Facultad del Ejército
Escuela Superior de Guerra
"Tte Grl Luis María Campos"

TRABAJO FINAL INTEGRADOR

Título: "Empleo de las redes informáticas en Ciberoperaciones en el marco de la Gran Unidad de Batalla".

Que para acceder al título de Especialista en Conducción Superior de OOMMTT, presenta el Mayor Cristian Iván CABRERA.

Director de TFI: Coronel Edgar Fernando CALANDIN.

Ciudad Autónoma de Buenos Aires, de diciembre de 2019.

Resumen

La falta de doctrina respecto a la ciberdefensa en los diferentes niveles permite al adversario explotar esta vulnerabilidad para desarrollar operaciones de información que modelen la opinión pública. Aspecto que se agrava ante la complejidad del campo de combate moderno, donde los elementos que conforman el nivel táctico tienen un papel trascendental a la hora de concebir un plan táctico. Por tal razón, la determinación del de las ciberoperaciones a ejecutar en el marco de la Gran Unidad de Batalla (GUB) adquiere un papel preponderante dentro del proceso de planificación de comando.

Dado que las ciberoperaciones puedan ser consideradas un objetivo para el nivel táctico y, que el nivel Táctico aún no ha desarrollado en profundidad al ciberespacio como un ambiente donde se ejecutan operaciones militares provoca un desafío cultural para las fuerzas armadas, donde la guerra centrada en redes soporta la capacidad de transformar la información en acción. Por ello, el objetivo general será Estandarizar el empleo de las redes informáticas en operaciones en el marco de la GUB. Esto, se ejemplifica en los conflictos de Estonia 2007 o Ucrania 2014, donde se evidenció la importancia de las ciberoperaciones a la hora de desarrollar cualquier operación militar.

La correcta determinación de las ciberoperaciones a ejecutar por la GUB, busco generar efectos que impacten sobre la percepción de la población o el decisor y alteren el proceso de toma de decisiones en todo momento. Estos efectos deben ser acompañados por un marco legal vigente.

La investigación exploratoria y cualitativa, permitió analizar la doctrina vigente en el ámbito específico y la bibliografía de autores internacionales. Se logró identificar las técnicas y tácticas; y así se arribó a una propuesta de ciberoperaciones en el marco de la GUB. Se concluye que es el arma de comunicaciones la que debe desarrollarse y entender específicamente las ciberoperaciones. Para lo cual debe organizar sus Batallones y Subunidades alcanzando estas capacidades hasta el nivel subunidad.

Con la ciberdefensa, los actores involucrados intentan producir el caos en el oponente y defenderse de estos ciberataques, para equilibrar el poder de combate tratando de obtener la victoria antes de desplegar su poder militar.

Palabras clave.

Ciberoperaciones, Ciberdefensa, Ciberseguridad, Ciberataque, Ciberresiliencia.

Introducción

La continua evolución de esta nueva dimensión de la guerra, la cual impacta severamente los diferentes sistemas de armas, pero que a través de acciones pueden causar efectos no sólo sobre los sistemas del ciberespacio en este mundo globalizado, sino también de otra índole, valiéndose de este medio.

Es de particular importancia que nuestras Fuerzas Armadas se aboquen al desarrollo y entendimiento de esta nueva dimensión, ya que su entorno de trabajo permanente es el ambiente operacional donde se ejecutan las ciberoperaciones. Las tecnologías informáticas han transformado la manera de pensar y actuar en el desarrollo de las operaciones, introduciendo importantes cambios estructurales, al permitirnos modelar objetos de todo tipo en forma de información, permitiendo de este modo su manipulación por medios electrónicos. Por tal motivo es de vital importancia que se establezcan bases doctrinarias para generar conciencia, tener un lenguaje en común general y establecer las medidas a adoptar ante posibles transgresiones. Cuya finalidad será mejorar las medidas de contrainteligencia, protegiendo nuestras redes, aplicando medidas preventivas y accionar ante los posibles ataques para proteger nuestro sistema de comando y control y afectar en la medida de lo posible, el del enemigo.

Este tema posee un vacío doctrinario desde el reglamento básico [1] del Ejército Argentino, el cual no lo tiene en cuenta aún como otra dimensión de la guerra, tampoco cuenta con una doctrina específica, que al menos aborde temas generales y fundamente el desarrollo de esta actividad en el marco de la GUB.

Por tal motivo, los lineamientos para el análisis de estudio consistirán en, desarrollar este trabajo en función de las siguientes áreas de investigación: Operaciones, Inteligencia, Metodología para la toma de decisiones militares y Comunicaciones. De esta manera se busca integrar todas ellas para señalar aspectos relevantes que permitan determinar las capacidades de las redes informáticas para contribuir a las operaciones que ejecuta la GUB en esta nueva dimensión y poder estandarizar parámetros generales para el apoyo de las ciberoperaciones.

---

[1] ROB 00-01: reglamento de orden básico, aquellos reglamentos desde los cuales emana la doctrina derivada, denominados ROD.

El tema posee algunas dificultades, la primera es la permanente evolución de esta dimensión y el letargo del Ejército para determinar una doctrina que establezca pautas generales que determinen las capacidades de nuestras redes informáticas y su proyección. El segundo está basado en la dificultad para establecer el alcance de las políticas de ciberseguridad o las medidas de seguridad de contrainteligencia sobre el marco legal vigente.

El trabajo se ejecutará sobre el Arma de comunicaciones, la cual ha desarrollado este tema parcialmente y posee la responsabilidad del manejo de las redes informáticas y la seguridad informática del Ejército y, cuenta con los medios para ejecutarlo en la actualidad. Para aquellos vacíos que pudieran aparecer durante el desarrollo, se tomará como referente, lo concretado por otros países.

El Objetivo General es **"**Estandarizar el empleo de las ciberoperaciones en el marco de la GUB". Para ello se ve necesario desarrollar tres objetivos secundarios y secuenciales. **Objetivos Específico Número 1.** Determinar las políticas de seguridad a nivel GUB o equivalente y el marco legal vigente en la República Argentina para accionar sobre las diferentes transgresiones. **Objetivos Específico Número 2.** Identificar los principales objetivos de ataque de las ciberoperaciones, como una nueva dimensión de la guerra que incide en las condiciones del ambiente operacional y en las capacidades de la GUB y equivalentes. **Objetivos Específico Número 3.** Definir las operaciones a ejecutar en el ciberespacio para proteger la información y los circuitos en el nivel GUB y equivalentes.

El TFI que se desarrolla, contará con elementos del Marco Teórico, constituidos por las leyes de la República Argentina y la doctrina conjunta y especifica en vigencia al año 2019.

La bibliografía de base que se empleara y constituirá el punto inicial, será el reglamento "Conducción de las Fuerzas Terrestres" – ROB 00-01 (2015) en su capítulo VII sección XV dónde se refiere a conceptos generales de Ciberdefensa, su finalidad y quién lo debe ejecutar siendo la doctrina rectora en el Ejército Argentino y el reglamento "Conceptos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza" ROD 05-01 (2016).

El concepto de redes y guerras en red fue trabajado en profundidad por John Arquilla y David Ronfeldt a inicios de siglo XXI dentro del laboratorio de ideas de la

corporación RAND (Research and development). Sus aportes comienzan en los orígenes de esta actividad, diferenciando la guerra en red en su estructura organizativa. Estos autores, destacan que muchos grupos no cuentan con líder y son altamente flexibles para juntarse y atacar como enjambre un objetivo (Arquilla y Ronfeldt, 2003).

En el año 2005, Enrique Stel estableció conceptos básicos que abordan la guerra cibernética e hizo una descripción de este ambiente y sus componentes (Stel E. , 2005).

También se reconoce como antecedentes de este estudio al trabajo de Especialización realizado por Javier Anca (2015), el cual abordó el tema de la conducción de las operaciones de ciberdefensa y de sus principios básicos para la conducción.

Asimismo, Adriana Llongueras Vicente (2013) realizó un trabajo sobre la ciberdefensa que fue editado en su obra de la guerra inexistente y la ciberguerra sobre la guerra inexistente. En esta obra, la autora aborda la problemática del ciberespacio al definir en forma clara los objetivos de la ciberguerra dentro de este ambiente.

Durante el año 2015 el Doctor Roberto Uzal hace un importante aporte con respecto a las reglas de empeñamiento en el espacio cibernético y modifica la matriz de Tobias Feakin. Esta matriz desarrolla un esquema que contribuye al proceso de toma de decisiones estratégicas en el espacio cibernético. La Matriz de Tobias Feakin modificada facilita la identificación de los componentes a las respuestas de ciber incidentes generales. El conocimiento de estos componentes otorga al conductor político y militar variables ante un ciberataque (Uzal, 2015).

En lo que respecta a ciberseguridad y ciberoperaciones defensivas, se tendrá en cuenta lo desarrollado por Alejandro Corletti Estrada en sus obras *Ciberseguridad, una Estrategia Informático/Militar* y *Seguridad en Redes*. El autor desarrolla en esta bibliografía los términos de ciberseguridad, ciberresiliencia y ciberdefensa fundamentando su teoría en una defensa en profundidad comparándola con una acción retardante, donde el que se defiende intenta recobrar la libertad de acción en cada línea de retardo. Esta defensa en capas permite al que se defiende organizar sus

medios e información a proteger de manera resiliente estableciendo un lugar a no ceder y de esta manera restablecer en un breve tiempo los sistemas a su estado inicial (Corletti Estrada, 2017), (Corletti Estrada, A, 2016).

Para abordar las operaciones militares en el ambiente cibernético se tendrá en cuenta lo desarrollado por el General Evergisto De Vergara y el Contraalmirante Trama en operaciones militares cibernéticas, ambos autores hacen un análisis profundo y detallado del planeamiento y la ejecución de las ciberoperaciones en el ambiente cibernético (De Vergara y Trama, 2017).

Durante el año 2018 y 2019, el estado argentino actualizo sus normativas en lo que respecta a ciberdefensa y ciberseguridad. En la Directiva de Política y Defensa Nacional vigente, dónde el poder ejecutivo nombra al ciberespacio como un dominio. También menciona que el desarrollo tecnológico incrementó los riesgos asociados a la militarización de este dominio, la disuasión se ha extendido al espacio cibernético producto de una mayor conectividad, la privacidad y los derechos de la ciudadanía, dando como resultado general la ciberdisuación[2] (Poder Ejecutivo Nacional, 2019).

Otro documento importante es la directiva de Ciberseguridad de agosto de 2019, donde el estado nacional establece los objetivos y principios rectores que guían este (Poder Ejecutivo Nacional, 2019)

En el presente trabajo se emplea un proceso metodológico descriptivo desde un enfoque cualitativo sobre conceptos esenciales y sobre la posible aplicación de las ciberoperaciones en el nivel táctico.

Para la realización del presente trabajo, se recurre primeramente al análisis documental y bibliográfico sobre las publicaciones más recientes presentadas por los países avanzados referentes al objeto de estudio, para luego cotejar con la doctrina propia la mejor articulación dentro del nivel táctico.

---

[2] Según David Simon, es la capacidad en el ciberespacio que tienen las grandes potencias y otros actores para utilizarlas en su competencia geopolítica directa a modo de disuasión para proteger su seguridad nacional. David E. Simon (2017), Raising the Consequences of Hacking American Companies", Centre for Strategic and International Studies, octubre de 2017.

También se utilizan, entrevistas en profundidad a profesionales en ejercicio dentro de la estructura de ciberdefensa. Ello sirve a los fines de un mayor acercamiento a la situación que se investiga y permitirá eventualmente capitalizar las lecciones aprendidas con respecto al tema que se analiza. De esta manera y a través de la triangulación intrametodológica, se procura aumentar la validez de la investigación.

En el primer capítulo se realiza una introducción del marco doctrinario y las ciberoperaciones, posteriormente se desarrollan los efectos que persiguen las ciberoperaciones ofensivas y defensivas en el nivel operacional. Para ejemplificar esto, se tiene en cuenta el desarrollo de un conflicto moderno como Estonia 2007.

Posteriormente, en el segundo capítulo se aborda al marco doctrinario y las ciberoperaciones, posteriormente se desarrollan los efectos que persiguen las ciberoperaciones ofensivas en el marco de la GUB. Para ejemplificar esto, se tiene en cuenta el desarrollo de un conflicto moderno como Estonia 2007.

Por otro lado, en el tercer capítulo se analizan las ciberoperaciones defensivas, de exploración y la ingeniería social para llegar a una conclusión de con que profundidad deben planificarse y ejecutarse las ciberoperaciones en el marco de la GUB o equivalente. Por tal motivo, se intenta demostrar en qué momento se planificaría la neutralización del oponente y la protección propia en el nivel táctico.

El marco legal y las políticas de seguridad de las ciberoperaciones

En la República Argentina se establece una diferenciación conceptual en cuanto a Defensa Nacional y Seguridad Interior, a través de las leyes 23.554 y 24.059, el Decreto 727/2006, el Decreto 683/2018, que reglamentó la Ley de Defensa y la Directiva de Ciberseguridad de junio de 2019, que interesa para el presente trabajo. El concepto de Seguridad nacional que gran parte de los países del mundo la conciben de manera integrada la seguridad interior y la defensa nacional no se aplica en nuestra legislación. Este aspecto adquiere relevancia a la hora de determinar los límites del marco legal, debido a la naturaleza de la actividad, sumado a las ciberoperaciones que se ejecutan en el ciberespacio.

La Ley de Defensa Nacional 23.554 y los límites que determina.

La Ley 23.554 (1988), determina las bases jurídicas, orgánicas y funcionales para la preparación, ejecución y control de la defensa nacional.

El artículo 2, establece que "la defensa nacional es la integración de la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieren el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva para enfrentar las agresiones de origen externo. Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y libertad de sus habitantes" (Honorable Congreso de la Nación, 1988).

Se señala en este artículo, una definición muy clara a considerar; "agresiones de origen externo". Por otro lado el artículo 4 de esta ley menciona que "para dilucidar las cuestiones atinentes a la defensa nacional, se deberá tener permanentemente en cuenta la diferencia fundamental que separa la defensa nacional de la seguridad

interior. La seguridad interior será regida por una ley especial" (Honorable Congreso de la Nación, 1988).

Como se señaló al comienzo del capítulo, la República Argentina, separa en forma clara, el ámbito de la Defensa Nacional, con el ámbito de la Seguridad Interior. Se hace hincapié en el artículo 15, como un elemento de juicio más a considerar para la elaboración posterior de conclusiones parciales, considerando la estrecha relación que existe en materia de Ciberoperaciones entre la Dirección de Comunicaciones e Informática e Inteligencia.

El Articulo 5, establece que "la defensa nacional abarca los espacio continentales, Islas Malvinas, Georgias y Sandwich del Sur, y demás espacios insulares, marítimos y aéreos de la República Argentina, así como el sector antártico argentino, con los alcances asignados por las normas internacionales, y los tratados suscriptos o por suscribir por la Nación esto sin perjuicio de lo dispuesto por el artículo 28"; por su parte el artículo 28 de dicha ley, establece que para el caso de guerra o conflicto armado internacional "el Presidente de la Nación podrá establecer teatros de operaciones, delimitando las correspondientes aéreas geográficas" (Honorable Congreso de la Nación, 1988).

De estos artículos, se resalta el concepto, de un espacio definido, con límites geográficos, comprendidos dentro de un teatro de operaciones, los cuales tendrán una clara incidencia a la hora de determinar los efectos de las ciberoperaciones que ejecute nuestro sistema de ciberdefensa.

Decreto 703/2018. Directiva Política de Defensa Nacional (DPDN)

La transformación que han experimentado los desafíos que enfrenta la Defensa de la República Argentina, resultó necesaria la aprobación de una nueva Directiva de Política de Defensa Nacional que se adapte a las amenazas que afectan a

los estados en la actualidad. En este marco, la República Argentina debe desarrollar la capacidad para anticiparse, ciberdisuadir[3] y superar cualquier riesgo o amenaza que aféctenla seguridad de sus objetivos estratégicos (Poder Ejecutivo Nacional, 2018).

En lo que respecta al ciberespacio el desarrollo tecnológico incrementó los riesgos asociados a la militarización del mismo. La disuasión se ha extendido al ámbito cibernético, donde no solo los estados cobran gran importancia en su desarrollo sino también diferentes entes privados y organizaciones están desarrollando capacidades en este espacio. Por tal razón, diariamente surgen nuevos desafíos producto de las tensiones entre una mayor conectividad, la privacidad y los derechos de la ciudadanía (Poder Ejecutivo Nacional, 2018).

Es por eso que, tanto los estados como los actores no estatales están desarrollando medios cibernéticos para explotar las vulnerabilidades inherentes a los sistemas de comando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento. De igual forma, las redes terroristas explotan el ciberespacio para reclutar miembros, recaudar fondos y difundir su propaganda (Nacional, 1988).

El espacio cibernético es un lugar donde prevalece el anonimato, sin embargo las amenazas cibernéticas sofisticadas provienen de organizaciones militares y agencias de inteligencia de otros Estados. De esta manera los gobiernos tecnológicamente

[3] Según David Simon, es la capacidad en el ciberespacio que tienen las grandes potencias y otros actores para utilizarlas en su competencia geopolítica directa a modo de disuasión para proteger su seguridad nacional. David E. Simon (2017), "Raising the Consequences of Hacking American Companies", Centre for Strategic and International Studies, octubre de 2017.

avanzados explotan sus ventajas comparativas con relación al resto de los países, desarrollo de ciberoperaciones también está al alcance de actores secundarios o menos desarrollados en su tecnología. Esta problemática requiere adoptar medidas para armar un sistema lo suficientemente resiliente[4] en ciberseguridad que permita neutralizar cualquier amenaza o riesgo que atente contra nuestras infraestructuras críticas y la información de ellas por medio de la Defensa Nacional (Nacional, 1988).

Por tal razón el sistema de Defensa Nacional se debe abocar a generar las capacidades que permitan proteger de manera eficiente los objetivos estratégicos que puedan ser objeto de una agresión de origen externo. Además se debe contemplar lo que marque el plexo legal vigente con respecto a los ciudadanos argentinos y bienes nacionales en terceros países, aguas y espacios aéreos internacionales, los arreglos del país anfitrión, el derecho internacional y la Carta de las Naciones Unidas.

El ciberespacio se ha instalado como un dominio que cruza transversalmente a los otros dominios, por tal razón configura una amenaza de interés estratégico para la defensa nacional. Por esto, el componente militar como parte del Ministerio de Defensa debe desarrollar capacidades que permitan fortalecer las capacidades de vigilancia y control del ciberespacio. Esto permite anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar el Sistema de Defensa Nacional, como así también acciones contra la infraestructura critica del país o que

[4]En tal sentido y a los efectos de la presente ponencia, se considerará como concepto de **resiliencia** el expresado por el CERT (equipo de respuestas ante emergencias informáticas) de seguridad e industria español, *"Cuando un sistema es capaz de soportar todo tipo de presiones sin cambiar su comportamiento, entonces es robusto. Cuando un sistema no es capaz de soportar más presiones, pero puede integrar cambios para disminuirlas y puede seguir adelante, entonces es ciber-resiliente* (Bruce Schneier, 2018)*."*

posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia, a fin de garantizar la seguridad de sus infraestructuras informáticas críticas o estratégicas (Poder Ejecutivo Nacional, 2018).

Las Fuerzas Armadas Argentinas y en particular el Arma de Comunicaciones deben adecuar sus organizaciones militares al impacto que emerge de estos nuevos riesgos. La política de ciberdefensa debe orientarse al desarrollo de capacidades cibernéticas que permitan tener un sistema resiliente ante ciberataques, ya que es casi imposible ser invulnerable en la actualidad en este dominio. Esta tarea debe contemplar la cooperación con otras áreas del Estado y diferentes organismos privados que tengan responsabilidad en la política de ciberseguridad nacional.

Resolución 829 (2019) Estrategia Nacional de Ciberseguridad.

Para atender la problemática de la ciberseguridad, la Argentina se rige por lo que marca el Comité de Ciberseguridad dentro de la Secretaría de Gobierno de Modernización. Es este Comité del Estado Argentino que tiene la misión de desarrollar la Estrategia Nacional de Ciberseguridad y hacer cumplir los principios y objetivos que marca el Poder Ejecutivo Nacional en el ciberespacio (Poder Ejecutivo Nacional, 2019).

La constante evolución de las Tecnologías de la Información y las Comunicaciones, han permitido mejorar las estructuras económicas, por tal motivo hoy constituyen uno de los principales motores del progreso y del bienestar humano. Esto modifico el mundo actual, ya no es posible prescindir de ellas, ni concebir un futuro próspero sin su evolución. Por ello, el contexto actual ubica al ciberespacio como un elemento esencial en la vida de las personas y las organizaciones, las proyectan en el mismo gran parte de su actividad, no habiendo aspecto de la vida

social que no se pueda desarrollar en este dominio. Sin embargo, esto implica graves riesgos a la seguridad de las personas, las organizaciones y los gobiernos, estando el entorno digital amenazado por nuevas formas de delitos, la acción de grupos terroristas y la confrontación entre los Estados que día tras día se encargan de fomentar la ciberconfianza[5]. Por la complejidad que plantea este este nuevo escenario la Estrategia Nacional de Ciberseguridad establece los principios esenciales y los objetivos centrales de la República Argentina en torno a su proyecto para la protección del ciberespacio. Entre los principios esenciales se destaca, el respeto por los derechos y las libertades individuales, el liderazgo en ciberseguridad, la fomentación de capacidades y el fortalecimiento individual. Otros principios se desarrollan bajo el concepto de cooperación como la integración internacional y la cultura de ciberseguridad y responsabilidad compartida. El último principio es el fortalecimiento del desarrollo socioeconómico, ya que el ciberespacio genera posibilidades para el progreso económico y social de la nación. También entre los objetivos podemos destacar la concientización del uso seguro del ciberespacio, la capacitación y educación del uso seguro del ciberespacio, el desarrollo del marco normativo y el fortalecimiento de las capacidades en ciberseguridad. También se destacan la protección y recuperación de los sistemas del sector público, fomentar la industria de ciberseguridad, la cooperación internacional y la protección de las infraestructuras críticas nacionales de información.

[5] Según el glosario de ciberseguridad. Esperanza firme que una persona tiene en que algo suceda, sea o funcione de una forma determinada en el espacio digital o ciberespacio.

El manual de Tallin 2.0.

El Tallin Manual 2.0 es la segunda edición del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN sobre el análisis y la aplicación del derecho internacional sobre el ciberespacio. El análisis se basa en la idea que las operaciones cibernéticas no se producen en un vacío legal, y las obligaciones preexistentes según el derecho internacional se aplican igualmente al dominio cibernético. Como tal, el Tallin Manual 2.0 se divide en cuatro partes con un total de veinte capítulos, cada uno examina un área diferente del derecho internacional existente. La primera sección trata sobre los principios legales generales, mientras que las últimas tres secciones abordan regímenes legales especializados específicos. De acuerdo con su premisa, el Tallin Manual 2.0 cita más de un siglo de tratados y jurisprudencia, extendiendo las premisas de los principios y regímenes de derecho internacional a sus aplicaciones en el ciberespacio (OTAN, 2017).

Las reglas 15 a 18 del manual de Tallin 2.0 resumen el derecho internacional consuetudinario de atribución de operaciones cibernéticas.

- **Regla 15:** “las ciberoperaciones realizadas por órganos de un Estado, o por personas o entidades facultadas por la ley nacional para ejercer elementos de autoridad gubernamental, son atribuibles al Estado”.

- **Regla 16:** “las ciberoperaciones realizadas por el órgano de un Estado que ha sido puesto a disposición de otro Estado son atribuibles a este último cuando el órgano actúa en el ejercicio de elementos de autoridad gubernamental del Estado al cual h sido colocado a disposición".

- **Regla 17:** “Las operaciones realizadas por un actor no estatal son atribuibles a un Estado cuando: (a) participan en de conformidad con sus instrucciones o bajo su dirección o control; o (b) el Estado reconoce y adopta las operaciones como propias.

– **La regla 69** dice que, una operación cibernética implica el uso de la fuerza cuando su escala y sus efectos son comparables a las operaciones no cibernéticas que se elevan al nivel de uso de la fuerza. Medido según esos criterios internacionales habituales, el Hackeo del Comité Nacional Demócrata de Estados Unidos (DNC) debe colocarse en el contexto amplio de las intrusiones cibernéticas. El ataque al DNC no fue un ataque armado o de uso de la fuerza. En cuanto al uso de la fuerza el hackeo ruso probablemente no fue un acto internacionalmente ilícito. Los rusos extrajeron y difundieron información privada, pero no alteraron las máquinas de votación ni cambiaron los votos. Según las medidas tradicionales, no hubo coerción ni intervención ilegal.

Por otro parte, este manual también establece que un estado no debe permitir conscientemente que las ciberinfraestructuras[6] situadas en su territorio o bajo control exclusivo gubernamental sean usadas para realizar actos que afecten adversa e ilegalmente a otros estados. También debe impedir que se utilice su territorio o ciberestructura con este fin. El ejemplo que cambio un paradigma de la guerra es, la "respuesta cinética" de Israel a la agresión "no cinética" de Hamás en mayo de 2019 marca un hito significativo en la historia militar pero no deja de ser una respuesta a un ataque de otra Nación.

Resolución 3314 (1974) de la Organización de las Naciones Unidas.

En acuerdo con la Resolución de 3314 (1974) de la Organización de las Naciones Unidas la República Argentina, define el término "agresión" como "el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la

[6] Es la "agregación" (conjunto) de gente, procesos y sistemas integrados al Ciberespacio o Quinto Dominio.

independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de Naciones Unidas". Asimismo, expresa que el término "Estado", "se utiliza sin perjuicio de las cuestiones de reconocimiento o de que un Estado sea o no Miembro de las Naciones Unidas" y que "incluye el concepto de grupo de Estados" cuando proceda" (ONU, 1974).

Dicha resolución en su artículo 3 enumera aquellos actos, que considera agresión, independientemente de que haya o no declaración de guerra, caracterizando los mismos, de manera no exhaustiva. Dichos actos, son los siguientes;

- "La invasión o el ataque por las fuerzas armadas de un Estado del territorio del otro Estado, o toda ocupación militar, aun temporal que resulte de dicha invasión.
- El bombardeo, por las fuerzas armadas de un Estado, del territorio de otro Estado.
- El bloque de los puertos o costas de un Estado por las fuerzas armadas de otro Estado.
- El ataque por las fuerzas armadas de un Estado contra las fuerzas armadas terrestres, aéreas, navales o aéreas, contra la flota mercante o aérea de otro Estado.
- La utilización de fuerzas armadas de un Estado, que se encuentren en el territorio de otro Estado con el acuerdo del Estado receptor
- La acción de un Estado que permite que su territorio, se ha puesto a disposición de otro Estado, sea utilizado por ese otro estado para perpetrar un acto de agresión contra un tercer Estado.
- El envió por un Estado, o en su nombre, de bandas armadas, grupos irregulares o mercenarios que lleven a cabo actos de fuerza armada contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerado, o su sustancial participación de dichos actos" (ONU, 1974).

Algunos países consideran a las ciberarmas directamente como un nuevo sistema de armas, distinto por ejemplo de la artillería pesada. Un ejemplo de esto fue el ataque realizado en mayo de 2019 por las Fuerzas de Defensa Iraní (FDI) por medio de un bombardeo aéreo sobre un edificio, en el cual se determinó que era el origen de ciberataques realizados por Hamas, en progreso y de otros fallidos anteriormente.

Como conclusión de estas acciones, las FDI lo consideraron decisivo, vale decir que Hamas no tiene capacidades operacionales cibernéticas. Esto fue una respuesta física a una amenaza cibernética. Pero no se trata de guerra híbrida, sino la utilización de otro sistema. Por esto se considera, a la luz de los contenidos, que los conceptos escritos en el año 1974, cuando la dimensión del ciberespacio no existía, eran adecuados para el contexto de la época, incluso, si se proyectan en la actualidad y a la luz del ejemplo citado son totalmente aplicables a esta nueva dimensión.

La Naturaleza de la actividad en el ciberespacio.

La carencia de doctrina militar en vigencia, en material del tema en desarrollo, hace que se recurra a la búsqueda de distintas fuentes, con el fin de comprender en su total dimensión, según dicta el estado del arte de forma contemporánea.

La Real Academia Española, define al ciberespacio, como "ámbito artificial creado por medios informáticos".

El ciberespacio es un escenario táctico, estratégico y operativo diferente de los espacios terrestre, marítimo, aéreo y espacial, que ha sido calificado en la doctrina, como uno de los Global Commons[7], su esencia está en el modo en que altera las realidades de los otros dominios (Carrillo, 2015).

[7] Según Gómez de Agreda, es un término utilizado para describir dominios de recursos internacionales, supranacionales y globales en los que se encuentran recursos comunes.

El ciberespacio no permite el ejercicio del poder físico, no controla la realidad, la puede cambiar, sus operaciones se basan en efectos. La realidad humana está mutando. Hoy prácticamente todas la actividades del hombre se realizan en el ciberespacio. En el ciberespacio existe la posibilidad de realizarse cuando el mundo real lo niega, por lo cual en oportunidades el hombre se aísla de la realidad. Sin embargo, el aspecto más importante en este dominio es que el contacto no implica fricción, según el conductor Prusiano Mottke el viejo definió este factor como el fenómeno que hace que "ningún plan resista el primer disparo del oponente ", la diferencia está en que el oponente puede actuar y causar daños muy superiores sin ser detectado como en las guerras de siglos XIX (Moressi, 2019).

Otra característica importante es la impunidad relativa en este dominio, ya que las acciones desarrolladas en este ambiente, carecen de la posibilidad de ser identificadas, en la medida que no exista un dispositivo tecnológico, o la voluntad del operador, para definir su origen e intenciones. Por tal razón, los límites basados en tecnologías transforman la intangibilidad como característica física primigenia a estos ambientes, esto hace que solo a través de ingenios tecnológicos se pueda establecer límites. En el espacio aéreo se emplean sensores que extienden los límites terrestres y marítimos hasta los 100 Km de altura (Línea Karman), ambiente operacional (Moressi, 2019).

Otro factor es la Intangibilidad, ya que en este dominio no es posible definir sus límites, las operaciones que en ellos se ejecutan, carecen de la posibilidad de discriminar o referenciarse por sí mismo, sino que lo hacen a través de otros ambientes la tierra y el espacio. Por esto si comparamos el ciberespacio, el espacio y la atmósfera el más pequeño es la atmósfera que ocupa la totalidad del globo terráqueo algo así como 51.010 millones de Km3. El ciberespacio es mayor aún dado

que su dimensión se encuentra en la mente del hombre, pudiendo llegar a límites inimaginables y finalmente el espacio, al que por el momento consideramos “finito pero ilimitado” (Moressi, 2019).

Por otro lado otra dificultad se encuentra en delimitar el empleo militar o civil de los medios, así como estos ambientes, poseen cierta impunidad relativa, debido a la dificultad de identificar los actores. Este dominio se caracteriza por un empleo civil constante aún en caso de conflicto, su importancia para el desarrollo de la actividad humana es tan elevada que en general existen numerosos acuerdos internacionales para su gestión.

Otra característica del ambiente cibernético es la transversalidad de ambientes operacionales. Dado que, todos ellos desde la perspectiva física y su inmensidad son envolventes de los ambientes clásicos como la tierra y el mar, inclusive el espacio es envolvente de la atmósfera. Sin embargo, el ciberespacio por las características de trabajar en la virtualidad se sitúa en la mente de las personas y por ello lo envuelve todo. Esta característica le da a estos ambientes una transversalidad que eleva la complejidad operacional, no sólo por sus implicancia sino por la conjugación de todas las otras características comunes entre ellos.

Las acciones en este dominio están basadas en efectos, por tratarse de un ambiente completamente tecnificado, las acciones tienen resultados tangibles en sus efectos a similitud de las operaciones aéreas, ya que los efectos pueden ser medidos, estudiados y determinados con exactitud. Esto hace que definir el ritmo de batalla y asimilarlo al cumplimiento de objetivos impuestos sea dificultoso por su la forma intangible de alcanzar objetivos concretos.

Otro aspecto a destacar en este dominio son los Recursos Humanos (RRHH) y su adaptación al medio en que operan. Las peculiaridades de cualquier ambiente

definen la necesidad de RRHH, adaptados a trabajar bajo las características del mismo.

La postura de la República Argentina en la Ciberdefensa.

La Ciberdefensa "comprende medidas técnicas, políticas y organizativas que protegen los sistemas y redes militares de ciberataques, como así también la capacidad de reacción y ataque propios de un conflicto armado. Desde un fundamento concreto, la Ciberdefensa se sustenta mayoritariamente en tecnología de ciberseguridad ampliamente probada, y desplegada en el sector civil" (Anca, 2015).

El reglamento ROB-00-01, "Conducción de las Fuerzas Terrestres", desarrolla la Ciberdefensa, dentro de las Operaciones Complementarias, y la define como "el conjunto de acciones que se desarrollan en el ciberespacio para prevenir, detectar, identificar, anular, impedir, evitar, contrarrestar, contener o repeler amenazas o agresión cibernética, sea esta inmediata, latente o potencial, a fin de permitir el empleo del Instrumento Militar de la Nación". Asimismo, en referencia a la finalidad, refiere dos modalidades (ROB00-01, 2015);

- "Ciberdefensa directa, con la finalidad de vigilar y controlar las redes y sistemas en los ámbitos especifico y conjunto.
- Ciberdefensa indirecta, cuya finalidad es la de disputar el control del ciberespacio necesario para accionar a las fuerzas militares (ROB00-01, 2015)."

Para el enfoque que se pretende dar a este trabajo, se considera que, la doctrina rectora mencionada en el ámbito de la fuerza, es obsoleta y restrictiva en cuanto a las tareas que enumera. Asimismo, se visualiza contradictoria en cuanto a su finalidad cuando se refiere a la ciberdefensa indirecta, ya que si se pretende disputar el control del ciberespacio como lo marca la última DPDN del 2018 o los

lineamientos dados en la directiva de ciberseguridad de 2019, no basta con medidas de carácter pasivo. Por tal razón, es necesario incorporar medidas de carácter activo que me permitan mantener la iniciativa.

El marco doctrinario, no responde a las necesidades que impone la naturaleza de las actividades en el ciberespacio, como una nueva dimensión de la guerra, tema que se desarrolla en el capítulo subsiguiente. También, la diferencia que hace nuestro país en cuanto a la separación en materia legal, de Defensa y Seguridad, es determinante en cuanto al ámbito de empleo de las fuerzas armadas. Sin embargo este aspecto fue subsanado a partir del Decreto 683/18. La aparición de una dimensión con características particulares propias, que no responde reglas obsoletas, plantea una larga lista de interrogantes al momento de enfrentar estas nuevas amenazas de forma integral y eficiente.

Reglas de empeñamiento en las operaciones cibernéticas

El conocimiento de la cibersituación ocurre en un marco de incertidumbre ya que los Comandantes en el Teatro de Operaciones (TO), en la actualidad aún no cuentan con las herramientas necesarias para controlar, identificar y neutralizar un ciberataque. Además, no tienen la capacidad de detectar los flujos de información del ciberatacante, es por esto que la determinación de la ciberreglas de empañamiento tiene un papel trascendental (De Vergara y Trama, 2017).

Las ciber reglas de empeñamiento, deben ser tratadas a nivel regional esto evidencia numerosas ventajas competitivas. Sólo como un ejemplo de dicha sinergia positiva, se cita la posibilidad de desarrollo conjunto de capacidades que llevan al plano de las realizaciones concretas a las ciber reglas de empeñamiento más sofisticadas. Tanto desde el punto de vista tecnológico, como en el de su implementación política deben ser adaptables a la vertiginosidad del cambio

tecnológico. Dichos cambios en el "quinto dominio" son de una velocidad tal que, ni siquiera admite ser comparada con la velocidad con la que evolucionan las características de los cuatro dominios anteriores. Las reglas de empeñamiento contra ciberagresiones, no deberán estar restringidas, necesariamente, por las actuales capacidades (Uzal, 2015).

Cuando los efectos de un ciberataque militar, reconocido como tal, sean equivalentes a los causados por "Ataques Armados" o "Desembarcos hostiles de unidades militares", dicho ciberataque militar deberá, en principio, tener un tratamiento que guarde proporcionalidad con las citadas equivalencias. Sin embargo, otras ciberagresiones, por ejemplo, la toma de control de un satélite de comunicaciones por parte del estado agresor o acciones de ciber reconocimiento para detectar vulnerabilidades, quedan comprendidas en la mencionada "zona gris". Esta es la zona donde los estados nación del Mercosur deben trabajar para poner reglas de empeñamiento claras (Uzal, 2015).

Hoy no hay criterios establecidos a nivel internacional para determinar cuándo un Estado Nación define la necesidad de legítima defensa.El manual de Tallin no es un cuerpo normativo oficial de la OTAN, pero es una guía importante de expertos internacionales para las situaciones que se pueden plantear en el ciberespacio, toma normas vigentes de carácter internacional sobre conflictos armados como la Declaración de San Petersburgo de 1868 o la Convención de Ginebra de 1949 y las aplica adaptándolas al ciberespacio.

Conclusiones Parciales al primer objetivo.

Para dar respuesta al primer capítulo, el objetivo específico persigue: Determinar las políticas de seguridad a nivel GUB o equivalente y el marco legal vigente en la

República Argentina para accionar sobre las diferentes transgresiones. En función de los contenidos desarrollados durante el primer capítulo, se considera que;

El marco legal la República Argentina establecido en la Ley de Defensa Nacional 23.554, el Decreto 683/2018, la DPDN18 aprobada con el decreto 703/18, la Directiva de Ciberseguridad aprobada el 5 de mayo de 2019 en la resolución 829/19 están en concordancia con la Resolución 334 (1974) de la Organización de las Naciones Unidas, no limitan de manera taxativa, las tareas a desarrollar por las FFAA, a la existencia de una agresión externa por parte de una fuerza armada de otro Estado exclusivamente.

La resolución reciente 1380/2019 del 25 de octubre de 2019 permite desarrollar las capacidades cibernéticas, el cumplimiento de objetivos y principios desde el punto de vista de ciberdefena con la creación del Centro Nacional de Ciberdefensa en el ámbito de la Subsecretaria de Ciberdefensa donde funcionara entre otros organismos el centro de respuesta ante emergencias in del Ministerio de Defensa (CSIRT de Defensa) y el centro inteligente de operaciones de seguridad (ISOC) del Comando Conjunto de Ciberdefensa.

La naturaleza de la actividad, que se desarrolla en un ambiente complejo, dónde el hecho de que la dificultad de identificar a un actor que actúa en el ciberespacio, impide en primera instancia, definir cuáles son los objetivos e intereses en pos de los cuales actúa. Estos podrían ser Estados, individuos y organizaciones de distinta índole, dificultan la planificación, ejecución y desarrollo de capacidades acordes con las acciones necesarias para anticipar, o neutralizar las amenazas emanadas de riesgos cibernéticos.

La actitud básica reactiva de la República Argentina, y el espíritu que da lineamiento a nuestro marco legal, separando Defensa de Seguridad Interior, sumado

a la ausencia de una legislación particular para las acciones ofensivas en el ciberespacio, dificultan el desarrollo de capacidades ofensivas para la defensa de las infraestructuras críticas y la información que las sostienen.

Se debe actualizar la doctrina rectora mencionada en el ámbito de la fuerza, es obsoleta y restrictiva en cuanto a las tareas que enumera. Asimismo, se visualiza contradictoria en cuanto a su finalidad cuando se refiere a la ciberdefensa indirecta, ya que si se pretende disputar el control del ciberespacio es necesario incorporar medidas de carácter activo que me permitan mantener la iniciativa.

Es por estos aspectos enunciados, que se considera, existe una necesidad de hecho, de buscar una visión más amplia acorde a las características de la naturaleza de la actividad en el ciberespacio.

El alcance de las Ciberoperaciones ofensivas y su influencia en las condiciones del ambiente operacional de la GUB o equivalente.

En el presente capítulo se desarrollan las diferentes ciberoperaciones ofensivas teniendo en cuenta lo que marca el libro de la Guerra Inexistente la ciberguerra (Llongueras Vicente, 2013), Redes y guerras en red (Arquilla y Ronfeldt, 2003), las Operaciones del ciberespacio de los Estados Unidos de Norteamérica (America, 2018) y, Operaciones Militares Cibernéticas (De Vergara y Trama, 2017), si bien no son prescripciones reglamentarias, estas publicaciones establecen claramente como entienden las ciberoperaciones las diferentes potencias precursoras en este dominio. Por otro lado las Fuerzas Armadas Argentina aún no han dispuesto en sus publicaciones doctrinarias como se subdividen las ciberoperaciones en los distintos niveles de la guerra. También se propone la incorporación de la matriz de Tobias Fekin modificada por el Dr Roberto Uzal en el planeamiento del nivel Táctico.

Conceptos básicos en el espacio cibernético.

La carencia de doctrina en ciberdefensa en el nivel táctico hace necesario que los especialistas en redes informáticas de las diferentes fuerzas establezcan rápidamente conceptos básicos, que permitan trabajar de manera conjunta en este dominio complejo y cambiante. Solo en pocos documentos y directivas del nivel estratégico nacional el poder ejecutivo establece una serie de objetivos y principios rectores (Nacional, Poder Ejecutivo, 2019).

Uno de estos es la Directiva de Política y Defensa Nacional vigente, dónde el poder ejecutivo nombra al ciberespacio como un dominio. También menciona que el desarrollo tecnológico incrementó los riesgos asociados a la militarización de este dominio, la disuasión se ha extendido al espacio cibernético producto de una mayor

conectividad, la privacidad y los derechos de la ciudadanía, dando como resultado general la ciberdisuación[8].

Otro documento importante es la directiva de Ciberseguridad de agosto de 2019, donde el estado nacional establece los objetivos y principios rectores que guían este (Poder Ejecutivo Nacional, 2019)

Por esto, tanto los Estados como los actores no estatales desarrollan medios cibernéticos para explotar las vulnerabilidades inherentes a los sistemas de comando y control, comunicaciones, inteligencia vigilancia y reconocimiento. Además, las redes terroristas explotan el ciberespacio para reclutar miembros, recaudar fondos y difundir propaganda.

También, el despliegue de ciberoperaciones disruptivas está al alcance de naciones menos desarrolladas. El despliegue de esta problemática desde la Defensa Nacional requerirá adoptar medidas desde el punto de vista de la ciberseguridad. Estas medidas facilitarán el resguardo y protección de las infraestructuras críticas del sistema de Defensa Nacional y de aquellas designadas para su preservación.

Por esto, en el presente capítulo se abordan los conceptos referidos a las ciberoperaciones ofensivas que afectan el ambiente operacional de la GUB. Para ello, es necesario desarrollar algunos conceptos básicos como ciberdefensa, ciberoperaciones y ciberseguridad. La resolución 1380/19 del 25 de octubre de 2019,

[8] Según David Simon, es la capacidad en el ciberespacio que tienen las grandes potencias y otros actores para utilizarlas en su competencia geopolítica directa a modo de disuasión para proteger su seguridad nacional. David E. Simon (2017), "Raising the Consequences of Hacking American Companies", Centre for Strategic and International Studies, octubre de 2017.

considera a la ciberdefensa como “las acciones y capacidades desarrolladas por el Ministerio de Defensa, El Estado Mayor Conjunto y La Fuerzas Armadas para anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar al ministerio de Defensa y al Instrumento. Como así también a las infraestructuras críticas operacionales soporte de los servicios esenciales de interés para la Defensa nacional (Defensa, 2019)”.

Por otro lado, la ciberseguridad son todas aquellas actividades que se ejecutan en el ciberespacio o espacio cibernético contra el uso indebido del mismo, defendiendo sus infraestructuras tecnológicas, los servicios que prestan y la información que manejan (Llongueras Vicente, La Guerra Inexistente, la Ciberguerra. Ciberdefensa, 2013).

De esta manera se define a las ciberoperaciones, mediante operaciones ejecutadas en el ciberespacio para obtener información, negar, degradar o destruir la información existente en diferentes dispositivos que operan dentro de una red de computadoras o redes informáticas.

Las ciberoperaciones ofensivas operan dentro del ciberespacio, espacio operacional creado tecnológicamente por el hombre donde las organizaciones y personas utilizan las tecnologías de la información y la comunicación (TIC) necesarias para interactuar (Llongueras Vicente, 2013).

Ciberoperaciones ofensivas.

Las ciberoperaciones ofensivas se ejecutan en el ciberespacio para comprometer la confidencialidad, la integridad o la disponibilidad de la información del oponente. Estas actividades tienen la finalidad de proyectar el poder en el ciberespacio para obtener los objetivos militares buscando infligir efectos temporales o permanentes a

fin de reducir la confianza del adversario en sus redes o capacidades y facilitar las operaciones militares a ejecutarse dentro del teatro de operaciones (De Vergara y Trama, 2017).

De acuerdo cómo las desarrollan países como Estados Unidos, Brasil, Israel y España las ciberoperaciones ofensivas presentan objetivos generales. Estos objetivos sirven para, propagar un virus contaminando el flujo de la información enemiga y los diferentes dispositivos de esa red, controlar los elementos temporales que transitan sobre la internet con la finalidad de alterar la percepción de actores. También se utilizan con la finalidad de interrumpir los sistemas de comando y control del oponente para ejecutar operaciones de información, obtener información, cambiar los datos en las redes (De Vergara y Trama, 2017).

En el uso del componente militar sirven para concentrar los fuegos, las armas y las fuerzas de las propias fuerzas y favorecer la dispersión de las fuerzas enemigas. En cuanto al manejo de información se aplican para diseminar propaganda, transmitir información falsa al enemigo para tergiversar la información real y divulgar información (De Vergara y Trama, 2017).

La cadena de un ciberataque.

Según Lockeed Martin Corporation[9], un ciberataque se ejecuta en siete fases. Esto se denomina cadena de un ciberataque donde el ciberatacante intentará crear la oportunidad para el cumplimiento del efecto deseado. Aquellos que tienen sus redes bien organizadas desde el punto de vista de ciberseguridad, cada una de estas fases es

[9] Es una compañía multinacional de origen estadounidense de la industria aeroespacial y militar.

una oportunidad para neutralizar la amenaza. Esta cadena de un ciberataque se puede resumir en las siguientes fases (De Vergara y Trama, 2017):

- Fase reconocimiento: en esta etapa el ciberatacante busca adquirir la información e inteligencia en el ciberambiente de un blanco del adversario e identificar los objetivos específicos. Estos objetivos manejan datos valiosos en sus redes y presentan alguna vulnerabilidad con respecto a ciberseguridad.

- Fase desarrollo del armamento: en esta fase los ciberatacantes crean los códigos de computadora (troyano) que generan las condiciones explotando las vulnerabilidades identificadas del sistema a atacar.

- Fase entrega: en este momento se transmite la carga al sistema de destino usando vectores como: adjuntos de correos electrónicos, sitios web y medios extraíbles (por ejemplo USBs o poniendo un troyano de acceso remoto en un archivo que simula tener información crucial, para incitar al destinatario a ejecutarlo).

- Fase explotación: una vez que la carga haya sido entregada al sistema de destino, esta fase desencadena la carga, explotando la vulnerabilidad del sistema operativo, si saben que software utiliza el usuario a atacar o servidores se pueden aumentar las posibilidades de esta etapa.

- Fase instalación: esta fase se utiliza para instalar un acceso remoto o puerta trasera en el sistema de destino que permita al oponente mantener una presencia dentro del sistema infectado.

- Fase mando y control: en este paso el atacante crea un canal de comunicación para facilitar la transmisión de comandos en forma remota.

- Fase efectos deseados creados: la última fase permite el atacante lograr sus objetivos de manera remota.

Figura 1: Medidas de protección para contrarrestar las fases de un ciberataque

FASE	PROTECCIÓN	OBSERVACIONES
Reconocimiento	Ingeniería social.	El atacante intenta obtener información sobre la organización y sus redes. Busca vulnerabilidades en redes y en IICC.
Desarrollo del armamento	Parches de seguridad.	El atacante busca explotar las vulnerabilidades encontradas.
Entrega del malware en el sistema	Sandbox , Ingeniería social. Separar placas de red de la internet e intranet, Anular USB. Evitar drives de MP3; MP4.	El atacante busca alojar el malware en los sistemas.
Explotación del malware	Sandbox - Limitar uso de Plugs – in.(Java o Flash)	Obtener información. Afectar los sistemas.
Instalación	Inspecciones SSL. Filtros URL.	El atacante recibe los datos de los ordenadores atacados y puede tomar el control de ellos.
Mando y control	Monitorear capa 3 y 4 del modelo OSI	Reconocer que el sistema ha sido atacado.
Efectos deseados creados	Servidores con información sensible desconectados de internet.	El atacante busca permanecer lo más posible sin ser detectado.

Fuente: elaboración propia, en base a Operaciones Militares Cibernéticas del General De Vergara y el Contraalmirante Trama.

Efectos de las ciberoperaciones ofensivas.

La superpotencia cibernética de los Estados Unidos, a las misiones militares en el ciberespacio la describen por intenciones. Estas ciberoperaciones se ejecutan desarrollando capacidades que permitan generar los efectos en el ciberespacio.

Por esto, un ciberataque está compuesto por las diferentes acciones que crean efectos directos de negación en el ciberespacio, tales como, -degradación, interrupción o destrucción- y la manipulación que conduce a la negación que se manifiesta en los espacios físicos. Las diferentes acciones desarrollan los siguientes efectos (America, 2018):

- El efecto de negar se traduce en degradar, interrumpir o destruir el acceso a, operación de, o disponibilidad de un objetivo por un nivel especifico durante un tiempo específico. La negación le impide al adversario el uso de recursos. La descripción de estos efectos es la siguiente:

- De acuerdo al párrafo precedente, el primer efecto para negar es degradar, este se utiliza para impedir el acceso a una operación de un objetivo en un nivel representado como un porcentaje de capacidad. El nivel de degradación debe ser especificado. Si se requiere un tiempo específico debe ser manifestado oportunamente.

- El segundo efecto de negar es interrumpir, este significa negar completamente durante un tiempo el acceso a, o la operación de un objetivo durante un período de tiempo. Normalmente, debe especificarse el tiempo de inicio y de finalización. La interrupción puede ser considerada un caso especial de degradación donde el nivel de degradación seleccionado es ciento por ciento.

- El tercer efecto de negar es destruir, el cual sirve para negar de forma permanente, completa e irreparable. En este efecto las funciones de tiempo y cantidad son maximizadas en el acceso a, o la operación de un objetivo.

- El efecto de manipular se utiliza para controlar o cambiar la información del adversario, sistemas de información y/o redes de tal manera que respalden los objetivos del Comandante.

Al finalizar los efectos que producen las operaciones ofensivas, cabe destacar que, la degradación o destrucción de la capacidad de las redes y los sistemas informáticos enemigos puede realizarse por un tiempo limitado.

La publicación JP 3-12121 Cyberspace Operations establece que: "La ejecución exitosa de operaciones cibernéticas requiere el empleo integrado y sincronizado de las operaciones ofensivas, defensivas y DODIN[10] (America, 2018)

Lineamientos metodológicos para elaborar una respuesta adecuada ante un ciberataque perpetrado o apoyado por otro Estado Nación con el empleo del poder militar

Estos lineamientos tienen el objeto de establecer posibles respuestas luego de haber desarrollado las ciberoperaciones ofensivas y sus efectos. Las respuestas a un ciberataque pueden ejecutarse en forma complementaria de las respuestas de las

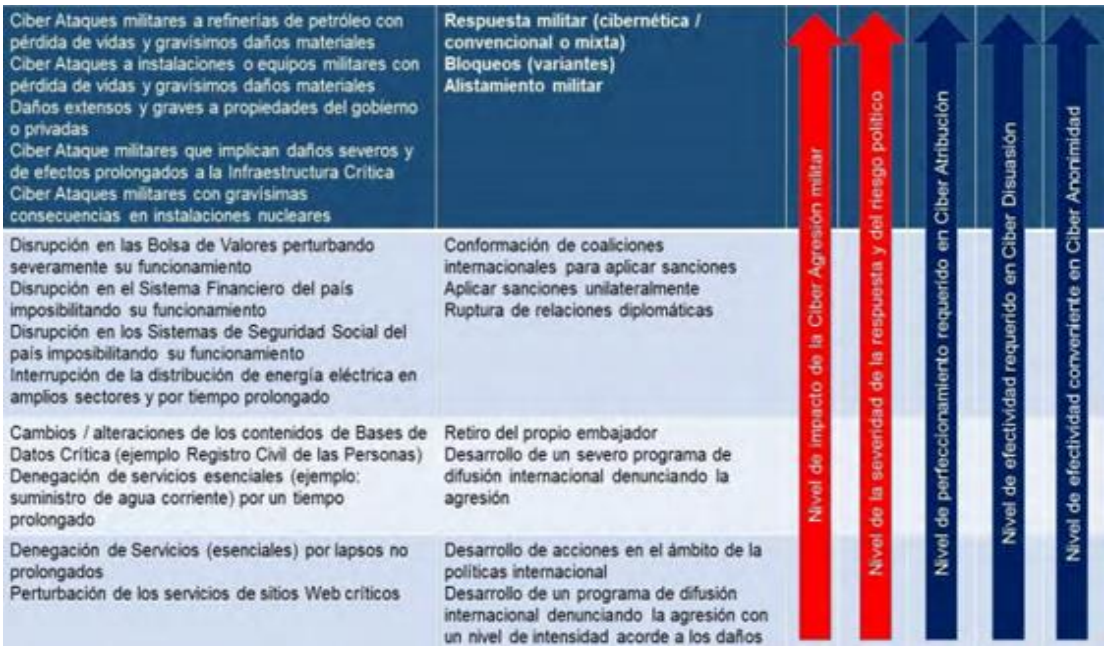
[10] De acuerdo a lo que señala la doctrina de ciberdefensa de EEUU. El área de operaciones del Departamento de Defensa (DODIN), son las operaciones donde el comando de ciberdefensa diseña, construye, configura, asegura, opera, sostiene y mantiene, el entorno de la información que le es asignado para las operaciones. Estas operaciones se ejecutan de manera proactiva y enfocadas en las TIC es decir el hardware, software, datos, usuarios individuales y los administradores de sistemas (De Vergara y Trama, 2017).

relaciones internacionales, económicas o del empleo del poder convencional militar. Estas se ejecutarán con dificultad si el gobierno no incorporó previamente capacidades en este dominio (Uzal, 2015).

Por esto, el reconocimiento de una ciber respuesta a un ciberataque en forma pública puede ser leído como incorrecto políticamente. Esto podría causar la pérdida de legitimidad internacional contra otros objetivos en un futuro. Para evitarlo, en general se utilizan respuestas *proxies* - servidores de comando y control desplegados.

Los tiempos de respuesta para accionar frente a un ciberataque del nivel operacional y estratégico son escasos, los estados mayores deben elaborar un marco general que catalogue respuestas alternativas tipo ante la ocurrencia de un ciberincidente disruptivo o destructivo con el empleo del poder militar.

Figura 2: Matriz de Tobias Fekin modificada por el Doctor Roberto Uzal.



Fuente: elaboración del Dr Uzal, matriz de Tobias Feakin modificada por el Doctor Uzal. La cual contribuye al proceso de Toma de Decisiones en la planificación del Nivel Táctico (GUB o equivalente) (Uzal, 2015).

Esta herramienta de ciberrespuestas ante un ciberataque detalla en su primera columna ejemplos de diferentes ciberagresiones. Posteriormente, en la segunda columna se desarrollan distintos tipos de respuestas a las ciberagresiones expuestas.

La flecha de la tercera columna marca el crecimiento de los daños causados por potenciales ciberagresiones militares, por otro lado la cuarta columna indica el nivel creciente de severidad, la potencial respuesta a una ciberagresión militar.

La quinta columna indica, la importancia que la Argentina incorpore capacidades para resolver las variantes del problema de atribución, aspectos que están completamente relacionados con la ciberdisuación y la ciberanonimidad.

Seguidamente, en la sexta columna esta flecha indica el nivel de efectividad en ciberdisuación que debería contar para cada caso para no ser considerado un blanco fácil. Finalmente, la séptima columna indica el nivel de ciberanonimidad requerido para cada caso (Uzal, 2015).

La Matriz de Tobias Feakin modificada facilita la identificación de los componentes a las respuestas de ciber incidentes generales. El conocimiento de estos componentes otorga al conductor político y militar variables ante un ciberataque (Uzal, 2015).

Si bien no hay conflicto igual a otro, este marco general le proveerá a las autoridades civiles y militares diferentes opciones de respuestas generales.

Finalmente este esquema contribuye al proceso de toma de decisiones que desarrolla la matriz de Tobias Feakin modificada por el Doctor Uzal. Esta matriz debe ser perfeccionada por los integrantes del elemento de defensa cibernética a

nivel táctico, operacional y estratégico, para intentar limitar la incertidumbre frente a un oponente que se perfecciona segundo a segundo (Uzal, 2015).

Conclusiones parciales al segundo objetivo.

Para dar respuesta al segundo capítulo, el objetivo específico persigue: Identificar los principales objetivos de ataque de las ciberoperaciones, como una nueva dimensión de la guerra que incide en las condiciones del ambiente operacional y en las capacidades de la GUB y equivalentes.

La descripción de las ciberoperaciones ofensivas con sus efectos permite tener un análisis general de las principales causas y consecuencias de las operaciones en el ciberespacio. Esto coadyuva a entender que, la obtención de la superioridad en el ciberespacio es un prerrequisito para la efectividad de las operaciones militares en todos los dominios.

La pérdida del control en este dominio se traduce en la carencia de comunicaciones fiables, de precisión, lo cual dificultará el comando y control del Comandante en el Teatro de Operaciones.

La alta dependencia de los medios militares a las TIC los expone como un objetivo rentable a ciberataques, este aspecto se puede comprobar en la actualidad ya que las principales potencias, organizaciones supraestatales y ejércitos están llevando el conflicto al espacio cibernético.

Por esto, es fundamental abordar la ciberdefensa de manera pasiva y activa, protegiendo las infraestructuras críticas por parte de las fuerzas armadas como lo marca la Directiva de Política y Defensa Nacional vigente.

El conocimiento de los efectos de las ciberoperaciones ofensivas como el desarrollo de estas capacidades, permitirá desarrollar un sistema ciberresiliente ante los ciberataques que sufren nuestras infraestructuras críticas.

Ciberoperaciones a ejecutar en el ciberespacio para proteger la información y los circuitos en el nivel GUB y equivalentes

Si bien, para proteger los circuitos y la información en el nivel GUB se emplearan principalmente las ciberoperaciones defensivas. El armado de un sistema ciberresiliente ante cibertataques implica el uso de todas las ciberoperaciones y otras técnicas relacionadas. El propósito de este capítulo es determinar las ciberoperaciones defensivas, de exploración e información y sus efectos. Para alcanzar este objetivo se completa el análisis de las diferentes ciberoperaciones desarrolladas en el capítulo, con conceptos de ingeniería social. Estos conceptos se desarrollan de acuerdo a lo que marca el manual de Operaciones Cibernéticas de (De Vergara y Trama, 2017), la publicación de Operaciones del Ciberespacio de las Fuerzas Armadas de Estados Unidos (America, 2018) y, la Ciberguerra, la guerra Inexistente de Adrianna Llongueras Vicente (Llongueras Vicente, 2013). Esto será complementado con el desarrollo del Centro de Gravedad Cibernético (CDG), el cual es un concepto que el nivel táctico no puede desconocer ya que la concreción de un punto decisivo cibernético o un objetivo táctico será contribuyente a la protección del propio CDG y la destrucción o neutralización del oponente.

Ciberoperaciones defensivas

Estas ciberoperaciones son acciones activas y pasivas que se ejecutan en el ciberespacio espacio cibernético para preservar la libertad de acción, para utilizar las capacidades del ciberespacio y proteger datos, redes y capacidades centradas en las redes (America, 2018). Las ciberoperaciones defensivas se enfocan sobre una amenaza específica y vinculan las vulnerabilidades con la intención y capacidad del adversario. De esta manera, se identifican las zonas de riesgo principal donde se deberá focalizar el esfuerzo defensivo (De Vergara y Trama, 2017).

Las acciones activas son aquellas que se ejecutan fuera del entorno propio, para bloquear o detener un ciberataque de manera similar a lo que sería un ataque convencional ejecutado fuera del dispositivo defensivo para defendernos como si fuera un ataque de desarticulación[11]. Sin embargo, acciones pasivas son aquellas que se realizan dentro del propio entorno (De Vergara y Trama, 2017).

Efectos de las ciberoperaciones defensivas

Los efectos en estas ciberoperaciones incluyen proteger, detectar, caracterizar, contrarrestar y mitigar. Tales acciones defensivas son creadas generalmente por el Comandante Conjunto o por la Fuerza Armada específica que posee u opera la red. (America, 2018) (De Vergara y Trama, 2017).

Ciberoperaciones de exploración y efectos:

Son aquellas actividades que se ejecutan en las redes para obtener datos, siendo el fin último de estas detectar vulnerabilidades, debilidades y amenazas (America, 2018).

Las potencias desarrolladas en el ciberespacio como Estados Unidos y Rusia dividen la exploración, en dos fases. En la primera se concentran en la recopilación de información, que atacan principalmente el software, hardware, el personal que opera las diferentes redes o sistemas y las políticas de seguridad informática operacional, como la conformación de sus redes desde el punto de vista de ciberseguridad. La segunda fase o ciberoperación se concentra en generar las

[11] Acción ofensiva planeada por la defensa y ejecutada, normalmente, delante del campo principal de combate cuyo objetivo son fuerzas enemigas que se están organizando o reuniendo para ejecutar un ataque. En su ejecución se debe explotar al máximo la sorpresa. De acuerdo a lo que marca el ROB-00-01 Reglamento para la Conducción de las Fuerzas Terrestres, 2015, Cap IV pág 8.

condiciones para vulnerar un sistema más sofisticado, del cual, ya se posee la información básica pero se precisa de datos específicos, avanzados y actualizados para sostener un efecto por un tiempo determinado (De Vergara y Trama, 2017), (America, 2018).

En el nivel táctico lo más correcto en las ciberoperaciones de exploración es hablar de acciones dirigidas contra los sistemas de tecnologías que protegen las infraestructuras críticas o el centro de gravedad del oponente. Estas ciberoperaciones serán ejecutadas para obtener información relevante que permitan producir un nuevo conocimiento de la situación y de esta manera detectar las vulnerabilidades en el oponente. Además dirigir sobre estas vulnerabilidades ciberataques que permitan, interrumpir, negar, degradar, corromper o destruir, la información almacenada en redes de computadoras, dispositivos o comunicaciones del oponente (De Vergara y Trama, 2017).

A pesar de esto, esta información también sirve para proteger nuestro centro de gravedad cibernético contra cualquier ciberataque y permitir organizar un dispositivo que sea lo suficientemente resiliente para poder contrarrestar estos ciberataques en contra de los dispositivos de origen. Este último permite aumentar la eficiencia de las redes, los diferentes dispositivos que interactúan en ellas y sistemas de armas mejorando de manera proactiva su ciberseguridad ante una posible situación de conflicto (Corletti Estrada, 2017), (De Vergara y Trama, 2017).

Otra herramienta que garantiza el correcto desempeño de una red dentro del hacking ético[12] es un penetration test, la cual ataca software, sistemas de computadoras y puertos para ejecutar un informe por períodos cortos. En períodos largos se utilizan los Red Teams en ciberoperaciones ofensivas, Blue Teams en ciberoperaciones defensivas o, Purple Teams en metodología integradora del equipo Rojo y Azul. Este último sería al más apropiado para chequear los efectos y detectar vulnerabilidades en el nivel operacional (Miessler, 2019).

Finalmente, teniendo en cuenta lo que el nivel estratégico nacional desarrolla en la última Directiva de Política y Defensa Nacional con respecto a la vigilancia y control del ciberespacio. El Nivel Táctico debe poseer las capacidades necesarias que le permita en las ciberoperaciones en desarrollo o ante la conformación de un Teatro de Operaciones neutralizar cualquier tipo de amenaza. Para lograr eso, debe conducir las capacidades de vigilancia y control del ciberespacio a fin de anticipar y prevenir ciberataques y ciberexplotación en las redes informáticas que afecten cualquier Sistema de Defensa dentro del TO (Poder Ejecutivo Nacional, 2018).

También conduce ciberoperaciones para proteger la infraestructura crítica del país o la información que posibilite el acceso a ellas. Esta misión la desarrollara bajo la supervisión y el control del Comando Conjunto de Ciberdefensa y las diferentes agencias del estado. Los efectos que excedan al Comandante del Teatro de Operaciones se requerirán a la estrategia Nacional (Poder Ejecutivo Nacional, 2018).

---

[12] Hacking ético. Según el manual de Ethical Hacking en su glosario dice que, es el acto de una persona al usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, con el objeto de reportarlas y que se tomen medidas sin producir daño.

Figura 3. Relaciones entre las ciberoperaciones y el ciberespacio.

Ciberoperaciones	EFECTOS	CIBERESPACIO
Ofensivas	Negar, degradar, interrumpir, destruir, manipular.	
Defensivas (Activas / Pasivas)	Proteger, detectar, caracterizar, contrarrestar y mitigar.	
Exploración	Detectar y neutralizar.	
Información	Manipular, neutralizar, desgastar.	

Fuente: elaboración propia, del dominio ciberespacio y su interacción permanente con las ciberoperaciones en base al JP 3-12 Cyberspace Operations, junio 2018, pág II-3, Primer Seminario de Ciberdefensa y Ciberseguridad en la Argentina y Curso de Ciberdefensa y Ciberseguridad dictado en la Escuela Superior de Guerra Conjunta.

Ciberoperaciones de información y efectos.

Las ciberoperaciones de información buscan alterar el proceso de toma de decisiones en el oponente utilizando el ciberespacio. Un error frecuente es tratar de diferenciar aquellas ciberoperaciones que se desarrollan en el ciberespacio, tipificándolas como operaciones de información (De Vergara y Trama, 2017).

A pesar de que el control del ciberespacio otorga poder, también genera vulnerabilidades como puede ser la transmisión en tiempo real de imágenes o hechos

por parte de los habitantes que condicionan el proceso de toma de decisiones de las Fuerzas Armadas dentro del Teatro de Operaciones. Esto facilita la divulgación de información secreta otorgándole ventajas al oponente. La saturación de mensajes a través de las redes sociales dificulta el control y hace mucho más compleja la información y desinformación (De Vergara y Trama, 2017).

Por esto, las ciberoperaciones de información persiguen efectos que solo ellas pueden ejecutar y, en todo momento buscaran otorgar libertad de acción para la ejecución de la maniobra y la conquista del objetivo táctico. Por tal razón, es pertinente vincularlas con las ciberoperaciones ofensivas y defensivas que busquen proteger el proceso de toma de decisiones propio e intenten alterar el del adversario (De Vergara y Trama, 2017). El desarrollo de estas capacidades lograra introducir al oponente en el ciclo OODA (observación, orientación, decisión y acción) propio, lo cual contribuirá a la desarticulación del adversario (Rio, 2013).

Por lo descripto anteriormente, las ciberoperaciones de información buscan explotar el uso de las capacidades del ciberespacio. Por esto, las ciberoperaciones ejecutadas en las redes informáticas tienen por finalidad modificar los datos o algoritmos de una red o sistema para que se produzcan resultados contrarios a los que se esperaban, estas conforman parte de las ciberoperaciones a ejecutar para generar las condiciones dentro del TO (De Vergara y Trama, 2017).

Sin embargo el elemento determinante en este sistema hombre máquina, sigue siendo el factor humano, el cual se reconoce en ciberdefensa como ingeniería social.

Ingeniería Social.

El eslabón más débil de todo sistema donde se maneja información es el hombre. La ingeniería social es el arte de engañar a las personas para convencerlas de que

ejecuten las acciones o actos que el atacante necesite para lograr su cometido. Para esto se utiliza técnicas psicológicas y habilidades sociales de manera consciente y premeditada (Salis, 2010).

Un ingeniero social, usa por lo general internet o el teléfono para engañar a otros usuarios de relevancia. Una forma de acceder es fingir ser el proveedor de algún servicio, un compañero de trabajo o un cliente, donde a través de mensajes enviados por internet de aparente procedencia legal, se obtiene información confidencial (Salis, 2010).

De esta manera los ingenieros sociales aprovechan la tendencia general de la gente a confiar y reaccionar en forma predecible en ciertas circunstancias ante los datos que recibe por internet o vía telefónica obteniendo información sin la necesidad de vulnerar un algoritmo u otro sistema (Salis, 2010), (De Vergara y Trama, 2017).

Un icono de esto para el gobierno de los Estados unidos fue Edward Snowden quien después de trabajar como antiguo empleado de la CIA y la NSA traicionó a su país de origen. Actualmente, este hacker vive en Rusia exiliado y vende sus servicios a otras potencias o diferentes organizaciones cibernéticas. Este caso es de gran relevancia porque, se trata de un hacker con capacidades ilimitadas cuando es respaldado por potencias opositoras o diferentes organizaciones (Snowden, 2019).

La ingeniería social puede llevarse a cabo de muchas maneras, tanto en el ordenador como utilizando una llamada por teléfono, en persona o con métodos tradicionales de correo postal. La existencia y variedades en la ingeniería social es tan numerosa en la actualidad que a cualquier lista que intentemos catalogar siempre faltará alguna. Sin embargo, entre las más conocidas podemos destacar, el pishing o suplantación de identidad, la ejecución de troyanos, fraudes por compras, en persona,

por teléfono y la zanahoria o el palo. Por esto, cuando la ingeniería social se origina en un ordenador se realiza por electrónico o internet, pero también hay casos donde se ha llevado a cabo por mensajería instantánea y otros programas informáticos (Grimes, 2018).

Por esto, las empresas que se dedican en la actualidad al cibercrímen o los estados que intentan manipular permanentemente la percepción de las personas para obtener un beneficio trabajan sobre la ciberconfianza[13]. Por tal razón, los estados, organismos de ciberdefensa y ciberseguridad para frenar esta ciberguerra[14] permanente desarrollan la ciberdisuación[15] (De Vergara y Trama, 2017).

El Centro de Gravedad Cibernético.

La respuesta cinética[16] de Israel a un supuesto ciberataque palestino en el mes de mayo de 2019 deja claro que las potencias cibernéticas consideran a las ciberarmas[17]

[13] Según el glosario de ciberseguridad. Esperanza firme que una persona tiene en que algo suceda, sea o funcione de una forma determinada en el espacio digital o ciberespacio.

[14] Según el glosario de ciberseguridad. Es un área que tiene como objetivo encontrar las vulnerabilidades técnicas de los sistemas o redes informáticas del enemigo para penetrarlas y atacarlas a fin de extraer datos e información sensible.

[15] Para el Dr Roberto Uzal es lograr que los estados naciones agresores, reales y potenciales, perciban claramente que los costos esperados a una Ciber Agresión a la Infraestructura Crítica Nacional de otro estado nación, superan ampliamente a los resultados esperados de dicha hipotética Ciber Agresión..

[16] Acto de atacar desde el espacio una parte de la superficie terrestre con un proyectil donde la fuerza destructiva proviene de la energía cinética liberada durante impacto del proyectil.

como a otros sistemas de armas de la guerra convencional con la capacidad de producir daños superiores a cualquiera de ellos. Esto se relaciona directamente con la determinación del CDG desde que quedo confirmado que las ciberarmas tienen efectos físicos y cinéticos (De Vergara y Trama, 2017).

La determinación del Centro de gravedad[18] propio y del oponente es una de las actividades más importantes de todo estado mayor. Empero, un aspecto importante a tener en cuenta en el campo de batalla actual es que el combate, se libra en forma permanente en la mente de las personas debido a la dependencia cada vez mayor de las nuevas tecnologías. Por tal razón, solo aquel que tiene las capacidades para controlar parcialmente el ciberespacio, posee un sistema ciber resiliente[19] en este dominio (Corletti Estrada, 2017).

Por tal razón, la ciberresiliencia se logra cuando la ciberseguridad se desarrolla de manera eficiente y es capaz de resistir un ciberataque, detectarlo, neutralizarlo y volver el sistema a su estado inicial. A pesar de que la ciberseguridad, se la asocie con las ciberoperaciones defensivas y, que en los otros dominios el esfuerzo principal se encuentre en la defensa, en las ciberespacio no sucede eso. En el ciberespacio la libertad de acción la otorgan las ciberoperaciones ofensivas. Estas son las únicas que

---

[17] Según Kaspersky, compañía Rusa dedicada a la seguridad informática. Una ciberarma es un tipo de código malicioso, script, llámese como sea, destinado normalmente para atacar y defender en el espacio cibernético. Ejemplo de esto es Stuxnet o Flame.

[18] Según Eikmeier el CDG es el ente primario que tiene la capacidad inherente de alcanzar el objetivo. El Manual de Arte y Diseño Operacional lo tipifica como un elemento innovador del diseño operacional.

[19] Según el Doctor Roberto Uzal es la capacidad de volver un sistema a su estado inicial.

tienen la capacidad de garantizar el funcionamiento del sistema de comando y control, las diferentes redes, la información y las infraestructuras críticas (Estrada, Ciberseguridad, Una Estrategia Informático/Militar., 2017), (De Vergara y Trama, 2017).

La legitimidad[20] en este dominio hace que a las ciberoperaciones defensivas se las relacione con el esfuerzo principal. Otro aspecto a destacar es el marco legal vigente actual que, al ser difuso cuando se menciona un ciberataque y el despliegue de medios que necesita para sostener un efecto en el nivel operacional es muy superior. Esto hace que para el desarrollo de un sistema ciberresiliente debe ser tratado de manera interagencial con todos los organismos del estado y privados (De Vergara y Trama, 2017).

La determinación del tipo de ciberoperación a ejecutar es trascendental en el momento de analizar el CDG ciberespacial propio y del oponente, ya que esta me permite durante la planificación identificar las capacidades críticas (CC)[21], los requerimientos críticos (RC)[22] y las vulnerabilidades críticas (VC)[23] (Kenny, Locatelli, Zarza, 2015), (Ejército Argentino, 2015).

---

[20] Consenso o acuerdo entre los miembros de una comunidad, el cual es referido a valores culturales, normas y niveles más profundos y detallados.

[21] Según Strange, son las habilidades primarias que ameritan que un Centro de Gravedad sea identificado como tal en el contexto de un escenario, situación o misión dados. (Kenny, Locatelli, Zarza, 2015, pág. 66)

[22] Según Strange, son condiciones, recursos y medios que son esenciales y que hacen que una capacidad crítica sea totalmente operativa. (Kenny, Locatelli, Zarza, 2015, pág. 67)

La dependencia de nuestros sistemas de armas de las TIC conforma una vulnerabilidad crítica, por tal motivo los Comandantes en el nivel táctico centran sus esfuerzos en la protección de estos sistemas para evitar que se generen debilidades (De Vergara y Trama, 2017).

El Comandante del TO debe analizar sus capacidades cibernéticas, las del oponente y aquellas organizaciones de otro tipo que dispongan de estas capacidades para interferir o neutralizar su sistema de comando y control. Además solicita el apoyo de las capacidades cibernéticas de la estrategia nacional cuando se trate de proteger el CDG cibernético propio o neutralizar el del oponente (De Vergara y Trama, 2017).

Análisis de los factores críticos del Centro de Gravedad cibernético.

Los factores críticos (capacidades críticas, requerimientos críticos y vulnerabilidades críticas), son los elementos que todo Comandante y su Estado Mayor en el Nivel Operacional debe analizar para proteger o neutralizar el CDG (Kenny, Locatelli, Zarza, 2015) . La eficiencia se logra si el elemento cibernético posee el poder de combate y alcance operacional necesario para proteger y afectar los factores críticos propios y del oponente (Kenny, Locatelli, Zarza, 2015).

La doctrina argentina establece que un CDG se concreta mediante el análisis de sus CC, estas funcionan de manera sistémica otorgando poder, libertad de acción y equilibrio (Ejército Argentino, 2015).

---

[23] Según Strange, son requerimientos críticos o componentes de ellos que son deficientes o vulnerables a la neutralización, interdicción o ataque, que permiten alcanzar resultados decisivos. (Kenny, Locatelli, Zarza, 2015, pág. 68)

De estas capacidades se desprenden los requerimientos críticos que hacen que estos se comporten como un sistema. Sin embargo lo más importante a detectar por el Oficial de Comunicaciones y Ciberdefensa en el Estado Mayor del nivel Táctico son las vulnerabilidades críticas. Estas debilidades surgen después de un intenso análisis del CDG ciberespacial propio y del oponente, las mismas son consideradas puntos decisivos[24] cuando la fuerza puede operar sobre ellas. Además, estas VC ofrecen oportunidad para minimizar costo y mantener la iniciativa (Kenny, Locatelli, Zarza, 2015).

Un aspecto importante a diferencia de las fuerzas militares que operan en los tres dominios tradicionales (terrestre, aéreo y naval), es que el elemento o sistema que opera en el ciberespacio puede alcanzar factores críticos que en la antigüedad eran muy difícil, como la empatía de una determinada población, la cual puede condicionar la libertad de acción de un Comandante en el Teatro de Operaciones (TO). Según Milan Vego, en la era de la información surge un nuevo concepto, el "punto decisivo cibernético" (Vego, 2007), debido a la dependencia de las comunicaciones e informática de los sistemas de armas que operan en el TO. Por esto, es importante que el Comandante del nivel táctico incluya el ciberespacio como dominio durante la planificación, esto le permitiría reforzar el sistema defensivo y establecer alternativas ante posibles amenazas (De Vergara y Trama, 2017).

---

[24] Según Alejandro Kenny, Omar Locatelli y Leonardo Zarza, son un conjunto de condiciones, vinculadas a ubicaciones geográficas, sucesos específicos claves, sistemas de capacidades, funciones críticas o entorno de la información, que cuando se alcanzan permiten al Comandante del TO, influir de sobremanera en el resultado de la maniobra operacional o de la campaña (Kenny, Locatelli, Zarza, 2015, pág. 78)

Por otro lado, según lo que marca Williams Brett, para estar en condiciones de ejercer el comando y control el Comandante debe conocer la arquitectura del sistema cibernético. Este sistema lo descompone en cinco componentes, la infraestructura de comunicaciones que incluye redes alámbricas en inalámbricas, redes que organizan y distribuyen información, capas de protección, conocimiento de herramientas para desplegar información que faciliten el proceso de toma de decisiones y sensores que entregan inteligencia, vigilancia y reconocimiento (Brett, 2011).

El conocimiento de esta arquitectura del sistema cibernético básica, permite estar en condiciones de analizar las capacidades críticas del CDG cibernético. Estas son las habilidades primarias que identifican al CDG en el contexto de un escenario, situación o misión dados (Kenny, Locatelli, Zarza, 2015, pág. 66).

Método para determinar el Centro de Gravedad cibernético.

Según Eikmeier el CDG es, *"*el ente primario que tiene la capacidad de alcanzar el objetivo" y teniendo en cuenta que una de las tareas más importantes del diseño operacional que enfrenta un Estado Mayor es la identificación del CDG. El análisis sistémico aporta una herramienta analítica que permite identificar fortalezas y debilidades propias y del oponente (Kenny, Locatelli, Zarza, 2015).

El método más apropiado que presenta ventajas para determinar el CDG y analizar en profundidad los factores críticos es el de la teoría de los sistemas "fines, modos y medios"[25]. Este método se desarrolla en ocho pasos cuatro para determinar

[25] Según Eikmeier Dale, este método brinda mayor certidumbre y menos discusión al responder a tres preguntas simples: ¿cuál es el objetivo?, ¿cómo lo puedo alcanzar? Y ¿qué recursos se requieren?. Eikmeier Dale. "Redefining the Center of Gravity". Op.cit. Pag158.

el CDG ciberespacial y cuatro pasos para determinar los requerimientos críticos y vulnerabilidades críticas que se deben afectar o proteger del CDG ciberespacial (Kenny, Locatelli, Zarza, 2015).

Figura 4. Método para determinar el Centro de Gravedad Cibernético.

PASOS	TAREA
PASO 1	Identifique los fines u objetivos del elemento bajo análisis
PASO 2	Identifique los modos o acciones cibernéticas posibles que le permitan a ese actor alcanzar ese fin y los modos del propio sistema.
PASO 3	Enumere los medios de la organización disponibles o necesarios de ciberdefensa para realizar el modo/CC.
PASO 4	De los medios elija el ente cibernético que tiene la CC de alcanzar el Objetivo.
PASO 5	De los ítems remanentes del listado de medios. Elija aquellos críticos para ejecutar la CC. Estos son los RC del CDG ciberespacial.
PASO 6	Identifique los RC vulnerables a las acciones del oponente.
PASO 7	Identifique en los RC del oponente las VC.
PASO 8	Relacione las VC con los puntos decisivos.

Fuente: elaboración propia, para determinar el CDG ciberespacial durante el planeamiento del NT en base al manual de Arte y diseño Operacional, pág 71, de Kenny, Locatelli y Zarza .

El campo de batalla actual se está librando en la mente de las personas, teniendo en cuenta que las operaciones en el ciberespacio se basan en efectos y uno de ellos es manipular la realidad. Es pertinente analizar los elementos en capacidad de producir estos efectos, ya que los mismos pueden tener consecuencias superiores a los de cualquier arma convencional (De Vergara y Trama, 2017).

Por esto, en el análisis de los factores críticos lo más importante es determinar los RC el cual es un elemento vital dentro del sistema, Estos se deberán atacar para producir la vulnerabilidad y como consecuencia, afectar o neutralizar el CDG del oponente. Esta vulnerabilidad constituye el foco hacia donde se materializa la maniobra. Según William Brett, un análisis de la situación exhaustivo me permite identificar cuando hay varios sistemas involucrados, con sus diferentes vulnerabilidades. La vinculación de estas vulnerabilidades y la intención y capacidad del adversario dan como resultado la zona de riesgo donde se debe incrementar el esfuerzo de la defensa (Brett, 2011).

Ejemplo de análisis de factores cibernéticos.

El ejemplo de este análisis se desarrolla en la Figura 5. En este, se analiza una situación simulada reducida dónde, el sistema e infraestructura de información militar de Israel, según analistas Iraníes es un CDG porque tiene la capacidad de integrar sistemas de información militar y civil aprovechando sus capacidades de acceso global para actividades de combate (De Vergara y Trama, 2017).

Figura 5. Ejemplo reducido de análisis de Factores cibernéticos

CDG CIBERESPACIAL	**CC**
Sistema e infraestructura de comunicaciones de Israel	Implementar ciberataques contra los sistemas e infraestructura de sistemas de información por medios manuales propios y utilizando a Rusia como proxy
	Infectar los sistemas de información militar del enemigo con virus informáticos, gusanos o malware para robar o reunir información infiltración en los sistemas o spear fishing – Stuxnet/Flame-.
	Implementar ataques DDOS
VC	RC
Falta de especialistas cibernéticos talentosos y especialistas en los ámbitos de planificación de las organizaciones militares.	Formar un equipo de redes sociales que trabaje permanentemente
Uso limitado de actividades de ciber información.	Un gran número de computadoras zombies y botnets

Fuente: elaboración propia modificada del ejemplo de Análisis presentado por el Grl Evergisto De Vergara y el Contraalmirante Adolfo Trama en el Manual de Operaciones Militares Cibernéticas de Karaman y otros.

Conclusiones parciales al tercer objetivo:

El contenido del tercer capítulo sigue la pregunta de: Definir las operaciones a ejecutar en el ciberespacio para proteger la información y los circuitos en el nivel GUB y equivalentes

Para lograr esto, es necesario desarrollar capacidades de respuesta cibernética que permitan responder a un posible ciberataque y estar preparados para entrar en acción de forma proactiva. Por esto, el desarrollo de las ciberoperaciones defensivas "activas y pasivas", de exploración y el entendimiento de la Ingeniería social permitirán conformar un sistema en condiciones de volver a su estado inicial en cortos períodos de tiempo al ser atacado. Esto permitirá ser efectivos en cuanto a la ciberresiliencia en las estrategias de ciberseguridad y estar en capacidad de recobrar la iniciativa.

También se explica un proceso reducido para determinar el CDG de las ciberoperaciones, ya que el nivel táctico tiene un papel preponderante con la concreción de los puntos decisivos y los objetivos del plan de campaña, el cual se lo relaciona con el desarrollo de la campaña.

Un aspecto fundamental a tener en cuenta es, que el campo de combate moderno se está librando permanentemente en la mente de las personas, diferentes organizaciones privadas y estatales manipulan la percepción emocional de las personas. También los elementos cibernéticos en la actualidad producen respuestas más destructivas que cualquier arma convencional.

Conclusiones Finales:

El objetivo general que da origen a esta investigación es, Estandarizar el empleo de las ciberoperaciones en el marco de la GUB.

Se puede afirmar que:

El marco legal vigente se está actualizando con respecto a las potencias de primer mundo en el ciberespacio. Sin embargo, la actitud básica reactiva de la República

Argentina, y el espíritu que da lineamiento a nuestro marco legal, separando Defensa de Seguridad Interior, sumado a la ausencia de una legislación particular para las acciones ofensivas en el ciberespacio, dificultan el desarrollo de capacidades ofensivas para la defensa de las infraestructuras críticas y la información que las sostienen. Esto genera incoherencias en su aplicación ya que para ejecutar ciberoperaciones defensivas se necesita de la ejecución de ciberoperaciones ofensivas y viceversa.

Se debe actualizar la doctrina rectora mencionada en el ámbito de la fuerza, ya que esta es obsoleta y restrictiva en cuanto a las tareas que enumera. Asimismo, se visualiza contradictoria, en cuanto a su finalidad cuando se refiere a la ciberdefensa indirecta, ya que si se pretende disputar el control del ciberespacio es necesario incorporar medidas de carácter activo que me permitan mantener la iniciativa.

La descripción de las ciberoperaciones ofensivas, defensivas, de exploración e informacion con sus efectos permite tener un análisis general de las principales causas y consecuencias de las operaciones en el ciberespacio donde interactua la GUB con sus sistemas de armas. Esto coadyuva a entender que, la obtención de la superioridad en el ciberespacio es un prerrequisito para la efectividad de las operaciones militares en todos los dominios. La pérdida del control en este dominio en la actualidad se traduce en la carencia de comunicaciones fiables, de precisión, lo cual dificultará el comando y control del Comandante.

El campo de batalla actual se está librando en la mente de las personas, teniendo en cuenta que las operaciones en el ciberespacio se basan en efectos y uno de ellos es manipular la realidad. Es pertinente llegar a la conclusión que el momento más propicio para que el CDG de las ciberoperaciones coincida con el de la campaña es

durante la fase preparación. En esta afirmación se tiene en cuenta que no hay un conflicto igual al otro. Sin embargo, los conflictos actuales tienen algo en común que es la influencia sobre la percepción emocional de las personas debido a la alta dependencia de las tecnologías de la información en la vida humana.

Por otro lado el dominio del ciberespacio debe estar en todo planeamiento y solo puede ser tratado por aquellos soldados que tienen el conocimiento y, la experiencia para planificar, organizar, controlar, coordinar y dirigir esta dimensión.

La naturaleza de la guerra subjetiva de Clausewitz cambió, por lo cual solo los cibersoldados están y estarán en condiciones de ver la fricción del combate, que el genio militar prusiano dispuso en su libro de la guerra.

Por otro lado, el factor más influyente en este ambiente es la alta dependencia de los sistemas de armas con respecto a las nuevas tecnologías. Estos factores hacen que el CDG de las ciberoperaciones tenga un papel protagónico en el campo de batalla actual y futuro.

BIBLIOGRAFÍA

ROB Convención Nacional Constituyente. (1994). *Constitución de la Nación Argentina.* Recuperado de http://www.infoleg.gob.ar.

Poder Ejecutivo Nacional. (2018). Directiva de Política y Defensa Nacional. CABA.

Decreto 1691, Directiva sobre Organización y funcionamiento de las Fuerzas Armadas (22 de noviembre de 2006).

America, D. o.-t. (8 de junio de 2018). Cyberspace Operations. GL-4 (5-70). Washington DC, United States of America: Joint Publication.

Anca, L. (2015). *La Conducción de Operaciones de Ciberdefensa.* Ciudad Autónoma de Buenos Aires.: TFI, Escuela Superios de Guerra.

Argentino, E. (2015). *Conducción para las Fuerzas Terrestres (Capítulo VII- Sec XV Art 7100 y Anexo 3).* Buenos Aires: Departamento Doctrina.

Argentino, E. (2016). *Conceptos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza.* Buenos Aires: Departamento Doctrina (Dirección de Comunicaciones e Informática).

Arquilla y Ronfeldt. (2003). *Redes y guerras en red. El futuro del terrorismo, el crimen organizado y el activismo.* Madrid, España: Alianza.

Brett, W. (2011). ten propositions regarding cyberspace operations. *Joint Force Quarterly 61 second quarter*, 11-17.

Bruce Schneier. (2018). *Resiliencia: Aproximación a una marca de medición.* España, España.

Carrillo, M. R. (15 de noviembre de 2015). El Ciberespacio y la ciberseguridad. Consideraciones sobre la necesidad de un modelo Jurídico. *Una aproximación a la naturaleza del ciberespacio y la ciberseguridad*. Madrid, España.

Cicerchia, C. D. (20 de mayo de 2019). Ingeniero en Sistemas. (C. I. Cabrera, Entrevistador) Buenos Aires.

Corletti Estrada. (2017). *Ciberseguridad, Una Estrategia Informático/Militar.* Madrid, Madrid, España: Recuperado de http://www.darfe.es/joomla/.

Corletti Estrada, A. (2016). *Seguridad en Redes.* Madrid, Madrid, España: Recuperado de http://www.darfe.es/joomla/.

Corletti Estrada, A. (2011). *Seguridad por Niveles.* España: Recuperado de http://www.darfe.es/joomla/.

De Vergara y Trama. (2017). *Operaciones Militares Cibernéticas.* (E. S. Armadas, Ed.) Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina: Visión Conjunta.

Defensa, M. d. (25 de octubre de 2019). Legislación y avisos Oficiales. *Legislación y avisos Oficiales*. CABA, Argentina.

Departamento de Comunicación del Ejército de Tierra. (30 de septiembre de 2015). *Ejército de Tierra del reino de España.* Obtenido de http://www.ejercito.mde.es/unidades/Valencia/boncimic/Actividades/index.html

Ejército Argentino. (2011). *Conducción del Batallón de Comunicaciones.* Recuperado de http://www.esgcffaa.mil.ar.

Ejército Argentino. (2015). *Conducción para las Fuerzas Terrestres.* Recuperado de http://www.esgcffaa.mil.ar.

Escuela Superior de Guerra Conjunta. (2015). *Arte y Diseño Operacional.* Buenos Aires: Visión Conjunta.

Estado Mayor Conjunto de las Fuerzas Armadas. (4 de octubre de 2015). *Página del Estado Mayor Conjunto de las Fuerzas Armadas*. Obtenido de http://www.fuerzas-armadas.mil.ar/CCTZI.aspx

Gniesko, C. I. (2017). *Análisis de las herramientas disponibles para la determinación de un CDG.* Escuela de Guerra Conjunta. CABA: Escuela Superior de Guerra.

Gomez de Agreda, A. (2012). *El ciberespacio. Nuevo escenario de confrontación.* Universidad Politécnica de Madrid. Malaga: Ministerio de Defensa.

Gómez, M. O. (2017). *La resiliencia aplicada al nivel operacional en el ambiente cibernético.* CABA: Escuela Superior de Guerra Conjunta.

Grimes, R. (2018). *Hackear al Hacker.* ESPAÑA: MARCOMBO.

Grogovinas, C. (2017). *Diseño de un Elemento de Ciberoperaciones en apoyo a la GUB.* Ciudad Autónoma de Buenos Aires.: TFI, Escuela Superior de Guerra.

Guimpel, L. A. (24 de mayo de 2019). Oficial de Estado Mayor, Analista de Sistemas. (C. I. CABRERA, Entrevistador) Buenos Aires.

Honorable Congreso de la Nación. (5 de Mayo de 1988). Ley de Defensa Nacional N° 23.554. *Boletín Oficial 26375*, 4. Ciudad Autonoma de Buenos Aires, Argentina.

Honorable Congreso de la Nación. (1988). *Ley de Defensa Nacional núm. 23.554.* Recuperado de http://www.infoleg.gob.ar.

Honorable Congreso de la Nación. (17 de Enero de 1992). Ley de Seguridad Interior N" 24.059. *Boletín Oficial 27.307*. Ciudad Autonoma de Buenos Aires, Argentina.

Honorable Congreso de la Nación. (18 de Febrero de 1998). Ley de Reestructuracion de las Fuerzas Armadas N° 24.948. *Boletín Oficial 28874*. Buenos Aires, Argentina.

Honorable Congreso de la Nación. (1998). *Ley de Reestructuración de las Fuerzas Armadas núm. 24.948.* Recuperado de http://www.infoleg.gob.ar.

Honorable Congreso de la Nación. (29 de Agosto de 2008). Ley Justicia Militar N" 26.394. *Boletín Oficial 31478* . Ciudad Autonoma de Buenos Aires, Argentina.

Howard y Paret . (1976). *Clausewitz, Carl von, On War.* Princeton University Press. Nueva Jersey: (Princeton University Press, 1976).

Kaplan, F. (2016). *The secret history of Cyber War.* New York: Simon & Schuster.

Kenny, Locatelli, Zarza. (2015). *Arte y Dideño Operacional.* Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina: Visión Conjunta.

Llongueras Vicente. (2013). *La Guerra Inexistente, la Ciberguerra. Ciberdefensa.* Saarbruchen, Saarbruchen, Alemania: Académica Española.

López Hernadez Ardieta, J. (2013.). *Capacidades Esenciales para una Ciberdefensa Nacional.* Panamá: Indra.

López Rosetti. (2019). *Equilibrio.* CABA: planeta.

Lucero, J. (2015). *Ciberdefensa. La dimensión desconocida.* Buenos Aires: Revista Visión Conjunta Nro 12.

Miessler, D. (octubre de 2019). *The Difference Between Red, Blue, and Purple Teams*. Recuperado el 15 de octubre de 2019, de The Difference Between Red, Blue, and Purple Teams: https://danielmiessler.com/study/red-blue-purple-teams/

Ministerio de Defensa de Argentina. (1998). *Diccionario para la Acción Militar Conjunta, RC 00-02*. Buenos Aires: Ministerio de Defensa de Argentina.

Moliner González, J. (2 de Agosto de 2016). *Instituto Español de Estudios Estratégicos(Varsovia, La cumbre de la OTAN en)*. Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO79bis-2016_CumbreOTAN_Varsovia_Moliner.pdf

Moresi, A. (Abril de 2019). *Observatorio Argentino del Ciberespacio*. Recuperado el 3 de mayo de 2019, de http://www.cefadigital.edu.ar/bitstream/123456789/1157/1/2019%2004%20BOLETIN%20OAC.pdf

Moressi, A. (octubre de 2019). Curso de Ciberdefensa y Ciberseguridad. *Relación entre los ambientes operacionales*. CABA, CABA, Argentina.

Nacional, P. E. (13 de Abril de 1988). Ley de Defensa Nacional 23554. *Ley de Defensa Nacional 23554*. CABA, CABA, Argentina.

Nacional, Poder Ejecutivo. (9 de Amyo de 2019). *Directiva Estratégica de Ciberseguridad de la República Argentina.* CABA.

NATO. (2008). *CCDCOE*. Obtenido de Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/

NATO. (2013). *Allied Joint Doctrine for Civil-Military Cooperation (AJP-3.4.9).* Bruselas.: NATO Standarzition Agency (NSA).

NATO, I. C. (2013). *CIMIC Capabilities Handbook.* Sofia: CIOR.

ONU. (1974). *Resolución 3314 de la Assemblea general de las Naciones Unidas sobre definición de la agresión.* Recuperado el 2019, DE ONU: https://www.acnur.org/fileadmin/Documentos/BDL/2007/5517.pdf

OTAN. (2017). *Manual de Tallin 2.0 Leyes Internacionales aplicables a las ciberoperaciones.* (C. University, Ed.)

PC20-01. (2017). Planeamiento para la Acción Militar Conjunta NO. 13-29. Buenos Aires: Ministerio de Defensa de Argentina.

Poder Ejecutivo Nacional . (22 de Diciembre de 2014). Decreto 2645. Directiva de Política de Defensa Nacional. *Boletín Oficial 33052*, 4. Buenos Aires, Argentina.

Poder Ejecutivo Nacional. (2006). *Decreto 1.691/06. Directiva sobre Organización y Funcionamiento de las Fuerzas Armadas.* http://www.infoleg.gob.ar.

Poder Ejecutivo Nacional. (22 de Noviembre de 2006). Decreto 1691. Directiva sobre Organizacion y Funcionamiento de las Fuerzas Armadas. *Boletín Oficial 31043*, 3. Buenos Aires, Argentina.

Poder Ejecutivo Nacional. (12 de Junio de 2006). Decreto 727. Reglamentacion de la Ley 23.554. *Boletín Oficial 30925*, 1. Ciudad Autonoma de Buenos Aires, Argentina.

Poder Ejecutivo Nacional. (2006). *Decreto 727/06. Reglamentación de la Ley núm. 23554.* Recuperado de http://www.infoleg.gob.ar.

Poder Ejecutivo Nacional. (10 de Noviembre de 2009). Decreto 1714. Directiva de Política de Defensa Nacional. *Boletín Oficial 31779*. Buenos Aires, Argentina.

Poder Ejecutivo Nacional. (9 de Amyo de 2019). *Directiva Estratégica de Ciberseguridad de la República Argentina.* CABA.

Quinn, J. B. (1980). Estrategias para el cambio. 293-305.

Ramió, C. (2019). *Inteligencia Artificial y Administración Pública.* Madrid: Catarata.

Real Academia Española. (2016). *Diccionario de la Lengua Española.* Recuperado de http://www.rae.es/.

Rio, A. G. (2013). El Ciclo OODA y la toma de decisiones en el Planeamiento. *Trabajo Final Integrador (Planeamiento Operacional)*, 4-13. CABA, Buenos Aires, Argentina: CEFA digital.

ROB00-01. (2015). Conducción para las Fuerzas Terrestres (Capítulo VII- Sec XV Art 7100). 54-56. Buenos Aires, Buenos Aires, Argentina: Departamento Doctrina.

ROD05-01. (2016). Conceptos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza(Ejército Argentino). Buenos Aires: Departamento Doctrina (Dirección de Comunicaciones e Informática).

Rosetti, D. L. (2019). *Equilibrio.* (E. Planeta, Ed.) CABA, CABA, Argentina: Planeta.

Salazar, J. (2016). *La migración de la guerra al espacio digital.* Recuperado de https://www.sites.oas.org/cyber/Documents/2016%20-%20La%20migracio%CC%81n%20de%20la%20guerra%20al%20espacio%20digital-Juan%20Pablo%20Salazar.pdf.

Salis, E. (2010). *Ethical Hacking.* Buenos Aires: Alfoamega.

Snowden, E. (2019). *Vigilancia Permanente.* Buenos Aires: Planeta.

Stel, E. (2005). *Guerra Cibernética.* Buenos Aires: Círculo Militar.

Teniente Coronel del Ejército de Portugal da Silva Perdigao, H. A. (s.f.). Lod.

Trump, D. (2018). *National Cyber Strategy of the United States of America.* Washington DC, United States of America: The White House.

US Army. (2014). *Civil Military Operations (FM 3-57).* Washington: TRADOC.

US Joint Publication. (2013). *Civil Military Operations (JP 3–57)*. Washington: DOCNET.

Uzal, R. (Noviembre de 2015). *http://www.cari.org.ar/pdf/boletin62.pdf*. (C. ". Internacionales", Editor, & ISIAE"Instituto de Seguridaad Internacional y Asuntos Estratégicos ") Recuperado el mayo de 2019, de http://www.cari.org.ar/pdf/boletin62.pdf: http://www.cari.org.ar/pdf/boletin62.pdf

Van Creverd, M. (2007). *La transformación de la Guerra.* (UCEDA, Ed.) Buenos Aires, ARgentina: Reimpresión Buenos Aires. 2007 . UCEDA.

Vargas Vargas, M. (2014). *CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA*. Bogota: Recuperado de http://repository.unimilitar.edu.co/bitstream/10654/12259/1/CIBERSEGURIDAD%20Y%20CIBERDEFENSA.%20TRABAJO%20DE%20GRADO.pdf.

Vego, M. (2007). *Joint Operational Warfare. Theory and Practise.*

Vergara, D. (2010). El estudio de la historia militar. La evolución del pensamiento estratégico. *Visión Conjunta*.

Anexo 1 : <u>Entrevista Cnl Daniel Cicerchia 140830May19 (100 minutos)</u>

1) La ciberdefensa es exclusiva de los militares.

Responde: No. Si bien la columna vertebral de la ciberdefensa es de los militares, en la actualidad hay muchas organizaciones y universidades que viven y trabajan sobre esta problemática a diario. Por tal motivo, la ciberdefensa debería manejarse de manera holística teniendo en cuenta todas las organizaciones (ejemplo: Israel, Rusia, EEUU y España).

2) Cómo se estructura la ciberdefensa que elementos la componen.

Responde: Recién en la actualidad se están estableciendo relaciones de Comando entre el Estado Mayor Conjunto y los ámbitos específicos, lo cual limita la preparación y el avance en este dominio debido a cuestiones culturales principalmente. Desde el punto de vista estratégico también hay cosas desnaturalizadas, como por ejemplo la inclusión del Ministerio de Modernización otorgándole las Infraestructuras críticas a ese Ministerio y no a Defensa. No así, como lo desarrolló Brasil, Alemania o Chile que rápidamente entendieron que este dominio necesita tomar decisiones con perentoriedad. Lo cual lo obliga a la Argentina a trabajar en la actualidad de manera reactiva.

3) Como dividiría a las ciberoperaciones. Y cuál es la finalidad de cada una de ellas. (Ofensivas, Defensivas y de Información).

Responde: En general se dividen en Ofensivas, Defensivas. Lo más importante es entender es que técnicamente quién se defiende bien no sabe atacar y, lo mismo a viceversa. Por esto potencias como Israel tienen divididas las operaciones ofensivas y defensivas en diferentes grupos.

4) Hasta que nivel es conveniente planificar las ciberoperaciones (Nivel Estratégico Nacional, Militar, Operacional, Táctico (BR?)).

Responde: La ciberdefensa debería planificarse en todos los niveles, sin lugar a dudas, esto permitirá que si bien un nivel como el táctico no disponga de los medios su

recurrencia ante la necesidad de lograr algún efecto en el desarrollo de las operaciones. Así mismo, rápidamente se debe dotar en todos los niveles a personal y fracciones capacitados inicialmente para trabajar en este dominio y fomentar el perfeccionamiento constante ya que el personal que opera en este dominio se debe perfeccionar a diario. Todos los elementos de comunicaciones deberían ser convertidos en elementos de ciberguerra debido a que manejan las redes y tienen la preparación básica para poder explotar este dominio.

5) Las operaciones de información se ejecutan en todo momento.

Responde: Si, pero son responsabilidad a mi juicio del Área de Inteligencia y utilizan al ciberespacio como medio. Ellas buscan afectar el proceso de toma de decisiones.

6) Qué relación tienen estas con los MCS.

Responde: Se relacionan con los medios de comunicación social para los cuales la ciberdefensa es un medio.

7) Cuál es la oportunidad para ejecutar ciber operaciones ante un conflicto.

Responde: Las ciberoperaciones se deben desarrollar en todo momento. Si pensamos en una campaña deberían ejecutarse en todas sus fases y al igual que las comunicaciones o la guerra electrónica comienzan a operar ante del despliegue de las tropas. En la actualidad la ciberdefensa, las comunicaciones y la guerra electrónica son inseparables.

8) Las ciberoperaciones pueden considerarse el CDG de las operaciones?.

Responde: Piense en un conflicto con intereses económicos, la zona de interés del ciberespacio puede ser el mundo. En el nivel Operacional que se encuentra acotado a un teatro de operaciones determinado, una fuerza cibernética ofensiva puede tener la misma forma de operar que las fuerzas especiales. Sin embargo, la principal diferencia es que esta va a estar constituida por todo tipo de personal incluso muchos civiles que tengan la capacidad de operar en este dominio, las fuerzas especiales utilizan partisanos

para operar dentro del dispositivo enemigo. En el ciberespacio es mucho más utilizado pero debe ser bien conducido.

Por otro lado la conducción de las operaciones en el TO deben ser del Comandante porque él tiene la responsabilidad de llevar a cabo los efectos en las operaciones cuente o no con los medios

8) Cuáles son los principales efectos que buscan las ciberoperaciones.

9) La Percepción de los pueblos o líderes se relacionan con los efectos a producir en las ciberoperaciones.

Responde: Sin duda es uno de los efectos pero también se relaciona con las operaciones de información

10) La ciberdefensa tiene un departamento que mide la aplicación de los efectos permanentemente.

Responde: Hoy se encuentra en desarrollo y lo más importante es generar las capacidades iniciales para poder ver efectos en este espacio.

11) Podemos decir que la afectación de la percepción de la población es un efecto importante a cumplir por la ciberdefensa cuando se intenta modificar el proceso de toma de decisiones al más alto nivel.

Responde: Sin dudas la ciberdefensa es un medio que actuara para modificar el proceso de toma de decisiones.

12) Quien determina o como se determinan los efectos en ciberdefensa.

Responde: Los efectos los determina el elemento que los ejecuta siempre y cuando se vaya a reconocer como autor del hecho.

13) Podrá responderse a un ataque cibernético de manera cinética

Responde: Sin dudas ya está ocurriendo, pero nuestro país aún no hay nadie que estudie lo que ocurre en medio oriente y en el mundo

14) Usted cree que la sociedad Argentina perciben las operaciones en las redes como una amenaza.

Responde: En general No, del 100 por ciento de la población solo un 10 por ciento está informada y conoce las implicancias de este dominio. Compare la historia reciente como por ejemplo Estonia 2007, que pasaría si la sociedad Argentina sufriese un ciberataque de esa magnitud. Que capacidades deberíamos formar para tratar de contrarrestar algo así o defender nuestras estructuras críticas.

15) Como ubicaría a nuestro país desde la conciencia con respecto a la ciberguerra en el contexto mundial.

Responde: Extremadamente bajo. Consulte la cantidad de intromisiones diarias que reciben todos los organismos del Estado o diferentes empresas privadas y podrá corroborar esta afirmación. En general es muy bajo con respecto a los países de la región incluso, como Brasil y Chile.

Anexo 2 : <u>Entrevista al Cnl Luis Pablo Guimpel 070800Jun19 (100 minutos)</u>

1. Que es la ciberdefensa

   Responde: Para entender la ciberdefensa es necesario aclarar algunos términos. Hay tres términos que siempre se confunden, seguridad informática, ciberseguridad y ciberdefensa. La seguridad informática es la protección de la triada CID (confiabilidad, integridad y disponibilidad de los datos). Datos: redes informáticas y digitales.

   La ciberseguridad, es una política estratégica nacional que está referido al logro de la protección de las infraestructuras críticas (ICC). Una ICC es una plataforma que provee un servicio esencial para los intereses nacionales. Ejemplo, si yo a traves de un ataque cibernético modifico la fórmula de un medicamento para que sea tóxico puedo llegar a matar gente, si yo rompo los controles de temperatura o presión atmosférica en una central nuclear puedo causar una explosión nuclear como Stuxnet en Irán y matar gente.

   Por otro lado la ciberdefensa es el logro de la política nacional de ciberseguridad en las infraestructuras críticas de la defensa nacional, las cuales incluyen las ICC militares y las que se le asignan al Ministerio de Defensa.

2. La ciberdefensa es exclusiva de los militares.

   Responde: No. Si bien la columna vertebral de la ciberdefensa es de los militares, en la actualidad los objetivos se cumplen de acuerdo a como son asignados por la Secretaria Nacional de Ciberdefensa.

3. Cómo se estructura la ciberdefensa que elementos la componen.

   Responde: Hay un Comité de Ciberseguridad creado en el ámbito de Modernización, lo integran representantes de todos los ministerios y organizaciones privadas que tienen ICC. La organización para el trabajo de ciberdefensa está dado en dos niveles el CERT y el SOC. El CERT está distribuido en todas las organizaciones y después cada organismos tiene su SOC que es el centro de operaciones. Las ordenes y efectos a lograr los establece el Poder Ejecutivo, en la actualidad se están desarrollando capacidades y nuestros SOC trabajan diariamente con más de 1000 intrusiones diarias.

4. Como dividiría a las ciberoperaciones. Y cuál es la finalidad de cada una de ellas. (Ofensivas, Defensivas y de Información).

Responde: En general se dividen en Ofensivas, Defensivas y de Exploración. Lo más importante es entender es que técnicamente quién se defiende bien debe desarrollar su capacidad para atacar. Esto va a depender del nivel de los actores, solo los actores de nivel 3 poseen los recursos para sostener un ciberataque en el tiempo. Los actores de nivel 1 y 2 son fáciles de bloquear.

5. Hasta que nivel es conveniente planificar las ciberoperaciones (Nivel Estratégico Nacional, Militar, Operacional, Táctico (BR?)).

Responde: La ciberdefensa debería planificarse en todos los niveles pero el mayor detalle en este caso lo tendrá el nivel estratégico. Sin embargo debe planificarse hasta el nivel Unidad Táctica.

6. Las operaciones de información se ejecutan en todo momento.

Responde: Si, son permanentes. Ellas buscan afectar el proceso de toma de decisiones. Hemos tenido muchos intentos de intrusión en el comando electoral, durante el G20 y permanentemente en las redes que controla el Comando Conjunto de Ciberdefensa con los CERT(s) Y SOC(s).

7. Qué relación tienen estas con los MCS.

Responde: Todos ya que las mismas planifican efectos para ser ejecutados en gran parte con los medios de comunicación social, en el cual la ciberdefensa es un medio.

8. Cuál es la oportunidad para ejecutar ciberoperaciones ante un conflicto.

Responde: Las ciberoperaciones se deben desarrollar en todo momento. Si pensamos en una campaña deberían ejecutarse en todas sus fases y al igual que las comunicaciones, estas se deben ejecutar en todas las capas del ciberespacio. La ciberdefensa, la guerra electrónica y las comunicaciones son inseparables en la actualidad.

9. Las ciberoperaciones pueden considerarse el CDG de las operaciones.?.

Responde: Pensando en los tres grandes conflictos Estonia, Georgia y Ucrania. Luego de estonia 2007 la OTAN estableció que cualquier ciberataque es considerado un acto de guerra, por este motivo los potencias intentan no atribuirse los ciberataques que ejecutan permanentemente. Si suponemos que Rusia estableció un plan de campaña para atacar a la nación más digitalizada del mundo en Estonia 2007, sin dudas la ciberdefensa fue el CDG. Ahora yendo a Georgia donde Rusia si se atribuyó el ciberataque Rusia durante una semana logro paralizar a ese país dejándolo sin comando y control y una vez frenado este invadió con tropas convencionales, ahí no es el CDG la ciberdefensa, habrá sido el CDG de esa fase. En esa fase el CDG fue ciberdefensa. En ucrania el ataque cibernético se hizo con tropas, EEUU divide al ciberespacio en tres capas. Una capa física, una capa lógica y una capa social siempre y cuando los objetivos se dirijan contra un backbone o cualquier. Las ciberoperaciones pueden ser el CDG dependiendo de la campaña. En una guerra convencional el CDG no es la ciberdefensa, pero el mundo hoy no está viviendo ese tipo de conflictos.

Todo va a depender también de cual sea el objetivo estratégico nacional para determinar si la ciberdefensa puede ser o no el CDG de la campaña.

10. Cuáles son los principales efectos que buscan las ciberoperaciones.

Responde: del tipo de ciberoperacion a ejecutar. Las ciberoperaciones ofensivas por lo general tienen efectos de neutralizar o manipular mientras que el principal efecto de las ciberoperaciones defensivas es proteger.

11. La Percepción de los pueblos o líderes se relacionan con los efectos a producir en las ciberoperaciones.

Responde: Sin duda es uno de los efectos más importantes que intentara modificar el proceso de toma de decisiones.

12. La ciberdefensa tiene un departamento que mide la aplicación de los efectos permanentemente.

Responde: Si tenemos ya que el Comando conjunto de Ciberdefensa funciona como cualquier Unidad. Hoy se encuentra en desarrollo y lo más importante es generar las capacidades iniciales para poder ver efectos en este espacio.

13. Podemos decir que la afectación de la percepción de la población es un efecto importante a cumplir por la ciberdefensa cuando se intenta modificar el proceso de toma de decisiones al más alto nivel.

Responde: Sin dudas las ciberoperaciones son un medio que actúan para producir efectos sobre la población, sino estudiemos los conflictos como Estonia, Ucrania y Georgia si uno de los actores no generó las condiciones sobre la población para inclinar los conflictos a su favor.

14. Quien determina o como se determinan los efectos en ciberdefensa.

Responde: Los efectos los determina el Poder Ejecutivo por medio de la Secretaria de Ciberdefensa.

15. Podrá responderse a un ataque cibernético de manera cinética

Responde: Sin dudas ya está ocurriendo, pero nuestro país aún no tiene desarrollado en forma completa el marco legal. Sin embargo la OTAN y el manual de Tallin lo establecen.

16. Usted cree que la sociedad Argentina perciben las operaciones en las redes como una amenaza.

Responde: En general No, la sociedad Argentina es extremadamente crédula.

17. Como ubicaría a nuestro país desde la conciencia con respecto a la ciberguerra en el contexto mundial.

Responde: Bajo. Pero estamos desarrollando las capacidades para estar a la altura de los países de la región como Brasil.