UNDEF Universidad de la Defensa Nacional

Ministerio de Defensa Argentina

DIPLOMATURA INTERNACIONAL EN COMUNICACIÓN Y DEFENSA NACIONAL

TRABAJO INTEGRADOR FINAL

"EL CIBERESPACIO COMO ELEMENTO DE PODER DEL ESTADO"

Una aproximación teórica a la consideración de su importancia para la Defensa Nacional

Autor: Lic. Jorge Alberto Antonio Santoro

DNI N°: 13.214.305

Email: jorge132004@yahoo.com.ar

Celular: 15-2691-7617

Tutora: Sandra Verónica Echevarne

Marzo de 2021

Comisión N° 1

Primera Cohorte

Índice

El ciberespacio como elemento de poder del Estado

Presentación:

De los ejes temáticos desarrollados en la cursada de la Diplomatura, se seleccionó el referido a Geopolítica para la Defensa, y dentro del mismo, la Ciberdefensa y sus desafíos.

Por ello, se intenta brindar un marco de referencia sobre el nuevo dominio de la guerra: el ciberespacio.

Se trata de analizar y difundir las distintas consideraciones que hacen a esta temática.

Se presenta un informe a fin de que sea publicado en la plataforma YouTube.

Se consultó bibliografía, especialmente en inglés, pero también ciertos trabajos académicos cuyo detalle figura en el anexo II del presente.

El trabajo incluye una Línea del Tiempo de ataques informáticos, en la plataforma Thinglink.

El alcance de este trabajo, es informar y concientizar sobre los peligros que acechan en el ciberespacio.

Se utiliza un lenguaje llano, para que lo interpreten distintas audiencias.

1 - Introducción

El Ciberespacio

En su uso común, se refiere a los sistemas de información y proceso de datos interconectados por redes de comunicaciones.

La palabra proviene del griego cibernético (κσβερνήτης) - “piloto” o “timón” usado por el matemático Norbert Wiener en su obra “Cybernetics: or Control and Communication in the Animal and the Machine” (Cibernética: o control y comunicación en personas y máquinas), para describir la tecnología de sistemas de control

La Real Academia Española lo define como “ámbito artificial creado por medios informáticos”.

El Pentágono lo reconoce como el quinto dominio de la guerra junto a tierra, mar, aire, y espacio.

El Capitán de Navío Ingeniero Pablo D. Sorrentino detalla temporalmente el origen de los diferentes ámbitos operacionales para la actividad:

1) El terrestre, que surgió 5000 años atrás, con la invención de la rueda.

2) Cuando el hombre se aventuró al mar, surgió el marítimo, hace 2500 años.

3) Debieron de pasar milenios para que el sueño de volar se convirtiese en realidad en 1903.

4) El espacio dejó de ser una frontera para la humanidad en 1961 (Sorrentino, 2018).

5) El ciberespacio es una realidad, habiéndose inmiscuido en nuestras vidas poco a poco, llegando hoy a un punto sin retorno; ya que nadie puede vivir sin él. Aunque el ciberespacio existe desde la invención de la transmisión electromagnética, en su percepción contemporánea nació con la aparición de computadoras personales (alrededor de 1975), el protocolo de Internet (alrededor de 1982) y la World Wide Web (alrededor de 1989). Hoy en día, una porción en continuo aumento de la actividad humana internacional, se lleva a cabo dentro o a través de este espacio en expansión. Los gobiernos se han vuelto cada vez más dependientes del ciberespacio.

Se debería pensar en el ciberespacio como el espacio que no está restringido a Internet, sino que incluye también redes aisladas, todos los sistemas industriales conectados a Internet o redes aisladas a través de los sistemas de control de supervisión y adquisición de datos (SCADA), las industrias de la comunicación y de los sistemas de la información, así como las industrias de producción de software y repuestos, todas las instituciones académicas relacionadas con la tecnología de la información en general, y las personas y la interacción social dentro de ellas.

La protección del ciberespacio es esencial para preservar la seguridad y defensa de la nación y su economía, por lo tanto, la adopción de una Política Nacional de Ciberseguridad y Ciberdefensa que involucre a todos los sectores de la sociedad, bajo el liderazgo del Ministerio de Defensa en coordinación con los demás entes del Estado, es un imperativo al que debe darse la mayor de las prioridades.

Son pocas las personas que tienen conocimientos en temas relacionados con Ciberdefensa y Ciberseguridad y son menos las personas que tienen conciencia de las amenazas y peligros que a través del Ciberespacio afronta el país y por ende puede afectar no sólo a las Fuerzas Armadas sino a sus habitantes.

La defensa y protección del Ciberespacio, se ha convertido en uno de los retos más importantes del Estado, debido a la continua evolución, crecimiento y complejidad de los ataques cibernéticos. De ahí surge la necesidad de disponer de personal idóneo que se adapte a entornos de continuos avances tecnológicos que permitan proteger al Estado ante posibles nuevas amenazas.

Para abordar con éxito esta problemática, se debe avanzar significativamente en concientizar y organizar en relación a la Ciberdefensa y Ciberseguridad.

2 - Características Generales

¿Qué es Ciberdefensa?

Es la capacidad del Estado para cumplir con las responsabilidades que le permitan prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales. También se conoce como el conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición. Se ha planteado iniciar el proceso de la Ciberdefensa por la Inteligencia Informática con el Ciberespacio como ambiente, para poder obtener los elementos que conformen la identificación de los escenarios y las amenazas, para poder dimensionar los riesgos y así posibilitar el diseño de los instrumentos de defensa.

¿Qué es Ciberseguridad?

Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno, lo que conlleva a la existencia de una situación de normalidad donde la población goce de niveles apropiados para utilizar los medios cibernéticos libres de cualquier amenaza o peligro.

El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una

preocupación común a nivel mundial dado que impacta de manera significativa la seguridad informática de las diferentes empresas en los ámbitos tanto público y privado, como al ciudadano mismo.

Si bien es cierto que la necesidad del Estado en aspectos de seguridad de la información es un factor crítico que requiere ser atendido, este es un campo muy amplio que abarca diferentes conceptos de seguridad física como de seguridad lógica (aplicación de barreras y procedimientos que resguarden la información), para proteger todos los medios en donde se encuentra la información.

En esta nueva era cibernética se hace necesario garantizar la seguridad de la información o por lo menos brindar pautas para que esta pueda ser segura dentro de determinados lineamientos, siendo cualquiera el carácter de la misma, sobre todo cuando es confidencial y puede afectar a una persona, a un grupo o a la Nación completa.

3 - Antecedentes

Como referentes de la normativa internacional en la materia es importante hacer mención de los siguientes esfuerzos:

La Organización de las Naciones Unidas – ONU ha abordado el tema desde 1998 bajo la denominación “Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, mediante la cual la Asamblea exhorta a los estados miembros a continuar promoviendo la revisión de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.

El Consejo de Europa adoptó en noviembre de 2001 el Convenio sobre Ciberdelincuencia (CCC, por sus siglas en inglés), entrado en vigor desde el 1° de julio de 2004, único instrumento vinculante vigente sobre el tema en el ámbito internacional, y su protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos.

En el ámbito hemisférico, la Asamblea General de la Organización de los Estados Americanos adoptó mediante la Resolución AG/RES 2004 (XXXIV-O/04) la Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética.

En Argentina, en 2011 se creó el Programa Nacional de Infraestructuras Críticas de la Información y la Ciberseguridad. Con él, se comenzó a pensar formalmente en la seguridad de información, creando recursos tales como un CERT (del inglés Computer Emergency Response Team: Equipo de Respuesta ante Emergencias Informáticas) nacional, brindando recomendaciones para los organismos de la Administración Pública Nacional, estableciendo políticas de seguridad de la información y más.

Por su parte, el Ministerio de Defensa empezó a pensar en cuestiones relacionadas a la defensa cibernética antes de 2010. Su proceso de creación de estructuras culminó en 2015, luego de creado el Comando Conjunto de Ciberdefensa y la Dirección Nacional de Ciberdefensa (denominada Subsecretaria de Ciberdefensa a partir de 2016). Por su parte, el Comando posee funciones operativas, siendo el encargado de detectar ciberamenazas, contrarrestarlas, lograr la resiliencia de los instrumentos afectados y alertar al Instrumento Militar sobre las vulnerabilidades del sistema. En consonancia con esto, la Subsecretaría tiene funciones relacionadas a las negociaciones para compras de insumos, trazados de políticas de ciberdefensa, supervisión del Comando Conjunto de Ciberdefensa, entre otros.

De esta forma, el instrumento militar se encuentra dotado de instrumentos tales como un Centro de Operaciones Cibernéticas y un Centro de Ingeniería Cibernética, aunque cada una de las fuerzas ha ido desarrollando su propia estructura y cuenta también con funciones y direcciones operativas que complementan al Estado Mayor Conjunto y al Ministerio de Defensa, pero que a la vez cumplen funciones propias de cada fuerza con el objeto de apoyar sus operaciones militares.

4 - Marco Conceptual

El delito cibernético contempla desde el acceso abusivo a un sistema informático, el diseño y propagación de código malicioso (virus), la pornografía infantil, el uso de la tecnología para fines delictivos como el hurto, la estafa y el tráfico de drogas, hasta la amenaza a la seguridad de los sistemas financieros, servicios públicos y demás infraestructuras críticas para cualquier Estado.

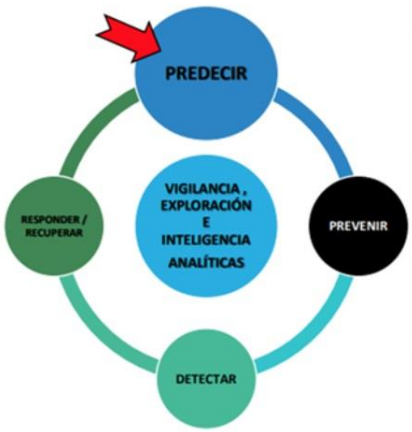
Es un delito dinámico que se vale de un supuesto anonimato para atentar contra la confidencialidad, integridad y disponibilidad de la información. Se ha constituido en un delito transnacional que plantea retos importantes a las autoridades en la labor de prevención, reacción, investigación y judicialización.

Los lineamientos para el desarrollo e impulso de la Ciberseguridad y Ciberdefensa consisten en la estructuración y articulación de las capacidades y mecanismos coordinados por el gobierno nacional con el fin de identificar y establecer acciones y responsabilidades tendientes a prevenir, preparar, controlar, recuperar y responder frente a todo tipo de incidentes o amenazas cibernéticas a las que puede estar expuesto el país.

Con el fin de lograr los objetivos propuestos es necesario involucrar todos los sectores e instituciones del Estado con responsabilidad en el campo de Ciberseguridad y Ciberdefensa. Igualmente, es de vital importancia crear conciencia y sensibilizar a la población en todo lo referente a la seguridad de la información.

Así mismo, se debe fortalecer los niveles de cooperación internacional en aspectos de Ciberseguridad y Ciberdefensa que permitan la integración, colaboración y cooperación con organismos dedicados a este mismo fin.

Ciclo de la ciberdefensa



PROCESO	ACTIVIDAD	TECNOLOGÍAS
PREDECIR	• ANÁLISIS PROACTIVO DE LA EXPOSICIÓN Y DEL RIESGO • PREDICCIÓN DE CIBERATAQUES • ANÁLISIS DE TENDENCIAS, TTP DE AMENAZAS Y VULNERABILIDADES (LÍNEA BASE DE SISTEMAS TIC)	• TECNOLOGÍAS BI • TECNOLOGÍAS AI / ML • HERRAMIENTAS ANALÍTICAS (HA) • SOFTWARE DE GESTIÓN DE VULNERABILIDADES Y AMENAZAS (SGVA)
PREVENIR	• ROBUSTECIMIENTO, SEGMENTACIÓN Y AISLAMIENTO DE SISTEMAS CRÍTICOS • VELO Y ENGAÑO DE ATACANTES • PREVENCIÓN DE INCIDENTES (ENSAYOS Y SIMULACIÓN)	• SGVA • SISTEMAS DE AUTOMATIZACIÓN DE LAS OP SEG (SAOS) • HERRAMIENTAS DE VIRTUALIZACIÓN Y SIMULACIÓN • TECNOLOGÍAS AI / ML
DETECTAR	• DETECCIÓN DE INCIDENTES • CONFIRMACIÓN Y PRIORIZACIÓN DEL IMPACTO • CONTENCIÓN DE INCIDENTES	• HA • SGVA y SIEM • SAOS • ML
RESPONDER / RECUPERAR	• SOLUCIÓN / IMPLEMENTACIÓN DE CAMBIOS DE SEGURIDAD • MODELADO / DISEÑO DE NUEVOS PROCEDIMIENTOS Y CONTROLES • INVESTICACIÓN INFORMÁTICA FORENSE	• SAOS • HA • SGVA y SIEM

Fuente: Ciberdefensa.online (Webinar *CIBERDEFENSA ¿cómo enfrentar este nuevo dominio militar?)*.

5 - Actores y amenazas en el ciberespacio

El ciberespacio se está volviendo cada vez más central para la economía de los estados y sus sociedades. El creciente papel del ciberespacio ha abierto nuevas oportunidades, pero al mismo tiempo ha creado nuevas amenazas, con las que los estados tienen que vivir, encontrando formas de identificarlas y mitigarlas.

Los actores del ciberespacio suelen agruparse en cuatro categorías a saber: delincuentes organizados, activistas, gobiernos extranjeros y grupos terroristas.

1. **Los delincuentes organizados:** están involucrados en todo tipo de actividades ilegales, como el robo de datos de tarjetas de crédito y otros robos de datos personales, que se utilizan para obtener beneficios económicos.

2. **Los grupos activistas motivados políticamente (hactivistas) o los individuos motivados ideológicamente:** buscan hacerse con el control de los sistemas informáticos o sitios web y utilizarlos para promover su causa particular, hacer una declaración política o interrumpir los servicios, y así ganar publicidad.

3. **En tiempos de paz, los gobiernos extranjeros, a través de sus servicios militares y de inteligencia,** realizan ciberespionaje contra los sistemas gubernamentales, la infraestructura nacional y las empresas que buscan

acceso a información comercialmente sensible, propiedad intelectual y secretos comerciales o estatales. En crisis o incluso en conflictos armados, los gobiernos extranjeros pueden (y utilizarán) el ciberespacio para infligir daño a sistemas críticos en apoyo de sus objetivos más amplios.

Los gobiernos extranjeros, en pos de sus objetivos en el ciberespacio, pueden solicitar servicios cibernéticos a representantes en forma de piratas informáticos "patrióticos" o incluso mercenarios en forma de piratas informáticos individuales, grupos o delincuentes solitarios y pagar por esos servicios.

4. Existe un fuerte razonamiento por el cual los grupos terroristas recurrirían al poder cibernético para infligir daño, dolor y terror a sus estados objetivo y sus sociedades; las armas cibernéticas son baratas, fáciles de adquirir o incluso de desarrollar; los ciberataques no requieren la presencia física de los perpetradores en los estados-objetivo y pueden ser lanzados desde casi cualquier punto del mundo; los estados-objetivo preferidos por los terroristas (occidentales) presentan un entorno rico en objetivos y exponen progresivamente objetivos de alto valor a posibles ciberataques; las tácticas de "disparar y olvidar" y el anonimato encajan perfectamente con el modus operandi de esos grupos; las represalias prácticamente no son posibles. A pesar de todas las ventajas mencionadas, los terroristas parecen hasta ahora reacios a utilizar el ciberespacio como campo de batalla prioritario, porque es dudoso que generen el nivel de pánico y terror generalizados que desean.

La actividades de los hactivistas y los delincuentes organizados, caen dentro de la autoridad de los organismos encargados de hacer cumplir la ley; las actividades de los gobiernos extranjeros y los grupos terroristas, son actividades cibernéticas puramente políticas, principalmente contra la seguridad nacional de un estado rival.

Estos actores, por la naturaleza de su actividad en y a través del ciberespacio, crean un entorno de ciberamenazas en evolución. Las ciberamenazas así creadas aumentan y evolucionan continuamente en sofisticación y frecuencia. Comprender esas amenazas es de suma importancia para la protección del ciberespacio por parte de los profesionales de la seguridad.

Hoy, ningún estado es inmune a los ciberataques. Los sistemas de gobiernos y empresas privadas han sido atacados a través del ciberespacio durante muchos años. Un ciberataque bien planificado puede interrumpir los servicios públicos, interferir con la producción y la entrega de bienes y servicios esenciales y tener un impacto negativo en la economía o resultar en el robo de propiedad intelectual o información personal y, en última instancia, amenazar la seguridad nacional.

La ciberamenaza merece y de hecho atrajo la atención de los estados como una amenaza nueva y en evolución que se ha convertido en una de las principales preocupaciones de seguridad de los líderes políticos y militares de todo el mundo. La

seguridad en la política mundial, no es una idea neutral ni simple y su percepción varía entre políticos y científicos por igual.

Las ciberamenazas planteadas por los actores del ciberespacio contra los estados-nación, pueden provenir de gobiernos extranjeros y sus representantes, así como de grupos terroristas, pero no únicamente de ellos.

Existen ciertas características del ciberpoder, que explican su creciente popularidad, lo que lo hace atractivo para diversos actores que recurren a actividades ilegales en el ciberespacio para sus propios fines. Esas características son únicas y, por lo tanto, los medios y las formas de combatirlas deben adaptarse al tema, si se quiere tener alguna posibilidad de éxito:

• Los ciberataques en el ciberespacio son económicos en el sentido de que el malware respectivo puede adquirirse fácilmente por un precio modesto o incluso descargarse gratuitamente de Internet.

• Los recursos necesarios para lanzar un ataque están limitados, en su extremo inferior, a computadoras o teléfonos inteligentes y malware que se puede adquirir fácilmente. Al mismo tiempo, los actores con habilidades básicas, con la ayuda de numerosos sitios en Internet, pueden causar daños considerables.

• Los ciberataques pueden lanzarse desde orígenes lejanos y geográficamente dispersos, contribuyendo así a dificultades en la detección y el enjuiciamiento ya problemático de los perpetradores.

• Los autores de actividades ilícitas corren un bajo riesgo de ser detectados y enjuiciados, pudiendo ocultar sus huellas.

6 - Conclusión

Con cada día que pasa, crece la dependencia del ciberespacio; y ya no hay vuelta atrás a un mundo sin él. Por otro lado, con el uso y dependencia cada vez mayores de Internet y las tecnologías digitales, aumenta la exposición y la vulnerabilidad a las ciberamenazas.

Las vulnerabilidades son una característica inherente de todo sistema creado por el hombre y el ciberespacio no es una excepción. Esas vulnerabilidades, siempre que puedan explotarse adecuadamente, constituyen la base para la creación de un entorno de amenaza en constante expansión para las actividades humanas realizadas dentro y a través del ciberespacio. Las ciberamenazas llamaron desde el principio la atención de los Estados-nación, ya que constituían una grave amenaza contra su seguridad, ya sea en el sentido más amplio o en su forma de seguridad nacional. Por lo tanto, defender el ciberespacio contra las ciberamenazas se convirtió en una prioridad para la mayoría de los gobiernos. Dado que, aunque las ciberamenazas trascienden las fronteras internacionales, existe una creciente necesidad de

cooperación entre naciones-estados, el sector privado y las entidades académicas para hacer frente a ellas.

Paralelamente al desarrollo de capacidades defensivas para la protección de su ciberespacio, los gobiernos, habiendo comprendido que el poder cibernético puede utilizarse para el logro de objetivos políticos, desarrollan sus capacidades ofensivas y llevan a cabo operaciones ofensivas en el ciberespacio que en tiempos de paz se limitan al espionaje y preparación para posibles conflictos cibernéticos. Dadas las capacidades cibernéticas actuales, parece que el poder cibernético puede por sí solo lograr objetivos políticos limitados, por lo que es un equivalente de los otros elementos del poder de un estado, a saber, la diplomacia, la información, el ejército y la economía.

Por otro lado, esas capacidades, combinadas con el nivel existente de infraestructura de comunicación e información de la mayoría de los oponentes potenciales estatales o no estatales, no son adecuadas para librar una ciberguerra autónoma, excepto en escala limitada e incluso entonces siempre combinadas con la amenaza del uso de fuerza.

Anexo I

Línea del Tiempo de Algunos Ataques Informáticos: 1960 - 2020
https://www.thinglink.com/scene/1434618372191944706

Comando Conjunto de Ciberdefensa
https://fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/Default.aspx

Resolución 1523/2019
DEFINICION DE INFRAESTRUCTURAS CRÍTICAS
SECRETARIA DE GOBIERNO DE MODERNIZACION; 12-sep-2019;

Publicada en el Boletín Oficial del 18-sep-2019 Número: 34200 Página: 15

Resumen: Apruébese la definición de infraestructuras críticas y de infraestructuras críticas de información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados, que como Anexo I (if-2019-78452510-apn-sgm#jgm) forma parte de la presente medida. Apruébese el glosario de términos de ciberseguridad.

http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=5F1C7B5DB6B35C24E1B5A310CC6641E2?id=328599

Anexo I - Estructuras críticas:

http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/328599/res1523-1.pdf

Anexo II - Glosario de Términos de Ciberseguridad:

http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/328599/res1523-2.pdf

Anexo II

Bibliografía:

Albarracín Keticoglu, Ana Alicia: Tesis de Maestría en Inteligencia Estratégica Nacional: *Inteligencia Nacional y Estrategia de Ciberseguridad Nacional*, UNDEF; 2019.

Porche III, Isaac R.: *Cyberwarfare: An Introduction to Information-Age Conflict*; Artech House; 2020.

Singer, P.W. y Friedman, Alan: *Cybersecurity and Ciberwar: What everyone needs to know*; Oxford University Press; 2014.

Capitán de Navío Ingeniero Sorrentino, Pablo D.: *Ciberespacio, Ciberseguridad y Ciberdefensa* (Confrontación de vulnerabilidades vs. agresiones como base de desarrollo de un Sistema Integrado de Ciberdefensa); Boletín del Centro Naval N° 848; Agosto de 2018.

Springer, Paul J.: *Cyber Warfare: A Reference Handbook*; ABC-Clio; 2015

Springer, Paul J.: *Cyber Warfare: A Documentary and Reference Guide*; ABC-Clio; 2020.

Winterfeld, Steve y Andress, Jason: *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*; Elsevier; 2013.

Webinar on Line CIBERDEFENSA ¿cómo enfrentar este nuevo dominio militar?); Ciberdefensa.on line; 2019.