en cuenta algunos aspectos que De Vergara y Trama sintetizan en el siguiente listado (2017, pág. 184):

a. Determinar los hechos conocidos, el estado actual o las condiciones de las fuerzas conjuntas.
b. En coordinación con el Comando y Control, analizar algunos de los siguientes aspectos del adversario:
    1. Determinar la dependencia del adversario sobre el uso del espectro electromagnético.
    2. Determinar la capacidad de ataque cibernético y de comunicaciones del adversario.
    3. Determinar la capacidad de recolección de inteligencia del oponente.
    4. Analizar las vulnerabilidades propias de Comando, Control, Comunicaciones Inteligencia e Informática relacionadas con el ataque cibernético y de comunicaciones. Una debilidad “representará un elemento vital dentro de la situación o del sistema propio o enemigo y que, al poder ser explotado con los medios de que se dispone, se constituirá en una vulnerabilidad. Una vulnerabilidad constituirá el foco hacia donde se

materializarán las acciones dentro de cada Modo de Acción (MA), con el objeto de degradar, afectar o neutralizar al enemigo o sus Centros de Gravedad (CDG)" (PC-20-01, 2015, pág. 54).

c. Desarrollar hipótesis para reemplazar datos faltantes o desconocidos.
d. Analizar la misión del comandante y su intención desde el punto de vista cibernético.[66]
e. Determinar las limitaciones.
    1. Qué debe hacerse (imposiciones).
    2. Qué no puede hacerse (restricciones).
    3. Otras limitaciones (políticas, legales, diplomáticas, etc.).
f. Determinar los centros de gravedad propios y del adversario y los puntos decisivos tentativos.

    Centro de gravedad: conceptualmente esta expresión remite a la idea de un punto en el sistema que siendo afectado comprometa en forma determinante al mismo. Sobre él debe aplicarse la masa del esfuerzo. Su determinación es difícil y el mismo puede variar en determinados momentos de la campaña u operación. Para De Vergara y Trama, en el Nivel Operacional, el esfuerzo principal cibernético estará en la defensa, para garantizar el correcto funcionamiento de los propios sistemas.

    1. Determinar los posibles Centros de Gravedad del adversario.
    2. Determinar las formas de ayudar en la protección de los Centros de Gravedad propios.

    En el análisis del centro de gravedad propio, según Karama y otros (De Vergara & Trama, 2017, pág. 190), hay varias preguntas que deben ser respondidas:

> ¿Cuál es el estado final que desea el enemigo?, ¿qué tipo de actividades puede realizar el enemigo para alcanzar el estado final?, ¿qué requerimientos apoyan tal actividad del enemigo?, ¿qué actividades impiden alcanzar el propio estado final? En el análisis del centro de gravedad, se puede obtener la ventaja del análisis de los factores cibernéticos que consisten en las capacidades críticas propias y del enemigo, las misiones y las vulnerabilidades (Karaman & Catalkaya, 2016).

Las ciberoperaciones "no son una cuestión técnica, ni administrativa, ni logística; son un asunto de operaciones. Las defensivas dan protección a sistemas y procedimientos vitales para las operaciones propias, mientras que las ofensivas contribuyen concretamente a degradar las capacidades enemigas. En ambos casos, actúan sobre potenciales centros de

[66] La misión específica del Comandante es emanada de una orden superior o autoimpuesta bajo los límites de las atribuciones conferidas y la misión general recibida. Las operaciones en el ciberespacio son parte del ámbito de desarrollo de sus acciones y la inteligencia militar aporta la información necesaria para reducir la incertidumbre.

gravedad (Gomez Arriagada, 2013)" Gómez Arriaga en (De Vergara & Trama, 2017, pág. 191)

Los Centros de Fusión de Datos "son centros de gravedad en el espacio cibernético porque es por donde pasa la orientación. Los Centros de Fusión en el nivel operacional incluyen los nodos de mando y control y los nodos de procesamiento, explotación y difusión de la información de inteligencia, vigilancia y reconocimiento del enemigo. Destruyendo, degradando o neutralizando estos Centros de Fusión de Datos, se limitará la efectividad operacional del adversario para orientar y concentrar los efectos en tiempo y/o espacio (Bonner, 2014, pág. 108)" Bonner en (De Vergara & Trama, 2017, pág. 191).

g. Identificar las tareas a llevar a cabo.
   1. Determinar las tareas explícitas.
   2. Determinar las tareas implícitas.
   3. Determinar las tareas de los subordinados.
   4. En función de las tres anteriores determinar las tareas y objetivos de las operaciones cibernéticas.
h. Analizar la estructura de las fuerzas propias a fin de establecer la disponibilidad adecuada de medios para llevar a cabos las tareas.
i. Efectuar un análisis de riesgos.
   "Vinculando las vulnerabilidades con la intención y la capacidad del adversario, se pueden identificar las áreas de riesgo primario sobre las cuales enfocar los esfuerzos defensivos propios (Williams, 2011, pág. 13)".
j. Determinar el estado final desde el punto de vista cibernético.

Consideraciones particulares respecto de la formulación de proposiciones.

A la hora de estudiar los posibles modos de acción, cobrarán particular importancia las limitaciones impuestas por el nivel superior. Fundamentalmente en el Nivel Operacional, las opciones en estudio no deben perder de vista la siempre latente posibilidad de escalada del conflicto y su relación con los efectos y acciones de los otros componentes tradicionales. En este nivel, las Ciberoperaciones son una línea de operaciones más y no un fin en sí mismo.

Durante la confrontación, "el comandante operacional debe centrar su preocupación en el qué hacer y no en el cómo hacerlo. Qué estado final, qué efectos, qué objetivos, qué tareas, qué capacidades y todos ellos enlazados por el cuándo, el dónde y el quién" (De Vergara & Trama, 2017, pág. 197).

La oferta formativa especializada en planeamiento.

La oferta formativa en materia de metodologías de planeamiento, encuentra distintos enfoques en virtud del nivel de servicio de cada estructura.

La ya citada Especialización en Inteligencia Estratégica y Crimen Organizado de la Universidad de Buenos Aires (UBA), comprende el dictado de una densa e interesante materia titulada "Planeamiento". La misma contiene, en términos generales, la mayoría de los temas descriptos en este capítulo como necesarios para el dominio del proceso de toma de decisiones aplicable a la problemática del ciberespacio.

Algunos de los contenidos de la materia[69] son de interés particular para la formación de especialistas multidisciplinarios, a saber: el concepto de planificación y visión sistémica del proceso, la formulación del plan, la administración de personal, recursos de inteligencia y comunicacionales, las instrucciones de comunicaciones y enlaces con el decisor, la formulación de planes de alternativa, entre otros tópicos.

Si bien la Maestría en Ciberdefensa y Ciberseguridad de la UBA "se orienta al gerenciamiento (…) y no forma tecnólogos, busca que puedan interactuar y comprender a aquellos cuando dirijan y tomen decisiones ciber" (Rutz, 2020, pág. 63). La carencia de esta importante temática en la curricula de la misma, puede ser sin dudas salvada con la profundización del vínculo con la Especialización anteriormente mencionada de la misma casa de estudios y con la Escuela Superior de Guerra Conjunta.

Universidad de la Defensa Nacional, a través de la Escuela Superior de Guerra Conjunta, dicta una Especialización en Estrategia Operacional y Planeamiento Militar Conjunto (ESGC-Arg, Especialización en EO y PMC)**.** En el ámbito específicamente castrense, esta institución dicta cursos de planeamiento de nivel operacional de acceso restringido a personal militar. La especialización, profundiza la temática de la planificación de los Estados Mayores Específicos, Conjuntos y Conjuntos Combinados a niveles Estratégico Operacional y Estratégico Militar. Asimismo busca capacitar a los cursantes en el análisis de escenarios complejos en el ámbito de la Defensa.

Es de destacar que en las Fuerzas Armadas de casi todos los países, es común la impartición de cursos de planeamiento de nivel operacional en ámbitos académicos de similar nivel a la ESGC de nuestro país. Más aún, en el seno de alianzas multinacionales estables (como la OTAN o la Unión Europea), las instituciones académicas se encuentran coordinadas

[69] EXP-UBA: 28.284/2018. Anexo I – Contenidos mínimos – 4. Planeamiento. Disponible en http://www.uba.ar/archivos_uba/2018-06-27_RES%20CS%2018-00767.pdf

y los cursos que imparten son homologados entre sí. Esto es posible por compartir una doctrina común y la frecuente conformación de fuerzas multinacionales.

En el entorno de la OTAN, es particularmente interesante el enfoque del NATO Crisis Response Planning (ISSMI, 2015, pág. 5) el cual consiste en iniciar y desarrollar planes en respuesta a una crisis actual o en desarrollo. Este proceso de planeamiento se desarrolla en línea con las teorías y doctrinas occidentales detalladas en el capítulo II del presente trabajo. El abordaje omnicomprensivo de la problemática y el empleo de todos los factores de poder son una nota distintiva de este enfoque, al cual se añade la complejidad de amalgamar fuerzas de distintos países en el marco de la alianza.

Capítulo V. El adiestramiento de equipos multidisciplinarios formados.

Los equipos debidamente formados, deben adiestrarse continuamente para mantener e incrementar sus capacidades y reforzar la calidad de su producto en base a la sinergia resultante de su interacción eficiente.

Una forma de adiestramiento eficaz la constituyen los llamados ejercicios. Esta modalidad es de uso muy antiguo y difundido en esferas militares en todos los niveles de conducción. Básicamente consiste en el planteo de una situación hipotética que requiere de la aplicación de las habilidades alcanzadas de los participantes para la resolución de un problema concreto.

Los expertos convocados deben participar regularmente de ejercitaciones donde se planteen escenarios que impliquen el desarrollo de opciones de respuesta en el ámbito de la Ciberdefensa. Es realmente útil y necesario, la programación y ejecución de ejercicios en los distintos niveles de conducción, los cuales deben ser seguir una estructura lógica jerárquica definiendo objetivos y efectos hacia los niveles inferiores. Incluso deberían ser coordinados con los ejercicios de nivel técnico impuestos a las entidades de ejecución con la finalidad de verificar la factibilidad de implementación de sus resoluciones y/o evidenciar la necesidad de desarrollo de capacidades técnicas concretas.

Los ejercicios (REF-00-06, 2019, págs. I-1) como tal, requieren conocimientos previos a su ejecución, tanto para los participantes, como para quien deba desempeñarse como director de los mismos. Esta técnica didáctica está orientada a lograr que los participantes apliquen los procedimientos y técnicas particulares en el marco de una situación planteada. Ello exige que el personal que participa de un ejercicio haya sido previamente instruido y evaluado en el "saber hacer" de estos temas. Asimismo, el director del ejercicio deberá tener conocimientos profundos sobre las particularidades de cada una de las operaciones que se ejecutarán. Su conocimiento y creatividad permitirán generar el contexto adecuado, para producir situaciones durante el desarrollo del ejercicio lo más parecidas a las que se sucederán en la realidad, provocando en los participantes una motivación que posibilitará diferenciar esta técnica de una simple clase de instrucción.

Los ejercicios podrán ser desarrollados (REF-00-06, 2019) como:

1. Ejercicios de explicación: en términos generales, la explicación se llevará a cabo en forma similar a una clase, en la que el director o sus auxiliares, basados en la actividad prevista en el ejercicio, desarrollarán brevemente los aspectos doctrinarios del planeamiento, o la ejecución de la operación planteada. Para alcanzar su mayor rendimiento, será necesario permitir a los participantes preguntar e intercambiar opiniones, pudiendo ordenárseles la ejecución de determinadas tareas en apoyo al planeamiento en desarrollo.
2. Ejercicios de instrucción: su desarrollo busca iniciar a los participantes en la práctica de las ciberoperaciones. Las actividades que se realicen en forma incorrecta se repetirán tantas veces como sea necesario, con el objeto de perfeccionar la técnica de aplicación de la doctrina, tanto por parte del conductor como por parte del ejecutor.
3. Ejercicios de conducción: se utilizarán para consolidar en los participantes los conocimientos adquiridos durante el desarrollo de los ejercicios de instrucción, y comprobar el nivel alcanzado. A diferencia de los de instrucción, no se deberán interrumpir durante su desarrollo. Las actividades que se fiscalicen se centrarán en el jefe del elemento de trabajo y la eficiencia del conjunto.

Los ejercicios de instrucción y conducción pueden ser elaborados y ejecutados considerando uno o dos bandos participantes a partidos contrapuestos. Esto dependerá de la finalidad perseguida y del grado de libertad de acción concedido a los grupos participantes.

Juegos de Guerra.

En el nivel técnico es importante realizar ejercicios bajo la modalidad de Juegos de Guerra. Corletti (2017, pág. 185) propone la ejecución de los mismos cumpliendo los pasos que establece la doctrina militar orientándose a acciones de ciberataques.

Si bien lo explicado precedentemente se ajusta al nivel técnico, su planificación y ejecución se potenciaría con el desarrollo de ejercicios paralelos de Nivel Operacional / Estratégico. Las situaciones planteadas, las acciones y contra reacciones ejecutadas requerirán de la participación de niveles de decisión superiores [74] (por las consecuencias multidimensionales que desencadenan). Es allí donde los equipos multidisciplinarios en función de asesoramiento y asistencia pueden poner a prueba sus capacidades y sacar valiosa experiencia de cada situación en particular y del método de toma de decisiones en general.

Ejercicios de planeamiento.

[74] Para que un Juego de Guerra pueda ser llevado adelante en forma eficaz es condición indispensable que esté involucrado (y lo dirija) el más alto nivel de la organización (Corletti Estrada, 2017, pág. 185).

Dentro de la temática específica de este trabajo, se considera a la ejecución de ejercicios de planeamiento, como la herramienta más sólida para entrenar a los equipos multidisciplinarios en la metodología de toma de decisiones en los distintos niveles de conducción. Paralelamente, es útil extraer conclusiones y experiencias no sólo metodológicas, sino también de orden práctico en la determinación de objetivos, el análisis de situación y los modos de acción. Como consecuencia ulterior, fundamentalmente en el nivel estratégico, es normal que surjan requerimientos relacionados con el desarrollo de capacidades para el área de Ciberdefensa y/o alertas de debilidades detectadas en partes del sistema que exigen su atención.

Los expertos deben ser capaces de reconocerse a sí mismos en las etapas de asesoramiento (antes de la resolución del jefe de equipo o comandante) y asistencia del planeamiento (después de la resolución) y su particular incidencia en cada paso del proceso. Reafirmando el carácter multidimensional del ciberespacio, la inclusión de diversos especialistas es fundamental para una mejor comprensión de la situación y para elaborar eficientes modos de acción como alternativas de solución a los problemas planteados.

Es evidente que los resultados generados por equipos no preparados en la metodología y reunidos espontáneamente serán diferentes, en calidad, a aquellos capaces de lograr sinergia en el proceso producto de un grado mayor de involucramiento de sus miembros.

La injerencia de los especialistas en todo el proceso de toma de decisiones, requerirá del conocimiento y experiencia de su formación de base, la comprensión de las particularidades de las amenazas híbridas, el ciberespacio y las habilidades adquiridas para el análisis de inteligencia.

La intervención de los expertos sectoriales tendrá puntos de particular relevancia en:

1. La identificación y definición de problemas.

   Corresponde más al jefe del elemento de trabajo, sin embargo, cada experto expone las particularidades de su área que coadyuvan a la comprensión total del problema.

2. La reunión, organización y procesamiento de información.

   Es común a todo el equipo. Cada integrante aporta lo concerniente a su área de incumbencia. Es fundamental el método común para la organización, registro y diseminación de la información de modo tal que sea asequible y comprensible para todos.

3. La apreciación de situaciones.

   El carácter multidimensional de los escenarios actuales hace indispensable el involucramiento de los expertos sectoriales en la etapa de análisis de la situación. Por más formado que sea la cabeza de la organización, no sería posible abarcar con detalle y

profundidad todos los aspectos a ser tenidos en cuenta. Del mismo modo la información debe ser resumida en su esencia siempre a la luz de la misión que guía el planeamiento.

4. La formulación de proposiciones.

   La participación de los especialistas será esencial para la determinación de los centros de gravedad y la identificación de las debilidades y fortalezas de los sistemas considerados. Simultáneamente, cada participante observará, desde su óptica particular, las consecuencias potenciales de cada modo de acción concebido en los subsistemas específicos y podrá advertir al conjunto sobre ello, e incluso aportar ideas para desarrollar alternativas no vistas inicialmente.

5. La preparación de planes y órdenes.

   En este paso, los especialistas aportan las particularidades que afectan a su área y preparan documentos que luego servirán para el planeamiento de niveles inferiores.

Como resultado de esta gimnasia en la metodología de toma de decisiones, surgirán consideraciones que motoricen políticas, estrategias y acciones concretas en el ámbito de la Ciberseguridad y la Ciberdefensa.

Es necesario remarcar el carácter derivado del planeamiento, encuadrado siempre en la necesidad de dar opciones de respuesta, desde el ámbito de las ciberoperaciones, a una situación compleja multidimensional superior.

No obstante, las características de la Estrategia Nacional de Ciberseguridad, acotadas a una visión restrictivamente defensiva con énfasis en medidas más propias de la seguridad informática, impulsan en cierta manera a las entidades involucradas a plantear *per se* escenarios más complejos que requieran de la participación de todo el espectro del poder nacional.

Algunos ejemplos prácticos pueden surgir de modelar y desarrollar ejercicios que consideren amenazas globales / regionales con foco en problemáticas tales como la implementación de tecnología 5G, ataques a infraestructura crítica de salud (en el marco del desarrollo de pandemias), afectación de sistemas energéticos o de potabilización y distribución de agua, e incluso la injerencia ya verificada en otros países en procesos electorales.

En cuanto a la formación específica de metodologías para la toma de decisiones, la oferta académica se centra con mayor preponderancia en el personal de origen militar. Se considera importante explorar las ventajas que comprendería incluir la participación de personal civil especialmente seleccionado, en cursos de planeamiento de nivel operacional y

fundamentalmente de nivel estratégico. Seguido de ello, lógica y consecuentemente, su involucramiento activo en el desarrollo de ejercicios que consideren líneas estratégicas u operacionales de Ciberdefensa.

Naturalmente el nivel Estratégico Militar y Operacional se desarrollan frecuentemente ejercicios de planeamiento propios de su nivel con una metodología particular. Los mismos se aprenden en instituciones académicas militares y se desarrollan ampliamente en los Comandos de cada nivel.

En el ámbito local, ejercicios de planeamiento de Nivel Operacional se realizan en la Escuela Superior de Guerra Conjunta, donde son planteados diversos escenarios complejos que naturalmente requieren de una intervención del componente militar para su resolución.

En el caso específico de la OTAN, el Centro de Excelencia de la Defensa Cibernética Cooperativa (CCDCOE), organiza y contribuye al desarrollo de ejercicios de defensa cibernética dirigidos a expertos técnicos, personal militar y responsables de toma de decisiones en los países miembros y dentro de la propia organización. Destacan dos ejercicios (por el nivel y el planeamiento):

1. TRIDENT JAGUAR (NATO-TJE). El ejercicio se focalizó en la planificación y realización de operaciones de respuesta a crisis en operaciones conjuntas de la OTAN. El ejercicio de nivel operacional obligó a sus participantes a operar y planificar en el marco de un escenario ficticio con aportes e implicaciones a nivel estratégico, operacional y táctico. El ejercicio simuló un entorno en el que el equipo debía considerar una variedad de inquietudes y nuevos elementos de juicio mientras trabaja para encontrar una solución a sus dilemas operativos.
2. FINAL PLANNING CONFERENCE HELD FOR NATO CYBER COALITION (NATO-Shape, 2018). Representantes de países miembros y socios de la OTAN y de la Unión Europea (UE) se reunieron en Praga para preparar el escenario de un ejercicio que reflejara las tendencias y amenazas contemporáneas en seguridad cibernética. Es uno de los ejercicios de seguridad cibernética más grandes e importantes del mundo que convoca a alrededor de 900 expertos de 27 países.

Capítulo VI. Conclusiones

La génesis y el desarrollo de los conflictos modernos, signados por la característica multifacética de sus procedimientos y actores, exponen a cualquier Estado a una situación de permanente incertidumbre y volatilidad. El llamado 5to dominio, es el escenario presente y futuro que, en forma transversal, y por sobre los otros dominios tradicionales en los períodos de aparente paz o estabilidad, adquiere especial relevancia en épocas de conflicto. Este espacio de acciones no se activa con el inicio del conflicto, a diferencia de los dominios terrestre, aéreo y marítimo, más bien es omnipresente en lo temporal como lo es el dominio espacial.

Esa transversalidad penetrante del 5to dominio, combinada con la característica híbrida de los conflictos modernos, imponen sin duda un abordaje mucho más amplio en el empleo de medios, la seguridad de infraestructuras críticas esenciales y la concepción de opciones factibles a ser presentadas al decisor.

Las opciones de respuesta no pueden ser únicamente militares. De hecho, las amenazas no lo son.

Las características de las ciberoperaciones balancean en algún modo la asimetría de facto que se evidencia en los otros dominios, pero esta no es una sentencia absoluta. Quienes tomen ventaja del cambio de mentalidad y se acoplen a la velocidad de la evolución tecnológica, acrecentarán la brecha respecto de aquellos con una visión puramente reactiva. Consecuentemente, estos últimos desgastarán su tiempo en conceptualizaciones etéreas que no producen ni políticas, ni estrategias de peso y mucho menos, organismos debidamente equipados, con recursos humanos de alta calidad y presupuestos acordes para enfrentar los desafíos en ciernes.

Quienes tienen la responsabilidad de producir y concretar estas acciones deben necesariamente ser formados y entrenados constantemente para servir mejor a las instituciones que los convocan.

Es deber del Estado identificar dónde están esos profesionales referentes de cada sector, motivarlos a desarrollar sus capacidades al servicio de la Nación, trazar un itinerario formativo de calidad en el país y en el extranjero, y adiestrarlos constantemente.

La identificación requiere focalizarse en individuos con conocimientos de gestión en las áreas prioritarias. No se puede reducir el espectro a nivel meramente técnico por más excelencia que demuestren los candidatos en la materia. Se precisan expertos en la gestión del

área de salud (sean o no médicos de profesión); personal con experiencia sólida en las distintas subáreas de generación de energía; abogados especialistas en ciberdelitos y derecho internacional; licenciados en relaciones internacionales en capacidad de interpretar la evolución de los acontecimientos mundiales y vincular los hechos con las acciones en el ciberespacio; personal de las Fuerzas Armadas y de Seguridad que aporten opciones de respuesta mixtas o puramente militares perfectamente coherentes con las otras líneas estratégicas que se tracen; etc. No obstante ello, este es sólo el primer paso.

Como puede observarse, existe una variada oferta formativa en ámbito nacional e internacional en relación a la Ciberseguridad y la Ciberdefensa. Cada institución se centra en objetivos distintos, los cuales plasman en sus planes curriculares y perfiles de egreso. En general, el enfoque técnico prevalece en la mayoría de ellas. La inclusión de los tópicos del área de entorno general (Capítulo IV – Sección I), no siempre se verifica en los planes de estudio. Paralelamente, las llamadas diplomaturas suelen circunscribirse al ámbito de la Seguridad Informática.

En el contexto del presente trabajo, el abordaje multidisciplinario de la Ciberseguridad y la Ciberdefensa, requiere de contenidos que exceden lo estrictamente técnico y la capacidad de gestión. Una posible explicación a la orientación mayormente técnica de la oferta formativa, podría deberse a la asimilación sintáctica de las palabras Ciberseguridad y Ciberdefensa. Las mismas parecieran sesgar el concepto reduciéndolo a una actitud defensiva y apenas reactiva (sólo para alcanzar la restitución de los sistemas o infraestructuras afectadas a partir de un mínimo nivel de resiliencia). Las posibilidades ofensivas concretas (al menos con carácter disuasivo) parecieran no estar contempladas. A nivel nacional, esto supondría un grave error y restringe el concepto a un mero esfuerzo coordinado de actividades y políticas de seguridad informática expectantes de la voluntad agresora externa.

Respecto de la capacitación en el área de inteligencia, se destaca la habilidad de anticipación estratégica y la destreza para la identificación de los sutiles hilos que conectan actores visibles y encubiertos, sus procedimientos e intencionalidad aparente y real.

Los especialistas que se convoquen para la conformación de equipos multidisciplinarios deben estar capacitados básicamente para analizar por sí mismos las fuentes de información, utilizar los medios de obtención a su alcance, generar pedidos de información a agencias especializadas, conocer el proceso de inteligencia y formar parte del mismo en su ámbito de trabajo. Es imprescindible una visión global del entorno, las amenazas reales y potenciales y la capacidad de adoptar las contramedidas adecuadas para enfrentar las acciones de inteligencia que estas generen (siempre bajo la tutela de las actividades permitidas

por la legislación vigente). Habilidades como el análisis prospectivo, la prognosis y el pensamiento complejo, son de gran utilidad no sólo para maximizar los resultados, sino también para tornar el proceso de eficaz a eficiente.

En particular la Ciberinteligencia está orientada a la actividad propia dentro del Ciberespacio, recordando la dualidad físico-virtual de su esencia. Por otro lado, no se debe confundir la habilidad estrictamente técnica de búsqueda y obtención de información con el proceso completo que exige este nivel de capacitación.

Respecto de la oferta académica analizada, se destaca un amplio interés nacional en la formación de analistas en Inteligencia Estratégica tanto en ámbito público como privado, civil como militar. No obstante, instituciones extranjeras ofrecen adicionalmente capacitación direccionada a la Ciberinteligencia, aspecto que no es especialmente considerado en el entorno local.

La metodología de toma de decisión o planeamiento, es un catalizador de las capacidades adquiridas. Aquí encuentran aplicación práctica en forma integral. El planteamiento sobre escenarios complejos pone a prueba las destrezas para identificar amenazas, debilidades y fortalezas; identificar capacidades faltantes y sobre todo pone en práctica el trabajo heterogéneo de los especialistas que, debidamente liderados, pueden ofrecer al decisor las mejores opciones que coadyuven a la solución de problemas.

La oferta académica en esta materia se vincula más con el área castrense. Sin embargo, no está abierta en nuestro país a la integración de personal civil en sus claustros. Otros países (fundamentalmente europeos) sí contemplan esta posibilidad y expanden la capacidad de omnicomprensión del problema. Obviamente, esta apertura está en línea con el enfoque multiespectral y multidimensional del conflicto que sostienen las doctrinas occidentales modernas.

Si bien se ha identificado el contenido de la materia “planeamiento” en la especialización de Inteligencia Estratégica de la Escuela Nacional de Inteligencia (ENI), esta no es suficientemente densa para el fin perseguido. Una opción obvia, sería generar una apertura a especialistas civiles en unidades académicas militares como la Escuela Superior de Guerra Conjunta. La otra opción sería generar una capacitación particular en una entidad superior como por ejemplo la Facultad de la Defensa de la Universidad de la Defensa[78].

[78] En particular queda planteada la posibilidad de estudios ulteriores para el diseño e implementación de una especialización en “planeamiento”. La misma debería orientarse a personal civil y militar que deba capacitarse para desempeñar funciones en ámbitos de asesoramiento y asistencia en el nivel estratégico. La estructura curricular debería contener especificamente la metodología de toma de decisiones del nivel estratégico nacional y militar y en forma genérica del nivel operacional.

Este itinerario formativo y posterior esfuerzo de adiestramiento continuo debe necesariamente anclarse en un presupuesto acorde y de largo plazo. Esfuerzos aislados o sujetos a cambios de visión ideológica y/o funcional, romperían la cadena de generación de recursos humanos de calidad. Es necesario aquí insistir en la idea de analizar la inclusión de esta propuesta como política de Estado. Una vez más el trabajo de campo de Rutz enfatiza la dirección propuesta: "[…] En la orientación de la formación, es necesario trabajar sobre un plan de acción o propuesta para presentar a la CONEAU, de modo que, como política universitaria, las universidades promuevan sumar esta disciplina en sus carreras de posgrado" (Rutz, 2020, pág. 46).

Entendida esta capacitación integradora y ascendente, se lograría como efecto secundario una jerarquización de los expertos seleccionados y un incentivo para futuros aspirantes a estas áreas de dirigencia.

Formado el personal, servirían con mayor potencialidad en organismos nacionales dentro de la Jefatura de Gabinete de Ministros (Secretaría de Innovación Pública / Dirección Nacional de Ciberseguridad) o en la Secretaría de Asuntos Estratégicos de la Nación.

Durante épocas de crisis, cuando se convoque a los llamados Comité de Crisis, los expertos podrán ser reunidos y rápidamente encarar la tarea asignada con conocimiento personal previo y una metodología de trabajo común. Por derivación de este concepto, son igualmente útiles a este fin, aquellos expertos que desempeñen tareas en otros organismos del Estado (Secretarías y Ministerios) y aquellos que trabajen en entes regulatorios y empresas (públicas y privadas) relacionadas a servicios esenciales vinculados a infraestructuras críticas.

Posteriormente, en épocas de escalada del conflicto, pueden ser asignados temporalmente para asesorar al Comité de Defensa Nacional e incluso ser convocados *ad hoc* al Comando Conjunto de Ciberdefensa[79]. La diferencia aquí, estará en la capacidad de asimilar rápidamente expertos con formación básica común en los campos de interés del área castrense y el irremplazable conocimiento personal previo.

Para concretar este trabajo coordinado, es necesario un proceso de adiestramiento continuo. El desarrollo de ejercicios en distintos niveles de conducción es sin dudas la herramienta más adecuada. Los mismos deben integrar personal civil, agentes de seguridad y militares, e incluso fomentar el desarrollo de ejercicios combinados con otros países aliados que potencien las fortalezas de nuestro sistema defensivo.

[79] Debe tenerse en cuenta la catalogación del problema enfrentado (ámbito de Ciberseguridad o de Ciberdefensa) y la pertinencia de las aptitudes de cada especialista según cada ámbito en consonancia a la legislación vigente.

La formación de estos especialistas requiere una política de estado firme en el tiempo. No se puede pretender dejar la formación de los especialistas, a su simple iniciativa y recursos. Las organizaciones estatales de más alto nivel los necesitan y es el Estado quien debe permitir y dirigir la capacitación. Una opción a ser considerada es la creación de un organismo de formación y perfeccionamiento de carácter federal, que vinculando y articulando casas de estudio de excelencia, permita el desarrollo de instancias de capacitación, externas e internas, orientadas a una formación coherente y completa.

Tal entidad debería contemplar el desarrollo completo de las tres funciones sustantivas de la educación (docencia, investigación y extensión). Enmarcado bajo esta premisa, el desafío se centrará en la articulación de estas tres esferas. La actividad docente puede tener su núcleo primario dentro del organismo, pero a su vez puede articular capacitación paralela con otros de los institutos identificados. La generación del conocimiento (propia del área de investigación) debería ser prioritaria dentro del mismo, dado que su producto concreto evidenciaría la excelencia del organismo. Las actividades de extensión académica a su vez, como vector de transposición del conocimiento, podrían incluir el desarrollo de los ejercicios para adiestramiento de los equipos multidisciplinarios tanto a nivel nacional como internacional.

Dada las características de las áreas de formación citadas en el Capítulo IV del presente trabajo, y el grado de *expertise* alcanzado por instituciones de las Fuerzas Armadas, bien podría ser este el ámbito de desarrollo de tal entidad abierta a personal civil y militar. Se descarta la inmediata y necesaria vinculación con el Instituto de Inteligencia de las Fuerzas Armadas, la Escuela Nacional de Inteligencia, la Escuela Superior de Guerra Conjunta y de la Universidad de la Defensa, como así también de las casas de altos estudios universitarios con carreras orientadas a la Ciberdefensa y la Ciberseguridad.

Un hito trascendente en este sentido, lo marca la reciente creación del Instituto de Ciberdefensa de las Fuerzas Armadas[80]. Esta novel entidad busca estandarizar la formación del personal que se desempeñará en las Direcciones de Ciberdefensa de cada Fuerza y en el Comando Conjunto de Ciberdefensa. Si bien su orientación inicial es de carácter técnico-operativo y restringida al personal militar, sería interesante a futuro aprovechar su estructura para desarrollar las propuestas de formación multidisciplinar aquí expuestas, extensibles a civiles y militares con un enfoque de gerenciamiento. El instituto podría ejercer un rol de

[80] https://www.fuerzas-armadas.mil.ar/Noticia-2021-03-31-ciberdefensa-instituto.aspx

articulación con las entidades operativas y académicas antes mencionadas a efectos de concretar la formación de los especialistas sin necesidad de duplicar contenidos ya existentes.

A modo de ejemplo, cabe destacar en el plano internacional la vigencia y trayectoria del ya mencionado Centro de Excelencia de la Defensa Cibernética Cooperativa de la OTAN en Estonia (CCDCOE).

Como ejemplo relevante de la esfera de investigación, el área de leyes es particularmente reconocida por el extenso desarrollo de la problemática legal a nivel internacional, el cual se concreta en la elaboración y permanente actualización del documento mundialmente conocido como *Tallin Manual*[82].

A su vez, el área de *training* es realmente amplia, ofreciendo actividades muy relacionadas con la perspectiva omnicomprensiva de los conflictos modernos en el ámbito del ciberespacio.

Figura 12: Training Portfolio (CCDCOE)

Los Estados Unidos de América presentan un modelo interesante y posible de ser aplicado. Tanto el Department of Homeland Security (DHS) como la National Security Agency (NSA) designan instituciones con el carácter de "Center for Academic Excellence" (CAE)[83]. La misión del programa de los Centros Nacionales de Excelencia Académica en

[82] Se presenta como la guía más completa para asesores de políticas y expertos legales sobre cómo se aplica el derecho internacional existente a las operaciones cibernéticas.
[83] The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program is managed by the National Cryptologic School at the National Security Agency. Federal Partners include the Cybersecurity and

Ciberseguridad (NCAE) es crear y administrar un programa educativo de ciberseguridad colaborativo con colegios comunitarios, colegios y universidades.

Las unidades académicas seleccionadas que logran esa categoría tienen programas asociados a las necesidades de capacidades de Ciberseguridad enunciadas por el DHS y la NSA. Existen tres áreas de interés donde se enfocan los programas: Cyber Defense Education - Cyber Research - Cyber Operations. De este modo, se ordena la capacitación y se incentiva a entidades académicas a participar de los programas de capacitación en áreas previamente identificadas como necesarias.

Para la evolución de la propuesta de creación o designación de un organismo local de referencia con el objetivo de concretar el itinerario formativo de equipos multidisciplinarios desarrollado en este trabajo, queda planteada la posibilidad de ulteriores estudios que aborden la problemática de los programas de selección, formación y adiestramiento de los especialistas; como así también la vinculación y articulación con las entidades receptoras de los recursos humanos formados (públicas o privadas) y el ámbito académico periférico, a fin de optimizar los esfuerzos de capacitación.

Finalmente, se propone profundizar esta temática con la intención de incorporar esta idea en el desarrollo de la Política Nacional de Ciberseguridad y como un punto más dentro de la Estrategias Nacional de Ciberseguridad. De allí en más, con cimientos firmes en el consenso, podrían darse los pasos necesarios para concretar la presente propuesta: identificar los expertos más adecuados, desarrollar y dirigir el itinerario formativo y adiestrarlos continuamente.

La resultante, será una expresión concreta del concepto de SINERGIA!.

Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST)/National Initiative on Cybersecurity Education (NICE), the National Science Foundation (NSF), the Department of Defense Office of the Chief Information Officer (DoD-CIO), and US Cyber Command (CYBERCOM).
https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

Trabajos citados

Aguirre, J. (2015). *Sciencedirect.* Obtenido de Inteligencia Estratégica: un sistema para gestionar la innovación: https://www.sciencedirect.com/science/article/pii/S0123592314001594

Bonifacio, A. (2009). *Estado, Políticas y Gestión Pública en tiempos del bicentenario.* Bs As, Argentina: Fundación Unión.

CAECE. (s.f.). *Diplomatura en Ciberseguridad*. Obtenido de http://www.ucaece.edu.ar/agenda/diplomatura-en-ciberseguridad/

Carpenter, R., & Mendoza, M. (2017). *Strategy + Business.* Obtenido de https://www.strategy-business.com/blog/How-to-Unlock-the-Full-Potential-of-Diverse-Teams

CCDCOE. (s.f.). Obtenido de https://ccdcoe.org/

Clark Richard & Knake Robert. (2012). *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins.

Clark Richard & Knake Robert. (2019). *Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* Hardcover.

De Vergara, E., & Trama, G. (2017). *Operaciones militares cibernéticas.* Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Decreto 577/17. (2017). *Comité de Ciberseguridad*.

Decreto-480. (11 de Julio de 2019). *Comité de Ciberseguridad.* Obtenido de Boletín Oficial de la República Argentina: https://www.boletinoficial.gob.ar/detalleAviso/primera/211277/20190712

Def, M. (2019). Decreto 1380/19 - Anexo 4 - Política de Ciberdefensa.

DPDN. (2014). Directiva Política de Defensa Nacional.

DPDN. (2018). Directiva de Política de Defensa Nacional.

Eissa, S. (2010). Guerra híbrida. ¿Una nueva forma de pensar la guerra del Siglo XXI? *Revista Militar, 781*.

Ejército, E. S. (1991). *Bases para el pensamiento estratégico.* Bs As: ESG "Tte Grl Luis María Campos".

Enzensberger, H. (1994). *Perspectivas de la guerra civil.* Barcelona: Anagrama.

ESGC-Arg. (s.f.). *Especialización en Estrategia Operacional y Planeamiento Militar Conjunto*. Obtenido de https://www.esgcffaa.edu.ar/esp/especializacion.php

ESGC-Arg. (s.f.). *Programa Avanzado en Introducción a la Ciberdefensa y la Ciberseguridad*. Obtenido de https://www.esgcffaa.edu.ar/esp/actividades-detalle.php?id=164

ESG-Col. (s.f.). *Maestría en Ciberseguridad y Ciberdefensa*. (E. N. Colombia, Editor) Obtenido de https://esdegue.edu.co/es/maestria-en-ciberseguridad-y-ciberdefensa

FIE. (s.f.). *Maestría en Ciberdefensa*. Obtenido de http://200.69.236.66/fie2020/index.php/ciberdefensa/

Flores, R. (2015). Una visisón de las amenazas ciberespaciales y la defensa. *CARI / ISIAE - Boletín 61*.

Galeira Vazquez, R. (2017). *Scielo.* Obtenido de http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0376-78922017000400221

Gerasimov, V. (2016). *El valor de la ciencia está en la capacidad de prever lo que sucederá en el futuro* (Vols. Tomo 71 - Nro 2). Military Review.

Hoffman, F. (2009). *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict.* Institute for National Strategic StudiesNational Defense University.

IIFA. (s.f.). *Especialización en Análisis de Inteligencia Estratégica*. Obtenido de http://www.fuerzas-armadas.mil.ar/iifa/aei.html

INAP. (s.f.). *Curso de Posgrado en Inteligencia Estratégica*. Obtenido de https://capacitacion.inap.gob.ar/beca/curso-de-posgrado-en-inteligencia-estrategica/
ISSMI, I. S. (2015). *Operations Planning Course, Student Handbook.* Roma: ISSMI.
Koenig. (s.f.). *Certified Threat Intelligence Analyst (CTIA) Certification Course*. Obtenido de https://www.koenig-solutions.com/certified-threat-intelligence-analyst?keyword=&device=c&gclid=CjwKCAjwk6P2BRAIEiwAfVJ0rDMVk_XS6KQ1l6yq_E0CdoPGNZ68gF7d3KB4QDp-ppQ4En7ff_NwKhoCNVsQAvD_BwE
Liang, Q., & Wang, X. (1999). *Unrestricted Warfare – Thoughts on War and Strategy in a Global Era.* Beijing: La Casa de Publicaciones de Arte y Literatura del EPL.
LISA-Institute. (s.f.). *Curso de Experto en OSINT*. Obtenido de https://www.lisainstitute.com/collections/cursos/products/curso-experto-osint-tecnicas-de-investigacion-online
LISA-Institute. (s.f.). *Curso-Certificado de Experto en Ciberinteligencia*. Obtenido de https://www.lisainstitute.com/collections/cursos/products/curso-experto-en-ciberinteligencia
Martín, L. (2019). *Atalayar*. Obtenido de La importancia de la inteligencia para combatir la guerra híbrida: https://atalayar.com/content/la-importancia-de-la-inteligencia-para-combatir-la-guerra-h%C3%ADbrida
Mattis, J., & Frank, H. (Noviembre de 2005). *U.S. Naval Institute.* Obtenido de https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars
Modernización, S. d. (2019). Resol 829/19 - Anexo I - Estr Nac Ciberseguridad. Argentina.
NATO. (8 de Agosto de 2019). *NATO's response to hybrid threats*. Obtenido de https://www.nato.int/: https://www.nato.int/cps/en/natohq/topics_156338.htm
NATO. (s.f.). *NATO Multimedia library*. Obtenido de NATO Comprehensive Approach: http://www.natolibguides.info/comprehensiveapproach
NATO-Shape. (2018). *FINAL PLANNING CONFERENCE HELD FOR NATO CYBER COALITION*. Obtenido de https://shape.nato.int/news-archive/2018/final-planning-conference-held-for-nato-cyber-coalition-2018
NATO-TJE. (s.f.). *Trident Jaguar Exercises*. Obtenido de https://jwc.nato.int/articles/jwc-concludes-trident-jaguar-series-exercises
OAC. (s.f.). *Observatorio Argentino del Ciberespacio*. Obtenido de https://www.esgcffaa.edu.ar/esp/oac-boletines.php
PC-10-04. (2018). *Planeamiento para la Acción Militar Conjunta - Nivel Estratégico Militar.* Bs As: EMCOFFAA.
PC-20-01. (2015). *Planeamiento de Nivel Operacional.* BsAs: EMCOFFAA.
PC-20-09. (2018). *Procedimientos para el Planeamiento Estratégico Militar.* Bs As: EMCOFFAA.
Perkins, D. G. (Grl Perkins, David G.,1er Trimestre 2018). La batalla multidominio. Impulsando el cambio para ganar en el futuro. *Miltary Review*.
PTE, A. . (s.f.). Decreto 480/19. *Ampliación del Comité de Ciberseguridad*.
REF-00-06. (2019). *Manual de Ejercicios.* Bs As: Ejército Argentino.
Resol 1523/19. (2019). Infraestructuras críticas. Argentina.
ROB-00-01. (2015). *Conducción para las Fuerzas Terrestres.* Bs As: Ejército Argentino.
ROD-71-01-I. (1998). *Organización y funcionamiento de los Estados Mayores.* Bs As: Ejército Arhgentino.
SANS. (s.f.). *FOR578: Cyber Threat Intelligence*. Obtenido de https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/

TECH, T. (s.f.). *CYBER SECURITY ENGINEERING (BSC)*. Obtenido de https://taltech.ee/en/cyber-bsc?utm_source=studyportals&utm_medium=cpc&utm_campaign=admission
Tepedino, S. (12 de Septiembre de 2017). *Espacio estratégico.* Obtenido de http://espacioestrategico.blogspot.com/2017/09/guerra-irrestricta-guerra-civil_12.html
Tepedino, S. (2019). *La Doctrina Gerasimov. ¿Un salto cuántico en la teoría militar rusa?* Obtenido de Espacio Estratégico: http://espacioestrategico.blogspot.com/2019/03/la-doctrina-geramismov.html
UBA. (s.f.). *Especialización en Inteligencia Estratégica y Crimen Organizado*. Obtenido de http://www.uba.ar/posgrados/noticia.php?id=283
UBA. (s.f.). *Posgrado FCE*. Obtenido de https://posgrado.economicas.uba.ar/servicios-y-tic/s-tic-ciberdefensa-y-ciberseguridad/
UCA. (s.f.). *Curso de Posgrado en Inteligencia Estratégica*. Obtenido de http://uca.edu.ar/es/eventos/curso-de-posgrado:-inteligencia-estrategica
UCA. (s.f.). *Curso de Posgrado: Inteligencia Estratégica*. Obtenido de http://uca.edu.ar/es/eventos/curso-de-posgrado:-inteligencia-estrategica
UCEMA. (s.f.). *Diplomatura en Gestión y Estartegia en Ciberseguridad*. Obtenido de https://ucema.edu.ar/educacion-ejecutiva/ciberseguridad
UFV. (s.f.). *Maestría en Ciberinteligencia*. Obtenido de https://www.campusciberseguridad.com/masters/master-en-ciberinteligencia
UM. (s.f.). *Magíster de Ingeniería en Seguridad de la Información*. Obtenido de https://www.umayor.cl/postgrados/programas/ingenieria-seguridad-informacion/
UNLP. (s.f.). *Maestría en Inteligencia Estratégica Nacional*. Obtenido de https://posgrados.acaula.com.ar/ciencias-politicas/maestria-en-inteligencia-estrategica-nacional/12410/cp
UP. (s.f.). *Diplomatura en Ciberseguridad*. Obtenido de https://www.palermo.edu/carreras/diplomatura-en-ciberseguridad/index.html
US Joint Chiefs of Staff. (2013). *Joint reporting structure for cyberspace operations status.*
US Joint Chiefs of Staff. (2018). *JP 3-0 (Joint Operations).*
US JP 3-12. (2018). *Cyberspace Operations.* US Joint Publication.
van Creveld, M. (1991). *La transformación de la guerra.* Bs As: José Luis Uceda.