a

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

## CARRERA DE ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRÍMEN ORGANIZADO

## Argentina, su estado actual y sugerencias para afrontar Guerras de Quinta Generación (G5G)

**AUTOR: Pablo Alberto Luchetti**

**DOCENTE DEL TALLER: Mag José Pibernus**

Mayo, 2021

## Resumen

El problema a encarar son qué medidas se deben tomar ante una Guerra de Quinta (G5G) en tierra, en el aire, en el ciberespacio, en donde su componente “no cinético” es alto, como ser sus componentes en la inteligencia artificial (IA), cibernética y neurociencias en la Argentina. Es importante empezar a conocer las propiedades y características del cerebro y la mente humana para entender de raíz una G5G.

Ante todo, es necesario demarcar el problema de los peligros de la era cibernética en el Siglo XXI, amenazas en un mundo multipolar en donde los ciberataques pueden provenir o no de Estados, instituciones y/o organismos públicos y/o privados, y grupos al margen de la ley como terroristas, narcotraficantes y crimen organizado que de a poco están alcanzando la misma tecnología emergentes disruptivas de las potencias mundiales.

Estas son las tecnologías de la información y telecomunicaciones y la inteligencia artificial (TIC, IA) creadas por los Estados Unidos (EE.UU.) y obtenidas y en un proceso de mejoramiento constantes por Rusia, China y otros emergentes en estas tecnologías.

Es imperativo comprender cómo las potencias hegemónicas se valen de técnicas para quebrantar la personalidad humana y por ende la toma de decisiones del alto mando de las Fuerzas Armadas (FF.AA.), sector castrense y la Fuerzas de Seguridad (FF.SS.) del rival. Las G5G son mucho más económicas, no se pierden tantos soldados en una batalla, y el daño colateral es mínimo. La metodología a utilizar es de carácter no probabilístico, holístico y fenomenológico. Por otro lado, es comprensiva, integradora y explicativa.

La integración de la IA a las TIC está en pleno proceso de mejoramiento, ya que los programas utilizados, como *Machine Learning* (máquinas que aprenden, por su nombre en inglés), que se utilizan para que máquinas entrenen a otras y estas aprenden solas, imitando a las redes neuronales del hombre. Este concepto está en concatenación con el de guerras algorítmicas. La propuesta para enfrentar estas amenazas es la de mejorar las FF.AA., sector castrense y las FF.SS. y actualizar el AFI.



Palabras claves: G5G, guerras cinéticas y no cinéticas.

Índice

# 1.0 Introducción

## 1.1 Problemática

Este trabajo dará a cuenta qué medidas deberían adoptarse en nuestro país para evitar impactos de las Guerras de Quinta Generación (G5G).

En el ciberespacio, las TIC y la IA, son una amenaza a la Defensa y Seguridad de Argentina y su Geopolítica. Se debatirán ante todo la falta de cohesión, cooperación, financiamiento a profesionales entrenados en ciberseguridad, a las ciber geopolíticas existentes con una embrionaria nueva "Estrategia Nacional de Ciberseguridad".

La pregunta clave de este TFI es de qué manera impactan las Guerras de Quinta Generación (G5G) en una Argentina subdesarrollada e indefensa en el campo cibernético, de la Inteligencia Artificial (IA), de ataques a la mente/psicología. A su vez, seguir el lineamiento de cómo han sucedido las diferentes generaciones de guerras, es un punto crucial para comprender las G5G.

Con esos objetivos alcanzados, el bando que recibe dichos "golpes" cae abatido psicológicamente. Sin saberlo, el bando atacado mediante las operaciones psicológicas (se explicarán más adelante en este TFI) se rinde.

## 1.2 Objetivos

Plantear el orden de aparición de las G5G, desde las Guerras de Primera Generación para así identificar los riesgos de las primeras mencionadas.

## 1.3. Objetivos Específicos

Proponer procedimientos para mejorar las respectivas organizaciones de las Fuerzas Armadas y Fuerzas del Orden en las G5G.

Reducir el costo del entrenamiento y los materiales a utilizar.

Describir un plan de acción para desarrollar la logística en contra de una G5G.

Describir las técnicas de las G5G con conceptos generales.

Explicar la relación entre la mente humana y las G5G.

## 2.0 Marco Teórico

### 2.1 Las nuevas tecnologías, disruptivas y convergentes (TIC e IA)

Según Pauwels, “estas son conjuntamente con computación afectiva, e-psicología, neurociencias, las entendidas para permitir a los sistemas multilaterales con limitadas herramientas anticipar y prevenir riesgos catastróficos” (Pauwels, 2019).

> Un nuevo término acuñado recientemente es la Cibergeopolítica, ya que al pensar en un “territorio”, si bien no es de carácter físico y geográfico, lo es virtualmente, y es en donde las prácticamente nuevas “Ciber-Relaciones Internacionales” se llevarán a cabo en el ciberespacio.

Para lograr este objetivo, la innovación responsable se basa en lo que los expertos llaman gobierno anticipatorio o formas de responsabilidad predictiva. Cuando se enfrentan resultados tecnológicos inciertos y complejos, la anticipación implica el desarrollo de habilidades individuales y colectivas para la adaptación, la resiliencia y la preparación (ieee.es, 2019).

> Dichas habilidades requieren comprender escenarios plausibles relacionados con los futuros de convergencia de IA. Equipados con análisis prospectivos, los inventores, productores y reguladores de tecnologías de doble uso están en mejores posiciones para mejorar el diseño tecnológico para dar cuenta y mitigar las consecuencias no deseadas. (Pauwels, 2019)

Anticipándose a la desigualdad distributiva y su impacto sobre la seguridad humana, los países que se queden rezagados detrás de la convergencia de la IA son más probables de ser eslabones vulnerables en las futuras ciberguerras. (Pauwels, E., 2019).

Más y más datos sensitivos, biométricos, y de salud hasta de datos del genoma humano de las personas son colectados acerca de individuos y poblaciones. Los individuos necesitan controlar y tener acceso a los completos datos de este tipo de datos, capturados, analizados y olvidados (ieee.es, 2019).

La IA (Inteligencia Artificial) relativamente nueva en el terreno de las TIC, lo hace “tierra de nadie”, más específicamente hablando, “tierra virtual de nadie”, en donde se llevan a cabo ciberataques de toda índole (ieee.es, 2019).

Esto pone a Argentina en una posición endeble ya que se duda de su capacidad de repeler un ciberataque de actores de toda naturaleza, como ser de terroristas, criminales, hackers y espionaje solo para nombrar algunas pocas. (Luchetti, P., 2019).

Argentina recibió un posible ciberataque el pasado 16 de junio de 2019, que no solo dejó a oscuras al país entero, sino también a Paraguay, Uruguay, Chile y Brasil. Si bien los oficiales del gobierno no le atribuían un carácter de ataque cibernético, tampoco pudo probarse lo opuesto. (Vargas Alarcón, 2017).

Un "problema técnico" grave o simplemente humedad relacionada con la caída de precipitaciones en la región, podrían haber desencadenado la avería, informó Carlos García Pereira, jefe de Transener, el mayor operador de transmisión de energía de Argentina. Esa cadena de eventos fue "anormal", aseguró Lopetegui. (El Economista., 2019).

Esto deja en claro la vulnerabilidad de la Seguridad y Defensa de Argentina en temas de ciberseguridad. Si bien el gobierno argentino sancionó una ley de Estrategia Nacional de Ciberseguridad en 2019, dicha estrategia está recién implementada, pero carece de practicidad por lo ya descrito previamente. (Luchetti, P. 2019).

### 2.1.1 Convergencia de la IA

Fase Exploratoria: "en esta fase, el investigador aún no ha decidido lo que específicamente desea conocer acerca del tema escogido. Solo sabe que "algo le llama la atención", le preocupa, le interesa o le causa curiosidad. En la fase de indagación el investigador observa lo relativo al contexto y particularmente a la situación que le inquieta. Además, consulta con expertos o con personas vinculadas a una situación, revisa bibliografía, reflexiona e identifica posibles preguntas acerca de la investigación. De hecho, surge un abanico de posibilidades entre las cuales, en una fase posterior, deberá seleccionar una. Es este momento del proceso el que le permite, en la fase siguiente, justificar la investigación, es decir describir las razones, inquietudes, necesidades entre otros; que lo llevaran a elegir un tema y una pregunta en particular. (Gutiérrez, R. A., 2015).

Definición de ciberarma: no existe un consenso global sobre estos tipos de armas. La siguiente es una definición enmarcada en la opción de varios expertos sobre el tema: "instrumento, medio o máquina destinados a atacar o defenderse en cualquier ámbito (material o virtual) del conflicto", (García, A., 2016).

Debido a que este tema abarca mucha teoría, conceptos y explicaciones, se dará una breve sinopsis de la Revolución de Colores.

“La espina dorsal básica para iniciar y difundir una Revolución de Color es la difusión de la información entre la población, sea un segmento demográfico especifico o la sociedad como un todo. Debido a la necesidad de diseminar determinado mensaje (en el caso de la Revolución de Color, uno que incentive a las personas a derribar el gobierno), es imprescindible discutir la famosa obra de Edward Bernays llamada Propaganda publicada en 1928.

Bernays creía que un pequeño número de personas en gran parte invisibles influye y orienta la forma de pensar de las masas, y que esa es la única manera de mantener la apariencia de orden en una sociedad de lo contrario caótica. (Korybko, A., 2019).

Parafraseando a Korybko, la psicología juega un rol muy importante, ya que entendiendo la psicología de las masas cómo funcionan se podría manipularlas por actores externos al proceso. Lo importante es que las masas no se den cuenta que están siendo manipuladas (Korybko, A., 2019).

“La inteligencia artificial (IA) y el aprendizaje automático están creciendo a una velocidad sin precedentes. LA IA está presente en muchos aspectos de nuestra sociedad. Está en el corazón de cada búsqueda en Internet y de cada aplicación. Uno de los recientes avances que han hecho más interesante la IA es el aprendizaje automático. El aprendizaje automático implica el desarrollo y la evaluación de algoritmos que permiten a un ordenador extraer funciones de un conjunto de datos. El aprendizaje profundo es el subcampo de la IA que se centra en la creación de grandes modelos de redes neuronales que son capaces de tomar decisiones precisas basadas en datos. Muchos desarrollos de la IA pueden mejorar nuestras vidas, pero algunos tendrán consecuencias no deseadas que amenazan aspectos importantes de la vida humana. En los últimos tiempos la amenaza del uso malicioso de la IA, está cobrando importancia.

La IA está adquiriendo gran importancia en la desestabilización psicológica selectiva de los sistemas políticos y el sistema de relaciones internacionales. Este factor establece nuevos requisitos para garantizar la seguridad psicológica internacional. Cuando se plantea la cuestión de la ciberseguridad, algunos científicos piensan, si el ser humano podría simplemente ser sacado del bucle, porque uno no se da cuenta de que el problema está en la silla y no en el ordenador. En 2019, un grupo internacional de expertos en la investigación de las amenazas de IPS a través de la IA fue formado para colaborar en investigaciones

conjuntas, conferencias y seminarios científicos. El grupo de miembros formaron un grupo de panel, "El uso malicioso de la inteligencia artificial y la Seguridad Psicológica Internacional" en la Segunda Conferencia Internacional sobre Información y Comunicación en la Era Digital: Impactos Explícitos e Implícitos. Una monografía titulada *Strategic Communication in EU-Russia Relations*: Tensiones, retos y oportunidades (editado por Evengy Pashentsev) se ha preparado para su publicación por parte de Palgrave Macmillan.

Este ensayo presenta algunos de los resultados de la investigación de un grupo internacional de expertos de Francia, Rumanía, Rusia y Vietnam, se centra en los riesgos del uso malicioso de la inteligencia artificial (MUAI) por parte de actores estatales y no estatales para desestabilizar la estabilidad psicológica de sociedad, así como en la actividad pertinente para neutralizar tales amenazas. Evgeny N. Pashentsev, destacado investigador y profesor de la Academia Diplomática del Ministerio de Asuntos Exteriores de la Federación Rusa y de la Universidad Estatal de San Petersburgo, en su artículo titulado "Los niveles de la MUAI y el SIP" sugiere que algunos factores objetivos y subjetivos y subjetivos del desarrollo de la IA pueden amenazar al SIP. Opina que las amenazas son creadas artificialmente. Evgeny ha identificado tres niveles de amenazas. En el primer nivel, las amenazas del MUAI al SIP están asociadas a una interpretación deliberadamente distorsionada de las circunstancias y consecuencias del desarrollo de la IA en beneficio de grupos antisociales. En el segundo nivel, el MUAI no tiene como objetivo principal el manejo de las audiencias en la esfera psicológica, sino a cometer otras acciones maliciosas, por ejemplo, la destrucción de infraestructuras críticas. En el tercer nivel, la MUAI tiene como objetivo principal causar daños en la esfera psicológica. Este nivel merece mucha atención, porque tiene como objetivo las amenazas al SIP. El autor sostiene que "los impactos de los dos primeros niveles de amenazas al SIP afectan a la conciencia y al comportamiento humano en diversos grados. Sin embargo, el impacto del tercer nivel puede, en una determinada etapa de desarrollo facilitar la influencia o el control de grupos egoístas sobre la conciencia pública; esto puede dar lugar a una repentina desestabilización de la situación en un país concreto o de la situación internacional en su conjunto, especialmente en la época de la pandemia de coronavirus y sus consecuencias cada vez más peligrosas para la economía mundial, la estabilidad social y la seguridad internacional.

En su artículo titulado "¿Cómo se preparan los terroristas para utilizar las tecnologías de inteligencia artificial? Aspecto psicológico del problema", Darya Bazarkina, investigadora de la Universidad Estatal de San Petersburgo, sugiere que el desarrollo de tecnologías avanzadas, incluida la inteligencia artificial (IA) aumenta significativamente su

disponibilidad no sólo para las instituciones estatales, sino también para una serie de actores no estatales, así como para una amplia gama de sujetos potencialmente peligrosos de la política mundial. Las tecnologías de aprendizaje automático están cada vez más disponibles. Darya identificó nuevos públicos objetivos, como los jóvenes apasionados por la tecnología, los profesionales de las TIC y un amplio público interesado en temas políticos, la ciencia ficción la literatura de ciencia ficción y las tecnologías avanzadas. Darya sugiere además que si los terroristas se hacen con un mecanismo de análisis predictivo podrían organizar actos terroristas a gran escala durante periodos de malestar social. Para evitar esta situación, es aconsejable que los organismos estatales y supranacionales utilicen ampliamente los mecanismos de análisis predictivo para prevenir los disturbios sociales. para prevenir el malestar social mediante medidas sociales, económicas y políticas oportunas para lograr la estabilidad social a largo plazo. Marius Vacarel, de Rumanía, en su artículo titulado "*Malicious use of artificial intelligence in electoral: manipulación psicológica y riesgos políticos*" argumentó que la consecuencia de tal desproporción - entre las enormes capacidades de la inteligencia artificial para de la inteligencia artificial para utilizar la información y el cerebro humano, favorece una fuerte manipulación psicológica, porque la IA nunca se cansa, siempre está dispuesta a encontrar el mejor argumento para convencer a cada mente, sin importar su nivel de educación. Marius sugiere que debemos seguir la dimensión ética de la vida y la inteligencia artificial debe tener más prioridad, porque sólo la moral puede proteger a las personas contra el abuso de poder. Por lo tanto, es necesario crear nuevas técnicas para el uso genuino de la inteligencia artificial siguiendo el camino de la ética. En un artículo titulado "Uso malicioso de la inteligencia artificial en el ámbito político: el caso de deepfakes", Konstantin Pantserev, de la Universidad Estatal de San Petersburgo, observó que la guerra psicológica contemporánea cuenta con una serie de instrumentos, entre ellos los deepfakes, en los que se sintetiza la imagen humana, basándose en algoritmos de IA. Al principio, los deepfakes aparecieron para el entretenimiento. Un software especial basado en la inteligencia artificial ofrece la posibilidad de crear clones que se parecen, hablan y actúan como sus plantillas. Konstantin opinó que el que el potencial de los deepfakes para ser utilizados de forma maliciosa es cada vez mayor, ya que se crea un clon de una figura conocida y se manipula su imagen. figura conocida y manipula sus palabras. Konstantin también propuso que resolver este reto sólo será posible combinando métodos tecnológicos y legislativos. En el plano legislativo, es necesario elaborar una concepción jurídica del uso malintencionado de los deepfakes y quién debe ser el responsable de detectar y bloquear los contenidos tóxicos. Al mismo tiempo, un algoritmo viable basado en la inteligencia artificial que permita identificar y bloquear rápidamente los de los deepfakes creados con fines

maliciosos. El reto es que no existe un algoritmo viable que sea capaz de detectar el deepfake con una precisión del 100%. Esto significa que es un serio desafío distinguir la información verdadera de la falsa información falsa mientras se navega por el espacio informativo. Dos investigadores de Vietnam llamados Phan Cao Nihat ANH y Dam Van Nhich, en su uso malicioso de la inteligencia artificial y la seguridad psicológica en el sudeste asiático. Asia" sugieren que no existe un sistema de seguridad regional en la región del sur de Asia que proteja y sirva a todos los países de la región. Los investigadores vietnamitas sugieren que el uso de la inteligencia artificial (IA) para desestabilizar las relaciones internacionales a través de información psicológica sobre las personas es un peligro evidente. Opinan que todos los países de la región deberían cooperar estrechamente en el campo de la IA para controlar, prevenir y minimizar los riesgos del uso malicioso de la inteligencia artificial (MUAI). En un documento titulado "Inteligencia artificial y competencia geopolítica: ¿Cuál es el nuevo desafío y el papel de Europa en relación con la MUAI y la IPS en un contexto de competencia entre grandes potencias? Pierre-Emmanuel Thomann, de Francia, presidente de la Comisión Europea, sugiere que "el mundo se enfrenta a un nuevo continente sugiere que "el mundo se enfrenta a una creciente fragmentación geopolítica con la multiplicación de los actores, el refuerzo de la brecha de poder entre los Estados y el cambio de las anteriores jerarquías geopolíticas. Además, la confrontación geopolítica se desarrolla cada vez más en el escenario de la guerra híbrida guerra híbrida, incluida la guerra psicológica. En este contexto, la digitalización asociada a la de la IA se está utilizando como arma geopolítica a través de la desestabilización de los IPS". El autor observó que el enfoque principal de la Unión Europea con respecto a la IA es el aspectos éticos y económicos y esto se refleja en su principal estrategia de comunicación. ¿Esto está en línea con la promoción de la UE del “multilateralismo” como doctrina internacional, pero el autor se pregunta si esto es suficiente para hacer frente a la MUAI y a las amenazas a la IPS en un contexto de rivalidad entre grandes potencias? Del documento de los investigadores mencionados se desprende que el *big data* es crucial para combatir crisis de salud pública en la actual pandemia de coronavirus, pero ¿cómo pueden la IA y el *big data* en el contribuir en el futuro a un resultado positivo en lo que respecta a la cooperación internacional en tiempos de crisis agudas globales que impliquen la desestabilización de sociedades enfrentadas a riesgos naturales, industriales o la IA y los macrodatos siguen siendo un desafío. No hay una solución fácil solución para nuestra futura seguridad en el ciberespacio. Sin embargo, los trabajos de los investigadores mencionados anteriormente muestran alguna luz al final del túnel. Además, debemos considerar algunas cuestiones morales y éticas en relación con el uso de la inteligencia artificial en nuestra vida cotidiana.” (Purkayastha, K., 2020).

### 2.1.2. Entrando en las G5G

Mientras las generaciones de guerra se tornan de una a la otra, hay algunos elementos que van a persistir en la próxima era. Entre la transición de las Guerras de Primera Generación (G1G) y las de Segunda Generación (G2G), las culturas de obediencia, orden y disciplina persisten. De las de G2G y las de G3G, si bien el foco cambió a maniobrabilidad, el concepto de soporte de fuego indirecto es aún mantenido. En las G4G, la noción de flexibilidad e iniciativa fue un tema prestado de las G3G.

De la misma manera, en las G5G, algunos elementos de las G4G van a seguir adoptados. En las G4G. Nathan Freier parece pensar que los conflictos de naturaleza irregular y asimétrica en un conflicto permanecerán como una característica de guerras futuras, especialmente en contra de los EE.UU. De todos modos, él también opina que los futuros potenciales adversarios seguramente emplearán también estrategias que son tradicionalmente catastróficas y disruptivas al mismo tiempo. De esta forma, alineados con el pensamiento de Freier, no sería ilógico sugerir que el elemento de luchas asimétricas puedan ser la característica que llevaría de una G4G a una G5G.

Las líneas borrosas entre las modalidades y elementos de guerra se ven exacerbadas aún más por el rápido cambio tecnológico. Estados patrocinados por otros estados y actores no estatales ahora tienen una gama más amplia de opciones en términos de tácticas y tecnologías y podrían explotarlas creativamente para sus ventajas en formas que antes no se creían posibles, para promover sus respectivos intereses y objetivos.

Las tecnologías que son tradicionales para la guerra convencional, como los sistemas de información de comando, control y comunicaciones; y las armas modernas de alta tecnología, como los sistemas de bloqueo antisatélite, se pueden usar en concierto con dispositivos explosivos improvisados y cohetes antiaéreos portátiles para efectos devastadores.

Esta combinación de capacidades convencionales e insurgentes dará como resultado una dimensión adicional de complejidad en futuros conflictos. La combinación de capacidades de guerra provocaría una forma coordinada de conflicto conocida como guerra híbrida. Hoffman describió la convergencia de los actores físicos y psicológicos, estatales y no estatales, combatientes y no combatientes, así como el enfoque cinético e informacional como una característica de la guerra híbrida. Otro defensor, William Nemeth, también expuso el caso de que las fuerzas híbridas pudieran asimilar de manera creativa la tecnología en su estructura de fuerza y doctrina al utilizar las tecnologías más allá de los parámetros de empleo previstos.

La efectividad con la que estos actores no estatales utilizan la creciente prominencia del poder blando para influir y enjuiciar sus respectivas agendas provocaría que la naturaleza hibridada de los futuros conflictos ocupara un lugar central. Por ejemplo, hemos visto cómo Al-Qaeda y otros grupos extremistas religiosos hacen uso de las computadoras, las redes sociales e internet para difundir su propaganda y reforzar sus filas a través del reclutamiento y el adoctrinamiento. De manera similar, otros actores no estatales y organizaciones terroristas podrán superar su influencia en esferas no tradicionales. Por lo tanto, dentro de su espectro operativo limitado, las fuerzas híbridas podrán ejercer hábilmente, el elemento de sorpresa fundamental para vencer a los adversarios más avanzados, haciéndolos más difíciles de predecir y mitigar.

Sin embargo, es importante señalar que el surgimiento de guerras híbridas no connota la desaparición de la guerra convencional. Simplemente sugiere que los conflictos del futuro presentarían una combinación de diferentes elementos de guerra, conducidos simultáneamente y coherentemente hacia el adversario. Las líneas entre combatientes regulares e irregulares, la guerra convencional y la asimétrica se están volviendo cada vez más borrosas. Un estudio detallado de la literatura prevaleciente reveló que la definición de guerra híbrida no es lo suficientemente clara. De hecho, la mayoría de las definiciones, como las presentadas por Hoffman y Nemeth, se centran principalmente en las fuerzas irregulares que adoptan las tácticas de las fuerzas convencionales.

Se descuida el aspecto de las fuerzas convencionales que adoptan tácticas que no lo son. Por lo tanto, tal vez se proponga una definición más amplia de la guerra híbrida, para ilustrar mejor su conducta de la siguiente manera:

Una forma de guerra que podría involucrar fuerzas asimétricas utilizando la estrategia, tácticas y métodos típicos de las fuerzas armadas convencionales que utilizan estrategias, tácticas y métodos asimétricos. En esencia, durante futuros conflictos, los actores estatales ya no serían adversos a la utilización de estrategias no convencionales. Del mismo modo, se vería que los actores no estatales pueden adquirir sistemas de armas que anteriormente estaban en el ámbito de las capacidades militares estatales. La guerra híbrida, por lo tanto, incorporaría muchas capas adicionales de complejidad que harían que el futuro entorno de seguridad fuera particularmente desafiante, y calificaría como una posible dimensión de una G5G.

### 2.1.3. El regreso a la guerra interestatal como una característica de una G5G

Desde el final de la Guerra Fría, los Estados Unidos han disfrutado de la posición dominante e indiscutible como la única superpotencia del mundo. Esta conducta unipolar no ha tenido rival en las últimas décadas. El alcance de esto ha sido tan grande que algunos investigadores han dado por sentado que la guerra interestatal se está convirtiendo en una curiosidad histórica. Sin embargo, esta visión puede no necesariamente ser cierta en la generación G5G.

Con un análisis profundo de los diversos factores geoestratégicos que darían forma al entorno futuro, se podría concluir que existe una clara posibilidad de que la guerra interestatal pueda regresar. Uno de esos académicos que tiene el mismo punto de vista es George Friedman. Argumentó que, en un G4G, el enfoque se había desplazado a las amenazas asimétricas, pero más allá de la G4G, se anunciaría un futuro regreso a las amenazas del Estado Nación. Como lo ha demostrado la historia, los cambios en el poder global aumentan y disminuyen a lo largo del flujo y reflujo del tiempo. Los antiguos grandes imperios, como el Romano y RR. UU, han visto su poder alcanzar su punto máximo y, a partir de entonces, finalmente se erosionan. Sería ingenuo pensar que, en una línea similar, la hegemonía de Estados Unidos mantendría su estatus indiscutible por toda la eternidad. La percepción de la permanencia de la hegemonía global de esta nación del norte podría muy bien ser una ilusión transitoria, si el desarrollo mundial continúa en su trayectoria actual. Eventualmente, los estados rivales de gran poder, a medida que continúen aumentando el poder económico y militar, alcanzarán un estado en el que podrán desafiar el orden mundial existente. Las potencias globales emergentes, en su frenesí por asegurar los recursos para impulsar su crecimiento en el futuro, posiblemente se animen a adoptar estrategias híbridas combinadas para involucrar a los Estados Unidos a través de guerras subsidiarias (*proxies* en inglés) o incluso tácticas asimétricas. La forma en que volvería la guerra interestatal no solo podría ser en forma de guerra asimétrica, sino que a medida que aumentan las tensiones y aumentan los conflictos, podría incluso señalar el resurgimiento de la guerra convencional. Una combinación de tácticas asimétricas y convencionales tendería, por lo tanto, a creer más en el argumento de que las guerras híbridas dominarán el G5G.

### 2.1.4. La dimensión de las guerras subsidiarias (*proxy* en inglés) para poder involucrarse en las guerras interestatales

El concepto de guerra de poder (o guerras *proxy*), introducido por Karl Deutsch en 1964, no es reciente. La historia está cargada de instancias de guerras de poder, con ejemplos contemporáneos prominentes durante la era de la Guerra Fría. Sin embargo, avanzando hacia el futuro, si bien el concepto de conflicto por poder permanecería en gran medida, el carácter de la guerra por poder estaría destinado a cambiar. Si bien hemos establecido la plausibilidad del resurgimiento de la guerra interestatal peleada de manera híbrida como una característica potencial de G5G, ese esfuerzo probablemente sería muy caro. Los costos no solo se refieren a los aspectos financieros o económicos, sino también a los costos que también tendrían importantes repercusiones políticas. Los gobiernos tendrán que rendir cuentas ante el público sobre el impacto de tal guerra. El enjuiciamiento de las guerras interestatales puede incluso contravenir los parámetros constitucionales o legales, y los beligerantes probablemente enfrentarían una gran presión internacional o sanciones hasta el cese de las hostilidades. Estos costos y repercusiones serían aún más evidentes si los beligerantes se involucrarán a un gran estado rival de poder contra una hegemonía global.

La probabilidad de que se usen armas nucleares y armas de destrucción masiva (ADM) (en inglés: *WMD, weapons of mass destruction*) en tal caso sería muy real, dado el alto riesgo que estaría involucrado. Este es un escenario que incluso puede tomar una escala global cuando las naciones aliadas de cualquiera de las partes se ven inevitablemente involucradas en el conflicto cuando están obligadas a tomar partido. Por lo tanto, un curso de acción menos arriesgado sería perpetuar el cambio de poder global mediante el enjuiciamiento de una guerra de poder, desafiando así el orden mundial sin tener que involucrarse en una Guerra Total Interestatal. Además, hay una ventaja adicional con el elemento de negación plausible, donde cualquier conexión con los estados beligerantes podría calibrarse para ser tan aparente o tan tenue como lo desee el estado patrocinador. Por lo tanto, es muy probable que, en una G5G, las guerras por poder continúen siendo una característica, especialmente en conflictos que involucran a grandes potencias de estados rivales.

### 2.1.5. Implicancias de las futuras G5G

Para prepararse efectivamente para enfrentar los desafíos que traerá G5G, la planificación de la defensa tendrá que hacerse usando múltiples enfoques. Mirando el estado de desarrollo actual de los militares de EE. UU. Las estrategias nacionales, los conceptos de combate de guerra y las estructuras de fuerza son inadecuados para cumplir con la naturaleza convergente de un G5G, tanto a nivel estructural como intelectual para enfrentar las amenazas emergentes. Sin sospechar, la mayoría de los otros ejércitos del mundo también enfrentan este mismo problema. Por lo tanto, la forma en que comenzamos a ver nuestras políticas nacionales, la arquitectura de seguridad y la planificación de la defensa tendrá que cambiar, para ser relevantes en la era G5G.

Un enfoque de todo el gobierno, que comprende políticas internas sólidas, controles financieros estrictos, diplomacia astuta y mantenimiento de una fuerza militar capaz, sentará las bases sólidas para que un estado pueda enfrentar efectivamente las amenazas de G5G en el futuro. La fuerza militar solo debe usarse como último recurso cuando todos los otros enfoques de poder blando como la diplomacia y el diálogo fracasan. Con el mundo cada vez más complejo e inestable, se necesita un esfuerzo especial para construir relaciones a nivel internacional, fomentar el diálogo a través de formas regionales y participar en la cooperación económica internacional. Las respuestas militares directas solo a las amenazas de seguridad y defensa ya no serán adecuadas. Más bien, la acción militar debe formar parte de un plan más amplio, bien considerado y holístico destinado a abordar la raíz del problema en lugar de simplemente abordar los síntomas.

Mientras más integradas estén las economías, más cooperación y diálogo pueden usarse como un medio para resolver disputas. En consecuencia, las polémicas menos probables se convertirán en conflictos armados. Fomentar un clima inclusivo, tolerante y respetuoso es clave para promover la desradicalización. Garantizar un estado de derecho sólido con salvaguardas apropiadas de los poderes de detención, como el equivalente de las leyes de seguridad interna, junto con inteligencia precisa y oportuna, ayudará a mantener el terror bajo control. El riesgo de un ataque catastrófico en una guerra híbrida con las ADM puede mitigarse mediante un mayor énfasis en las convenciones y tratados mundiales sobre la prevención del uso, así como un esfuerzo global concertado para reducir las existencias de materiales fisibles y la fuerza nuclear. Sin embargo, a veces la guerra y los conflictos armados no se pueden anular cuando se ataca a un Estado. En primer lugar, debe existir una salvaguarda adecuada para protegerse contra los ataques disruptivos en caso de una guerra

híbrida. Estas defensas incluyen la inversión en el desarrollo de una fuerza de seguridad cibernética capaz o un comando dedicado de guerra cibernética para proteger contra ataques a sistemas de infraestructura críticos e instituciones económicas. Será necesario incorporar redundancias apropiadas en la arquitectura del sistema para garantizar la solidez y la continuidad operativa. Las fuerzas armadas militares tendrán que desarrollar sus conceptos de guerra para abordar las amenazas de actores estatales y no estatales en una guerra híbrida. Esto implicaría el desarrollo de una fuerza armada bien desplegada, flexible capaz de abordar el espectro completo de amenazas en el complejo entorno geoestratégico.

Con los conflictos en la última década caracterizados por guerras luchadas contra fuerzas irregulares o asimétricas, muchos Estados han dado mucha prioridad en su presupuesto para desarrollar contramedidas contra los adversarios. En el advenimiento de una G5G, las naciones deberán cambiar su énfasis de nuevo al desarrollo de sus capacidades de guerra convencionales, reposicionando su estructura de fuerza para asegurar que más allá de las capacidades tradicionales de tierra, aire y mar, se aborden los nuevos dominios del espacio exterior y el ciberespacio. También es fundamental desarrollar la gama completa de capacidades, de flexibilidad, desde unidades de fuerzas especiales desplegables de manera elástica, hasta aviones expedicionarios autosostenibles con base de portaaviones y tropas marinas capaces de realizar operaciones en todo el mundo en cualquier momento. Por lo tanto, esto abordará el espectro completo que va desde amenazas de guerra asimétricas hasta convencionales. Los militares del futuro ciertamente necesitarán ser una fuerza equilibrada y versátil y no una sola fuerza de misión para enfrentar las amenazas híbridas en el nuevo entorno G5G.

En términos de capital humano, los soldados y líderes de estas últimas guerras mencionadas deben ser entrenados de manera que sean culturalmente sensibles, estén en sintonía internacional y posean las habilidades necesarias para enfrentar los desafíos en el entorno operativo incierto y complejo del mañana. El concepto de la Guerra de Tres Bloques de Krulax, donde se espera que los soldados realicen acciones militares a gran escala, mantenimiento de la paz y ayuda humanitaria en el espacio de Tres Bloques de la ciudad, puede que ya no sea suficiente. Más bien, en una G5G, los soldados ahora necesitan operar en un Cuarto Bloque adicional.

Esto es principalmente en el dominio de la información o la operación psicológica, donde los futuros soldados deben poder competir con el adversario para defender sus respectivas ideologías, incluso sin estar físicamente ubicados en el teatro de operaciones. Un habilitador de este bloque es el advenimiento de las redes sociales en la batalla constante por el espacio

mental del público. Esto requerirá un cambio de mentalidad; el soldado del futuro no es un combatiente sin sentido, sino un guerrero altamente educado, versátil, culturalmente sensible y tecnológicamente inteligente. Desarrollar tales soldados no es tarea fácil. Por lo tanto, los militares del futuro necesitarán hacer cambios de paradigma en sus esfuerzos de reclutamiento, retención y entrenamiento para desarrollar, entrenar, mantener y desplegar eficazmente a este guerrero de la G5G altamente experto.

Este ensayo ha presentado la tesis de que el mundo está ahora en la cúspide de presenciar otro cambio generacional de guerra. Al analizar de manera crítica la evolución de los enfrentamientos y las tendencias que dominan el clima geoestratégico de hoy en día, se pueden extraer los impulsores y determinantes claves que finalmente darán forma a la próxima generación de guerra. Se sugirió que una forma de guerra híbrida podría ser el sello distintivo de una G5G. También existe la posibilidad de que la guerra interestatal regrese en el entorno de una G5G, y si se desata un conflicto de esta naturaleza, será casi una certeza de que sería una guerra de poder en lugar de un conflicto convencional. Las capas adicionales de complejidad presentan el cambio de paradigma de G4G a G5G. En general, esto ofrece un cambio significativo en el paradigma en términos de cómo uno se prepara y emprende el conflicto bélico. Por lo tanto, al poder participar de la forma y la manera que tomará el futuro ambiente de guerra, los líderes nacionales, los encargados de formular políticas y los profesionales militares podrán prepararse adecuadamente para garantizar la supervivencia y relevancia nacional continúa en el futuro.

### 2.1.6. Revolución de color/Psicología de las masas/Inteligencias (tipos)

Korybko agrega que, en la Revolución de Color, “los procesos cognitivos llevan también un lugar muy relevante en estos mecanismos de control mental, a base de controlar a las masas en contra de un objetivo (ejemplo Venezuela y Siria). Se trata de crear una mentalidad de colmena, en donde hay nodos como células sin líder y cada célula sabe lo que debe hacer, pero existe un líder virtual”. (Korybko, A., 2019).

Como instrumento de guerra se utilizan todas las formas de comunicación que existen en el ciberespacio, tanto sea internet, Facebook, Twitter y afines. Para agrupar esta teoría, todas estas tácticas caen en la denominada “guerras en red”.

## 2.1.7. Psicología de las masas / Diferentes tipos de inteligencia / Ingenierías (inteligencias)

La ingeniería social, en el contexto de la seguridad de la información, es la manipulación psicológica de las personas para que realicen acciones o divulguen información confidencial. Esto difiere de la ingeniería social dentro de las ciencias sociales que no se refiere a la divulgación de información confidencial. Un tipo de truco de confianza con el propósito de recopilar información, fraude o acceso al sistema difiere de una "estafa" tradicional en que a menudo es uno de los muchos pasos en un esquema de fraude más complejo.

Ciberdelitos: Se crea el Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos (2019 – 2023).

Ciberdelito: "delitos realizados por a través de las tecnologías de la información y comunicación (TIC) en el ciberespacio. La ingeniería cognitiva combina ingeniería de sistemas y ergonomía cognitiva. Ergonomía significa el estudio del trabajo. La ergonomía cognitiva significa estudiar el trabajo mental. A diferencia del pensamiento de diseño donde las personas están en la oficina tratando de imaginar el trabajo humano y los problemas en el comité, el ingeniero cognitivo primero realiza un análisis cognitivo de la tarea. El análisis cognitivo de la tarea (*Cognitiva Task Análisis*) consiste en observar uno por uno a los usuarios, idealmente en el entorno de trabajo, haciendo su trabajo y pidiéndoles que piensen en voz alta. Las observaciones se registran y se analizan textualmente. El análisis cognitivo incluye el análisis de objetivos y submetas, información consultada, conocimiento, decisiones y acciones realizadas. Se analizan los problemas que se encuentran y las estrategias efectivas (Turnero, Pablo, 2018).

Después del análisis cognitivo de la tarea, el ingeniero cognitivo simula o modela las soluciones utilizando prototipos interactivos para validar las soluciones de forma iterativa. Existen interrelaciones entre las maneras en que las personas procesan la información y cómo esta se organiza en el sistema. En consecuencia, el ingeniero cognitivo debe dominar las ciencias y las técnicas para la realización, ya sea un sistema electrónico, mecánico o informático. Este profesional continuará especificando el sistema a partir de los prototipos de interfaz. Es muy raro encontrar personas interesadas en dominar ambos campos, pero cada vez existen más especialistas de sistemas que entienden que al dominar la ergonomía cognitiva serán más eficientes para la especificación de sistemas. La guerra de redes, también conocida como guerra de cuarta generación, se aplica a las luchas sociales más frecuentemente asociadas con conflictos de baja intensidad por parte de actores no estatales.

Intenta interrumpir, dañar o modificar lo que una población objetivo sabe o cree que sabe sobre sí misma y el mundo que la rodea. La G4G se dirige a la élite y / o la opinión pública a través de campañas de propaganda y tácticas psicológicas, subversión política y cultural, engaño o interferencia con los medios locales y esfuerzos para promover movimientos disidentes u opositores a través de las redes informáticas.

### 2.1.8. Inteligencia Humana (Icia Humana/HUMINT)

Principales características que los colectores de Icia tienen para la adecuada personalidad al llevar a cabo estas operaciones, un alto grado de conocimiento del área en cuestión, tener una decente familiaridad de donde recolectar información, que los decisores posean habilidades superiores en las bases de recolección humana de Icia, y que tengan soporte independiente de la contrainteligencia. Icia de Fuentes Abiertas: una fuerte credibilidad de la Icia recolectada de las fuentes abiertas pueden proveer sobre, o al menos equiparar un adversario en una G4G. Las fuentes abiertas pueden proveer soporte en términos de indicadores de alerta, planes de contingencia, asistencia a la seguridad, y para las operaciones tácticas. Algunos entusiastas de las fuentes abiertas opinan que estas pueden llegar a proveer un 80% de Icia necesaria para misiones no convencionales de baja intensidad en contra de actores no estatales. Aquí se hallan el Dark y Deep web. (Rodríguez, Y. 2019).

La mayor ventaja de esta Icia es que la información no está clasificada es de dominio público, como diarios y revistas. Tiene como desventaja la baja confiabilidad ya que el oponente puede distribuir falsa información.

Icia Cultural: este tipo de Icia se basa en el estudio en la cultura del adversario, se requiere un entendimiento de sus hábitos, intenciones, creencias, su organización social y símbolos políticos. No solo contribuye a establecer relaciones interpersonales, sino que también ayuda a determinar la forma de guerra, estructura organizacional, y las motivaciones del oponente en una G4G. Indicadores de Icia: para prevenir ataques sorpresa de G4G, el Ministerio de Seguridad debe de redefinir los indicadores de Icia. Los indicadores de Icia tienen como objetivo detectar información de tiempo- sensible o eventos que puedan involucrar una amenaza a un Estado y sus Fuerzas Armadas (FFAA), su política, intereses económicos o a sus ciudadanos. Incluyen el preaviso de acciones enemigas o sus intenciones, la inminencia de hostilidades, insurgencia, armas de destrucción masiva, sus fuerzas en el extranjero, alianzas y/o coaliciones de naciones, reacciones hostiles a las actividades de reconocimiento

al Estado, ataques terroristas y afines. Análisis y procesamiento de Icia: para obtener resultados positivos en este tipo de Icia, se debe recolectar una vasta información bruta sin procesar y convertirla en productos que puedan ser procesados y analizados por analistas de Icia. El Ministerio de Seguridad debe incrementar sus capacidades en las áreas de interpretación de datos, traducción de los documentos, conversión de datos, análisis técnicos de material capturado del adversario y decodificación de material encriptado.

Diseminación de la Icia: el Ministerio de Seguridad debe de rediseñar sus redes de comunicación para permitir comunicaciones fluidas en tiempo real. Debe construir redes planas con una arquitectura estándar para aumentar el flujo de inteligencia tanto vertical como horizontalmente. Las redes deben proporcionar un acceso de cualquier parte u omnipresente de información, en un entorno seguro y colaborativo para compartir la información y la capacidad de los usuarios para obtener dicha información de cualquier fuente disponible en el globo o localmente.

## 2.2. El Bucle OODA Explicado (OODA Loop)

El ciclo OODA es una forma de pensar sobre el proceso de toma de decisiones. Desglosado, este bucle representa cuatro bucles más pequeños, distintos pero interrelacionados: observar, orientar, decidir y actuar. El ciclo OODA anima a los responsables de la toma de decisiones a pensar críticamente, anticipar amenazas y neutralizarlas antes de que se vuelvan críticas. En la práctica, las organizaciones utilizan dicho bucle para comparar su capacidad de reacción, con el objetivo de mejorar continuamente (acortar / acelerar) sus ciclos de decisión.

Al seguir el ciclo OODA, las partes interesadas observan los escenarios en desarrollo, se orientan para asumir una base estratégica, deciden el mejor curso de acción para aprovechar esa base importante y actúan para asumir el mando de la situación. Si bien este proceso parece lineal, se basa en la retroalimentación constante de una gran cantidad de puntos de datos para actualizar cada paso en beneficio de los pasos posteriores.

Observar

Esta es la fase de recopilación de datos: aquí, los tomadores de decisiones están tratando de ingerir toda la información que pueden. Todavía no están pensando en cómo priorizar o qué hacer con él, solo están agregando lo que está disponible.

Oriente

Durante la fase de orientación, los datos se procesan, por así decirlo. Las estadísticas sin procesar se aprovechan para obtener información. La información se analiza, evalúa y prioriza. Los fundamentos de la situación: amenazas, oportunidades, competidores, socios, todos son evaluados y debidamente evaluados.

Decidir

Desde datos en bruto hasta información procesable, los responsables de la toma de decisiones ahora deben estar bien posicionados para decidir la respuesta adecuada. En última instancia, este paso del proceso consiste en elegir entre una gran cantidad de opciones. Cada opción será informada por el punto de apoyo establecido en la fase de orientación, pero esta es la parte prospectiva de la ecuación. Dadas las variables presentes que se han establecido, ¿qué curso de acción producirá el resultado óptimo?

Invariablemente, esta fase produce una hipótesis: el tomador de decisiones predice cuál será el mejor curso de acción basándose en su comprensión de la situación. Op. cit.

Actuar

Este paso consiste en probar la hipótesis generada en la fase de decisión.

Aquí, está haciendo dos cosas: ejecutar su decisión y determinar si su hipótesis era correcta. Debido a que el ciclo OODA es, después de todo, un ciclo, la acción nunca es el último paso del proceso. Lo que se aprende sobre la validez de la hipótesis se reutiliza a lo largo de la totalidad del siguiente ciclo del ciclo OODA. Idealmente, los ciclos futuros serán más precisos y rápidos.

### 2.2.1. Conceptos Generales Finales del Ciclo OODA

Para los comandantes militares, las fuerzas del orden y los ejecutivos corporativos, el ciclo OODA representa una metodología para mejorar los procesos de toma de decisiones. El concepto ha tenido un poder de permanencia notable y, de hecho, en el ecosistema tecnológico actual parece aún más relevante. A medida que Internet de las cosas y los activos digitales conectados contribuyen a una bóveda cada vez mayor de datos valiosos, convertir esos datos en conocimientos prácticos requiere metodologías de toma de decisiones cada vez más rígidas, repetibles y orientadas a procesos. Para esto, el bucle OODA sirve para este propósito.

Con el ciclo OODA, la información crucial se puede interpretar dentro de los parámetros de objetivos claros y contextos variables. Al seguir cada paso en el ciclo OODA y actualizar su evaluación de estas instancias en función de datos en tiempo real, es posible identificar cuellos de botella sistémicos, desarrollar estrategias efectivas e implementar soluciones con propósito en un cronograma más competitivo.

### 2.2.2. Generaciones de Guerras y OODA

Las Guerras de Cuarta Generación son las únicas que han conseguido derrotar a las superpotencias (EEUU y la ex-Unión Soviética). (Jamison, E. P., Rovegno, J., 2006). Zona Cero: es cuestionable e incluso poco probable que la supremacía cibernética pueda ser alcanzada por capacidades abrumadoras manifestadas al apilar más capacidad técnica y agregar vectores de ataque. La alternativa es usar el tiempo como vehículo para la supremacía acelerando la velocidad de los enfrentamientos más allá de la velocidad a la que el enemigo

puede apuntar, y ejecutar y comprender con precisión los eventos que se desarrollan. El espacio creado más allá de la barrera comprensión del adversario se llama Dominio Cero. OODA: el ciclo OODA es el ciclo de observar, orientar, decidir y actuar, desarrollado por el estratega militar y coronel de la Fuerza Aérea de los Estados Unidos, John Boyd aplicó el concepto al proceso de operaciones de combate, a menudo a nivel operativo durante las campañas militares. Ahora también se aplica a menudo para comprender las operaciones comerciales y los procesos de aprendizaje. El enfoque explica cómo la agilidad puede superar el poder bruto al tratar con oponentes humanos. Es especialmente aplicable a la seguridad cibernética y la guerra cibernética. Desde un punto de vista operativo, la acción más allá de la barrera de la comprensión se evapora y anula el esquema tradicional de comando y control. En términos generales, el comando y control militar sigue los pasos de observar, orientar, decidir y actuar, como se describe en el bucle OODA desarrollado por John Boyd en la década de 1960. La guerra acelerada más allá de la barrera de la comprensión anula el OODA del adversario porque no hay nada que pueda observarse con precisión, no hay objetivos para orientar debido a una falta de información y conciencia de la situación para tomar una decisión, y la capacidad de actuar se limita a acciones espurias que no tienen relación con el desarrollo de los eventos. Los principios únicos del ciberespacio socavan la utilidad del bucle OODA. El bucle OODA requiere la capacidad de evaluar eventos en curso (como en el paso inicial de "Observar"), pero en condiciones de anonimato, la velocidad computacional en la ejecución cibernética, y la falta de permanencia del objeto, es probable que las observaciones que alimentan el ciclo sean inexactas, si no espuria, a medida que comienza la aceleración. En la guerra acelerada, el bucle OODA desaparece para la parte más lenta en el compromiso si el actor más rápido rompe la barrera de comprensión. El actor rápido mantiene su bucle OODA en el dominio cero, y a la inversa, si el actor rápido ya no puede mantener su posición en el Cero Dominio, el bucle OODA volverá a aparecer para el actor más lento, como el actor anteriormente rápido no puede mantener la velocidad más allá de la barrera de comprensión.

### 2.2.3. Reconociendo la Revolución: la urgente necesidad de contrarrestar la contrainteligencia cibernética

Las computadoras y la tecnología de la información (TI) han cambiado fundamentalmente la forma en que las personas y las organizaciones crean, comparten y almacenan información. Esto hace que los militares estadounidenses reconsideren la ejecución de la misión y generen conceptos como la Revolución en los Asuntos Militares, (*Revolution of Military Affairs*) guerra centrada en la red o transformación simple. Si la inteligencia se define como una

actividad secreta del Estado para comprender o influir en entidades extranjeras, entonces uno podría argumentar que las redes de computadoras han causado un cambio tan grande en la inteligencia como lo han hecho en los asuntos militares. Después de todo, comprender e influir en una entidad requiere acceder, explotar o manipular información.

Más importante aún, al cambiar las prácticas comerciales de los gobiernos, los sectores militar y privado de los EE. UU. las redes de computadoras han alterado la forma en que los adversarios de dicha nación han mutado la forma en su contra. Sin embargo, no se ha discutido sobre las actividades de Contrainteligencia de los Estados Unidos (CI) con anuncios paralelos de una revolución o transformación. Incluso la atención prestada a la Guerra de Información (*Information Warfare, IW*) u Operaciones Informáticas (IO) tiende a abordar los conceptos defensivos de forma conservadora, centrándose en el aseguramiento de la información (*Information Assurance, IA*) y la seguridad simple. Se ha producido poca discusión profesional o académica sobre la necesidad de un enfoque fundamentalmente diferente de la contrainteligencia cibernética (CI). De hecho, incluso la Estrategia Nacional de Contrainteligencia de los Estados Unidos de América trata los problemas cibernéticos como un objetivo a largo plazo, llamando a la Comunidad de Inteligencia (CI) a ampliar sus esfuerzos en el ciberespacio. Esta transformación no anunciada ha sido llevada a cabo por el Servicio de Inteligencia Extranjero (*Foreign Intelligent Services, FIS*), y la exploración de las redes de Estados Unidos está claramente en marcha. La comunidad de contrainteligencia de la misma nación (CI), por lo tanto, necesita acelerar sus esfuerzos.

Este artículo comienza definiendo la misión de ciber contrainteligencia (CI) y proporciona algunos conceptos sobre cómo la comunidad informática (CI) puede implementar tal misión, así como proteger la información pública y privada. Las secciones finales sugieren lagunas en la estrategia actual de EEUU y describen posibles amenazas cibernéticas.

La cibernética de Estados Unidos (CI) ha existido "de facto" desde la introducción de TI a la inteligencia, la defensa y la seguridad nacional y ha crecido a medida que FIS ha adoptado el comercio cibernético. La explotación remota de los sistemas informáticos, en particular, permite un mecanismo de bajo costo para el acceso anónimo, si no subrepticio, a la información que minimiza la necesidad de reclutar activos.

En la década de 1990 y principios de la del 2000, la contrainteligencia informática (CI) cibernética comenzó a identificar áreas de intereses comunes entre los diversos programas de CI de las agencias gubernamentales. De esta manera, la comunidad de CI comenzó a definir un subconjunto de CI que se ocupa específicamente de las capacidades y

vulnerabilidades adicionales de las computadoras y las redes de computadoras. Según lo definido por el Departamento de Defensa (DOD), las actividades de CI cibernética son aquellas que identifican, penetran o neutralizan las operaciones extranjeras, que utilizan el ciberespacio como la principal metodología de comercio, así como la colección FIS utilizando métodos tradicionales para evaluar otras capacidades e intenciones de EEUU. En otras palabras, la contrainteligencia cibernética (CI) trata con la colección (Servicios Foráneos de Inteligencia, FIS) donde las computadoras y las redes de computadoras son la herramienta principal o el objetivo. Desde los ataques terroristas de 2001, el enfoque de la Comunidad de Seguridad Nacional se ha desplazado principalmente al terrorismo y la amenaza cibernética recibió relativamente menos atención. Por esta razón, la mayor parte de la discusión de los problemas de CI cibernética se ha llevado a cabo en áreas del gobierno que se ocupan de la IW defensiva. Si bien los dos términos no son intercambiables, ambos se ocupan de proteger la información y los sistemas de información o de manipular la información para obtener una ventaja defensiva. Las estrategias que contrarrestan activamente la recopilación de información confidencial o clasificada por el FIS se relegan a apoyar únicamente los esfuerzos de guerra o casos claros de espionaje extranjero. La mayor parte del esfuerzo de EE. UU. para proteger la información del gobierno se limita a la seguridad o garantía de la información, lo que le da a la Comunidad de Inteligencia de los EE. UU. (CI) un papel reactivo en la protección de los sistemas gubernamentales -y en gran medida- ineficaz con respecto a la información privada y los sistemas cibernéticos.

En teoría, el papel de CI en el marco de seguridad de la información podría ser menor; el gobierno debería poder asegurar su propia computadora redes. El gobierno controla la compra de *hardware* y *software* establece políticas, ordena la capacitación, gestiona parches y la seguridad de las actualizaciones y revisiones de implementación, de todos modos, cualquier cantidad de reportes del gobierno. Sin embargo, los informes revelan que la IA es muy difícil lo que con frecuencia resulta en seguridad ineficaz. En la práctica, la vulnerabilidad a la explotación cibernética solo ha crecido en los últimos años. Las redes de TI almacenan más información ya que lo transfieren más rápidamente y lo hacen para un mayor número de usuarios e interfaces entre redes. La ley de Metcalfe establece que el valor de una red de telecomunicaciones es proporcional al cuadrado de la cantidad de usuarios dentro del sistema. En ninguna parte esto es más evidente que para un adversario externo que intenta penetrar en una red. Una gran cantidad de usuarios significa más oportunidades para encontrar prácticas de seguridad deficientes, mientras que más conectividad denota

potencialmente puntos de entrada vulnerables. Del mismo modo, cuanto más se use una red, más información potencialmente útil contendrán para los FIS.

No obstante, el problema es mayor que intentar arreglar la seguridad de un sistema individual o de una gran cantidad de estos. El confiar sobre la seguridad de la información para proteger material confidencial o clasificado de adquisición extranjera, ignora el hecho de que las personas a menudo se mueven sensible información fuera de los sistemas que tienen la protección adecuada, como se ha demostrado en muchos casos de alto perfil.

El ex director de inteligencia central John M. Deutch, mientras en su casa, transfirió material clasificado a su computadora que era propiedad del gobierno, que se designó como "Uso no clasificado, usar solamente." Para empeorar las cosas, esta computadora estaba conectada a Internet.

En la campaña aérea de Kosovo en 1999, la falta de interoperabilidad de los sistemas de comunicaciones sin fallas entre los socios de la OTAN resultó en el uso frecuente de comunicaciones no seguras que la seguridad operativa fue reducida y probablemente condujo a la interceptación serbia de las comunicaciones estadounidenses durante el conflicto.

Wen Ho Lee, un científico informático en Los Laboratorios Nacionales de Los Álamos, (Los Álamos National Labs) se declaró culpable de transferir información de defensa nacional en una computadora insegura y haciendo una copia en una cinta de computadora. La división para la que trabajó, Lee tenía acceso a información técnica específica sobre las armas nucleares de EE. UU.

En 2007, el Comité de Supervisión y Gobierno de la Cámara de Reforma, comenzó una investigación sobre si los miembros del personal del presidente de los Estados Unidos usaron cuentas de correo electrónico aparte de las direcciones oficiales del gobierno para compartir información sobre cuestiones de política delicadas. Independientemente de la legalidad, la supuesta comunicación revela que alguna comunicación de la política gubernamental de alto nivel de políticas se produce fuera del control de sistemas del gobierno.

La confluencia (software) de ambos y la dificultad de adherirse a una estricta política de seguridad de la información y la disposición de los usuarios para mover datos fuera de las redes protegidas ha cambiado radicalmente el ambiente de la seguridad.

La comunidad de CI no ha participado activamente en la alteración del marco de seguridad de la información, incluso mientras que el número de sistemas sensibles aumentan en redes no seguras, aumentan. Un claro ejemplo es la logística militar como la tecnología comercial

ha mejorado, ha desempeñado un papel más importante en el gobierno y el ejército de los EE. UU. Los sistemas de servicios habilitados para la web e identificación por radiofrecuencia (RFID); son ejemplos de la modernización de la logística militar de EE. UU., principalmente en el sistema de apoyo de mantenimiento del comando de batalla (BCS); Los sistemas RFID y de rastreo de vehículos permiten el tránsito en tiempo real y visibilidad en el BCS3. Aunque existen precauciones para limitar información sobre las fuerzas azules a través de controles de acceso y capas múltiples de seguridad, la información logística detallada puede ser clave para los FIS. Redes con el software COTS es probable que tengan vulnerabilidades que pueden resultar en la pérdida de confidencialidad de la red; como ejemplo, en 1998,

Los piratas informáticos adolescentes, en un incidente conocido como “Amanecer Solar", penetraron con éxito este mismo tipo de sistemas: "logística no clasificada”, administración y sistemas de contabilidad que controlan la capacidad de gestionar y desplegar fuerzas militares ". FIS que intentan medir el poder de combate actual de los EE. UU., por lo tanto, es más probable que apunten a la información sobre un sistema no seguro, que asumir la tarea más compleja de obtener información clasificada sobre sistemas seguros.

La infraestructura crítica representa "sistemas y activos, ya sean físicos o virtuales tan vitales para un país cuya capacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la económica nacional, salud pública o seguridad nacional, o cualquier combinación de esos asuntos. Fuente.

Se reconoce que la infraestructura crítica de un Estado es en gran parte su propiedad y operada por el sector público y/o privado; sin embargo, los gobiernos federales y provinciales también poseen y operan infraestructuras críticas al igual que entidades y empresas extranjeras.

Escritos militares sobre la guerra cibernética definen a una guerra asimétrica como: “las estrategias y tácticas no convencionales adoptadas por una fuerza cuando las capacidades militares de los poderes beligerantes no son simplemente desiguales, sino que son tan significativamente diferentes que no pueden realizar el mismo tipo de ataques entre sí”

El Departamento de Seguridad de EE. UU define infraestructuras críticas como "los activos, sistemas y redes, ya sean físicas o virtuales, tan vitales para los Estados Unidos que su incapacitación o destrucción tendría un efecto debilitante en seguridad, seguridad económica nacional, salud o seguridad pública nacional, o cualquier combinación de estas.

Ciberataques en el entorno de la información son facetas importantes de la proyección de fuerza, particularmente contra objetivos blandos tales como sistemas de comunicación, puertos, aeropuertos, áreas de concentración civil, poblaciones, infraestructura crítica y centros económicos.

En este contexto, las armas cibernéticas son una encarnación ideal de una estrategia asimétrica: cuanto más técnicamente sofisticada la infraestructura de información de una nación poderosa es, más vulnerable es a los ciberataques. (Iasiello, E., 2015).

### 2.2.4. Elementos de Guerras Neurocognitivas

El sueño (Sub-Divisiones).

Es un estado biológico activo, periódico, en el que se distinguen las etapas NREM y REM, que se alternan sucesivamente durante la noche.

NREM

Sueño NREM: el sueño NREM (movimiento ocular no rápido) es un sueño sin sueños. Durante NREM, las ondas cerebrales en el registro electroencefalográfico (EEG) suelen ser lentas y de alto voltaje, la respiración y la frecuencia cardíaca son lentas y regulares, la presión arterial es baja y el durmiente está relativamente quieto. (Wikipedia, 2020).

REM

El sueño REM es importante para el ciclo de sueño porque estimula las áreas del cerebro que son esenciales para aprender y crear o retener recuerdos. (Wikipedia, 2020).

Neurociencias

Es la especialidad científica que se dedica al estudio integral del sistema nervioso, teniendo en cuenta sus funciones, su estructura y otros aspectos. De este modo ayuda a explicar diversas características de la conducta y de los procesos cognitivos a través de la biología. (Wikipedia, 2020).

Cognición

La cognición (del latín *cognoscere,* 'conocer') es la facultad de un ser vivo para procesar información a partir de la percepción, el conocimiento adquirido (experiencia) y características subjetivas que permiten valorar la información.

Neurociencia Cognitiva

Área académica que se ocupa del estudio científico de los mecanismos biológicos subyacentes a la cognición con un enfoque específico en los sustratos neurales de los procesos mentales y sus manifestaciones conductuales. Se pregunta acerca de qué manera las funciones psicológicas y cognitivas son producidas por el sistema nervioso. Esta disciplina es una rama tanto de la psicología, así como de la neurociencia, unificando e interconectando con varias subdisciplinas tales como neuropsicología, psicología cognitiva, psicobiología y neurobiología.

El Hipotálamo

El hipotálamo se encuentra en el cerebro y es un órgano fundamental. Es una diminuta estructura y es la responsable de gran parte de las funciones vitales del ser humano. Controla el sistema nervioso autónomo. (Rodríguez, M. 2018).

Se debería hablar de las funciones del hipotálamo. Este órgano es fundamental para mantener a los seres humanos vivos, ya que controla y coordina muchas de las funciones vitales, así como otras funciones importantes.

- Mantenimiento de la temperatura corporal
- Regula el sueño y los ritmos circadianos.
- Participa en la regulación de la memoria.
- Participa en el nivel de energía disponible.
- Participa en las emociones y actúa como neurotransmisor en el cerebro y en el miedo.
- Está relacionada con el estrés y el equilibrio de energías.

La alteración de este órgano puede causar el Síndrome de Korsakoff, o amnesia retrógrada. Quien la sufre es incapaz de generar nuevos recuerdos a largo plazo, rellenando los huecos de su memoria mediante invenciones para compensar los olvidos. Se produce por alcoholismo, pero también por la alteración del hipocampo. (Costas, G., 2018).

Biaural

Onda que se realiza y llega simultáneamente a los dos oídos. Magnetita (Óxido de Hierro, mineral hallado en la naturaleza).

La electroencefalografía (EEG) es una exploración neurofisiológica que se basa en el registro de la actividad bioeléctrica cerebral en condiciones basales de reposo, en vigilia o sueño, y durante diversas activaciones (habitualmente hiperpnea y estimulación luminosa intermitente) mediante un equipo de electroencefalografía.

Es la ciencia de la comunicación y el control, ya sea en el animal o en la máquina. La cibernética comprende los procesos y sistemas de transformación y su concreción en procesos físicos, fisiológicos, psicológicos, etc., de transformación de la información.

La ingeniería humana, también conocida como ergonomía es una ciencia cuyo principal objetivo es ayudar a que el ser humano interactué más cómoda y eficientemente con su medio ambiente. (Alarcón, A. V. 2017): Ingeniería Humana.

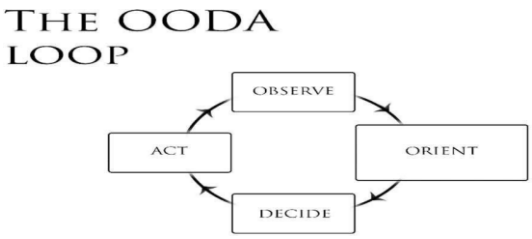


Figura 1

El Ciclo (bucle) OODA

Explicación del Ciclo OODA: el ciclo OODA es el ciclo de observar, orientar, decidir y actuar, desarrollado por el estratega militar y coronel de la Fuerza Aérea de los Estados Unidos, John Boyd.

### 2.2.5. Dentro de la G5G

A medida que las generaciones de la guerra electrónica pasen de una a la siguiente, habrá ciertos elementos que persistirán y se trasladarán a la próxima era. En la transición entre la primera generación de guerra (G1G) y (G2G), la cultura de obediencia, orden y disciplina permanece de G2G a G3G, aunque el enfoque cambió a la maniobra, el concepto de apoyo de fuego indirecto aún se mantiene. En G4G, la noción de flexibilidad e iniciativa fue un tema tomado de G3G. Asimismo, en G5G, se conservarán algunos elementos de la cuarta. Nathan Freier, parecía pensar que la naturaleza "irregular" y asimétrica del conflicto seguirá siendo una característica de las guerras futuras, especialmente como una amenaza contra Estados Unidos. Sin embargo, también opinó que los posibles adversarios futuros probablemente también emplearán estrategias que son "tradicionales", catastróficas y disruptivas "al mismo tiempo. Por lo tanto, alineado con el pensamiento de Freier, no sería descabellado sugerir que el elemento asimétrico de la lucha podría ser quizás la característica que se trasladaría de G4G a G5G.

Las líneas borrosas entre las modalidades y los elementos de la guerra se ven agravadas por el rápido cambio tecnológico. Los actores estatales, patrocinados por el estado y no estatales, ahora tienen una gama más amplia de opciones en términos de tácticas y tecnologías y podrían explotarlas creativamente en su beneficio de formas que antes no se creían posibles, para promover sus respectivos intereses y objetivos. Se pueden utilizar tecnologías que son tradicionales a la guerra convencional, como sistemas de información de comando, control y comunicaciones, y armamento moderno de alta tecnología, como sistemas de interferencia antisatélite. Los sistemas de interferencia se pueden utilizar en conjunto con artefactos explosivos improvisados y cohetes antiaéreos portátiles con efectos devastadores. Esta combinación de capacidades convencionales e insurgentes dará como resultado una dimensión adicional de complicidad en conflictos futuros.

La combinación de capacidades bélicas provocaría una forma combinada de conflicto conocida como guerra híbrida. Hoffman describió la convergencia del actor físico y psicológico, estatal y no estatal, combatiente y no combatiente, así como el enfoque cinético e informativo como una característica de la guerra híbrida. Otro proponente, William Nemeth, también expuso el caso de que la guerra híbrida agregaría más complejidad al futuro entorno de la guerra en el sentido de que las fuerzas híbridas serían capaces de asimilar creativamente la tecnología en su estructura de fuerza y doctrina, y utilizar las tecnologías más allá del "previstos parámetros de empleo a futuro ". La eficacia con la que estos actores

no estatales utilizan la creciente prominencia del poder blando para influir y perseguir sus respectivas agendas llevaría a la naturaleza híbrida del conflicto futuro al centro del escenario. Por ejemplo, hemos visto cómo Al-Qaeda y otros grupos extremistas religiosos hacen uso de las computadoras, las redes sociales e Internet para difundir su propaganda y reforzar sus filas mediante el reclutamiento y el adoctrinamiento. De manera similar, otros actores no estatales y organizaciones terroristas podrán ejercer su influencia en esferas no tradicionales. Por lo tanto, dentro de su espectro operativo limitado, las fuerzas híbridas podrán ejercitar hábilmente el elemento de sorpresa fundamental para vencer a adversarios más avanzados, haciéndolos más difíciles de predecir y mitigar.

Los impulsores del cambio transformador futuro podrían provenir de cualquiera de las siguientes áreas: inteligencia artificial, genómica, combustibles alternativos, nanotecnología, robótica, realidad aumentada y computación cuántica.

Sin embargo, es importante señalar que el auge de las guerras híbridas no connota la desaparición de la guerra convencional. Simplemente sugiere que los conflictos del futuro incluirían una combinación de diferentes elementos de guerra, conducidos de manera simultánea y coherente hacia el adversario. Las líneas divisorias entre combatientes regulares e irregulares, guerra convencional y asimétrica son cada vez más borrosas. Un estudio detallado de la literatura predominante reveló que no hay suficiente claridad en la definición de guerra híbrida. De hecho, la mayoría de las definiciones, como las de Hoffman y Nemeth, se centran principalmente en las fuerzas irregulares que adoptan las tácticas de las fuerzas convencionales. Se descuida el aspecto de las fuerzas convencionales que adoptan tácticas no convencionales. Por lo tanto, tal vez se propone una definición más abarcadora de guerra híbrida, para ilustrar mejor su conducta, de la siguiente manera: "Una forma de guerra que podría involucrar fuerzas asimétricas utilizando la estrategia, tácticas y métodos.” En esencia, durante conflictos futuros, los actores estatales no seguirán siendo reacios a utilizar estrategias no convencionales. Del mismo modo, se consideraría que los agentes no estatales podrían adquirir sistemas de armas que anteriormente estaban en el ámbito de las capacidades militares estatales. La guerra híbrida incorporaría así muchas capas adicionales de complejidad que harían el futuro entorno de seguridad particularmente desafiante, y calificaría como una posible dimensión G5G.

Desde el final de la guerra fría, Estados Unidos ha disfrutado de una posición dominante e indiscutida como única superpotencia mundial. Esta posición unipolar no ha tenido rival en las últimas décadas. El alcance de esto ha sido tan grande que algunos investigadores incluso han dado por sentado que la guerra interestatal se está convirtiendo en una "curiosidad

histórica". Sin embargo, esta opinión puede no ser necesariamente cierta en la quinta generación. Con un análisis profundo de los factores geoestratégicos que darían forma al entorno futuro, se podría concluir que existe una clara posibilidad de que la guerra interestatal regrese. Uno de esos académicos que sostiene la misma opinión es George Friedman.

Argumentó que en G4G, el enfoque se había desplazado a las amenazas asimétricas, pero más allá de la cuarta generación, se anunciaría un regreso futuro a las amenazas del Estado-Nación.

Como ha demostrado la historia, el poder global cambia con altibajos a lo largo del flujo y reflujo del tiempo. Antiguos grandes imperios, como el Imperio Romano y Gran Bretaña, han visto cómo su poder alcanzaba su punto máximo y luego se erosionaba. Sería ingenuo pensar que, de manera similar, la hegemonía estadounidense mantendría su estatus indiscutible por la eternidad. La permanencia percibida de la hegemonía global de Estados Unidos podría muy bien ser una ilusión pasajera, si los desarrollos mundiales continúan en su trayectoria actual.

Eventualmente, los estados-rivales de las grandes potencias, mientras continúan construyendo su poder económico y militar, llegarán a una etapa en la que podrán desafiar el orden mundial existente. Es posible que las potencias globales emergentes, en su frenesí por asegurar recursos para impulsar su crecimiento en el futuro, se animen a adoptar estrategias híbridas combinadas para involucrar a los EE. UU. A través de poderes o incluso adoptar tácticas asimétricas. La forma en que volvería la guerra interestatal no solo podría ser en forma de guerra asimétrica, sino que a medida que las tensiones se intensifiquen y los conflictos aumenten, podría incluso señalar el resurgimiento de la guerra convencional. Por tanto, una combinación de tácticas asimétricas y convencionales daría más crédito al argumento de que las guerras híbridas dominarán el G5G.

A modo de comentario, un enfoque de todo el gobierno, que comprende políticas internas sólidas, controles financieros estrictos, una diplomacia astuta y el mantenimiento de una fuerza militar capaz, sentará bases firmes para que un estado pueda abordar eficazmente las amenazas de G5G en el futuro.

El concepto de guerra por poderes introducido por Karl Deutz en 1964, no es reciente. La historia está cargada de casos de guerras por poderes, con destacados ejemplos contemporáneos durante la era de la Guerra Fría. Sin embargo, avanzando hacia el futuro, aunque el concepto de guerra por poderes permanecería en gran medida, el carácter de la guerra por poderes estaría destinado a cambiar.

Si bien hemos establecido que la flexibilidad del resurgimiento de la guerra interestatal librada de manera híbrida como una característica potencial de G5G, tal tarea probablemente sería muy costosa económicamente. El alto valor no solo se refiere al financiero o económico, sino al que también tendría importantes repercusiones políticas. Los gobiernos deberían rendir cuentas al público sobre el impacto de tal guerra. Enjuiciar las guerras interestatales puede incluso contravenir los parámetros constitucionales o legales, y la beligerancia probablemente enfrentaría presiones o sanciones internacionales de los hombres hasta el cese de las hostilidades. Estos altos valores y las repercusiones serán aún más evidentes si los beligerantes involucran a un gran poder rival de carácter estatal en contra de la hegemonía global.

La probabilidad de que se utilicen armas nucleares y armas de destrucción masiva, en tal caso sería muy real, dados los riesgos que implicaría. Este es un escenario que incluso puede tomar una escala global cuando las naciones de cualquiera de las partes se vean inevitablemente arrastradas al conflicto y cuando se ven obligadas a tomar partido. Por lo tanto, un curso de acción menos arriesgado sería perpetuar el cambio de poder global mediante la persecución de una guerra subsidiaria (*proxy war*), desafiando así el orden mundial sin tener que estar involucrado en una guerra total interestatal. Además, hay una ventaja adicional con el elemento de negación plausible, donde cualquier conexión con el Estado beligerante podría calibrarse para ser tan aparente o tan tediosa como lo desee el Estado patrocinador. Es muy probable que, en la quinta generación, las guerras subsidiarias sigan siendo una característica, especialmente en los conflictos que involucran a Estados rivales de gran poder.

Una forma de guerra que podría involucrar fuerzas simétricas utilizando la estrategia, tácticas y métodos típicos de las Fuerzas Armadas (FF. AA) convencionales; y a la inversa, las Fuerzas Armadas convencionales que utilicen estrategias, tácticas y métodos asimétricos.

## 2.4. Implicancias de la futura Guerra de la Quinta Generación.

Para prepararse de manera efectiva para enfrentar los desafíos que traerá G5G, la planificación de la defensa deberá realizarse utilizando múltiples enfoques. Al observar el estado de desarrollo actual del ejército de los EE. UU., las estrategias nacionales, los conceptos de guerra y las estructuras de fuerzas son inadecuados para cumplir con la naturaleza convergente de las G5G, tanto a nivel estructural como intelectual para enfrentar las amenazas emergentes. Como era de esperar, la mayoría de los demás ejércitos del mundo también enfrentan el mismo problema. Por lo tanto, la forma en que comenzamos a ver nuestras políticas nacionales, la arquitectura de seguridad y la planificación de la defensa deberá cambiar para ser relevantes en la era de las G5G.

Cuanto más integradas estén las economías, mayor será la cooperación y el diálogo que se puedan utilizar como medio para resolver disputas. En consecuencia, la discrepancia menos probable se convertirá en conflicto armado. Garantizar un estado de derecho fuerte con poderes apropiados de salvaguardas de arresto, como el equivalente a las leyes de seguridad interna o las leyes de prevención del terrorismo, junto con inteligencia precisa y oportuna, ayudará a mantener el terror bajo control. El riesgo de un ataque catastrófico en una guerra híbrida utilizando "Armas de Destrucción Masivas" (en inglés: *WMD, weapons of mass destruction*), se puede mitigar mediante un mayor énfasis en las convenciones y tratados mundiales relacionados con la prevención del uso, así como un esfuerzo global concertado para reducir las existencias de materiales fisibles y fuerzas nucleares.

Sin embargo, a veces la guerra contra los conflictos armados es inevitable cuando un estado es atacado. En primer lugar, se deben establecer las salvaguardias adecuadas para protegerse contra ataques interrumpidos en caso de una guerra híbrida. Estas salvaguardas incluyen el desarrollo de inversiones en una fuerza de seguridad cibernética capaz o un comando dedicado a la guerra cibernética para proteger contra ataques a sistemas de infraestructura crítica e instituciones económicas. Será necesario incorporar redundancias prepagas en la arquitectura del sistema para garantizar la solidez y la continuidad operativa. Militarmente, las Fuerzas Armadas tendrán que evolucionar contra conceptos para abordar tanto a actores estatales como no estatales en una guerra híbrida. Esto implicará el desarrollo de una fuerza armada completa, flexible y capaz de abordar el espectro completo de amenazas en el entorno complejo geoestratégico.

Con los conflictos de la última década, al lado de guerras luchadas contra fuerzas irregulares o asimétricas, muchos estados han dado mucha prioridad en su

presupuesto para desarrollar contramedidas contra tales adversarios. En el advenimiento de G5G, los Estados deberán cambiar su énfasis de nuevo al desarrollo de las capacidades de guerra convencionales, reposicionando la estructura para garantizar que las capacidades tradicionales de tierra, aire y mar, los nuevos dominios del espacio exterior y el ciberespacio son dirigidos también. Es fundamental desarrollar la gama completa de capacidades, desde unidades de fuerzas especiales desplegables de manera flexible, hasta fuerzas expedicionarias autosostenibles, aviones alocados en portaaviones y tropas marinas capaces de realizar operaciones en todo el mundo en cualquier momento. Por lo tanto, esto abordará el espectro completo que va desde las amenazas de guerra asimétricas hasta las convencionales. Los militares del futuro ciertamente necesitarán ser una "fuerza equilibrada y versátil", y no una fuerza de misión única, para hacer frente a las amenazas híbridas en el nuevo entorno G5G.

En términos de capital humano, los soldados y líderes de G5G deben estar capacitados de manera que sean culturalmente sensibles, internacionalmente agudos y posean las habilidades requeridas para enfrentar los desafíos en el incierto y complejo entorno operativo del mañana. El concepto de “Guerra de Tres Bloques” de Krulax, C., donde se espera que los soldados realicen una acción militar a gran escala, mantenimiento de la paz y ayuda humanitaria dentro del espacio de tres bloques de la ciudad, puede que ya no sea suficiente. Más bien, en una G5G, por lo que no es necesario operar en un cuarto bloque adicional.

Es en el dominio de la información o de las operaciones psicológicas donde los soldados del futuro deben poder competir con el adversario en la defensa de sus respectivas ideologías, incluso sin estar físicamente ubicados en el teatro de operaciones. Un facilitador de este blog es la ventaja de las redes sociales en la batalla constante por el espacio mental del público. Esto requerirá un cambio de marca de cualquier tipo de automóvil a lo largo del hombro del futuro gruñido sin sentido, pero altamente educado, versátil, insensible a *Country Heights* y tecnológicamente Hisense, un guerrero. Por tanto, no hay hazaña fácil. Por lo tanto, los militares del futuro deberán hacer un cambio de paradigma de los loros en los esfuerzos de reclutamiento, retención y entrenamiento para competir, entrenar, sostener y desplegar de manera efectiva esta Fuerza Guerrera de 5 vías altamente atacada. Mirar allí.

Un facilitador de este “bloque” es el advenimiento de las redes sociales en la batalla constante por el espacio mental del público. Esto requerirá una especie de cambio de estandarte; el soldado del futuro no es un gruñido sin sentido, sino un guerrero altamente educado, versátil, culturalmente sensible y conocedor de la tecnología. Desarrollar tales defensores no es tarea fácil. Por lo tanto, los militares del futuro deberán hacer un cambio de

paradigma en sus esfuerzos de reclutamiento, retención y entrenamiento para poder reclutar, entrenar, mantener, motivar y desplegar de manera efectiva esta fuerza militar G5G altamente hábil.

En síntesis, este ensayo ha presentado que el mundo está ahora a punto de presenciar otro cambio generacional de guerras. Al analizar críticamente la evolución de los conflictos bélicos y las tendencias que dominan el clima geoestratégico actual, es capaz de destilar los factores clave que definen a cada generación e identificar los impulsores y determinantes claves que eventualmente afectarán la próxima generación de guerra. Se sugirió que una forma de guerra híbrida podría ser el sello distintivo de una G5G. También existe la posibilidad de contiendas interestatales o regresar al entorno de G5G, y si estalla un conflicto de esta naturaleza, casi por certeza sería una guerra subsidiaria en lugar de una convencional. Las capas adicionales de complejidad representan el cambio de paradigma que finalmente propuso el cambio generacional de una guerra de cuarta a quinta generación. En general, esto ofrece un cambio significativo en el paradigma, en términos de cómo uno se prepara y conduce la guerra. Por lo tanto, al poder anticipar qué forma tomará el ambiente de lucha en el futuro, los líderes nacionales, sus responsables políticos, y los profesionales militares podrán prepararse adecuadamente para asegurar la supervivencia y relevancia nacional continúa en el futuro. (Kanghao, V. C., 2018).

## 2.5. Diagnostico

"La G5G. Generación y la conquista de las mentes."

Parafraseando a Daniel Trujillo, en su obra "Guerra de 5ª Generación; la conquista de las mentes" dentro de la bibliografía analizada, datos, hechos recogidos, y ordenados sistemáticamente, que permiten describir, analizar y determinar mejor que es lo que está pasando en la realidad, es muy probable que la mayoría de las personas no han oído hablar jamás. Seguro que no lo han escuchado tampoco en el *mass media*, ya que estas forman parte integral del esquema de las G5G. Se debería realizar primero una síntesis de la evolución de la doctrina militar y los conceptos diferentes sobre la guerra a lo largo de la Historia, quizás demasiado simplificada, pero suficiente para adentrarse en el concepto que se quiere plantear.

Las diferentes generaciones de la guerra, primeramente, hay que reseñar que estas clasificaciones tienen que ver con un punto de vista occidental actual, léase OTAN-EEUU, y por lo tanto se debería tener constantemente en cuenta este enfoque a la hora de entender las tácticas y estrategias empleadas. Se entendería, así como las Guerras de Primera Generación (G1G), serían aquellas que tenían por objetivo el aseguramiento de soberanía y de territorios, con sus correspondientes recursos, libradas desde la aparición de las armas de fuego hasta el Siglo XX, y donde los contendientes solían corresponderse con imperios, naciones o entidades diversas que aspiraban a convertirse en una cosa o en otra.

Se caracteriza también por la formación de ejércitos profesionales al servicio de los estados en reemplazo de milicias mercenarias alcanzando su punto de máxima ebullición durante las Guerras Napoleónicas del Siglo XIX.

Por excelencia es la Primera Guerra Mundial (1914-1918), donde se confrontan fuerzas imperiales con fuertes proyecciones colonialistas, en pos de ampliar las posesiones territoriales y el acceso y control de los recursos naturales estratégicos por parte de estos imperios, en un mundo industrializado y cuyas necesidades en materias primas habían evolucionado (carbón, caucho, hierro, petróleo, etc.). Sus características más importantes es la industrialización y la mecanización, y uno de sus elementos fundamentales es la capacidad de movilización de grandes ejércitos y el uso de maquinaria bélica.

Englobaría a la Segunda Guerra Mundial y al periodo posterior, la denominada Guerra Fría, donde lo que se disputaba principalmente era la supremacía político-ideológica para enfrentarse entre sí bloques o alianzas ideológicas antagónicas; Fascismo frente a Democracia - Capitalismo y Comunismo durante la II Guerra Mundial y que posteriormente, tras la derrota del III Reich, se tornó en un enfrentamiento democracia-capitalismo frente al comunismo, que sin llegar a enfrentar nunca directamente a las dos superpotencias (EE. UU. y la URSS), se disputaron las esferas de influencia de la geopolítica mundial y el avance de sus respectivos bloques o alianzas.

Se basa en la velocidad y sorpresa de un ataque (concepto de Blitzkrieg o Guerra Relámpago), sobre la base de una superioridad tecnológica sobre el enemigo que impide cualquier ejecución de defensa coordinada del atacado. Esto hace intenso uso de la concentración de fuerzas aéreas y terrestres coordinadas, de la interrupción de comunicaciones del enemigo y del aislamiento logístico de sus defensas, lo que causa un intencional impacto psicológico aterrador. En esta etapa se ataca, además de a la propia

capacidad industrial del enemigo, masivamente a los civiles para impedir que estos sostengan la industria bélica que necesita el enemigo para continuar la guerra.

En 1991, Martin Levi Van Creveld, historiador militar israelí y entre otras cosas instructor de la Escuela de Guerra Naval de EEUU, publicó *The Transformation of War*[1], obra que le daría cuerpo intelectual a la Guerra de Cuarta Generación (G4G). Básicamente, resumiría que la G1G se basa en movilizar la mano de obra, la G2G en el poder de fuego, y la G3G en la libertad de maniobra.

La G4G o también definible Guerra Asimétrica donde tanto los recursos empleados como los objetivos e intereses a alcanzar engloban tanto al interés público (estatal) como privado (intereses de corporaciones, multinacionales, etc.).

El teórico principal de este concepto sería William Lind, experto en asuntos militares y exdirector del Centro de Conservadurismo Cultural de la "*Free Congress Foundation*", autor de "*Changing Face of War: Into the Fourth Generation*" (1989). ("Cambiando la Cara de la Guerra; Dentro de la Cuarta Generación"), cuyos conceptos se derivan de la idea principal de que el Estado ha perdido su monopolio de los conflictos bélicos, y por tanto este tipo de guerra tiene por objeto hacer frente a los nuevos retos que plantea esta situación. ¿Por qué es llamada también "Guerra Asimétrica"?

Debido a que es una teoría a nivel táctico que oscila desde el aspecto armamentista al psicológico y abarca cualquier aspecto político, económico, social y cultural de una nación con el objetivo de alcanzar el sistema mental y organizativo del adversario, esencialmente por esto la convierte en totalmente asimétrica.

Los conceptos tácticos se fundamentan en que dada la enorme superioridad tecnológica alcanzada durante la etapa anterior (G3G), frente a esta asimetría de fuerzas entre contendientes, solo es concebible el uso de fuerzas irregulares ocultas que ataquen sorpresivamente al enemigo, para provocar su derrota al desestabilizar a su rival, es decir, con el uso de tácticas no convencionales de combate.

Por esta razón es también por lo que se denominan guerras asimétricas y por lo que conflictos como la Guerra de Vietnam, la Guerra de Afganistán (1979- 1992), o el largo conflicto colombiano, entre otros, caerían dentro de esta categoría. Las Guerras de Quinta Generación (G5G) y la mente humana. La denominada GW5 o también denominada por

[1] Van Creveld, Martin Levi. *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*

otros como la “Guerra sin Límites”, donde no interesa ganar o perder, sino demoler la fuerza intelectual, obligando al oponente a buscar un compromiso, para lo cual se valdrá de cualquier medio y que supone incluso que no sea estrictamente necesario el uso de armamento.

Se podría hasta considerarla solo un complemento de las GW4, y ha sido introducida desde los años 2009 y 2010 como concepto estratégico operacional en las intervenciones EEUU-OTAN, es decir una implantación reciente.

Sin embargo, hay una diferencia significativa respecto a la GW4, en las GW5, no hay un condicionamiento tal y como ocurre en las GW4, sino una manipulación directa del ser humano a través de su parte neurológica.

Es evidente que esto se escapa al ámbito de comprensión de varias personas, pero las investigaciones respecto a lo que son las ondas biaurales y componentes de cristales de magnetita del cerebro y los métodos sobre las posibles manipulaciones, y, en general, todo lo que tiene que ver con la neurología, son una constante en el ámbito militar, tanto o más que el desarrollo de otros proyectos de investigación militar avanzada.

Para los jefes del Ejército, la Armada y la Fuerza Aérea de las Fuerzas de Defensa de Australia, el futuro es la 'quinta generación'. Siendo así, recientemente se escribió un artículo sobre la guerra aérea de quinta generación que, si bien utiliza cuestiones de la fuerza aérea para explicar algunos aspectos, tiene relevancia más ampliamente en particular a los conceptos en general de esta misma.

Probablemente, habrá algunos que sean inherentemente cautelosos con aquellos que fragmentan la historia de la guerra en varios períodos o épocas. Sin embargo, la expresión "quinta generación" no forma parte de un análisis histórico considerado. En cambio, que se originó como un eslogan de marketing de la empresa, la expresión se ha convertido en un término general útil, una simple palabra de moda, que abarca varios conceptos importantes sobre cómo se podrían librar guerras futuras.

Las ideas de lucha bélica de quinta generación datan de hace más de dos décadas. En la década de 1990, los pensadores militares aprovecharon los avances en la tecnología de la información comercial, los aplicaron a los conceptos operativos militares y luego popularizaron el término 'Guerra centrada en la Red'. En 1999, el Estado Mayor Conjunto J-6 de Australia afirmaba que: “el mecanismo principal para generar un mayor poder de

combate en 2010 serán las redes de sensores, comando y control y tiradores ". Los conceptos de guerra aérea de quinta generación actuales incorporan cuatro elementos genéricos:

Redes. “El pensamiento centrado en la red” prevé cuatro cuadrículas virtuales interconectadas e interdependientes (información, detección, efectos y comando) que se superponen al teatro de operaciones. Los diversos elementos de fuerza, desde individuos y plataformas individuales hasta grupos de batalla, son nodos interactuando en las cuadrículas. Cada nodo puede recibir, actuar o transmitir datos proporcionados desde las diversas redes según corresponda.

Combatir en la nube. Al trabajar juntas, las cuadrículas pueden formar una nube de combate de la que los distintos nodos pueden extraer datos y agregarlos según sea necesario. Esto trae varios beneficios tácticos que incluyen mejorar considerablemente el conocimiento de la situación, hacer que los compromisos de largo alcance sean más prácticos, garantizar que ningún nodo sea crítico para el éxito de la misión, permitir que cada nodo designe objetivos para otros nodos y garantizar que se haga el mejor uso de las diferentes capacidades. ofrecido por cada nodo.

Batalla de dominios múltiples. Los cinco dominios operativos se consideran tierra, mar, aire, espacio y cibernético. La idea clave que anima la batalla multidominio es la sinergia entre dominios, el uso de la fuerza armada en dos o más dominios para lograr una ventaja operativa. Actuando de manera complementaria, en lugar de aditiva, cada capacidad mejora la efectividad del conjunto al tiempo que disminuye las vulnerabilidades individuales de cada plataforma. Además, la vinculación entre dominios significa que la fuerza integrada en general puede “auto curarse” en el sentido de que la destrucción de cualquier nodo individual puede ser compensada por otro nodo en un dominio diferente.

Guerra de fusión. El concepto de guerra de fusión busca abordar las preocupaciones de mando y control que surgen del creciente volumen y velocidad de los flujos de información, incompatibilidades de software y vulnerabilidades intrínsecas al ataque y el engaño.

Ciberseguridad: ¿está la Argentina preparada para dichos desafíos? Liderado por el Programa Nacional de Infraestructura Crítica de Información y Ciberseguridad (ICIC) en coordinación con diversas agencias, instituciones académicas y el sector privado, el Gobierno de Argentina ha desarrollado un borrador de Estrategia Nacional de Ciberseguridad que actualmente se encuentra pendiente de adopción. Argentina se destaca por formar uno de los primeros CSIRT nacionales en 1994. Desde 2011, ha funcionado bajo el ICIC. ICIC-CERT que mantiene un registro central de eventos y amenazas de ciberseguridad. Las Fuerzas

Armadas (FFAA) realizan ejercicios anuales de respuesta a incidentes cibernéticos para compartir las mejores prácticas y revisar las funciones de comando y control; sin embargo, actualmente tienen una capacidad limitada de resiliencia cibernética.

Anteriormente, CNI se gestionaba de manera más o menos informal; sin embargo, en junio de 2015, la Presidencia de la República Argentina emitió el Decreto N ° 1067/2015, que reestructuró el control gubernamental de la CNI, estableciendo una Oficina Nacional dentro de la Subsecretaría de Protección de la Información Crítica e Infraestructura de Ciberseguridad, bajo la Dirección Oficina del Gabinete de Ministros - Secretaría de Gabinete. Este nuevo programa trabajará para desarrollar normas y estándares de ciberseguridad, así como colaborará con el sector privado para mejorar la resiliencia de la CNI. En medio del aumento de los delitos cibernéticos, el Gobierno de Argentina construyó un marco legal integral para las TIC, incluido el Código Penal-Ley 26.388 y la Ley 25.326 sobre protección de datos. También está desarrollando leyes procesales para el manejo de pruebas digitales. Si bien existen mecanismos para la divulgación, el sector privado no está legalmente obligado a informar sobre las infracciones a la ciberseguridad. Sin embargo, la conciencia de los riesgos de ciberseguridad entre las empresas ha aumentado significativamente. La División de Delitos Tecnológicos de la Policía Federal de Argentina es responsable de investigar los casos que desproporciona información sobre cómo detectar y reportar ciberataques ciberdelito, y asume una serie de capacidades, que incluyen recientemente, el Gobierno de Argentina también estableció un Punto Focal sobre Delito cibernético dependiente del Ministerio Público.

Como gobierno electrónico y comercio electrónico de Argentina los servicios continúan expandiéndose, el gobierno agencias han llevado a cabo campañas de sensibilización para educar al público sobre la ciberseguridad. Dos para educar al público sobre la ciberseguridad. Dos ejemplos notables son Internet Sano (–*Healthy*– o –*Sound*– Internet) liderado por el ICIC, que se centra sobre las mejores prácticas para el uso seguro de Internet, y Con para educar al público sobre la ciberseguridad. Dos ejemplos notables son Internet Sano (–sana– o –solida– Internet) liderado por el ICIC, que se centra sobre las mejores prácticas para el uso seguro de Internet.

### 2.5.1. G5G: Conceptos de Condicionamiento y Manipulación.

Volviendo a los conceptos de “condicionamiento” y “manipulación”, al principio de este artículo se hacía referencia a los “*mass media*” como una parte integral del esquema de las G5G.

Las G5G, hacen uso de medios electrónicos y de comunicación de masas para generar desestabilización en la población a través de operaciones de carácter psicológico prolongado; se busca afectar la psiquis colectiva, afectar la racionalidad y la emocionalidad, además de contribuir al desgaste político y a la capacidad de resistencia.

Brezinski, se permitía afirmar abiertamente que la clave estaba en el ataque al recurso emocional de un país por medio de la revolución tecnológica.: "El Tercer Mundo es víctima de la revolución tecnotrónica". Sea que los países menos desarrollados crezcan rápido o lentamente o que no crezcan en absoluto, es casi inevitable que muchos de ellos sigan dominados por sentimientos cada vez mayores de carencia psicológica". (LET, 1969: 71). La táctica a seguir para mantener la desintegración política en la sociedad consiste en crear complejos de inferioridad y en convertirse en referencia externa en todos los ámbitos, evitando que los proyectos y modelos colectivos o alternativos se consoliden en su identidad, pues la referencia será algo distinto a sí mismos; la referencia será el mundo desarrollado y su modelo prevaleciente.

Los medios de difusión masiva se han encargado de condicionar las mentes en las naciones subdesarrolladas, puesto que, otra vez según Brezinski, "en un mundo electrónicamente intercomunicado, el subdesarrollo absoluto o relativo será intolerable" (…) Ya no se trata de la "revolución de las expectaciones crecientes". El Tercer Mundo enfrenta, ahora, el espectro de las aspiraciones insaciables" (LET, 1969: 71).

El General Tommy Franks, durante la invasión a Irak, definió a la prensa no como cuarto poder, sino como cuarto frente y fue entonces cuando se puso en marcha lo de empotrar reporteros, que significa adoptar en buena medida la mirada de los soldados de un bando y proporcionarles desde los altos mandos los planes a los medios más allegados para que lo difundan, un trabajo bien coordinado por Victoria Clarke, asesora de comunicación y subsecretaria de Defensa para Asuntos Públicos bajo Donald Rumsfeld.

El principio de toda propaganda es recurrir a las emociones más que a la razón. Al sumergir a la audiencia o a los lectores en un mar de emociones se diluye y se distorsiona su capacidad para reflexionar; pero si además agregamos a la emoción el segundo principio básico de la propaganda, como es la simple repetición, se obtiene un poderoso efecto sobre las personas que no están al tanto del modo de funcionamiento de ese mecanismo, y que ni tan siquiera son conscientes de la manipulación a la que están siendo sometidas.

Decía Goebbles que podía convertir un círculo en un cuadrado si lo repetía las suficientes veces. La propaganda funciona con fórmulas simples y tremebundas. Es por ello que se

recurre sistemáticamente a ellas ya que resultan muy eficaces. Es un método clásico que siempre ha funcionado bien cuando se trata de acondicionar la opinión pública para que acepte que la guerra es necesaria.

Algunos ejemplos son: “horrible dictador que está masacrando a su propio pueblo”, el mismo método ya utilizado por los grandes medios de prensa comerciales para acondicionar a la opinión pública para el derrocamiento de Muammar el-Kadhafi y de Saddam Hussein, entre otros.

Realmente la propaganda funciona mediante la repetición de las mismas fórmulas. Dada la extrema similitud entre la mayoría de las informaciones que recibimos sobre tal o cual conflicto, simplemente se recurre a la misma retórica simplista, repleta de clichés emotivos y slogans simplistas, y funciona.

La otra vertiente de la manipulación es el silencio, que adquiere su mayor valor cuando se utiliza como instrumento de manipulación de la opinión pública. Es decir, si los periódicos, los noticieros de televisión y programas de debate u opinión no hablan de un acto de guerra, este simplemente no existe en las mentes de la gente que cree que solo existe aquello que se menciona en los medios de difusión.

Y la vertiente contraria al silencio es directamente la “fabricación” de noticias.

Si se reflexiona un momento con la operación que supuestamente acabó con la vida de Bin Laden en Pakistán.

Esa operación seguramente nunca existió, pero para darle credibilidad se realizó una espectacular película e incluso afloró un “escándalo” con filtraciones de datos oficiales. A ello se suman detalles que añaden una pátina de verosimilitud, como contar las penalidades económicas por las que pasan los soldados que supuestamente participaron en esa ridiculez de operación, e incluso acceden a sacrificar una parte inofensiva de su imagen, todo para dar verosimilitud a su versión.

El objetivo a alcanzar, y por desgracia frecuentemente con éxito, es desviar la atención a aspectos secundarios, magnificándolos para que nadie se plantee el tema central, dándolo por obvio y por absolutamente verídico.

El objetivo final, la conquista y dominación de un territorio o nación, según la socióloga Ángeles Diaz, pasa por cuatro fases: aislar, demonizar, invadir y aislar nuevamente, siendo eje fundamental los medios de comunicación, en cada una de ellas.

Realizada y asentada en los subconscientes de la gente la idea de aislamiento, la primera fase queda completa. En una segunda fase el esfuerzo va dirigido a que todas las noticias que aparecen en los medios de comunicación sobre el enemigo tendrán connotaciones negativas. En cualquier noticia sobre el objetivo seleccionado, aparecerá en el titular el nombre del país o la facción enemiga o de sus líderes. Para el comunicólogo Vicente Romano, una de las técnicas de manipulación más efectiva para esta "conquista de la mente", es la personificación de la política, ya que mediante esta personificación se distrae la atención de las masas respecto de los problemas sociales que les afectan. Se podría añadir que proporcionan un icono sobre el que proyectar e identificar todos los valores negativos o contrarios a la visión del agresor.

Los resultados son binomios ya asociados en nuestra mente identificados de manera automática del tipo Irak—Saddam Hussein, Afganistán—Al Qaeda, Libia—Khadaffi o Siria—Al Assad, bomba atómica—Irán—Putin— agresión…

El campo de batalla, en este caso nuestras mentes están ya preparadas para pasar a la definitiva fase: la invasión y dominación. (Trujillo, Daniel, 2013).

Se llega a este concepto, pero con ejemplos, para tener más preciso el significado de estas y cuán difícil es pelear en contra de una de las mencionadas.

Cuando se dice Somalia (batalla de Mogadiscio, 1993), FARC (Plan Colombia, desde 2000), Operación Anaconda (Afganistán, desde 2001), Líbano (Herbola, 2006), ya se tiene una idea de que se trata.

Por otro lado, y acorde a la mirada de algunos autores, no solamente hay una fuerte asimetría tecnológica entre las fuerzas enfrentadas, sino que además aparecen actores antes impensados. A una fuerza estatal ahora se le oponen fuerzas no estatales y, además, la naturaleza de esta nueva forma de hacer la guerra indica que en términos generales las fuerzas estatales son las que pierden. Se podría citar a Mao Tse Tung (luchas civiles contra el Kuomintang/Chiang Kai Shek) aunque se aprecia que el ejército de Chiang, pese al apoyo de los EE. UU., no tenía ningún desnivel tecnológico superior. Se prefiere ver el inicio de las G4Ga través del accionar de Ho Minh, el Viet Minh y a su general Vo Nguyen Giap contra Francia primero y luego contra los Estados Unidos.

Otro ejemplo de guerra asimétrica es lo sucedido en Somalia en 1993. La milicia de ese país pobremente armada y que horrorizara a la sociedad occidental al arrastrar el cadáver de

un americano por las calles, resultó vencedora en esta batalla difusa y rápidamente todas las fuerzas de la ONU se fueron del país. (Pozo, Jorge, 2014).

En esta línea de pensamiento, los conflictos de G4G reconocen como campo de batalla a la Sociedad en su conjunto (y a su cultura), buscando su implosión. Estos eventos no reconocen límites claros entre la guerra y la paz, o entre combatientes y no los que no lo son, ni permiten identificar con precisión los frentes de batalla. Son eventos signados por una gran dispersión geográfica y valoran, en mayor medida que en cualquier generación anterior, el rol de las operaciones psicológicas y el manejo de los medios de comunicación social. (Bartolomé, Mariano Cesar, 2008).

Es importante anotar que estas "nuevas guerras" se evidencian en la proliferación de conflictos derivados de reiniciaciones culturales, étnicas y religiosas, así como por el protagonismo de actores no estatales. De acuerdo a lo anterior, los Estados ven la necesidad del establecimiento de relaciones de coordinación que se manifiestan en el diseño de las estrategias, cuyo principal objetivo es la reducción de la sensación de amenaza.

Para el diseño de estas estratégicas, los Estados deben tener en cuenta tanto la naturaleza de su oponente como la estructura mental y doctrinal de estos, lo cual puede llegar a constituir un escenario de guerra asimétrica en donde no solo se presente un diferencial de potencial en términos físicos, sino también ontológicos y procedimentales entre los actores involucrados. (Castro, Carlos A. Ardilla, 2014).

En un artículo de Young, reclamo para las ciencias del comportamiento un enfoque que superara las habituales referencias a los "grandes hombres" y a las "fechas inolvidables". Geuter comparte plenamente esta crítica de Young, pero, además señala que "la historia de la psicología se ha limitado durante muchos años a una historia de la teoría", y, manifiesta que -analizando su historia desde el punto de vista de la profesionalización- se muestra un amplio contexto de influencias mutuas y de interdependencias.

Cuando una disciplina se prepara para aplicar su saber en el campo profesional, ella se encuentra más unida por numerosos lazos a las condiciones sociales concretas.

La psicología halla en los gobernantes alemanes de la tercera década del Siglo XX su legitimación. Ya no se trataba únicamente, como había sucedido durante años, de una disciplina meramente académica, sino que ella mostraba además una utilidad práctica inmediata. (León, R., 1984).

En la Introducción, el Marco Teórico y gran parte del Diagnóstico del corriente TFI, se realiza un acercamiento al problema o a la "cuestión" de qué forma la Argentina haría frente a una G5G. Se introdujo el tema, se definieron conceptos, y se empezó a analizar el surgimiento de las G5G empezando por las G1G hasta la GW4.

Es indudable el rol que tienen el comprender la cibernética, la mente humana, las neurociencias, la psicología, la Inteligencia Artificial y las corporaciones mediáticas para entender las G5G.

Haciendo mención de las grandes hegemonías (mientras las grandes corporaciones mediáticas desarrollan sus estrategias en nuevos campos de batalla y donde se pelea con nuevas armas), el resto, entiéndase países tercermundistas -en vías de desarrollo y la Argentina- aún parecen no haber despertado de un sueño letárgico, pensando que a las G5G se las puede enfrentar con arcos y flechas.

Adentrándonos en estos temas, y basándose en lo anterior, se ha hallado lo siguiente para desarrollar y analizar.

Alrededor del mundo, una inmensa gama de organismos gubernamentales y partidos políticos están explotando las plataformas y redes sociales para difundir desinformación y noticias basura, ejercer la censura y el control y socavar la confianza en la ciencia, los medios de comunicación y las instituciones públicas.

El consumo de noticias es cada vez más digital y la IA, el análisis del Big Data (que permite a la información interpretarse a sí misma y adelantarse a nuestras intenciones) y los algoritmos de la "caja negra" son utilizados para poner a prueba la verdad y la confianza, siendo estas las piedras angulares de la llamada sociedad demócrata occidental.

Todas estas megacorporaciones son transnacionales y en su mayoría estadounidenses. Hoy, de las seis principales firmas que cotizan en bolsa, cinco de ellas son del rubro de las TIC: Apple, Google, Microsoft, Amazon y Facebook.

La conexión entre todo lo dicho en los títulos y subtítulos previos indica que mientras las corporaciones mediáticas hegemónicas desarrollan sus estrategias, tácticas y ofensivas en nuevos campos de batalla donde se pelea con nuevas armas (donde la realidad no importa) en lo que quizás ya ni se trata de la G4G, porque lo que se ataca es la percepción y los sentimientos humanos y no al raciocinio de este. Se da pie a una G5G, donde los ataques son masivos e inmediatos por parte de las megaempresas trasnacionales que venden sus "productos" (como el espionaje) a los Estados Unidos de América.

Los demás países por debajo de hegemonía de esta superpotencia, incluyendo a la Argentina, debieran estar más atentos a la integración vertical de los proveedores de los servicios de comunicación con compañías que producen contenidos. El arribo de este tipo de material directamente a los dispositivos móviles, a la transnacionalización de la comunicación, convierte a la información en campañas de terrorismo mediático mientras se denuncia lo fácil que está siendo convertir a la democracia en una dictadura manejada por las grandes corporaciones.

Un informe de Samantha Bradshaw y Phillip Howard, ambos investigadores de la Universidad de Oxford (RRUU), confirma que la manipulación de la opinión pública sobre las plataformas de medios sociales se ha convertido en una amenaza a la vida pública.

En 2017, el primer inventario de las "tropas de ocupación cibernéticas" globales realizado por estos investigadores arrojaron luz sobre la organización mundial de la manipulación de los medios de comunicación social por gobiernos y actores de partidos políticos. Revelan las nuevas tendencias de manipulación organizada de los medios y sus cada vez más crecientes capacidades estratégicas y recursos en las que se apoya este fenómeno, con evidencias de campañas de la manipulación organizada de los medios en 48 países, 20 más que el año anterior. (2017).

Los medios masivos y las redes sociales son parte integral del esquema de esta guerra para generar desestabilización en la población a través de operaciones de carácter psicológico prolongado; se busca afectar la psiquis colectiva, afectar la racionalidad y la emocionalidad, además de contribuir al desgaste político y a la capacidad de resistencia.

Los estudios neurocientíficos, de la conciencia, del cerebro y de la mente que se vienen dando -sobre todo- desde la década de los 90 del siglo pasado (La Década de Oro del Cerebro), están abriendo nuevos paradigmas psicológicos y psiquiátricos, especialmente en la manipulación de las personas.

Uno de los descubrimientos más importantes de las últimas décadas han sido los cinco millones de cristales de magnetita (Fe3O4) por gramo en el cerebro humano. Este mineral no es absorbido de manera externa, sino que es generado por los tejidos del organismo humano.

Estos cristales actúan como un sistema -que se deja llevar por la especulación- hace que la selección de las áreas neurales se reclute, por lo cual los "Estados de conciencia" pueden provocar respuestas fenomenológicas, conductuales y afectivas.

Los lóbulos temporales son las partes del cerebro que median los estados de conciencia. Las lecturas de EEG de los lóbulos temporales son notablemente diferentes cuando una persona está dormida, lo que produce un ataque alucinógeno, o bajo el efecto de LSD (droga psicodélica). Trastornos de convulsiones confinadas a los lóbulos temporales (convulsiones parciales complejas) se han caracterizado por alteraciones de la conciencia.

Al utilizar "herramientas no convencionales", las G5G pueden atacar, no al corazón de un soldado con una bala, sino a la mente de ese ser humano. La *mass media* y las comunicaciones es una forma, y otras maneras son con el uso de las neurociencias aplicadas a interferir en las decisiones militares de los altos mandos. A su vez entorpece el campo magnético del cerebro originado por la magnetita en él, por lo cual causa alteraciones de sueño, de conciencia, alucinaciones, afectivas y emocionales en general, hasta el punto de quebrantar las voluntades del contrario. (Murphy, Todd; 1999).

Los EE. UU. se han dado cuenta luego de sus derrotas en Vietnam, Mogadishu y Afganistán. También que las guerras no se ganan solo con cazabombarderos, fortalezas volantes, tanques de guerra, misiles inteligentes, etc. Se puede hacer mucho más daño y sería mucho más económico y sin perder a ningún soldado, si se le ataca al contrario envenenándolo de a poco. Algunas de estas formas son con la "comida chatarra", el consumismo, sucumbir ante la diabetes, dominio moderno neoliberal, neurociencias, estrés mental, debilitamiento del sistema inmune, atrofiar el hipotálamo, persiguiendo como objetivos más cercanos el dominio por el petróleo y por el agua.

El futuro de la Fuerza de Defensa Australiana (*ADF* en inglés) es de Quinta Generación, al menos para los jefes del Ejército, la Marina y la Fuerza Aérea. Han sido solo una moda pasajera dado que el término se originó como un eslogan de marketing de una empresa que vendía un jet rápido retrasado durante mucho tiempo. No obstante, en los últimos años la expresión se ha transformado en una útil palabra de moda que encapsula varios conceptos más profundos. En esencia, la "Quinta Generación" se trata de ideas, de cómo concebimos librar las guerras del mañana y cómo prepararnos para ellas.

Redes (Networks)- la guerra moderna utiliza extensas redes digitales. Conceptualmente, cuatro cuadrículas virtuales interconectadas e interdependientes son: información, detección, efectos y comando, estas se superponen al teatro de operaciones. Los diversos elementos de fuerza son nodos interactivos en las cuadrículas que pueden recibir, actuar y transmitir datos.

Combates en la nube (*Combat Cloud*)- que trabajan en conjunto, las cuadrículas pueden formar una nube de combate virtual similar a la computación en la nube comercial, que

permite a los usuarios extraer y agregar datos según sea necesario. El resultado son enfrentamientos tácticos de mayor alcance. Ya no se trata de "disparar cuando veas el blanco de sus ojos", sino de "participar cuando aparece una etiqueta de símbolo adversario" en una pantalla compartida.

Batalla multidominio (*Multi-domain battle*)- son cinco dominios operativos; tierra, mar, aire, espacio y cibernética. La idea clave que anima es la sinergia entre dominios, donde la fuerza se aplica a través de dos o más dominios de manera complementaria para lograr una ventaja operativa.

Guerra de fusión (*Fusion Warfare*): los conceptos de guerra de fusión abordan las preocupaciones de comando y control que surgen de flujos de información adicional, incompatibilidades de software y vulnerabilidades intrínsecas al ataque y el engaño.

El orden de estos enfoques refleja principalmente la secuencia en la que se han incorporado al concepto de Guerra de Quinta Generación. El más antiguo es la Guerra centrada en la red (*Network-Centric Warfare*), que data de mediados de la década de 1990; los otros se han vuelto cada vez más prominentes en los últimos años. Su progresión destaca que la tecnología de la información comercial a menudo ha permitido desarrollos militares en la Quinta Generación. La computación en la nube, por ejemplo, se implementó inicialmente a mediados de la década de 2000, pero no fue hasta mediados de la de 2010 en que los pensadores militares adoptaron el concepto.

Cada una de estas cuatro conceptualizaciones es importante, pero en la Guerra de Quinta Generación no existen individualmente; funcionan juntos como un "sistema de sistemas" integrado e interdependiente cuyo todo es mayor que la suma de sus partes. La G5G es, en consecuencia, una forma dinámica de guerra, en constante evolución a medida que cambia el contexto y surgen nuevas demandas.

Obviamente hay dos vulnerabilidades técnicas integradas. Los sistemas digitales son intrínsecamente susceptibles a las intrusiones cibernéticas que pueden robar, eliminar o cambiar datos o insertar datos falsos que pueden propagarse rápidamente por la red. Si bien las técnicas de ciberseguridad mejoran constantemente, también lo hacen los métodos de intrusiones cibernéticas sin que ninguno de los dos permanezca en ascenso por mucho tiempo. Pero es más cibernético: las técnicas de guerra electrónica y de información están diseñadas para ingresar deliberadamente datos falsos en redes hostiles que se propagan a todos los usuarios, confundiendo y distorsionando la imagen compartida.

Además, este tipo de guerra se basa en enlaces de datos. Los emisores son intrínsecamente vulnerables a la detección, los participantes de la red pueden ser localizados y rastreados y -por lo tanto- atacados por armas guiadas con precisión. Algunos enlaces de datos son más difíciles de detectar que otros; sin embargo, al igual que con la cibernética, la tecnología mejora continuamente. La seguridad cibernética y el seguimiento de emisiones de enlaces de datos requerirán un esfuerzo constante durante la vida operativa de la guerra de quinta generación, estos son serios talones de Aquiles.

En segundo lugar, las guerras modernas implican inevitablemente operaciones de coalición, por lo que en cualquier red puede haber actores de muchos países diferentes. Todos los involucrados harán todo lo posible, no obstante, dentro de las fuerzas de cada país y -dentro de la coalición en general- habrá elementos que utilizan diferentes fuentes de inteligencia, diferentes bibliotecas de amenazas y diferentes datos de firma electrónica para tomar decisiones sobre la identidad; ubicación de hostiles, amigables fuerzas y entidades neutrales.

Los peligros operativos implícitos en el aforismo "basura entra, basura sale" sugieren que algunos elementos de la fuerza serán más confiables que otros en la guerra de Quinta Generación. Es probable que las redes "balcanizadas" (en las que algunos nodos no se tengan en cuenta o reciban datos degradados), permite que algunos nodos luchen potencialmente en sus propias guerras separadas en lugar de ser parte de una aplicación coherente y cuidadosamente coordinada de la fuerza militar de la coalición.

En tercer lugar, la soberanía nacional individual se ve debilitada, especialmente en el concepto de nube de combate, ya que la información se extrae de la nube digital con quizás un conocimiento limitado de su fuente. El uso de dicha información externa, en lugar de la derivada de los propios sensores integrados como sucede hoy, para involucrar objetivos reduce inherentemente la responsabilidad y la rendición de cuentas de cada nación. Un exoficial de alto rango de la RAF se quejó de que mata la postura legal del Reino Unido en una cadena clara, inequívoca y soberana.

En cuarto lugar, la idea de la G5G se relaciona con lo que Edward Luttwak llamó "la estrategia de la dimensión técnica". La tecnología influye en cómo libramos las guerras, pero hay más para tener éxito que la tecnología. La de punta fue insuficiente para vencer las guerras de Vietnam, Irak y Afganistán, y la Guerra de Quinta Generación hasta ahora no parece diferente.

Y, por último, el final de la G5G puede estar a la vista. En la década de 1990, los futuristas Alvin Toeffler y Heidi Toeffler argumentaron que "cómo hacemos la guerra refleja cómo hacemos riqueza." Ellos previeron que la era de la tecnología de la información necesariamente obligaría a cambios en las batallas. En muchos aspectos, la G5G es el resultado de ahora, algunos ven que se acerca otra revolución industrial que cambiará la forma en que se genera la riqueza. (Layton, P. 2017)

Al evaluar las tendencias bélicas actuales, aparece el modelo conceptual de la Guerra de Cuarta Generación (G4G) y, por extensión, la Guerra de Quinta Generación (G5G), han alcanzado un nivel de preeminencia dominante hasta el punto de establecimiento doctrinal. Por supuesto, hay contraargumentos frecuentes (y convincentes) contra los preceptos de G4G, pero dichos argumentos parecen enfrentar una batalla casi cuesta arriba ya que los conceptos de G4G/ G5G han penetrado a través del espectro de la guerra irregular, estableciéndose como "conocimiento común". A medida de que estos términos se han convertido en un lugar común, hablado con frecuencia con una absolución segura de sí mismo, es bastante preocupante que estos conceptos de guerra futura, destinados a revelar (como argumentan los proponentes) la estasis miope de la comprensión "convencional", se hayan convertido en sí mismos en un concepto cerrado y en un limitado paradigma. Por lo tanto, el problema inherente con G4G/ G5G (y la dificultad para contrarrestar estos conceptos) es la naturaleza de su propia convencionalidad.

Uno de los conceptos erróneos más grandes de la teoría de G4G es la reconciliación excesivamente simplista de la historia de la guerra en cuatro categorías claramente delineadas (y evaluadas linealmente), o cinco, como se ha desarrollado conceptualmente G5G, la primera de las cuales solo dos siglos atrás. Tal punto de vista proporciona solo el tratamiento más superficial con respecto a la historia de la guerra, cualquier examen profundo del cual revela que los elementos de cada "generación" parecen desaparecer/reaparecer en el escenario mundial según lo dictan las circunstancias. Por supuesto, las herramientas han cambiado y parece que los defensores de la teoría G4G/G5G pusieron demasiado peso en el valor de dichas herramientas (es decir, las herramientas dictan los conceptos). Si bien es cierto que las herramientas pueden aumentar las ideas, esos atributos básicos de cualquier disciplina, las más "centrales" no cambian y posiblemente dictan el desarrollo e implementación de dichas herramientas.

Además, se valora mucho la aparente modernidad de la teoría subyacente de G4G, para incluir su conceptualización. Como afirma Hammes: "La guerra de cuarta generación utiliza todas las redes disponibles, políticas, económicas, sociales y militares, para convencer a los

responsables políticos del enemigo de que sus objetivos estratégicos son inalcanzables o demasiado costosos para el beneficio percibido. El único medio que puede cambiar la mente de una persona es la información. Por lo tanto, la información es el elemento clave de cualquier estrategia de G4G. Sin embargo, cualquier estudiante de Sun Tzu puede ver estos mismos argumentos dentro de su visión estratégica global. Por poner solo un ejemplo, Sun Tzu les dio un valor desmesurado a los espías, demostrando su comprensión del valor de la información, no solo como una mercancía en la guerra, sino como una fuerza políticamente poderosa por derecho propio. Por supuesto que el desarrollo de la tecnología basada en la información lo coloca a uno en una posición de reclasificar cuando se evalúa la filosofía estratégica histórica, pero tanto los "cruzados" como los "conservadores" (como los concibió Bacevich, particularmente cuando se consideran dentro del contexto del entorno teórico (G5G) pueden encontrar valor en estos argumentos de la antigüedad. Además, abundan ejemplos históricos que ilustran la práctica de esta teoría (sin necesariamente codificarla), particularmente como se demuestra a través de una conceptualización precursora articulada por Arreguin-Toft: ataque directo y barbarie versus defensa directa y estrategia de guerra de guerrillas, las cuales son ilustraciones exactas de lo que afirma Hammes, utilizando todos los recursos disponibles para convencer a los tomadores de decisiones de ambos (o todos) lados de que sus objetivos estratégicos son inalcanzables (por ejemplo, La Guerra Lusitana).

Además de valorar su relativa modernidad, parece haber un gran enfoque en su aparente singularidad. Como dice el Capitán Bellflower: “Aunque algunos comentaristas argumentaran que este término es engañoso… su resurgimiento como método principal de entrar en conflicto con las potencias mundiales es nuevo ". El capitán Bellflower refina aún más su afirmación:

Sin embargo, tal argumento no considera los innumerables ejemplos de la manifestación de este mismo fenómeno a lo largo de la antigüedad. El desarrollo y la utilización de los ninjas en Japón durante el período de la guerra de clanes (el asesinato es la herramienta más poderosa para "cambiar la mentalidad de políticos enemigos”) donde los sistemas políticos trascendían la jerarquía definitiva normalmente, aplicados regresivamente sirve como una ilustración más convincente de esto. Al igual que el empleo de mercenarios a lo largo de la historia de la guerra europea donde el tamaño y el alcance del compromiso "global" no importa ya que estas organizaciones políticas se preocuparon por lo que creían que los lugares de sus mundos constituir. Incluso la extensión "sin restricciones" de G4G, G5G, no es única

por los conceptos que abordan su actual (aun completamente definido) se pueden encontrar en Sun Tzu, Maquiavelo y otros filósofos estratégicos históricos.

Aunque hablar en términos de G5G proporciona conveniencia conceptual dada su preeminencia antes mencionada, la teoría subyacente de este tipo de guerras se toma con demasiada frecuencia por concedido como un absoluto. Quizás, entonces, el mayor problema con las mencionadas anteriormente esté relacionado con el mantra "el cambio simplemente proporciona la ilusión de progreso". Como se ha dicho, G5G reconcilia un tema muy complejo de manera demasiado simplista, intentando organizar conceptualmente una base de entendimiento para contrarrestar a un enemigo. Según la definición misma de G5G, desafía a la organización conceptual. Al hacerlo, este tipo de conflicto bélico cae en el convencional centrado en el futuro, (de contexto histórico), lógica a la que, (falsamente), afirma ser la antítesis. La G5G luego se enfoca en la explotación total de recursos con énfasis en las herramientas digitales puesto que no es tan diferente de la red y está centrado en la guerra cibernética. Esto ya se ha desarrollado por los defensores de G5G quienes han sido increíblemente críticos. Por lo tanto, la teoría G5G es un argumento inherentemente convencional disfrazado de "próxima cosa nueva" y permite a los proponentes participar en la teoría crítica: argumentar contra el *status quo* sin presentar una verdadera alternativa. Y, si la comunidad estratégica/doctrinal continúa restringiéndose a sí misma dentro de tales trampas de pensamiento apócrifas, independientemente de su intención, seguirá siendo sorprendido y obstaculizado por las actividades de insurgentes, terroristas y otros. (Barnett, D. K., 2010).

Durante más de dos décadas, la Fuerza de Defensa de Australia ha estado involucrada en operaciones continuas. Durante gran parte de este período, las operaciones se han realizado en una variedad de teatros en todo el mundo. A veces ha habido importantes concurrencias con elementos de fuerza únicos comprometidos simultáneamente a diferentes tiempos y escalas, a través de diversos terrenos, entornos operativos y amenazas. La capacidad de la Patrulla Marítima, por ejemplo, se ha dedicado a la lucha contra la piratería, las operaciones de llegadas irregulares, el reconocimiento y la selección por tierra, así como las patrullas de pesca y la supervivencia asistencia de Oriente Medio al Pacífico Sudoccidental.

Sin embargo, si se proyecta hacia las próximas dos décadas, una estrategia aún más compleja y desafiante en un medio ambiente cambiante nos enfrenta. No solo el entorno geopolítico se está tornando más complejo, sino también la guerra. Es probable que la introducción de capacidades de Quinta Generación haga que el combate potencial se extienda por todos los dominios de tierra, mar, aire, espacio y ciberespacio. A medida que se dependa

más de las redes y del acceso al espectro electromagnético, veremos tantas amenazas como oportunidades en el dominio cibernético. Las redes se formarán y desaparecerán en una "nube" de combate para producir un efecto en apoyo de una operación. El acceso a los sistemas basados en el espacio se convertirá cada vez más en una dependencia y un objetivo. No se producirá una única línea de operación y no se extenderá a la mayoría, sino a todos los dominios.

La disponibilidad de datos, de su garantía, la precisión, el engaño y la negación serán fundamentales para las operaciones futuras e involucrará tanto a militares como al sector comercial/empresarial a medida que se torne cada vez más dependientes del soporte para operaciones de montaje y mantenimiento. Estas dependencias y el riesgo asociado están dirigidos oportunidades al "talón de Aquiles" de capacidad de Quinta Generación.

Uno puede estar seguro de que la propia naturaleza de las redes y de las operaciones cibernéticas de Quinta Generación será acelerado y se reducirá el tiempo disponible para la toma de decisiones.

La capacidad de emprender una guerra algorítmica se basa en la informática. Existen avances tecnológicos en tres áreas principales. El primero, involucra varias décadas de crecimiento exponencial en el poder de procesamiento de computadoras que han permitido grandes mejoras en la implementación de técnicas de aprendizaje automático. El segundo, implica el crecimiento repentino del "*big data*"; conjuntos de muchos datos grandes, a menudo automatizados, extraídos y creados, adecuados para capacitar a las máquinas con la capacidad de aprender. El tercero, implica la evolución constante de la tecnología en la nube para que las computadoras puedan acceder fácilmente, procesar y suministrar los datos para resolver problemas. (Layton, P., 2018).

Al considerar estas áreas, es evidente que la guerra algorítmica no es una tecnología discreta como las armas de energía dirigida o hipersónicos. En cambio, los conceptos de estas técnicas tendrán un efecto amplio, omnipresente, que se vuelven progresivamente ubicuo en la guerra. Por primera vez, las máquinas militares se tornan inteligentes, potencialmente en dirección a dichas fuerzas de defensa que con éxito abrazan de forma más eficaces y eficientes entre sí. Tales aparatos astutos, aunque tienen distintas limitaciones, deberán entenderse para que puedan ser explotadas en este nuevo y novedoso recurso militar.

La guerra algorítmica involucra máquinas inteligentes, *big data* y la nube. Al considerar estos elementos, tendemos a basarnos instintivamente en nuestros conocimientos anteriores sobre las computadoras programables. Esto no es sorprendente porque se han convertido en

una parte esencial de nuestra vida familiar y laboral ya que su presencia no solo es muy corriente y común, sino necesaria. Si estas máquinas no producen resultados consistentes, sabemos que debe haber una falla de hardware o software. También sabemos que su software se puede replicar en millones de máquinas para que todas funcionen igual. Estos "entendimientos" están fuera de lugar en el nuevo mundo de las máquinas inteligentes. Quizás la frase "máquina inteligente" sea en sí misma algo engañosa. En algunos aspectos, estos aparatos reaccionan más como humanos que como artefactos tradicionales. En el extremo superior, son conscientes de sí mismas y evolucionan, mostrando una nueva forma de inteligencia en lo alto del tren evolutivo. Sus resultados pueden sorprendernos; aprenden cuanto más tiempo operan, por lo que probarlos puede requerir de la aplicación de técnicas que los humanos utilizan para analizarse entre sí. La implementación del concepto de guerra algorítmica en nuestras organizaciones bélicas puede requerir enfoques innovadores muy diferentes de los empleados anteriormente con nuestras máquinas no inteligentes.

En Occidente, con su tecnología y organización superior, han sido asesinados sujetos durante mucho tiempo por primitivos o salvajes cuyo estilo de guerra los occidentales malinterpretaron y cuyas habilidades excedieron las del occidente en guerras irregulares. Esta es la forma más antigua de guerra, y ha sido un fenómeno que posee muchos nombres, incluyendo guerra tribal, guerra primitiva, guerras pequeñas, y conflicto de baja intensidad. El término “guerra irregular”, parece un mejor término que amplía la variedad de estas pequeñas guerras. Tales conflictos bélicos plagan gran parte del mundo no occidental, y harán llamar la atención cada vez más de la comunidad de Asia occidental. Desde la Segunda Guerra Mundial, por un recuento, ha habido más de 80 conflictos irregulares. Incluyendo guerras civiles en Ruanda y Somalia, guerra de guerrillas en Sudán y rebeliones en Chechnya; involucrando elementos irregulares que luchan contra otros, fuerzas regulares de un gobierno central o una intervención de una fuerza externa de acción.

La adquisición y uso de moderna tecnología militar se ve a menudo como una solución a los problemas de la guerra a finales del siglo XX, con las luchas de información como el último ejemplo. La guerra irregular, sin embargo, permanece confusa y no se ve afectada por los cambios en tecnología. En un conflicto irregular, la sociología, la psicología y la historia tendrán más que decir sobre la naturaleza del conflicto, incluyendo su persistencia e intensidad.

Tradicionalmente, las mayores amenazas a las que se ha planteado la seguridad nacional de EE. UU. por naciones armadas con tecnología moderna y poseedoras de conceptos militares no fueron muy diferentes a de ellos. Esto permitió a la comunidad de inteligencia

centrarse en las fuerzas de similares oponentes, haciendo que la vida de un analista fuese más fácil, aunque la comunidad ha sido menos preparada para los conflictos que involucran a enemigos y aliados diferentes. El foco en los componentes tradicionales del análisis de capacidades militares, como el orden de batalla, doctrina, economía de defensa, etc. para los Estados Unidos prevalecieron en la guerra del Golfo contra Irak, aunque no tan bien en Somalia. La comunidad de inteligencia sabe actuar siempre que los Estados Unidos se enfrente a las amenazas convencionales, aunque la colectividad también necesita poder mirar con igual habilidad en los diferentes tipos de amenazas planteados por guerras irregulares.

PSYOP (Operaciones Psicológicas en ingles), es un elemento vital dentro de la amplia gama de EE. UU. de acciones políticas, militares, económicas e ideológicas. Correctamente empleado, PSYOP reduce la moral y la eficiencia de combate de tropas enemigas y crea disidencia y descontento dentro sus filas. Las operaciones psicológicas pueden promover la resistencia dentro de una población civil contra un régimen hostil o ser empleados para mejorar la imagen de un gobierno legítimo. El objetivo último de "American PSYOP" es convencer a las Fuerzas Armadas (FFAA) y naciones enemigas, amigas y neutrales para actuar favorablemente hacia los Estados Unidos y sus aliados. Debido a la naturaleza de la sociedad matriz y el caso comparativo de detección de falsedad en un mundo multimedia, las campañas públicas de OPSIC en los Estados Unidos son limitadas al presentar material objetivamente correcto. Podría ser poco sincero afirmar que se presenta una imagen equilibrada en propaganda estadounidense, pero el material real presentado en cualquier mensaje PSYOP abierto, particularmente, será verificable contra fuentes independientes. La verdad y la falsedad en la propaganda deben separarse de operaciones abiertas y encubiertas y la cuestión del blanco, gris y propaganda negra (falsa). (Goldstein & Findley, Jr., 1996)

La propaganda abierta es producida por un gobierno u organización que se responsabiliza por ello. Debido a las condiciones del estado policial o consideraciones tácticas, PSYOP es un elemento vital dentro de la amplia gama de EE.UU. que realiza acciones políticas, militares, económicas e ideológicas. Correctamente empleado, PSYOP reduce la moral y la eficiencia de combate de las tropas enemigas y crea disidencia y descontento dentro de sus filas. Las operaciones psicológicas pueden promover la resistencia dentro de una población civil contra un régimen hostil o ser empleados para mejorar la imagen de un gobierno legítimo. El objetivo último de el PSYOP americano es convencer a las Fuerzas Armadas y naciones enemigas, amigas y neutrales para actuar favorable hacia ellos. Debido a la naturaleza de la sociedad matriz y el caso comparativo de detección de falsedad en un mundo multimedia, las campañas públicas de OPSIC en los Estados Unidos están limitadas a

presentar material objetivamente correcto. La propaganda abierta es producida por un gobierno u organización que se responsabiliza por ello. Debido a las condiciones del estado policial o consideraciones tácticas, esas “OPERACIONES PSICOLOGICAS” pueden tener que ser difundidas por medios encubiertos, como agentes que arriesgan su vida para transportar y distribuir los materiales. La propaganda abierta (verdadera o falsa) depende de la credibilidad, fuentes abiertas que utilizan las falsedades rápidamente y pierden toda eficacia. Este tipo de propaganda es también conocida como blanca porque la fuente toma responsabilidad por ello.

La propaganda gris es material distribuido sin una fuente identificada. Puede ser cierta o errónea. La propaganda negra, en cambio, es material producido por una sola fuente que pretende haber emanado de otra. Tales producciones encubiertas pueden utilizarse para dañar la credibilidad de una fuente blanca (veraz) mediante la difusión de falsedades obvias bajo la etiqueta de la fuente de confianza anterior. La propaganda negra, si es efectiva en absoluto, pierde efectividad rápidamente, a menos que la población sea particularmente susceptible a los rumores, manipulación y distorsión de los hechos. Sin embargo, la mencionada anteriormente puede ser muy eficaz si se planifica adecuadamente. Por ejemplo, ¿deberían las fuentes de inteligencia determinar que una invasión es inminente, difundiendo ese hecho bajo una égida que pretende ser el del invasor potencial elimina toda sorpresa y falsifica todas las afirmaciones del invasor de una guerra "justa"? La propaganda puede legítimamente economizar la verdad. Por ejemplo, al describir el triunfo de la democracia no hay obligación particular de discutir el papel del tweed de Boss en política urbana. Las operaciones psicológicas militares son inherentemente conjuntas operaciones. Fuerza de tarea conjunta unificada y otras fuerzas armadas. Los comandantes identifican las audiencias objetivo y desarrollan PSYOP temas, campañas y productos. Estos se envían a través de canales a los jefes conjuntos para su aprobación. Los principios del desarrollo de una campaña OPSIC son aplicables a través del continuo operacional. Aunque la complejidad de la metodología varía con el nivel de conflicto.

Las consideraciones para el desarrollo de campañas de OPSIC son las lo mismo para el contraterrorismo que para la guerra global. La dimensión psicológica cubre tanto el campo de batalla como los efectos sobre los soldados que luchan en la batalla, sus fuerzas armadas líderes y personal, los líderes políticos y los civiles población. En el campo de batalla, las fuerzas estadounidenses quieren enfrentar un enemigo que no está seguro de su causa y sus capacidades y seguro de su inminente perdición; un enemigo que, incluso si estuviera dispuesto a rendirse, tendría poca voluntad para entablar combate. Es política de los Estados

Unidos que las operaciones psicológicas sean realizadas a lo largo del continuo operativo. Debe ser entendido que estos procedimientos se llevan a cabo continuamente para influir en las percepciones y actitudes extranjeras. A su vez, para efectuar cambios en el comportamiento exterior favorables a EE. UU. en objetivos de seguridad nacional. Cualquier tipo o nivel de OPSIC puede ser realizado en cualquier punto a lo largo del continuo operativo. Este entorno en el que las operaciones psicológicas son realizadas no dicta, por sí mismo, o limita las acciones de OPSIC o el nivel de OPSIC aplicado en entornos que no sean la guerra declarada, los PSYOP nacionales.

La política se deriva normalmente de declaraciones oficiales y sobre la política exterior y la seguridad nacional de EE. UU. Se requiere coordinación entre agencias. Durante una guerra declarada, la política emana del comando nacional de autoridades (NCA) tras la aprobación de los planes presentados por la Oficina del Secretario de Defensa (OSD). Esta política nacional es ejecutada a través de una estrategia de coherencia internacional programas de información, que consisten en datos de EE. UU. esfuerzos de difusión relacionados con la política y la información. Es esencial que los temas y productos de OPSIC reflejen y apoyen política nacional, estos mensajes abiertos son tan oficiales como cualquier Comunicado de prensa de la Casa Blanca. Por lo tanto, PSYOP una vez apropiada la política y la estrategia deben integrar completamente el Departamento de Defensa (DOD) PSYOP en estos programas de información internacional para aliviar el potencial de diseminación contradictoria. Acciones psicológicas como demostración de fuerza, encubrimiento y engaño se han utilizado a lo largo de la historia para influir grupos enemigos y líderes. Operaciones psicológicas modernas se ven reforzados por la expansión de la comunicación masiva. Las naciones pueden multiplicar los efectos de sus fuerzas armadas, comunicando directamente a sus enemigos una amenaza de fuerza o represalias, condiciones de entrega, seguridad pasaje para desertores, incitaciones al sabotaje, apoyo a grupos de resistencia, entre otros. La efectividad de esta comunicación con el público objetivo depende de su percepción de la credibilidad del comunicador. Este tiene la capacidad de llevar a cabo la amenaza y el ¿comportamiento? Las acciones de OPSIC transmiten información no solo a los destinatarios sino también a sistemas de inteligencia extranjeros.

Por lo tanto, los mensajes de OPSIC deben coordinarse con la cobertura y planes y actividades de engaño, junto con planificadores de seguridad, para garantizar que se cumpla el secreto esencial y que los mensajes de OPSIC refuerzan la cobertura y el engaño objetivos.

Los analistas de contenido hábiles pueden determinar intenciones analizando cuidadosamente estos mensajes y los planificadores pueden seleccionar sus propios

productos para asegurarse de que solo se transmite la intención abierta. La metodología de manifiesto y el análisis de la propaganda es arcano y difícil, tanto derivado del arte como ciencia. Algunos profesionales creen que el método es más válido cuando se dirige a la propaganda totalitaria que el PSYOP, producido por las democracias. La propaganda democrática normalmente es mucho menos estampada, posiblemente porque los productos reflejan un menor proceso organizado y arreglo ad hoc, que evolucionan rápidamente. La propaganda totalitaria, especialmente comunista, puede ser más fácil de analizar porque está muy formalizada y modelada.

Hay una dimensión psicológica dentro de cualquier elemento de proyección de poder nacional, particularmente el elemento militar. Las percepciones extranjeras de las capacidades bélicas estadounidenses son fundamentales para la capacidad de disuasión estratégica. Por lo tanto, los legisladores estadounidenses debemos articular nuestras acciones nacionales y militares (si no se realizan, otros lo harán). Comunicarse sin ambigüedades con aliados, enemigos, y neutrales es un elemento clave de la estrategia nacional de Estados Unidos. Las eficacias de la disuasión, proyección de poder y otras estrategias, y los conceptos depende de la capacidad de los EEUU para influir en las percepciones de otros. Para estas comunicaciones, cualquier actor del gobierno de EE. UU. o el cuerpo político en general puede convertirse en una táctica importante y un elemento independientemente de la posición estratégica que el jugador sostiene. Al transmitir la voluntad de esta nación, el firme conjunto de la mandíbula del presidente al trazar "una línea en la arena" puede tener como mucha influencia en el ámbito internacional, y especialmente en el adversario, y de la comprensión de la política estadounidense como las acciones tomadas por el gobierno, como las declaraciones de apoyo de otros funcionarios, incluyendo al secretario de estado, líderes del Congreso y comandantes militares, de manera similar son elementos tácticos que llevan la estrategia de información. Acciones tácticas de esta naturaleza, entregadas en el nivel estratégico, son análogos a las reales entrega tácticas de armas a objetivos de naturaleza valiosa en una guerra de disparos. Dado que gran parte de la política se dedica a lograr objetivos nacionales mientras se mejoran los conflictos genuinos y evitando una guerra de disparos, la ejecución táctica de estos roles elementos estratégicos del sistema político / militar es fundamental para la policía nacional. Uno de los beneficios de la política abierta proceso difundido y monitoreado por un libre y agresivo medios de comunicación es que los individuos serían tácticos inadecuados.

Los comunicadores tienden a ser desviados de posiciones para que el destino de la nación requiera de un desempeño hábil. Militarmente PSYOP puede realizarse a nivel estratégico,

aumentando otros sistemas de comunicaciones nacionales, particularmente en áreas para lo cual los sistemas nacionales en tiempos de paz, como los Estados Unidos, y la Agencia de Información de los Estados que no tienen acceso. En todos los casos, es crucial que los PSYOP militares estén integrados con otras comunicaciones nacionales, ya que las audiencias pueden aceptar mensajes de OPSIC y a los militares como posiciones oficiales. Asegurar este proceso, las operaciones psicológicas militares se basan en un proceso planificado y sistemático de transmisión de mensajes e influir en grupos extranjeros seleccionados. Los datos transmitidos por PSYOP militares están destinados a promover temas particulares que dan como resultado actitudes y comportamientos extranjeros deseados. Por tanto, PSYOP puede utilizarse para establecer y reforzar percepciones extranjeras de la capacidad militar estadounidense, determinación, y capacidad de respuesta a los objetivos políticos de EE. UU. y al apoyo general y la política de este país. Las operaciones psicológicas son una dimensión importante de operaciones militares en general. Pueden ser utilizados por los comandantes e influir en las actitudes y el comportamiento de grupos extranjeros en una manera favorable al logro de los objetivos nacionales estadounidenses. Por tanto, el objetivo principal del Departamento de Defensa, (DOD), PSYOP es persuadir audiencias extranjeras para cambiar o mejorar actitudes o comportamientos de manera favorable a uno o más objetivos de seguridad nacional. Además, PSYOP puede contrarrestar la propaganda extranjera que afecta negativamente el logro de los objetivos estadounidenses. Los Estados Unidos típicamente distinguen entre PSYOP a nivel estratégico y a nivel táctico en el campo de batalla.

Las operaciones psicológicas estratégicas generalmente se consideran un aspecto de la diplomacia pública y normalmente se establecen guiados por grupos de trabajo intergubernamentales creados para una situación particular a corto plazo o área regional de interés. Ellos se reúnen periódicamente para aclarar políticas estratégicas de OPSIC a la luz de los aspectos políticos y militares y novedades del día. En la actualidad, sin embargo, EE. UU. carece de un mecanismo permanente para institucionalizar este proceso. En PSYOP táctico o en el campo de batalla, los comandantes usan tales técnicas como transmisiones por altavoz y caída de folletos con la intención de generar un multiplicador de fuerza sin tener que aumentar el tamaño de la fuerza. Los Psyopsers apoyan el engaño táctico, contraterrorismo, contrapropaganda y otras actividades no tradicionales, medios según lo merezca la situación táctica. Mensajes de PSYOP no pueden reemplazar el desempeño táctico o canjear inadecuado entrenamiento, armas o tácticas que resultan en un combate de deficiente actuación. Sin embargo, la metodología puede aumentar la degradación funcional

general de la capacidad enemiga. Misiles, bombas, balas y maniobras establecen el contexto para multiplicación de PSYOP y acelerando los resultados acumulativos de competencia táctica. Las operaciones psicológicas aceleran los efectos positivos de la destreza militar, y puede, bajo ciertas condiciones, retrasar las consecuencias del fracaso militar porque dichas tácticas multiplican los efectos deseados, positivos y los resultados pueden dar como resultado una victoria más rápida a un costo menor en material, tiempo y bajas. Ya sea estratégico o táctico, NYOP utiliza cualquier medio de comunicación disponible para lograr fines deseados. En los círculos occidentales, la veracidad es deseable como objetivo en sí mismo y es el principal medio para generar credibilidad entre las audiencias objetivo.

El éxito en PSYOP se basa en análisis y planificación exhaustivos. La planificación de OPSIC moderna incluye un análisis de objetivos que consta de varias fases. La primera fase identifica posibles objetivos. Una vez que se identifica la audiencia objetiva, las características objetivas como vulnerabilidades, susceptibilidades se analizan las condiciones y la eficacia. Las vulnerabilidades son los cuatro factores psicológicos que afectan al público objetivo: percepción, motivación, estrés y actitud. Susceptibilidades que incluyen el grado en que la audiencia objetiva pueda ser influenciada para responder al mensaje que recibe.

Las condiciones del público objetivo incluyen todos los factores ambientales-sociales, económicos, políticos, militares y físicos que influyen en el público objetivo. La eficacia de la audiencia es la capacidad del público objetivo para llevar a cabo la respuesta deseada del servicio psicológico de servicio. El concepto de efectividad de la audiencia es fundamental para el éxito de PSYOP a nivel estratégico y táctico. Si el objetivo es destrucción funcional de una unidad táctica enemiga, el efectivo y la audiencia pueden ser soldados individuales, que pueden ser persuadidos de desertar en su lugar; es decir, simplemente no cumple sin resistirse abiertamente a sus comandantes. Otros objetivos requieren encontrar diferentes audiencias efectivas. Estas, en una campaña de interdicción aérea en el campo de batalla, podrían ser la de trabajadores civiles que reparan ferrocarriles y puentes dañados.

Estos informan con veracidad que están en riesgo de volver a objetivos previamente dañados para que puedan disuadirlos de seguir trabajando voluntariamente. Sin embargo, si son trabajadores esclavos, la audiencia puede no responder independientemente de su susceptibilidad. La audiencia receptiva pueden ser capataces o comandantes de alto nivel. Por ejemplo, la susceptibilidad de las audiencias de alto rango puede ser amenazas de enjuiciamiento por crímenes de guerra. Ambas conferencias deberán ser convencidas, por múltiples mensajes, para que la campaña sea eficaz. Una vez que se logra el análisis de las

audiencias, el *psyopser* busca determinar el plan psicológico específico que apoya el objetivo nacional.

La Guerra del Golfo Pérsico y el empleo de PSYOP por ambas partes fueron el capítulo más reciente en una larga historia de PSYOP como una parte integral de la estrategia militar. Históricamente, la presencia de PSYOP se ha sentido en campañas de campo de batalla. Las operaciones psicológicas se integraron en el esquema de maniobra del comandante antes de la etiqueta de PSYOP fue inventado y sin el beneficio de una investigación exhaustiva o científica planificación. Un ejemplo temprano de cómo se planificó y aplicada en la batalla antigua está contenida en los escritos del estratega chino Sun Tzu, quien afirmó que lo más noble de la victoria consistía en someter a su enemigo sin luchar. Otro fue las exitosas hazañas de Genghis Khan (del general mongol Temujin), quien suavizaría la voluntad de su enemigo para resistir difundiendo rumores sobre la fuerza de su propio ejército y ferocidad. Su planificación fue simple y, aparentemente, relevante y eficaz. Ya en la batalla de Bunker Hill, el ejército colonial los operadores de OPSIC utilizaron folletos diseñados para trabajar en susceptibilidades de la audiencia efectiva. Panfletos distribuidos entre las tropas británicas en Boston por agentes coloniales de confianza se basaron en el análisis de la situación y las condiciones anticiparon las tropas británicas, así como su motivación. Así, algunos folletos informaron que alimentos y provisiones entre las tropas coloniales eran muy superiores a los de los británicos, y que cambiar de bando daría lugar a una mejora en la dieta. Más importante y eficaz fue apelar a un deseo básico de mejorar el estatus del soldado británico en la vida, un factor importante para motivar el alistamiento. Muchas tropas se habían unido simplemente para obtener la subsistencia o con la esperanza de lograr riquezas suficientes para obtener tierras de cultivo. El mensaje más efectivo señaló ligeramente que para obtener tierras en las colonias, un soldado necesitaba simplemente desertar y caminar hacia el oeste hasta encontrar una parcela adecuada.

Mercenarios de Hesse en particular respondieron a este llamamiento más tarde en la guerra, y un considerable número de los holandeses de Pensilvania actuales deben su ascendencia a la eficacia de esta convocatoria ya que estos soldados se establecieron en un área compatible con el idioma en el que estaban, por ese motivo es poco probable que se entregue a la autoridad británica colonial. Las operaciones psicológicas estratégicas fueron magistrales desde inicio, con Thomas Jefferson y Thomas Paine efectivamente trabajando sus diversas audiencias elegidas mientras Benjamín Franklin utilizó su puesto en Francia para reforzar no solo continental apoyo, que finalmente dio lugar a la fuerza franco-americana que resultó victoriosa en Yorktown, pero también ayudó a traer Lafayette, Pulaski y Kosciuszko

a las costas estadounidenses las campañas dentro de Gran Bretaña que agotaron el apoyo político para que la guerra fuera más eficaz. La competencia en el campo de batalla era importante para el éxito de este esfuerzo e incluyó no solo victorias en Trenton y otros lugares, pero también las increíbles redadas de John Paul Jones sobre las ciudades costeras inglesas, cuyo efecto político eclipsó con creces su mínima importancia militar. James H Doolitle y su incursión en Japón, realizada con los mismos fines y con resultados militares análogos, fue presagiado en metodología y en medios tecnológicos equivalentes casi 150 años antes en la guerra civil americana, ambos lados del conflicto dirigieron campañas estratégicas en Inglaterra con la esperanza de ganar apoyo a sus respectivas causas. Sigue siendo cuestionable, sin embargo, que estas campañas hayan sido planificadas formalmente y que se reunieron los recursos adecuados para ejecutarlos.

La campaña del Sur fue virtualmente socavada por el rechazo confederado de vender algodón a Gran Bretaña. Este suicidio económico superó cualquier efecto positivo que los medios de las campañas pueden haber engendrado. Durante la Primera Guerra Mundial, PSYOP se convirtió en una actividad. Casi todos los países involucrados en la guerra utilizaron formas de PSYOP estratégico y táctico. Muchos países formaron unidades militares especializadas en propaganda. Las funciones principales de estas unidades incluyeron la distribución de folletos en globo y avión. Los vínculos entre planificación, movilización de recursos y ejecución por estas agencias parecía ser un asunto sencillo. Cómo se integraron los detalles de PSYOP en la guerra de disparos del día, o qué tan bien las entregas inducidas por PSYOP, no fue registrado para la historia. Lo que se sabe, sin embargo, es que las entregas ocurrieron con una correlación positiva con ocupaciones por PSYOP. Por lo tanto, los analistas militares comenzaron a analizar de nuevo PSYOP como ingrediente con sorprendente impacto en la batalla. Las operaciones psicológicas eran un recurso porque indujo estrés en las fuerzas civiles y militares el enemigo.

Durante la Segunda Guerra Mundial, las actividades de propaganda se dieron a conocer como guerra psicológica (guerra psíquica). Radio de difusión pública, alrededor de 20 años en este momento, fue llamado a jugar los altavoces montados sobre un tanque con un rango de aproximadamente dos millas, amplificaron la capacidad de la voz humana para alcanzar combatientes opuestos. Además de los programas de medios, los militares emprendieron acciones para su efecto PSYOP. Doolittle operó la incursión contra Japón que se consideró un evento importante de OPSIC por al menos dos razones. La expedición cuidadosamente planeada demostró de manera creíble a los japoneses que los EE. UU. bombardeaban su tierra natal, lo que los llevó a tomar innecesarios pasos para la defensa local. Más importante,

quizás, la noticia del éxito en casa hizo que la moral se disparara en una población estadounidense desesperada por una victoria. La ejecución funcionó en esta única instancia.

Sin embargo, durante esta guerra, las tripulaciones aéreas renunciaron a arriesgarse en misiones de entrega de folletos porque carecían de confianza en esa metodología como medios de acercar la victoria. En los años que siguieron, PSYOP maduró como fuerza de combate multiplicador, aunque a través de una serie de arranques y paradas..

Durante la década de 1950, la Unión Soviética hizo grandes avances tanto en PSYOP estratégico e interno. Los estados-clientes soviéticos comenzaron a elaborar operaciones psicológicas para insurgentes extranjeros y consumo en el hogar. Al mismo tiempo, aparentemente poco planeado en los círculos occidentales de OPSIC. Aunque las operaciones psicológicas estratégicas y tácticas fueron efectivamente integradas por los norvietnamitas durante la Era de Vietnam, la planificación de las OPSIC de EE. UU. o coordinado con operaciones y movilizaciones de tropas. Allí las actividades de propaganda asumieron el término actual PSYOP y la televisión era un nuevo medio. Los norvietnamitas dominaron el arte de utilizar los medios internacionales, particularmente la televisión, por su PSYOP. El gobierno de Estados Unidos fue ineficaz tanto en la información pública como en las políticas en movilizar a su público para la guerra. Como resultado de esta negativa experiencia en Vietnam, el gobierno de EE. UU. quita importancia al apoyo interno y externo de las principales políticas y metas. En los conflictos más recientes, PSYOP se ha integrado con operaciones de combate. En las Malvinas, Afganistán, África, América del Sur y Central, Granada, Panamá y el Golfo Pérsico, PSYOP fue incluido por todas las partes. PSYOP incluso se convirtió en una parte fundamental del modo de operaciones terrorista durante los años setenta y fueron parte del plan de OPSIC iraquí cuando amenazaron con actividades terroristas. Cualquier estudiante de PSYOP aprenderá rápidamente lo importante que PSYOP puede ser en estrategia política y militar. Que cada estudiante debe esforzarse es una interiorización del concepto propuesto por Sun Tzu, el estratega militar chino, que para luchar y conquistar en todas tus batallas no es la excelencia suprema; esta última consiste en romper el enemigo su resistencia sin recurrir a la lucha.

Las Guerras de Quinta Generación (G5G) buscan, independientemente de las neurociencias y afines, crear un super-soldado, y cambiar el futuro del campo de batalla. A un soldado “tradicional”, se le puede minar su voluntad a pelear, a tener pérdidas significativas en una batalla o mismo en escaramuzas de guerra. El “peso de la familia” del recluta va a influir en la motivación de actuar en el campo de batalla con un 100% de efectividad (idealmente) o muy por debajo del 50% de lo que este podría llegar a hacer.

Esta situación se hizo presente en la Segunda Guerra del Golfo Pérsico (2003), en donde la mayoría de los soldados eran hispanoamericanos y afroamericanos (casi todos rasos), en donde "los valores de familia" para ellos eran más importante que los objetivos militares en dicha guerra, queriendo volver sanos y salvos a sus respectivos hogares. Los soldados se cansan, se vuelven temerosos, sufren de miedos y de fatigas crónicas, de "debilidad afectiva", de cambios súbitos emocionales, todas estas debilidades humanas lógicas de un recluta común, promedio, que no está entrenado físicamente, psicológicamente y emocionalmente como los suboficiales y oficiales.

Estos últimos que eligieron la carrera militar y estar preparados para entrar en combate en cualquier momento, versus infantes de marina, infantes del ejército, fuerzas que están formadas por hombres y mujeres que en promedio tienen 25 años de edad, y que "ingresan" en las FFAA para poder pagarse la universidad y/o porque no pueden conseguir un trabajo tradicional en la vida civil. De allí que la DARPA de los EE.UU., *Defense Advance Research Projects* (Proyectos de Defensa de Investigación Avanzada, en español), sugirió crear un "exoesqueleto" de aplicación militar para equipar a sus soldados en batalla.

El recluta equipado con esta pieza avanzada de ingeniería militar sería llamado un *Supertroop* (ST), (Super-tropa), siendo que este exoesqueleto integrado con alimentación, protegería al ST contra armas biológicas, electromagnéticas, y amenazas balísticas, incluyendo el fuego directo de una bala de calibre 0,50. También poseería audio incorporado, visual, táctil y sensores ópticos, incluyendo imágenes térmicas para los ojos. Cada soldado (ST), tendría sus propias funciones fisiológicas en un chip en sus placas de identificación.

Las características de este exoesqueleto de combate para ST es mucho más extenso, esta descripción es lo que se avecina en las próximas G5G. A tal efecto, el expresidente Barack Obama, en un discurso, comentó que "estamos construyendo a Iron Man", (el Hombre de Hierro). Los EE. UU. están trabajando en este proyecto hace más de 25 años, a partir de los principios del Siglo XXI y hacia atrás en el pasado.

- Ley de Metcalfe

Establece que el efecto de una red de telecomunicaciones es proporcional al cuadrado del número de usuarios conectados del sistema (n2).

- Ataques en el Ciberespacio

Estos tienen varias motivaciones, ejecutores y objetivos. Los tres tipos conocidos de ataques (CNA, CNE y CNI).

Estas embestidas son ejecutadas por varias entidades, Estados no gubernamentales, grupos e individuos. Algunos son realizados por contratados agresores, principalmente cuando el Estado no desea ser asociado con el ataque. Las motivaciones para todo tipo de agresión pueden ser ideológicas, criminales (principalmente robo monetario), robo comercial o tecnológico, de secretos, patentes (información protegida bajo los derechos de los inventores); espionaje (robo de secretos de Estado), incrustado en luchas de poder o realización de políticas.

Los ciberataques son parte de un plan para que un Estado gane intereses. Sin embargo, no hay evidencia de que alguno se haya dado cuenta de su interés solo a través de ataques cibernéticos.

Aun así, se debe tener en cuenta que ninguna nación ha tomado crédito por un ciberataque y ha sido capaz de medir el éxito del ataque.

### 2.5.2. Intervención/Propuesta para G5G

En los últimos años, los pensadores militares se han centrado en la guerra de "cuarta generación", es decir, en los conflictos por ideas, librados por lo que el autor John Robb llama "guerreros ad hoc". Compárese con la guerra industrializada de "tercera generación" librada por los ejércitos tradicionales por la tierra y los recursos. Estados Unidos y sus aliados ya son buenos en la guerra de tercera generación. Y tras cinco años de guerra en Irak, también empiezan a ser bastante buenos en la 4GW, sobre todo a la hora de animar a los iraquíes de a pie a rechazar las visiones del mundo de los partidarios de la línea dura.

Pero la próxima generación de guerra -la llamada "quinta generación"- no tendrá ejércitos ni ideas claras. Será lo que el comandante del ejército estadounidense Shannon Beebe, máximo responsable de inteligencia en África, llama un "vórtice de violencia", una batalla campal de destrucción sorpresiva motivada más por la frustración que por cualquier plan coherente para el futuro.

La 5GW es lo que ocurre cuando los desafectos del mundo dirigen su desesperación hacia el símbolo más evidente de todo lo que les falta, aprovechando las tácticas y los campos de batalla iniciados por guerreros de cuarta generación más organizados. El símbolo es Estados Unidos, una superpotencia mundial. Y el arma elegida por los combatientes de quinta generación es el "estancamiento" político, afirma el teniente coronel de los marines Stanton Coerr, en un nuevo artículo publicado en la Marine Corps Gazette.

"Los combatientes de quinta generación ganarán al ... señalar la impotencia del poder militar secular. ... Estos combatientes ganan al no perder, mientras que nosotros perdemos al no ganar".

El campo de batalla será algo extraño: el ciberespacio, o el suministro de agua de Cleveland, o los sistemas bancarios de Wall Street, o YouTube. La misión será infundir miedo, y tendrá éxito.

La G5G está anclada en la yihad islámica global propugnada por Al Qaeda, escribe Coerr. Pero eso no significa que los guerreros de quinta generación sean necesariamente claramente ideológicos, con aspiraciones de establecer sistemas políticos alternativos. Son oportunistas, con la única intención de destruir. Pero incluso la violencia aparentemente inútil puede tener una lógica perversa, ya que la destrucción repentina e irracional socava la idea de que las naciones -y especialmente una nación poderosa, Estados Unidos- son viables en el mundo moderno.

Entonces, ¿cómo se vence a un enemigo de quinta generación? En primer lugar, no luchando. Beebe dice que acabar con la vorágine de violencia en África significa aliviar

"las condiciones de los seres humanos que crean estas inseguridades a través de las fronteras estatales". En otras palabras, centrarse en el desarrollo económico, la ayuda humanitaria y la comunicación, sin que haya un M-16 o un tanque Abrams a la vista.

En palabras de Coer, "el éxito variará inversamente a la violencia exportada". (Axe, D., 2009)

### 2.5.3. Objetivos de la Propuesta

Crear programas de intervención psicológica para filtrar información nociva de potencias neoliberales, colonialistas y hegemónicas.

Difundir dietas alimentarias sanas para desechar la “comida chatarra.”

## 2.6. Estrategia Organizacional y Organización de las FFAA, Castrense y FS (Fuerzas de Seguridad).

Se sabe desde tiempos pretéritos de las diferentes jerarquías militares que existen en las diferentes FFAA, Gendarmería, Prefectura y FS. Ya desde el Antiguo Egipto, la Antigua Babilonia, El Imperio Persa, El Imperio Romano, todos estos hacen más de 2.000 años, tenían en sus ejércitos un diferente o similar estilo de jerarquías o rangos militares.

Las armas por excelencia eran la espada y las flechas. No existían mensajes codificados, como el de la famosa máquina alemana de la Segunda Guerra Mundial llamada “Enigma”,

decodificada por las inglesas Alan Turing. No había toda la tecnología que existe ahora, y las batallas eran más “directas” y al grano.

Desde esos tiempos, dichas estructuras han sido verticales hasta la actualidad y mismo en las dos guerras mundiales, las diferentes FF.AA. (Ejército, Armada y Fuerza Aérea) se han mantenido desde un punto de vista independientes. Cada una en lo suyo.

Hoy en día, con las guerras asimétricas, guerra de guerrillas, enemigos “invisibles” (Vietnam), guerras psicológicas, psicotónicos, cibernéticas, informáticas en el ciber-espacio y afines, ha despertado otra Guerra Fría. Pero esta no es ideológica (Capitalismo vs. Comunismo), sino que es una guerra invisible y apropiación de los recursos naturales (RRNN), sobre todo el agua, y las superpotencias están muy conscientes de ello.

De allí, que una muy tímida estrategia a implementar para hacer frente a una G5G podría ser reestructurarse militarmente y de esa manera cada brazo de las FF. AA., Gendarmería, Prefectura y FS, cada una tiene acceso al conocimiento del actuar de la otra en este campo de batalla virtual.

Cada Fuerza (Ejercito, Prefectura, FS, etc.) podrian trabajar en tándem. El enemigo es virtual y ataca a la mente de las diferentes Fuerzas, no al cuerpo, y el trabajo de Icia (AFI) más la Icia de las respectivas Fuerzas será descomunal, cooperando para la acción de contrainteligencia.

Las “subdivisiones” se refieren a “romper” las estructuras tradicionales porque una Guerra de Quinta Generación dejó de ser una batalla tradicional. Las Fuerzas se deben “reinventar”. Un almirante debe trabajar con un teniente general y un brigadier, a ellos, se deberían sumar escalafones inferiores de las Fuerzas. Las demarcaciones de las Fuerzas deben de desaparecer, sin embargo, se deben intercambiar conocimientos básicos entre sí de cada Fuerza.

Cada Fuerza debe entender la jerga de la otra ya que el enemigo está por todas partes, nos rodea de manera invisible y por ese motivo es preciso detectarlo rápidamente.

En la distribución interna debe de haber especialistas abocados en una tarea específica, en cada Fuerza. Debe existir un cuadro/grupo/departamento de asuntos informáticos, de neurociencias, de todas las Ingenierías, psicólogos, químicos, bioquímicos, economistas, genetistas, Ing. Sociales/Humanos, geógrafos, programadores, de IA y un Comandante de Operaciones Especiales para Coordinar todos los esfuerzos (análogo a la NASA en las

Misiones Apolo 11 a 17). El conocimiento del idioma inglés es mandatorio para todas las Fuerzas o al menos básico para los altos rangos.

Para lograr una buena Estrategia de Gestión de las Fuerzas, se debe de hacer un previo Análisis. Esta cuenta de 5 pasos:

1 - Especificar los objetivos de las Fuerzas (ya hecho anteriormente).

2 - Realizar un análisis externo e interno (ver Fig. 1).

3 - Desarrollar una ventaja competitiva.

4 - Elegir la ventaja competitiva.

5 - Diseñar la Estructura Organizativa (ya hecha). Paso-1 (Análisis Externo)

También se deben estudiar los futuros clientes, posibles competidores, socios y los posibles proveedores. Desde un punto de vista militar, el aliado. Lo segundo se analiza al análisis externo comienza con los clientes ya que estos pueden pasar a ser proveedores porque es fundamental comprar tecnología de punta, obtener Icia foránea, y adquirir conocimientos inexistentes en Argentina. La competencia es lo tercero que se analiza ya que siempre están al acecho.

Para esto se analiza el Mercado (en donde está parada la Argentina en una posible G5G). Se debe analizar el sector de donde se encuentra ubicado nuestro país (la geopolítica y su corriente y futura dinámica).

Para identificar el Mercado (G5G), se debe de identificar el producto (los pros y contras que posee Argentina militarmente), con esto hecho se identifica o se capta mejor el mercado (G5G) y a los competidores (*hackers*, criminales cibernéticos, etc.). Se evalúa la estructura del Mercado (se analiza al enemigo y sus armas que lo haría fuerte en una G5G), su tamaño (tecnología, número de especialistas, etc.), y el número de las empresas (están solos, poseen aliados, etc.).

Son los socios y los posibles socios lo que más se debe analizar, estos pueden estar entre los clientes y proveedores. Tener el apoyo de los socios es muy significativo para lograr una ventaja competitiva (hacer replegar al invasor virtual).

En un segundo paso, se realiza éste para saber si hay que modificar algo en la estructura de la empresa (estructura y organización de las Fuerzas), para que se adapte a los nuevos objetivos fijados y a la estrategia (escenarios de batalla cambiantes).

El procedimiento en este caso incluye una serie de medidas de acción y no de pensamiento. Son pasos a seguir cronológicamente para desarrollar una labor eficaz. El procedimiento cuenta con actividades a desarrollar.

Una vez que las Fuerzas están organizadas y estructuradas de manera ágil y con una referencia horizontal y no vertical, y habiendo hecho los análisis externo e interno, se comienza con lo/s procedimiento/s.

En forma general, ya que no es la función de este TFI describir una y cada uno de todos los procedimientos de una Fuerza nacional, se dará una sinopsis de la técnica y de las actividades a desarrollar.

Las guerras modernas utilizan redes digitales extensivas. Conceptualmente hablando, cuatro cuadrículas virtuales interconectadas e interdependientes donde la información, detección, efectos y comando, están sobre el teatro de operaciones. Los elementos de varias fuerzas son nodos interactuando en las grillas en donde cada una recibe, actúa y transmite los datos hacia adelante.

Como corolario, las Fuerzas Argentinas deben “cablear” el territorio nacional en sus puntos más débiles, en donde los datos puedan fluir del campo de batalla hacia los centros de análisis de la información digital.

Al trabajar juntas, las redes pueden formar una nube de combate virtual, similar a la computación en la nube comercial, que permite a los usuarios extraer y agregar datos según sea necesario.

El resultado son compromisos tácticos de mayor alcance. Ya no es más, "dispara cuando veas el blanco de sus ojos", sino más bien, "activa cuando un símbolo etiquetado como ‘adversario’ aparece en una pantalla compartida".

Todas las Fuerzas argentinas deben comprender el funcionamiento de los “combates en la nube”. No se puede pelear una G5G siendo un ignorante en esta tecnología. El enemigo se puede ver a cientos de kilómetros, usando un monitor de computación, sin movilizar todo un regimiento. La capacitación y la práctica en simulaciones virtuales son imperativas.

Hay cinco dominios operativos: terrestre, marítimo, aéreo, espacial y cibernético. La idea clave de animación es la sinergia entre dominios, donde la fuerza se aplica a través de dos o más dominios de manera complementaria para lograr una ventaja operativa.

Todas las Fuerzas deben de trabajar al unísono ya que estas G5G son de multidominio y pelean en cuatro frentes en donde la sinergia entre dominios hace la diferencia para obtener una ventaja operativa.

Todas estas áreas están interconectadas de manera digital, por lo tanto, Ing. en Sistemas, especialistas en IA, programadores, ing. electrónicos, rastreadores de señales digitales, y oficiales de alto rango, deben de trabajar otra vez concatenadamente, con un Jefe de Operaciones. todo esto para multivariar en estas técnicas digitales, de rastreo, IA, electrónica, programación y con una base operativa en las Fuerzas para repeler y contraatacar.

El concepto de guerra de fusión aborda las preocupaciones de comando y control que surgen de flujos de información adicionales, incompatibilidades de *software* y vulnerabilidades intrínsecas al ataque y al engaño.

El procedimiento en este caso consiste en chequear la grilla de nodos de forma remota para identificar en dónde está la falla. Los programadores pueden encontrar errores en el *software*/s, los controles de calidad deben hacerse a la orden del día.

Al adentrarse a una GW5 las Fuerzas se encontrarán con varias implicancias, es decir, contrariedades. Primero, obviamente hay dos vulnerabilidades técnicas incorporadas. Los sistemas digitales son inherentemente susceptibles a intrusiones cibernéticas que pueden robar, eliminar, cambiar datos o insertar falsos que pueden propagarse rápidamente a través de la red. Si bien las técnicas de ciberseguridad están mejorando constantemente, también lo hacen los métodos de intrusión cibernética, sin que ninguno permanezca en ascenso por mucho tiempo. Las técnicas de guerra electrónica y de información están diseñadas para ingresar deliberadamente datos falsos en redes hostiles que se propagan a todos los usuarios, confundiendo y distorsionando la imagen compartida. Además, la Guerra de Quinta Generación se basa en enlaces de datos. Los emisores son inherentemente vulnerables a la detección; Los participantes de la red pueden ser localizados y rastreados, y por lo tanto dirigidos por armas guiadas con precisión. Algunos enlaces de datos son más difíciles de detectar que otros, sin embargo, como con el ciber, la tecnología mejora continuamente. La seguridad cibernética y el seguimiento de emisiones de enlace de datos requerirá un esfuerzo constante para la vida operativa de la Guerra de Quinta Generación son serios talones de Aquiles.

Segundo, las guerras modernas inevitablemente involucran operaciones de coalición, por lo que en cualquier red puede haber actores de muchos países diferentes. Todos los involucrados harán lo mejor que puedan, pero dentro de las fuerzas de cada país y dentro de

la coalición en general habrá elementos que utilizarán diferentes fuentes de inteligencia, bibliotecas de amenazas y datos de firma electrónica para tomar decisiones sobre la identidad y la ubicación de hostiles y amistosos. Fuerzas y entidades neutrales. Los peligros operativos implícitos en el aforismo de "basura adentro, basura afuera" sugieren que algunos elementos de fuerza serán más confiables que otros en la Guerra de Quinta Generación. Es probable que las redes “balcanizadas" (en las que algunos nodos sean ignorados o reciban datos degradados), dejen a algunos nodos potencialmente peleando sus propias guerras separadas en lugar de ser parte de una aplicación coherente y cuidadosamente coordinada de la fuerza militar de la coalición.

La reducción de una fuerza a una colección de redes pequeñas e independientes socava la lógica de la ley de Metcalfe de la G5G, que afirma que el "poder" de una red es proporcional al cuadrado del número de nodos en la red. La probabilidad de enfrentamientos azul sobre azul (dos elementos del mismo ejército se eliminan) también aumenta a medida que la ubicación de las fuerzas amigas se vuelve menos segura para todos los participantes de la coalición.

Tercero, la soberanía nacional individual se ve disminuida, especialmente en el concepto de nube de combate, ya que la información se extrae de la nube digital con un conocimiento quizás limitado de su fuente. El uso de dicha información externa, en lugar de la derivada de los propios sensores integrados como ocurre hoy para atraer objetivos reduce inherentemente la responsabilidad y la responsabilidad de cada nación. Un ex oficial de la RAF se quejó de que "esto mata la postura legal [del Reino Unido] sobre una cadena de asesinatos clara, inequívoca y soberana”.

Cuarto, la idea de Guerra de Quinta Generación se relaciona con lo que Edward Luttwak llamó "la dimensión técnica de la estrategia". La tecnología influye en la forma en que luchamos en las batallas, pero el éxito tiene más que la tecnología. Una de punta fue insuficiente para ganar las guerras de Vietnam, Irak y Afganistán, y la G5G hasta ahora no parece ser diferente.

Y, por último, el final de la Guerra de Quinta Generación puede estar a la vista. En la década de 1990, los futuristas Alvin y Heidi Toffler argumentaron que "cómo hacemos la guerra refleja cómo hacemos riqueza". Previa que la era de la tecnología de la información obligaría necesariamente a cambios en la guerra. En muchos aspectos, la G5G es el resultado de esa idea. Ahora, algunos ven que se aproxima otra revolución industrial que cambiará la

forma en que se hace la riqueza. Si los Tofflers tienen razón, la batalla puede cambiar nuevamente.

Los 3 tipos de ataques cibernéticos fueron identificados por “objetivos, diseño y estrategia”, como: Ataque a la Red Informática (CNA); Explotación de la Red Computacional (CNE); e Influencia a la Red Computacional (CNE).


Fig. 4 Ciberataques y sus componentes

Explicación de la Figura 4

VLC : Reproductor multimedia VLC: se puede utilizar como servidor y como cliente para transmitir y recibir transmisiones de red. VLC puede transmitir todo lo que puede leer la mayor parte de la funcionalidad

VLS ahora se puede encontrar en VLC Smart Grid: Grilla Inteligente

Red Celular Redes ópticas

IOT: Internet de las Cosas Comunicaciones Satelitales

WSN: La red inalámbrica de sensores (WSN) se refiere a un grupo de sensores espacialmente dispersos y dedicados para monitorear y registrar las condiciones físicas del entorno y organizar los datos recopilados en una ubicación central.

Al ser de naturaleza *ad hoc*, VANET es un tipo de redes que se crea a partir del concepto de establecer una red de automóviles para una necesidad o situación específica. Los VANET ahora se han establecido como redes confiables que los vehículos usan para fines de comunicación en carreteras o entornos urbanos.

La Tele-Healthcare (telesalud) implica el uso de telecomunicaciones y tecnología virtual para brindar atención médica fuera de las instalaciones tradicionales de atención médica.

mmWAVE:

La onda milimétrica es una banda de espectro no desarrollada que se puede utilizar en una amplia gama de productos y servicios como redes inalámbricas de área local (WLAN) de punto a punto de alta velocidad y acceso de banda ancha. Los enlaces de datos de corto alcance sin licencia se pueden usar en una onda milimétrica de 60 Ghz.

La interferencia entre múltiples estaciones base que coexisten en la misma ubicación limita la capacidad de las redes inalámbricas. En este teatro de operaciones se propone un método para diseñar un esquema de transmisión de enlace descendente cooperativo espectralmente eficiente que emplee la precodificación y la formación de haces para sistemas de múltiples usuarios de múltiples entradas-múltiples salidas (MIMO).

CRN convierte la radio en un poderoso medio de marketing que brinda a las marcas de consumo una notable ventaja competitiva. Es un arte y una ciencia.

5G es la quinta generación de tecnologías de comunicaciones inalámbricas que admiten redes de datos celulares. Una mejora muy anunciada para las tecnologías anteriores, los defensores afirman que revolucionará las comunicaciones móviles y acelerará el advenimiento de IOT. La adopción a gran escala comenzó en 2019 y hoy prácticamente todos los proveedores de servicios de telecomunicaciones en el mundo desarrollado están actualizando su infraestructura para ofrecer la funcionalidad 5G.

## 3.0. Conclusiones

Evaluación del Interrogante Inicial y Objetivos Propuestos

Si se realiza un enfoque regional, nuestro país podría convertirse en una potencia cibernética tanto en telecomunicaciones como en teatro de operaciones virtuales.

Si bien Argentina no parece tener hipótesis de conflicto inminentes, es mejor estar preparados que estar arrepentidos porque de obtenerse esos equipos y herramientas, colocarían a la Argentina en uno o el único país más adelantado en el cono sur, listo para enfrentar una G5G.

La importancia de las tecnologías de la telecomunicación queda evidenciada en una “nueva Guerra Fría” o “guerra tecnológica”. Nadie está afuera de esta carrera. La mayoría de

los países hegemónicos son víctimas de espionaje político, militar e industrial, sabotajes y cibernéticos.

Si esto ocurre en los países que son potencia mundial, qué nos queda los que estamos en vías de desarrollo y tercermundistas. Las TIC y las tecnologías digitales son fundamentales para pelear una G5G, y Argentina está "asomando" muy tímidamente su cabeza.

Con la prestación de territorio y espacio aéreo a otros países, eso dejó endebles los planes de seguir desarrollando lo que prometía un "despegue" satelital, como el ARSAT 1 y 2.

Existe una carrera hacia las telecomunicaciones móviles de 5G, donde la batalla o batallas que se liberan es por el control, supervisión e información del planeta.

Argentina, por causas que no vienen a este TFI, desactivo "El Programa Conectar Igualdad". De volver a ellos serían totalmente obsoletos. Se ha perdido poder de innovación y creatividad. Dichos proyectos fueron el Arsat 1 y 2. Nuestra nación cometió un grave error al no integrar las redes (habladas y nombradas anteriormente en este TFI) de los operadores privados y acrecentando su aislamiento.

El posicionamiento geopolítico del país en materia de telecomunicaciones no fue atendido convenientemente ya que no se consiguieron integraciones reales con países de la región ("socios"), tampoco se consiguieron sustanciales avances en conseguir los derechos de aterrizaje de satélites argentinos en países del continente.

## 3.1. Limitaciones

La posible falta de presupuesto, tan común en países latinoamericanos, en donde el gasto se utiliza en cosas superfluas, olvidándose, ya sea por ignorancia o desconocimiento o falta de experiencia mundial en atender conferencias en países potencia y tratar de venir con nuevas ideas para aplicarlas en Argentina. No es el caso de las FF.AA

La posible limitación de capital humano, tan esencial para desarrollar la estructura de telecomunicaciones en la Nación, la capacitación, limitante que no deja crecer a ingenieros, programadores, especialistas en IA, técnicos en electrónica, robótica, Ingenieros Aeronavales, y afines, hunden más a Argentina en arenas movedizas a corto plazo. Para aproximadamente el año 2030 y ni siquiera se podrá poseer un Centro de Investigaciones Aplicadas avanzado porque este será considerado anticuado y obsoleto.

La falta de diseminar horizontalmente estos conocimientos, hacen que no puedan "comunicarse" entre cualquier organismo/s. De esta manera "la mano derecha" sabe lo que "la mano izquierda" está haciendo.

## 3.2. Alcances

Argentina con sus políticas tuertas, que no saben si son a corto o largo plazo, es muy difícil que pueda dilucidar y con una mente criteriosa saber la importancia que debe de estar preparada para una G5G. La Nación se ha estancado en el tiempo, en G4G debido a la subversión en el país de los años 70s, contra la guerrilla, y en la G3G, la Segunda Guerra Mundial. Debe de existir una razón que podría ser analizada por un psicólogo que bucea en el subconsciente de las Fuerzas y de los Gobernantes de turno, que no solamente jueguen muy bien al fútbol, sino que se den cuenta de que nuestra Nación ya está haciendo atacada por todo tipo de herramientas "sutiles" que apuntan a la mente de, no solo de las Fuerzas, sino también de la población del país.

Tampoco Argentina cuenta con una infraestructura logística y presupuestaria para armar un teatro de operaciones electrónico, es decir, del uso a *full* de las telecomunicaciones. Para ello se debe capacitar en breve tiempo a las tres Fuerzas (FFAA, Castrenses y FS). Este TFI llegó a un punto en donde caería en la redundancia en cuanto a temas, porque todos se sumergirían en el mismo fango por lo cual sería aburrido y reiterativo.

Uno podría "meterse" en lo que hacen las potencias, pero se debería enviar a las mejores mentes y jóvenes aún para aprender de las telecomunicaciones 5G, drones más modernos, robótica, trajes de combate muchos más sofisticados totalmente "cableados y con sensores remotos que miden la fisiología del combatiente en tiempo real y muchas más técnicas, que hacen a una 5G y G5G.

En el aspecto cibernético, si uno toma en cuenta el ciberdelito que los EE. UU. sufren por día, si eso llegara a pasar en Argentina, a menor escala obviamente, no habría manera de defendernos y rastrear de dónde llegó la señal de un/os hackeador/es. Tampoco se sabría de qué país arribó. Podría ser cualquiera, todo sea para robar material *Top Secret*.

Para poder adentrarnos en la estrategia de Icia que Argentina debe adoptar para pelear una G5G, el Ministerio de Seguridad debe entender la teoría detrás de estas.

Como resultado del estudio de las nuevas formas de guerra en los últimos 30 años, dos tipos de guerras han sido identificadas. Una de ellas es la "guerra cibernética" (*cyberwars*), que está definida como un conflicto relacionado a la información al nivel militar, en donde se trata de lograr la disrupción o eliminar los sistemas de información y comunicación del enemigo.

Esta se caracteriza por una alta tecnología, especialmente en las comunicaciones y la Icia, en donde se requiere que las FFAA puedan operar como una red interconectada (*interconnected network*) versus jerarquías institucionales. En simples términos, "una guerra cibernética (G5G) es esencialmente una guerra de G3G hecha ampliamente más letal por el uso de las tecnologías de la información.

Los altos perfiles de ciberataques, fugas, y las campañas de desinformación en 2017, ha elevado la importancia de la Ciberseguridad. Los líderes corporativos y oficiales gubernamentales se han percatado que ahora la Ciberseguridad es un punto neurálgico y estratégico, uno que puede amenazar la reputación de una organización entera o inclusive socavar los procesos políticos de un Estado.

Si bien los líderes tal vez hayan reconocido la importancia de estar preparados para este tipo de ciber amenazas, pocos entienden cómo proceder. El año 2018 fue caracterizado como un tiempo de adaptación. Un punto muy importante fue el de construir organizaciones más cohesivas, comunicación simplificada (*streamlined comunicaciones*), yendo del departamento de Información Tecnológica (IT) hasta el nivel ejecutivo.

Muchos gobiernos han sido históricamente tardíos en temas de ciberseguridad, pero en dicho año los han visto más asertivos. Las nuevas medidas tomadas en torno a la ciberseguridad en la Unión Europea traerán aparejada medidas y regulaciones más rígidas, medidas que afectarán y están perjudicando al mundo de los negocios.

El programa nacional en el ciberespacio debe de incluir organizaciones y corporaciones locales, que, de ser perjudicados, ocasionaría daños a la economía y eventualmente a la seguridad nacional. La fragilidad del ambiente civil demanda una apropiada respuesta. Una de esas herramientas que pueden mejorar la defensa del espacio civil es la regulación en el campo de la ciberseguridad. Los puntos más importantes para una propuesta de mejora están descritos a continuación.

Se debe incluir en el campo de la ciberdefensa un componente estructurado de procesos estatutarios, en los estadios de establecer nuevas iniciativas de negocios (autorización en los varios comités de planeamiento), y en los procesos operacionales respectivos (ley de licencias comerciales).

El establecimiento de cualquier negocio en Argentina requiere el cumplimiento de los procesos legales de planificación y el empresario debe obtener la autorización de los comités

de planificación para varias áreas, incluidos los servicios de bomberos y rescate, salud pública, protección del medio ambiente, materiales peligrosos y protección frente al hogar.

La propuesta es que, dentro de esta estructura, cada empresario está requerido a relacionarse con el tema relevante de la defensa cibernética a través de una encuesta o informe. Este documento servirá como la herramienta principal para determinar la exposición de nuevas iniciativas a la posibilidad de ataque cibernético y para formular la defensa contra esta probabilidad.

Además de las nuevas iniciativas, se propone utilizar el proceso de licencia comercial que requiere renovación periódica para garantizar que la actividad de la empresa con el tiempo cumpla con los criterios obligatorios en varios campos, incluida la protección y defensa contra el ciberataque.

En cuanto a la identidad del regulador en el campo cibernético, existen dos opciones: El primero es establecer la regulación por sector con el regulador de los sectores relevantes. Por ejemplo, la regulación en el campo de la defensa cibernética del sistema de salud será determinada por el Ministerio de Salud; la de las corporaciones del agua será determinada por el Ministerio de Defensa o crear un Ministerio de Infraestructura; y así sucesivamente.

La segunda opción es la regulación a través de un regulador central, con sede en el ciber buró y la Autoridad de Defensa Nacional (la Defensa Nacional elevada al nivel de Autoridad, más jerárquica) que aún no se ha establecido. Debido a la complejidad tecnológica de los medios de defensa y la necesidad de preservar un nivel uniforme de seguridad, así como a la preocupación de que la regulación sectorial pueda crear una "Torre de Babel" de instrucciones de seguridad en los diversos sectores, la manera más eficiente es determinar un marco profesional uniforme para la defensa en el sector civil. Esto sería similar a otros reguladores centrales, como los Servicios de Bomberos y Rescate, y el almacenamiento de sustancias peligrosas. La defensa del sector civil es tan importante como la defensa del sector militar y sus dependencias. No pueden trabajar separadamente al momento de una G5G. Las empresas también guardan información muy sensible, como bases de datos de carácter económico que también hace a la defensa nacional. Las FFAA, el sector castrense y las FS deben de mantener una fluida comunicación, en donde la mano derecha sabe lo que la mano izquierda hace.

En una era en donde los ciberataques, los hackers, ciber terroristas y la violación del “espacio ciber aéreo”, munido con las tecnologías de la información, en donde una guerra se basa en la información de carácter digital, los militares y las corporaciones deben de trabajar

al unísono ya que estas últimas son un pilar muy fuerte en donde los militares pueden apoyarse.

"Un año atrás (2016), el Banco Interamericano de Desarrollo (*IDB* en inglés), y la Organización de Estados Americanos (*OEA* en inglés), se hicieron la pregunta si Latino América (LA), incluyendo a Argentina, y el Caribe estaban preparados para temas de ciberseguridad. La conclusión en un estudio de 200 hojas fue esencialmente "No". Esto hizo sonar la alarma acerca de Latino América y Argentina en este escenario de la ciberseguridad. El reporte demostró que LA y Argentina son extremadamente vulnerables a los devastadores ataques cibernéticos. Cuatro de cinco Estados carecen de estrategias de ciberseguridad o planes para proteger la crítica infraestructura. Dos en tres carecían de cualquier tipo de comando de control frente a un ataque de ciberseguridad. La ejecución de las leyes contra ciberataques era universalmente extremadamente débil.

En los últimos 12 meses hubo un giro positivo de 180 grados. Por ejemplo, Argentina, que fue anfitriona del G-20 en 2018, el presidente Macri se reunió con el de los EE. UU., Donald Trump, para tratar temas bilaterales en trabajos de ciberseguridad para que ambos estados estén unidos en la lucha contra la cibercriminalidad. A su vez, para que se apunte al espacio abierto del ciberespacio, seguro y confiable. Los dos aliados buscan incrementar la coordinación en sus políticas cibernéticas de seguridad y en la protección vital de sus infraestructuras estratégicas y tratar de ir hacia adelante con tratados de socios privados y gubernamentales en la protección de infraestructura clave.

Finalmente, Argentina estaría preparada para tomar medidas en una supuesta G4G. Los factores aquí presentes para ganar este tipo de guerras es la Icia en sus variadas formas. Es imperativo el contacto con los lugareños y el pueblo.

Según otras líneas de pensamiento americanas, es imprescindible conocer los métodos y tácticas de los actores que inician una G4G, como saber la dinámica de las Revoluciones de Colores, y de qué manera se usan las redes sociales para desparramar información. Las tecnologías son bajas, pero demostraron tener éxito frente a la ex Unión Soviética y contra los EEUU.

En una G5G, Argentina está en desventaja contra actores que aún no son jugadores principales en el tablero de ajedrez. Recién está organizándose con una nueva Estrategia Nacional de Ciberseguridad en 2019, y el PFPDTC puesto en acción también en 2019. La tecnología para contrarrestar un ciberataque ya sea del crimen organizado, otros Estados, no-

Estados, etc., está recién organizándose, capacitando a personal adecuado y adquiriendo *hardware* y *software* imprescindible para la ciberseguridad.

Argentina no cuenta con una contraofensiva cibernética. Adquirir tal tecnología no es fácil y solo las superpotencias como los EE.UU., Rusia y China están capacitadas de provocar ciberataques poderosos. (ejemplos, Siria y Venezuela), como el puesto en Estonia por Rusia en 2007, volviendo a un país a la edad de piedra por cierto tiempo.

Los actores mundiales principales son, como siempre, las naciones mencionadas anteriormente sumada Corea del Norte, y de a poco se le van sumando actores ya de segundo nivel como son Irán e Israel. Ya ha habido ciberataques a cuentas bancarias de empresas multinacionales, como UBER, Bancos, sistemas de seguridad en países de LA, el apagón general que aconteció en junio de 2019 que afecto a Argentina, Brasil, Paraguay, Uruguay, y Chile. Estos cibercriminales, pertenecientes a servicios de inteligencia de diferentes gobiernos o no, tienen la tecnología como para "apagar" una central nuclear, hidroeléctrica, geotérmica, mareomotriz, eólica o solar, etc., cortando el suministro de electricidad a un país entero, región o localidad.

En el aspecto militar, pueden interrumpir las telecomunicaciones entre los satélites geoestacionarios, a 30 mil kilómetros de la superficie terrestre ocasionando "silencios" en las telecomunicaciones móviles, de GPS, de tareas de monitoreo, militar o no, de celulares, canales de televisión, cortés a la internet y afines.

Utilizando la Ingeniería Social, juntamente con las TIC y un plan de Geopolítica Estratégica, se podría derrocar gobiernos no amigables a los intereses políticos, económicos e ideológicos de los EE. UU. o Rusia (caso Venezuela).

Un caso de libro de texto es la situación por la cual está pasando Bolivia con su expresidente Evo Morales. Aquí, se presenta una Revolución de Color con la agitación de las masas que obtienen una mentalidad de colmena.

Los militares le pidieron a Evo Morales su renuncia con la excusa de que dicho acto iba a calmar al pueblo. El exdirigente boliviano de ascendencia aimara renuncia y pide asilo político en México, aliado político de Bolivia bajo su administración.

## 4.0 Bibliografia


A., C. S. (s.f.). Initial Periods of Wars and Their Impact on a Country's. Preparations for a Future War. *Military Thought (English edition)*, pp. 24-25.

Axe, R. (2009). How to win a 5th generation warfare. WIRED.

Babacek, M. (2018). Psychotronic and Electromagnetic Weapons: Remote Control of the Human Nervous System. *Global Research*.

Birnbaum, M. (15 de octubre de 2014). Russia's Putin signs law extending Kremlin's grip over media. *The Washington Post*.

Blandy, C. (marzo de 2009). Provocation, Deception, Entrapment: The Russo-Georgian Five- Day War. *Defense Academy of the United Kingdom*.

Braidot, N. (2016). *Neurociencias para tu Vida*. Buenos Aires: Editorial Granica.

Brewster, M. (30 de junio de 2016). Canada to send troops to Latvia for new NATO brigade. *CBC*.

Committee, D. (2016). Oral evidence: Russia: Implications for UK Defence and Security, HC 763. *Parliament UK*.

Daugherty, J. (2015). How the Media Became One of Putin's Most Powerful Weapons. *The Atlantic*.

Gutiérrez, R. A. (2019). Investigación Holística. Global Cyber Security Capacity Centre at the University of Oxford. . *El Economista*.

Iasello, E. (2015). Fixing U.S. National Cybersecurity: A Modest Proposal for Swallowing Pride and Reducing Egos.

Jamison, E. R. (2006). Intelligence Strategy for Fourth Generation Warfare. Ciberataque en Argentina. *El Economista*.

Jamison, E. R. (2019). Intelligence Strategy for Fourth Generation Warfare. Ciberataque en Argentina. *El Economista*.

Kanghao, J. (2008). Beyond the Fourth Generation. A Primer on the possible Dimension of a GW5 Generation Warfare. *Pointer Journal of the Singapore Armed Forces: Vol. 44 No 3.*

Kasapoglu, C. (2015). Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control. *NATO Defense College*. Obtenido de http://www.ndc.nato.int/news/news.php?icode=877

Kinzinger, A. (2018). The 5th domain: Cyber defense needed in the 21st century. *The Washington Times*.

Korybko, A. (2019). Revoluciones de colores y guerra no convencional. En A. Korybko, *Guerras híbridas*. Buenos Aires: Batalla de Ideas.

Lavinder, K. (2016). Latin America: The New Frontier for Cyber Attacks. *The Cipher Brief. IEEE innovation at work*. Obtenido de The Cipher Brief: https://innovationatwork.ieee.org/latin-america- is-under-cyber-attack/

Layton, P. (2018). Fifth-Generation air warfare. *Australian Government. Department of Defence*.

Martorano, J. (2012). Nuevo teatro de operaciones. La Guerra de V generación se está aplicando en Venezuela. *aporrea.org*.

Mordovets, S. a. (1 de noviembre de 2014). Putin's Friend Profits in Purge of Schoolbooks. *New York Times*.

Nimmo, B. (s.f.). Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It. *stopfake.org*.

Pauwels, E. (02 de 05 de 2019). *The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI.* Obtenido de United Nations University: https://cpr.unu.edu/research/projects/the-new-geopolitics-of-converging-risks-the-un-and-prevention-in-the-era-of-ai.html#outline

Purkayastha, K., 2020. Fragments of Reality. Challenges from malicious use of AI. Dailyobserver. Recuperado: dailyobserverbd.com

Rodríguez, Y. (06 de junio de 2019). Inteligencia de Fuentes Abiertas (OSINT): Características, Debilidades y Engaños. *GESI, Grupo de Estudios en Seguridad Internacional*.

Shevardnadze, S. (19 de febrero de 2016). Intellectual level of British leadership so low, it's shocking – European Politics Scholar. *RT*. Obtenido de https://www.rt.com/shows/sophieco/332958-intellectual-level-british-leadership/

Shteyngart, G. (18 de febrero de 2015). Out of My Mouth Comes Unimpeachable Manly Truth. *New York Times*. Obtenido de http://www.nytimes.com/2015/02/22/magazine/out-of-my-mouth-comes- unimpeachablemanly-truth.html

Szostek, J. (7 de julio de 2016). News media repertoires and strategic narrative reception: A paradox of dis/belief in authoritarian Russia. *New Media & Society*.

Turnero, P. (5 de septiembre de 2018). ¿Qué es la Ingeniería Cognitiva? *The World Today*.

Vallejos Diaz, V. (2008). Forma de hacer un diagnóstico en la investigación científica. *Perspectiva holística*.

Vargas Alarcon, C. A. (agosto de 2017). *Ingenieria Humana*. Obtenido de es.scribd.com: https://es.scribd.com/document/367558533/Ingenieria-Humana

Veenendaal, P. B. (2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. *8th International Conference on Cyber Conflict, NATO Cooperative Cyber Defense Centre of Excellence*.

Watkins, A. (23 de junio de 2016). Senate Committee Looks To Revive Cold-War Era Body To Catch Russian Spies. *BuzzFeed.News*.

Wesolowsky, T. (16 de junio de 2016). Kremlin Propaganda In Czech Republic Plays Long Game To Sow Distrust In EU. *RFE/RL*.

# 5.0. Glosario

5G

La tecnología inalámbrica 5G está destinada a ofrecer velocidades máximas de datos de varios Gbps más altas, latencia ultrabaja, más confiabilidad, capacidad de red masiva, mayor disponibilidad y una experiencia de usuario más uniforme para más usuarios. Un mayor rendimiento y una mayor eficiencia potencian nuevas experiencias de usuario y conecta nuevas industrias., 110

ARSAT I

Satélite de comunicaciones geoestacionario operado por la empresa propiedad del Estado argentino ARSAT. Fue construido por la empresa argentina INVAP., 113

Arsat II

Satélite de comunicaciones geostacionario íntegramente diseñado, construido y ensayado por la empresa argentina INVAP,2 el cual es operado por la compañía ARSAT, también estatal y argentina. Fue lanzado el 30 de septiembre de 2015 y está localizado en el slot geoestacionario en la longitud 81 ° oeste. Su cobertura será tanto Sudamérica como gran parte de América del Norte.3, 113

Big Data

Los Datos Masivos es un término amplio para conjuntos de datos muy grandes o complejos que las aplicaciones de procesamiento de datos tradicionales no son insuficientes para su manejo., 69

Biométricos

La biometría es una tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas, como, por ejemplo, la huella digital, el reconocimiento del patrón venoso del dedo o el reconocimiento facial., 8

Bucle OODA

Se ha empleado este bucle inicialmente en el análisis para la toma de decisiones de combate entre pilotos de caza. Posteriormente en situaciones como el disparo de misiles intercontinentales.[4] Mediante el uso de este bucle los decisores pueden evaluar las amenazas antes de activar las contramedidas. El bucle fue implementado en los sistemas de ayuda a la toma de decisiones., 25

Ciberataques

Malware. Malware es un término que se usa para describir el software malicioso, que incluye spyware, ransomware, virus y gusanos:, 99

CNE

El CNE es esencialmente espionaje informático. El objetivo es espiar de una forma u otra. Básicamente, el atacante intenta recopilar información. Para lograr este objetivo, el atacante necesita obtener acceso a la red, realizar reconocimientos, identificar y obtener acceso a los sistemas relevantes para comprometer y encontrar y comprometer la información objetivo. Por lo general, es necesario mantener el acceso para seguir recopilando la información. También desea que la información que compromete sea precisa., 98

Cognitivo.

Rama de la ingeniería de sistemas que trata los entes cognitivos, sean humanos o no, como un tipo de sistemas capaces de tratar información y de utilizar recursos cognitivos como la percepción, la memoria o el procesamiento de información. Depende de la aplicación directa de la experiencia y la investigación tanto en psicología cognitiva como en ingeniería de sistemas. La ingeniería de sistemas cognitivos se enfoca en cómo los entes cognitivos interactúan con el entorno. La ingeniería de sistemas trabaja en la intersección de:, 18

Combat Cloud

Un conjunto de herramientas de seguridad cibernética que se ocupan de la higiene de la red detección de intrusos, servicios de identidad, monitoreo del flujo de red y protección avanzada contra malware., 59

Componente No- Cinético
La guerra de la información Cinetico
El final del siglo XX estuvo marcado por el relativo descenso de guerras interestatales y el correspondiente aumento de guerras intraestatales, 2

CRN
Su CRN está en las cartas que le enviamos o en su tarjeta de concesión, si tiene una. Si no puede encontrar su CRN, puede
iniciar sesión en myGov y en Soporte del gobierno para el coronavirus, seleccione Continuar, luego se vera., 110

DARPA
DARPA es una agencia del Departamento de Defensa de los Estados Unidos con una misión singular y duradera
realizar inversiones fundamentales en tecnologías innovadoras para la seguridad nacional. La Agencia busca explícitamente un cambio transformacional en lugar de avances incrementales. Para ello, trabaja dentro de un ecosistema de innovación que incluye socios académicos, corporativos y gubernamentales, con un enfoque constante en los Servicios militares de la Nación, que trabajan con DARPA para crear nuevas oportunidades estratégicas y opciones tácticas novedosas., 98

EEG
Prueba que detecta la actividad eléctrica del cerebro mediante pequeños discos metálicos (electrodos)., 33

Fusion warfare
En muchos sentidos la guerra y terrorismo son muy similares. Ambas implican actos de extrema violencia, están motivados por consideraciones políticas, ideológicas o fines estratégicos, y son causados por un grupo de individuos contra otro. Sus consecuencias son terribles para los miembros de la población, ya sea intencionadamente o no. La guerra tiende a ser más generalizada y la destrucción es probable que sea más devastadora porque a menudo se lleva a cabo por estados con ejércitos y grandes arsenales de armas a su disposición. Los grupos terroristas rara vez tienen los recursos financieros y profesionales de los estados., 60

Genoma Humano
El genoma es el conjunto de instrucciones genéticas que se encuentra en una célula. En los seres humanos, el genoma consiste de 23 pares de cromosomas, que se encuentran en el núcleo, así como un pequeño cromosoma que se encuentra en las mitocondrias de las células., 8

Grid
Grilla inteligente., 109

Guerras Aéreas de Quinta Generación
Un avión de caza (también llamado avión de combate), o simplemente caza, es una aeronave militar diseñada fundamentalmente para la guerra aérea con otras aeronaves, en oposición a los bombarderos, que están diseñados principalmente para atacar objetivos terrestres mediante el lanzamiento de bombas. Los cazas son pequeños, veloces y de gran maniobrabilidad. Muchos cazas poseen capacidades secundarias de ataque a tierra, y algunos son de doble propósito para actuar como cazabombarderos, término también usado para nombrar a los aviones de ataque a tierra con capacidades de caza., 48

Guerras Algorítmicas
El puente deseado es un marco para guiar y evaluar la operativización de la IA, con el rendimiento del algoritmo por un lado y la utilidad para la misión por el otro. Esa combinación garantiza que las ecuaciones matemáticas puedan probar o validar numéricamente un sistema de IA mientras que los puntos de referencia cualitativos garantizan la aplicación práctica. El resultado es una guerra algorítmica basada no solo en estadísticas, sino en una arquitectura más amplia para la relevancia operacional. Esa relevancia comprende cinco requisitos:, 2

Guerras cinéticas

La batalla multidominio se desarrolla en un marco del campo de batalla más extenso para luchar en todo el ancho y profundo de las capacidades enemigas, abarcando transversalmente desde el campo de batalla hasta la propia guarnición en múltiples dominios., 60

Network

Se le llama network o también red a aquellas series de ordenadores o dispositivos informáticos que se conectan por medio de cables, ondas, señales u otros mecanismos con el propósito de transmitir datos entre sí, además de recursos y servicios, con el fin de generar una experiencia de trabajo compartida, y ahorrar tiempo y dinero., 59

NYOP

Aparición de nuevos escenarios de combate que requieren el empleo de fuerzas militares o la necesidad de sostener misiones de larga duración, hacen necesario disponer de nuevas capacidades operativas, las que pretenden hacer frente a las nuevas acciones de guerra asimétrica del siglo XXI, en que los enfrentamientos no son entre ejércitos regulares sino a través de insurgencias, acciones terroristas o inestabilidad regional., 93

OPSIC

Las OPSIC son ejecutadas para llevar información seleccionada y direccionada a un grupo-objetivo definido, tales como son
gobiernos, organizaciones, grupos e individuos, cuya finalidad es la de influir en sus emociones, actitudes, motivos, percepciones, razonamientos y, princi- palmente, en su conducta., 93

Tecnologías disruptivas

Tecnología disruptiva es cualquier tecnología o innovación que deja obsoleta la tecnología anterior. Se usa el término disruptivo porque produce una ruptura brusca, en ocasiones causando cambios profundos en nuestro modo de vida., 8

VANET

Una red ad hoc vehicular (VANET) consiste en grupos de vehículos en movimiento o estacionados conectados por una red inalámbrica. Hasta hace poco, el uso principal de VANET era proporcionar seguridad y comodidad a los conductores en entornos vehiculares., 109

VLC

El software VideoLan se originó como un proyecto académico en 1996. VLC solía significar "VideoLAN Client" cuando VLC era un cliente del proyecto VideoLAN El nombre del proyecto se ha cambiado a VLC media player porque ya no hay una infraestructura cliente / servidor. SMART., 109

WSN

La red de sensores inalámbricos (WSN) se refiere a un grupo de sensores dedicados y dispersos espacialmente para monitorear y registrar las condiciones físicas del entorno y organizar los datos recopilados en una ubicación central. Las WSN miden condiciones ambientales como temperatura, sonido, niveles de contaminación, humedad, viento, etc., 109

# INFORME DE EVALUACIÓN DE TRABAJO FINAL INTEGRADOR – ESPECIALIACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO (097) ENAP -FCE – UBA.

**ALUMNO: Pablo Luchetti.**

**COHORTE:** 2018

**TEMA: "**Argentina, su estado actual y sugerencias para afrontar Guerras de Quinta Generación (G5G)".

1. **Conocimiento del tema**:
   Un marco teórico muy bien desarrollado, que nos indican la búsqueda de información actualizada respecto al tema. Que casualmente el mismo titular de cátedra admite que fue parcialmente abordado en la materia Def Nac y Seg Int. También en este apartado, otro indicador del esfuerzo son las traducciones de textos extranjeros realizadas por el mismo alumno para abonar en la profundización de su trabajo.

   La extensión total del trabajo, que si bien se excede en los parámetros de los TFE de la FCE, demuestran el interés por profundizar sobre las 5G y 6G, que aparecen con cierta innovación en la especialización.

2. **Actualización del Diagnóstico:**
   Recurrió a información de las distintas páginas de internet, consolidando un diagnóstico más bien teórico, aunque actualizado. En este sentido, se le hicieron varias observaciones durante el proceso de evaluación del TFI, logrando avanzar y objetivar la información aportada dándole distintas perspectivas.

3. **Pertinencia y coherencia de la propuesta de intervención.**
   Coherente y relacionada a materias de la especialización, además, actual e innovador en la temática investigada.

4. **Breve juicio del TFI**
   Buen trabajo final integrador, de extenso desarrollo con enfoque en las temáticas de las guerras de quinta generación, donde pone en relación la capacidad de la inteligencia estratégica y sus posibilidades de anticipación frente a situaciones específicas y actuales del uso de nuevas armas. También desnuda la incapacidad de nuestro país en la prevención y defensa frente a éste nuevo fenómeno como conflicto.

5. **Propuesta de calificación numérica**: Bueno – Calificación OCHO (8).

Evaluadores: Lic Esp Julio Hang (Profesor de la materia Defensa Nacional y Seguridad Interior) y Mag José Luis Pibernus (Profesor de Taller de TFI y C-Icia).

**JUICIO FINAL Y CALIFICACIÓN DEL DIRECTOR DE LA ESPECIALIZACIÓN:**

**Trabajo de desarrollo extenso que revela un gran esfuerzo de reunión de antecedentes y evaluación. No obstante, el tratamiento disperso de temas que aunque vinculados, genera dificultades de correlación en la lectura. Pese a ello, no empece la evidente tarea de exégesis que distingue al cursante y en mérito también a sus aportes sobre las cuestiones de guerra de quinta generación permiten discernir favorablemente su acceso a la especialidad. Coincido en las advertencias sobre las vulnerabilidades del país en los temas tratados y que merecen una especial atención de la política nacional. Valiosa la bibliografía que ha sido consultada.**

**Calificación Final: CHOC (8)**

**Dr. José Ricardo Spadaro**

**Director de la IEyCO (097)**