CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL

ISSN 0719-4110

CUADERNO DE TRABAJO N°1-2019

LA DIMENSIÓN DEL CIBERESPACIO: UNA PROPUESTA DE CIBERSEGURIDAD

CUADERNOS DE TRABAJO es una publicación orientada a abordar temas vinculados a la Seguridad y Defensa a fin de contribuir a la formación de opinión en estas materias.

Los cuadernos están principalmente dirigidos a tomadores de decisiones y asesores del ámbito de la Defensa, altos oficiales de las Fuerzas Armadas, académicos y personas relacionadas con la comunidad de defensa en general.

Estos cuadernos son elaborados por investigadores del CIEE de la ANEPE, pero sus páginas se encuentran abiertas a todos quienes quieran contribuir al pensamiento y debate de estos temas.

CUADERNO DE TRABAJO DEL CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS es una publicación electrónica del Centro de Investigaciones y Estudios Estratégicos de la Academia Nacional de Estudios Políticos y Estratégicos y está registrada bajo el **ISSN 0719-4110 Cuad. Trab., - Cent. Estud. Estratég.**
Dirección postal: Avda. Eliodoro Yáñez 2760, Providencia, Santiago, Chile.
Sitio Web www.anepe.cl. Teléfonos (+56 2) 2598 1000, correo electrónico ciee@anepe.cl

LA DIMENSIÓN DEL CIBERESPACIO: UNA PROPUESTA DE CIBERSEGURIDAD

Enero, 2019
Cristian Barría Huidobro*

"Cien victorias en cien batallas no es lo ideal. Lo ideal es someter al enemigo sin luchar".

El arte de la Guerra - Sun Tzu (600 años a.C.)

RESUMEN

El ciberespacio ha cambiado tanto paradigmas tradicionales como modernos, desde las relaciones sociales y los negocios hasta los dominios de guerra. Las últimas décadas han evidenciado el potencial del entorno digital como una herramienta real para los menesteres militares, yendo mucho más allá de los roles meramente colaborativos que antiguamente se le asignaban. Una defensa moderna requiere de una capacidad no solo técnica y tecnológica para abordar este espacio virtual y sus desafíos, sino también de una capacidad organizacional y administrativa que pueda ser transmitida claramente en los roles que cada unidad debe realizar en función del ciberespacio. Con esta realidad en mente, se presenta una propuesta de definiciones y estructuras de esta dimensión basada en funciones, con el objetivo de que puedan ser implementadas de forma eficiente y armónica en entidades tanto públicas como privadas.

PALABRAS CLAVE: Ciberespacio, ciberseguridad, funciones.

Introducción

Desde la antigüedad los ejércitos han competido por el dominio de la tierra y el mar. Durante los últimos 100 años han dominado en el aire y hoy están en los albores de una nueva era, enfrentados a una realidad de carácter cambiante con la aparición del ciberespacio y el espacio ultraterrestre como nuevos escenarios de conflicto[1].

Por lo mismo, las mayores potencias militares del mundo han abordado esta nueva realidad de forma integral, desarrollando capacidades humanas y tecnológicas especialmente dedicadas a enfrentar esta nueva problemática, teniendo que adaptar sus estructuras organizacionales para utilizar el ciberespacio como un medio en el cual puedan emplearse las distintas ramas de sus fuerzas armadas. Naciones como China,

* Doctor en Ingeniería Informática, Magíster en Ciencias de la Ingeniería Informática, y Magíster en Planificación y Gestión Educacional, Licenciado en Informática y Licenciado en Ciencias de la Ingeniería, cuenta con la Ingeniería en Informática, e Ingeniería en Administración, Investigador Universidad Mayor.

[1] LIBICKI, Martin C. Cyberspace is not a warfighting domain. ISJLP, 2012, vol. 8, p. 321.

Rusia y Estados Unidos han reconocido en esta dimensión oportunidades y amenazas reales, las cuales ameritan un enfoque proactivo e incluso una rama propia[2].

Tales ejemplos muestran que existe el imperativo de identificar, entender y definir apropiadamente los elementos y funciones que conforman el ámbito ciber, de modo tal que su integración al contexto militar (FF.AA.) —ya sea como dominio independiente o como parte de otros dominios—, tenga sentido para todos sus actores, tanto a nivel estratégico, operativo como táctico. Dicha necesidad es la que motiva el desarrollo de esta propuesta de ciberespacio basada en funciones.

"El uso de las redes, sistemas y datos como facilitadores de operaciones militares, o como herramienta que permita generar efectos reales sobre objetivos físicos de interés militar, ha dejado de ser una proyección fantasiosa, porque se ha convertido en una oportunidad que ya ha sido explotada por algunos países."

El uso de las redes, sistemas y datos como facilitadores de operaciones militares, o como herramienta que permita generar efectos reales sobre objetivos físicos de interés militar, ha dejado de ser una proyección fantasiosa, porque se ha convertido en una oportunidad que ya ha sido explotada por algunos países[3].

Tal es el caso de lo ocurrido el año 2007 en Estonia, país que sufrió una disrupción masiva de su infraestructura digital, generando mal funcionamiento de sus sistemas bancarios, de transmisión, entre otros. De igual modo, la proliferación de propaganda política que ocurrió a través de la intervención de sitios web estatales, cuyos contenidos fueron reemplazados por mensajes de corte político.

Todo esto, supuestamente perpetrado por Rusia, es lo que se ha llamado l**a primera ciber guerra del mundo, o Cyber War I**[4]. Para el lector, seguramente será evidente el beneficio estratégico que implica poder comprometer las redes de comunicación y financiamiento de un potencial adversario, especialmente si esto se realiza manteniendo a las fuerzas propias lo más alejadas posible del área en conflicto.

Si bien lo anterior se dio en el contexto de diferencias políticas entre los países, no existía una guerra declarada entre ambos. Distinto es el caso de Georgia, país que también fue objeto de incursiones cibernéticas, hipotéticamente de origen ruso. Aquí hay tanto similitudes como diferencias que resultan importantes observar: ambos países se encontraban en situación de guerra declarada, a pesar de que los primeros ciberataques registrados contra Georgia ocurrieron semanas antes de la ejecución real del empleo de fuerza por parte de Rusia.

Por otro lado, comienzan actividades maliciosas apuntadas a colapsar servicios web del país e intervenir contenido en los sitios, reemplazando su contenido original por propaganda, lo cual resulta muy similar a lo ocurrido en Estonia. Sin embargo, una diferencia importante es que la coordinación de estas incursiones se convirtió en un facilitador para operaciones militares

[2] ALEXANDER, Keith B. Warfighting in cyberspace. National Defense Univ. Washington DC Inst. for National Strategic Studies, 2007.

[3] DENNING, Peter J. y DENNING, Dorothy E. Discussing cyber attack. Communications of the ACM, 2010, vol. 53, no 9, pp. 29-31.

[4] RUUS, Kertu. Cyber war I: Estonia attacked from Russia. European Affairs, 2008, vol. 9, no 1-2.

convencionales. Además, otro aspecto relevante es que los accesos fueron perpetrados, en su mayoría, por civiles, lo cual habla de una sinergia entre la población y militares totalmente diferente a lo que usualmente se puede apreciar en conflictos bélicos tradicionales[5].

Ambos ejemplos nos hablan del ciberespacio como una herramienta complementaria a las operaciones militares tradicionales, pero en 2010 el descubrimiento de Stuxnet -un malware de clase gusano, presuntamente desarrollado en conjunto entre Estados Unidos e Israel en los sistemas de control de una central nuclear iraní-[6] expone otra cara del ciberespacio: una que puede generar daños por sí misma y de forma independiente.

“La idea de desarrollar un software que pueda convertirse en arma no es nueva, pues los mercados negros de malware hace años han ofrecido piezas de software creadas con la finalidad de causar algún perjuicio específico contra un objetivo dado”

La idea de desarrollar un software que pueda convertirse en arma no es nueva, pues los mercados negros de malware hace años han ofrecido piezas de software creadas con la finalidad de causar algún perjuicio específico contra un objetivo dado. En ese sentido, el rol que cumple el cibercrimen sobre el desarrollo de ciberarmas es algo que debe ser analizado con bastante cautela. Hay evidencia que apunta al uso directo o indirecto del código de origen *underground* en los ciberataques contra Estonia, Georgia e Irán[7].

La naturaleza gris que envuelve el empleo de software malicioso puede trazarse a ejemplos incluso más antiguos que los anteriormente mencionados. El año 2003 tuvo lugar la operación *Titan Rain*, la cual consistió en una serie de actividades maliciosas presumiblemente de origen chino, apuntando a sistemas computacionales de índole militar[8].

Estos ciberataques, además de generar desconfianza entre los países involucrados, también evidenció la dificultad para atribuir de forma concreta la autoría de este tipo de agresiones, dado que en varios casos terceros actores infectaban y utilizaban computadores localizados en China para llevar a cabo enfrentamientos contra Estados unidos y otras latitudes, aprovechándose de diferentes vulnerabilidades existentes en dispositivos y redes chinas[9].

Estos sucesos han dado pie a un extenso debate respecto de los límites legales de las acciones ejecutadas en y desde el ciberespacio, debate que está lejos de concluir, pero que ha ido avanzando, por cuanto se ha vuelto cada vez más evidente la importancia de definir de forma clara tanto conceptos como acciones que puedan ser entendidas en términos legales por distintos Estados[10][11].

[5] WHITE, Sarah, 2018. Understanding Cyberwarfare: Lessons from the Russia-Georgia War. Modern War Institute (MWI) at West Point.

[6] WAXMAN, Matthew C. Cyber-attacks and the use of force: Back to the future of article 2 (4). Yale J. Int’l L., 2011, vol. 36, p. 421.

[7] FARWELL, James P. y ROHOZINSKI, Rafal. Stuxnet and the future of cyber war. Survival, 2011, vol. 53, no 1, pp. 23-40.

[8] THORNBURGH, Nathan. Inside the Chinese Hack Attack. Times, august, 2005, vol. 25.

[9] LEWIS, James A. Computer Espionage, Titan Rain and China. Center for Strategic and International Studies-Technology and Public Policy Program, 2005, vol. 1.

[10] DENNING, Peter J. y DENNING, Dorothy E. Loc Cit.

[11] WAXMAN, Matthew C. Loc. Cit.

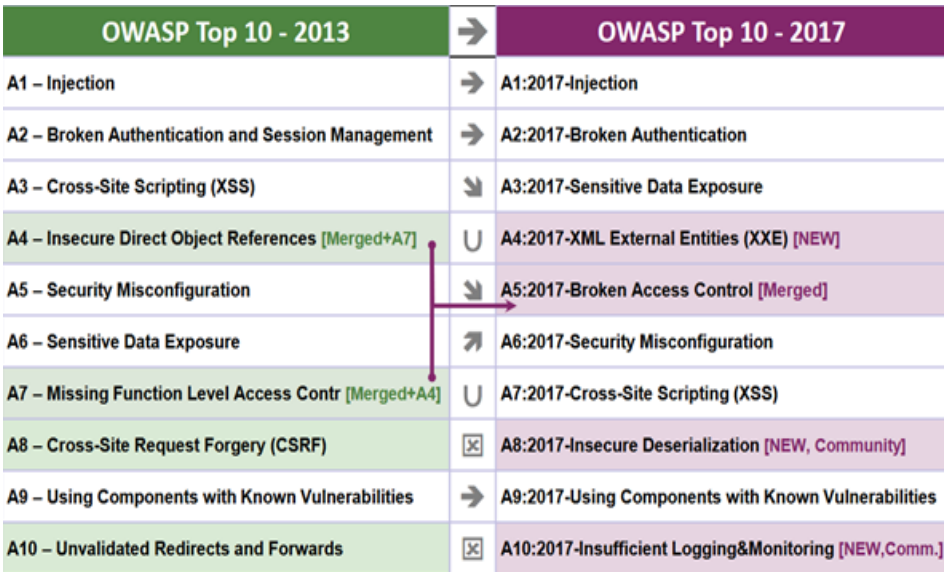
Por otra parte, las motivaciones detrás de los ataques informáticos han ido cambiando al igual que la sofisticación de los mismos. Hoy en día acechan una gran variedad de agrupaciones con distintos niveles de experticia en la materia y diferentes objetivos. Desde grupos con pretextos de activismo, hasta estructuras militares, pasando por agrupaciones independientes pero respaldadas por países específicos, e incluso organizaciones criminales. Todos forman parte de un nuevo ecosistema que ha dado lugar a infecciones maliciosas altamente sofisticados, tanto a nivel de planificación como a nivel de las tecnologías y técnicas empleadas.

Estos actores han sido clasificados bajo el término A*menazas Persistentes Avanzadas o APT*, por sus siglas en inglés, siendo la *Operación Aurora* el primer caso ampliamente reportado como tal en un comunicado emitido por Google en 2010. El concepto de *Avanzado* hace referencia a la elevada sofisticación anteriormente mencionada, mientras que el concepto de Persistente, apunta al hecho de que estos actores no sólo buscan explotar una vulnerabilidad, obtener control del recurso e irse, sino que mantener esa infección de forma efectiva, por extensos periodos de tiempo[12].

Ahora bien, no es razonable esperar que una institución (o un país) pueda lidiar correctamente con adversarios complejos, si no se parte abordando los aspectos elementales de ciberseguridad, especialmente aquellas consideraciones que dicen relación con servicios y/o recursos expuestos a Internet. Por muy elemental que esto pueda parecer, son precisamente los errores básicos los que posibilitan la explotación de vulnerabilidades, que a su vez, dan paso a vectores de ataque más avanzados.

De esto da cuenta OWASP (Open web Application Security Project), el cual regularmente entrega informes con las 10 vulnerabilidades web más comunes en el mundo, y cuyo resumen gráfico se ilustra en la figura 1. Cabe destacar,

Figura N°1 Ranking de vulnerabilidades en la web



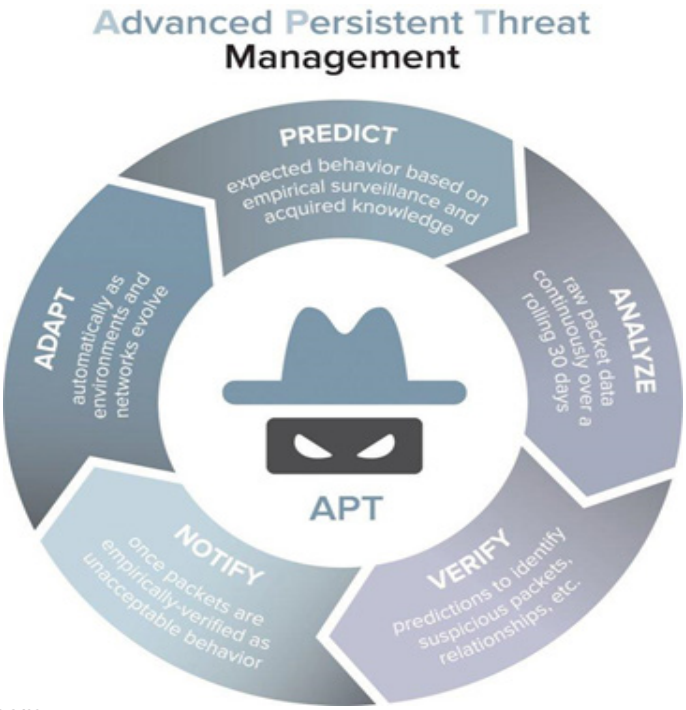
Nota: Top 10 de vulnerabilidades web. Al costado derecho se expone el listado 2017, mientras que al costado izquierdo, la versión 2013. Nótese los cambios aplicados entre una versión y la otra. uente: Open Web Application Security Project.

[12] TANKARD, Colin. Advanced persistent threats and how to monitor and deter them. Network security, 2011, vol. 2011, no 8, pp. 16-19.

que varias de estas vulnerabilidades pueden ser prevenidas mediante controles básicos durante el proceso de desarrollo y/o integración de software, o con otras acciones de similar simpleza[13].

En el caso de las APT, cubrir el aspecto tecnológico es un paso fundamental, pero no es suficiente. La utilización de técnicas de ingeniería social es práctica común dentro de las APT, por lo cual se hace indispensable velar por el factor humano de la institución, ya que es a través de las personas que un potencial atacante puede lograr que alguna acción no autorizada sea ejecutada[14]. Un esquema cíclico de referencia, orientado hacia la gestión de APT, se ilustra en la figura 2.

Figura N°2 Ciclo de gestión de APT



Fuente:Masergy.com

Entender la naturaleza de las potenciales amenazas a las que cada organización está expuesta resulta clave para poder diseñar una estrategia efectiva para hacerles frente. La seguridad no es una solución de software ni un dispositivo físico que proteja los datos, sino el resultado de un compromiso transversal en el cual debe participar toda la estructura de manera activa. Adquirir soluciones de protección de software no sirve si no existe una estrategia de seguridad bien definida. Y para poder desarrollar una estrategia de este tipo, resulta sumamente importante que exista claridad a nivel de conceptos y responsabilidades, de modo tal que todos los actores involucrados entiendan qué es lo que hacen, y con qué fin. En otras palabras, debe existir un alineamiento claro en la institución. Por ello es que esta propuesta de ciberseguridad considera funciones expuestas como un lineamiento que pueda ser entendido e integrado a nivel colectivo, ayudando a hacer frente a estas ciberamenazas que ya llevan años acechando el ciberespacio, desapercibidas por

[13] OWASP, Top. TOP 10–2017: The ten most critical web application security risks. The Open Web Application Security Project, 2017.

[14] TANKARD, Colin. Loc. Cit.

los usuarios y que asumen erradamente como un lugar seguro en vez de fiable.

I.CIBERESPACIO

Diversos autores e instituciones han intentado definir y/o clasificar al ciberespacio[15][16][17][18], reflejando una realidad que afecta a distintos conceptos relacionados con el mundo digital y sus abstracciones. Existen nociones del tema, pero no así un consenso definitivo respecto de qué significa cada concepto.

Asimismo, las experiencias específicas de cada individuo o sociedad durante su interacción con distintas tecnologías digitales, tanto a nivel físico como lógico, han ido moldeando una idea de ciberespacio. Tenemos así un fenómeno que añade complejidad a las más diversas instancias del orden global, pero que a la vez carece de definiciones claras, todo lo cual resulta sorprendente. Por lo mismo, desde un punto de vista tecno-científico, se considerará al ciberespacio como un entorno generado a partir de la interacción de distintos actores, tanto humanos como máquinas, basados en tecnologías digitales que, en distintas instancias, generan, transmiten, almacenan y/o procesan datos.

Dichos datos pueden o no haber alcanzado la denominación de información, al igual que pueden o no ser parte de redes masivas como Internet.

Este espacio, con prefijo ciber, comienza a cobrar relevancia cuando aparecen amenazas que afectan a la seguridad de la información, cuyo marco de referencia se ha ido acotando en la triada de confidencialidad, integridad y disponibilidad[19], esquema que se ilustra en la figura 3.

Figura N°3 Triada de la seguridad de la información

Fuente: Cyber Safe Solutions.

[15] MORUECO, Miguel. El ciberespacio como nuevo espacio político: notas para una ontología política nómada. [online]. UAM. [Accessed 29 october 2018]. Available from: http://www.uibcongres.org/imgdb/archivo_dpo1785.pdf

[16] JUSTRIBÓ, Candela. Ciberdefensa: una visión desde la UNASUR. En: VII Congreso del IRI/I Congreso del CoFEI/II Congreso de la FLAEI (La Plata, 2014). 2014.

[17] CJCS, JOINT CHIEFS OF STAFF, 2018, JP 3-12 “Cyberspace Operations”. Federation of American Scientists, Intelligence Resource Program, Department of Defense of the United States of America.

[18] KUEHL, Daniel T. From cyberspace to cyberpower: Defining the problem. Cyberpower and national security, 2009, vol. 30.

[19] EI-ISAC™ Cybersecurity Spotlight – CIA Triad. CIS Control 20: Penetration Tests and Red Team Exercises [online].

Dado el incremento en la complejidad de las amenazas, y las dificultades que existen para determinar autorías, culpabilidades y legalidad de los actos cometidos en el ciberespacio, es posible incorporar y así transformar la triada en un cuarteto de la seguridad de la información, adicionando como factor la legalidad. Ello se ilustra de forma gráfica en la figura 4.

Figura N°4 Cuarteto de la seguridad de la información

Fuente: Elaboración Propia.

La separación conceptual entre líneas de defensa y ataque en el ciberespacio resulta clave a la hora de articular estrategias y operaciones, tanto preventivas como reactivas, ante las ciberamenazas. Es en este contexto donde surge el concepto de cibergeografía, que se entiende como el estudio de la naturaleza espacial del ciberespacio y sus componentes subyacentes: internet, intranet, terminales, redes, entre otros[20].

La capacidad de dar un sentido relacional gráfico a las complejas interacciones que caracterizan al ciberespacio es una idea muy potente que colabora a incorporar la noción del mismo de una manera más fluida en la agenda militar, por cuanto esta forma de comprender el **mundo ciber** resultaría más cercana a los conceptos o términos tradicionales.

II.CIBERAMENAZAS

Para efectos de esta investigación, entenderemos como ciberamenaza a un actor humano o no humano, ya sea externo a la organización o que forme parte de ella, y que represente algún grado de riesgo para afectar al menos a uno de los pilares del cuarteto descrito anteriormente en la figura 4, sirviéndose para ello de algún recurso o cualidad del ciberespacio con independencia de que sus acciones sean intencionales o no.

[Accessed 13 november 2018]. Available from: https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/

[20] About Cyber Geography Research [online]. [Accessed 13 november 2018]. Available from: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/about.html

Algo semejante ocurre en la figura 5, donde se representan los riesgos en el ciberespacio, que comienzan a cobrar protagonismo cuando se involucran y afectan a alguno de los componentes del cuarteto, pero más aún si perturban a los sistemas, redes y/o datos que hacen posible el funcionamiento cotidiano de los ciberciudadanos, en donde la vida se presenta en un escenario más digital gobernada por la información y el conocimiento[21].

Este escenario se ha sectorizado, y en la actualidad a sus componentes se les denomina infraestructura crítica y de la información, y que como tal, es necesaria para la operación y gobernanza de un Estado. Un ejemplo de ello es la directiva presidencial Nº 13.010, firmada por el presidente norteamericano Bill Clinton en 1998, que define ocho sectores críticos cuyos servicios son vitales para el funcionamiento de la nación y cuya incapacidad de operación o destrucción tendría un impacto directo en la defensa o en la estabilidad y seguridad económica. Tales sectores son: energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, telecomunicaciones, bancos y finanzas, suministro de agua, transportes, servicios de emergencia y operaciones gubernamentales (mínimas requeridas para atender al público)[22].

En consecuencia, será considerada como ciberamenaza propiamente tal todo *acto deliberado* que tenga como propósito claro y reconocible afectar la estructura. El peligro, en cambio, se considerará como un acto perpetuado sin intención[23].

Figura N°5 Entorno de la ciberdefensa y las ciberamenazas

Fuente: Elaboración propia.

[21] HOLMNER, Marlene Amanda, “et al” A critical analysis of information and knowledge societies with specific reference to the interaction between local and global knowledge systems. 2008. Tesis Doctoral. University of Pretoria.

[22] CANO, Jeimy. Ciberseguridad y ciberdefensa : dos tendencias emergentes en un contextoglobal. sistemas (asociación colombiana de ingenieros de sistemas) (0119), 4-7. 2011.

[23] LÓPEZ, J. D., “III jornadas de ciberdefensa del mando conjunto de ciberdefensa.” [En línea] [Ultimo acceso: 29/10/2018] Disponible en: https://jornadasciberdefensa.es/

Cabe destacar que en torno a 2006 se hizo evidente un cambio estratégico en la difusión del malware con la irrupción de nuevas amenazas, el boom del espionaje y la explotación de la información, y la interrupción a gran escala, a los que deben sumarse otras formas de actuación de los cibercriminales. Todo ello, en el marco de un conjunto de capacidades nunca vistas hasta el presente. Estas provocaciones implican acciones de los ciberdelincuentes con un carácter mayor en cuanto a planificación, organización y coordinación, dirigidas sobre objetivos seleccionados según su importancia o vulnerabilidad[24].

Otro aspecto importante son los sistemas industriales SCADA (Supervisory Control and Data Acquisition, por sus siglas en inglés), tanto de la industria civil como de la militar. Un ataque cibernético directo y certero contra este tipo de infraestructura puede tener serias consecuencias para la continuidad operacional de la industria lo que hace necesario considerar todo tipo de acciones para proteger, asegurar y promover conductas de seguridad en el diseño y la implementación, y mantención de Sistemas de Control Industrial (ICS, por su sigla en inglés)[25].

Inclusive cuando surgen las amenazas en el ciberespacio (ciberamenazas), ellas requieren ser enfrentadas para brindar protección a la información, lo que estructuralmente se construye sobre los tres momentos básicos de cualquier episodio: un antes (ciberdefensa), un durante (ciberataque) y un después (informática forense).

"... la ciberdefensa será aquella que se preocupe del primer momento (antes), es decir, que las ciberamenazas no logren explotar una vulnerabilidad."

III. CIBERDEFENSA

La defensa nacional, como noción acuñada por las fuerzas militares de un país, requiere construirse en el contexto del nuevo rostro de la guerra, en una confrontación que enfrenta lo mejor de los entrenados en el arte de la generación de inseguridad de la información; es decir, en el adversario, y aquellos capaces de controlar y mantener la paz de una nación[26] considerándose como premisa que la ciberdefensa forma parte de la ciberseguridad[27].

Es así como, por ejemplo, Argentina a través de la Resolución N° 580/2011 ha desarrollado sus orientaciones de protección en un *Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad* (ICIC), que tiene como objetivo incentivar la creación y la adopción de un programa regulatorio que preserve las infraestructuras estratégicas de la información del Estado[28].

En síntesis, la ciberdefensa será aquella que se preocupe del primer momento (antes), es decir, que las ciberamenazas no logren explotar una vulnerabilidad. Para efectuar esta función el recurso humano asociado a ella debe ejecutar tareas que requieren un alto nivel de especialización y dedicación, entre las que destacan la configuración de firewall, proxies, implementación de IDS, IPS, software antimalware, entre otros.

IV. CIBERATAQUES O DEFENSA ACTIVA

En cuanto al concepto de ciberataque como un segundo momento (durante), CISCO nos

[24] LÓPEZ, J. D. "III jornadas de ciberdefensa del mando conjunto de ciberdefensa." [En línea] [Último acceso: 29/10/2018] Disponible en: https://jornadasciberdefensa.es/

[25] ANABALÓN, Juan, y DONDERS, Eric. una revisión de ciberdefensa de infraestructura crítica. ESD, 2014, p. 131.

[26] CANO, Jeimy. Loc. Cit.

[27] LÓPEZ, J. D. Loc. Cit

[28] JUSTRIBÓ, Candela. Loc. Cit.

provee de la siguiente definición: "*intento malicioso y deliberado por parte de un individuo u organización para vulnerar un sistema de otro individuo u organización. Usualmente, el atacante busca algún tipo de beneficio a partir de la disrupción de la red de la víctima*"[29].

Si bien esta definición puede no ser lo suficientemente amplia como para abarcar diversos casos, sí nos expone los principales puntos que caracterizan a este tipo de agresiones: Una acción premeditada, ejercida sobre algún recurso informático (sistemas, redes y/o datos), con la intención de obtener algún beneficio producto de dicha acción (extraer recursos financieros, información, entre otros) y/o ocasionar algún tipo de daño al objetivo o usuario (interceptación, interrupción, modificación, generación y/o destrucción).

Dado lo anterior, entenderemos el ciberataque como un concepto que engloba las acciones ejecutadas de forma directa o indirecta sobre un recurso informático, afectando uno o más del objeto de la seguridad de la información (preservar la confidencialidad, integridad, disponibilidad, legalidad).

V. INFORMÁTICA FORENSE

En un tercer momento (después) podemos identificar los procedimientos que se deben realizar, una vez que el ataque ya ha sido perpetrado.

Una definición de informática forense (o también forense computacional) nos habla de "*la disciplina que combina elementos de leyes y ciencia computacional, para recolectar y analizar datos desde sistemas computacionales, redes, comunicaciones inalámbricas, y dispositivos de almacenamiento, de forma tal que sea admisible como evidencia en una corte de justicia*"[30].

Si bien esta precisión ataña específicamente los usos judiciales del output obtenido, esto también puede aplicarse como parte de un ciclo de evaluación continua de la ciberseguridad institucional, por cuanto las labores de la informática forense proveen de información valiosa respeto del estado de nuestros sistemas.

"El hecho de poder identificar, almacenar, transportar y analizar correctamente las evidencias de un ataque, considerando la cadena de custodia respectiva , es fundamental..."

El hecho de poder identificar, almacenar, transportar y analizar correctamente las evidencias de un ataque, considerando la cadena de custodia respectiva[31], es fundamental por diversas razones: ayuda a investigar autorías de los hechos, entender el funcionamiento del ataque, aprender de lo sucedido, y a elaborar medidas preventivas para presentación de datos en procesos judiciales, entre otros.

Este aspecto se ocupa de la última fase: el después, o las acciones que se toman una vez ocurrido el incidente informático. Algunas tareas relacionadas con este ámbito incluyen la recuperación de datos borrados, el análisis de ingeniería inversa, la identificación de metodologías utilizadas para explotar el sistema, entre otras.

VI. CIBERINGENIERÍA

Dado que las tres funciones fundamentales anteriormente mencionadas funcionan en instantes distintos (antes, durante y después

[29] Computer Forensics, 2008. [En línea] [Ultimo acceso: 29/10/2018] Disponible en: https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

[30] Ibíd.

[31] DÍAZ DEL RÍO, J. "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio" Capítulo V:"La ciberseguridad en el ámbito militar." ISSN 1697-6924, Nº. 149, 2011.

del incidente), se requiere de una instancia que dé sentido a los esfuerzos de cada una de esas funciones, de modo tal que conserven un mismo norte. Este rol es el que debe asumir la función de ciberingeniería, es decir, un apoyo permanente articulando un flujo coherente de inputs y outputs para cada una de las funciones por momentos, y a su vez, convirtiendo la información generada por ellas en un canal único que pueda ser presentado a los tomadores de decisiones de la organización.

En términos simples, supervisa y coordina las labores de ciberdefensa, defensa activa e informática forense, proveyendo de información oportuna y actualizada a las unidades superiores encargadas de tomar las decisiones.

Esto implica que recae en la ciberingeniería la responsabilidad de brindar todo el apoyo a las distintas funciones, según se van desarrollando las etapas del incidente. Siendo la habilitación de ambientes de operación, adquisiciones afines (ciberadquisiciones), generación de perfiles, entre otros. Además, es donde también se debe velar porque las funciones a su cuidado operen dentro del marco de las leyes y normas (ciberderecho) que sobre ellos apliquen, principalmente aquellas que digan relación con legislaciones en materia de ciberseguridad.

En aquellas situaciones excepcionales que permiten un rango de operación más allá del usualmente permitido por la ley (por ejemplo, estados de excepción), debiendo articular las acciones de modo tal que no se cometan abusos, manteniendo siempre informados a aquellos encargados de tomar decisiones de mayor nivel.

Para efectos de esta investigación se considera fundamental que esta función no solo deba ser capaz de desarrollar planes de contingencia, continuidad operativa y recuperación ante desastres para sí misma, sino que también implementar estos planes a nivel de cada una de las funciones a quienes sirve y en ajuste a sus necesidades particulares. En este sentido, debe tener una visión holística y a la vez modular de su labor; por consiguiente, el desarrollo e implementación de planes debe aplicarse al ecosistema de ciberseguridad como un todo, pero también a nivel específico de cada una de las funciones, y también a nivel de la ciberingeniería misma.

VII.CIBERINTELIGENCIA

De modo idéntico a la ciberingeniería esta función resulta crucial puesto que los antecedentes que obtiene el sistema de inteligencia resulta fundamental, y en este caso la transformación de datos considera la gestión y aplicación de la información y su integración deliberada con otras funciones en conjunto pudiesen influir en las percepciones, el comportamiento, la acción o la inacción, la toma de decisiones, tanto humana como automatizada[32].

Se define en algunos casos como lo que es para las operaciones, es decir, que nutre de información a quien dirige la ciberoperación; incluso analistas de EE.UU. siguen estudiando las mejores prácticas para planificar y evaluar operaciones, así como la implantación detallada del marco C2 (mando y control) para la actuación de las fuerzas cibernéticas[33].

En este esquema, la ciberinteligencia debe velar por otorgarle validez a los datos a través de la generación de información, considerando aspectos tales como: volumen, velocidad, variedad, veracidad, viabilidad, visualización y valor[34]. Esto obliga a generar procesos de

[32] CJCS, JOINT CHIEFS OF STAFF, 2018, JP 3-12Loc. Cit

[33] LÓPEZ, J. D. Loc. Cit

[34] JOYANES, A. “Big Data Análisis de grandes volúmenes de datos en organizaciones” , 1era. Edición, México, AlfaOmega. ISBN-10: 8426720811, 2013.

búsqueda de respuestas y mejora continua para ser proactivos en el mundo global, por lo que se hace necesario el uso de técnicas para poder generar prospectiva, en este caso, la planificación de escenarios que permitan identificar las estrategias para responder con validez a esos desafíos.

En este sentido, la planificación de escenarios se erige como una herramienta fundamental para mantener informados a los órganos de decisión de los posibles cambios que se susciten y que acontecen en el entorno, los que nos permitan explotar oportunidades y contribuir en la toma de decisiones estratégicas[35].

"... la ciberinteligencia debe velar por otorgarle validez a los datos a través de la generación de información, considerando aspectos tales como: volumen, velocidad, variedad, veracidad, viabilidad, visualización y valor."

La naturaleza heterogénea, y a veces caótica de las acciones que ocurren en el ciberespacio, representan una dificultad importante para los especialistas encargados de realizar esta labor quienes deben identificar, recolectar, clasificar, procesar y analizar grandes volúmenes de datos, los cuales varían sustancialmente tanto a nivel de formatos y tipos, como también a nivel de orígenes y vías de obtención.

Por ejemplo, para poder apoyar correctamente la toma de decisiones, la ciberinteligencia debe lidiar con datos no estructurados, tales como publicaciones en blogs, foros, redes sociales y otros sitios web, datos que pueden ser cruciales para poder anticipar un ciberataque, o bien para identificar fuentes de información empleadas por adversarios actuales y potenciales. Estos datos, como es de esperar, no se encuentran ordenados de acuerdo a estándares industriales o académicos, muy por el contrario, es usual que tanto el acceso como el contenido de los mismos se encuentre obstruido por medidas de protección, precisamente establecidas para dificultar su obtención.

Al mismo tiempo, el análisis de distintas fuentes tales como computadores infectados, routers, firewalls entre otros, puede utilizarse para identificar actividades sospechas en las redes de manera más ordenada; sin embargo, suele ser una medida insuficiente por sí misma para obtener conclusiones precisas.

La gran variedad de dispositivos de hardware que interactúan con diferentes redes supone un desafío adicional, por cuanto el apropiado estudio e interpretación de los datos obtenidos, y sin ir más lejos, la sola interacción con estos medios de TI, requieren de experticias técnicas específicas. Distintos proveedores de tecnologías pueden operar de manera diferente sobre un mismo tipo de dispositivo, lo cual dificulta aún más poder abordar toda la variedad de tecnologías de red que nos pueden proveer de datos valiosos[36].

Ahora bien, el rápido crecimiento de Internet, así como de sus tecnologías relacionadas, han decantado en la generación de enormes volúmenes de datos, a nivel tal que no es realista esperar que un operador único o un equipo de operadores puedan recopilar y procesar todos estos antecedentes a la velocidad requerida para tomar decisiones informadas en pseudo tiempo real. En este contexto es que la utilización de tecnologías, técnicas y herramientas de Big Data no solo es necesario, si no que prácticamente obligatorio, considerando que un par de segundos pueden hacer la diferencia entre tomar una decisión acertada ante un ciberataque, o una decisión fatalmente errada[37].

[35] TASCÓN, M. y COULLAUT, A. "Big Data y el internet de las cosas", Catarata, ISBN:9788490970744, 2016.

[36] GOEL, Sanjay. Cyberwarfare: connecting the dots in cyber intelligence. Communications of the ACM, 2011, vol. 54, no 8, pp. 132-140.

[37] MAHMOOD, Tariq y AFZAL, Uzma. Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. En: Information assurance (ncia), 2013 2nd national conference on. IEEE, 2013. pp. 129-134.

De cualquier manera la ciberinteligencia fue diseñada desde un comienzo como una función ágil que haga uso de los datos para apoyar la toma de decisiones, sin dejar de lado la supervisión del personal técnico especializado que pueda dirigir la correcta extracción e interpretación de los antecedentes procesados. Así, una visión integral de la misma debe involucrar la correcta identificación de las habilidades técnicas y tecnológicas que serán necesarias para su funcionamiento, además de poder dirigir la extracción de datos desde múltiples fuentes, hacia las herramientas de Big Data que podrán procesarlos.

Resumiendo lo planteado, ciberinteligencia como función debe adaptarse a los rápidos y vertiginosos cambios tecnológicos, considerándose de suma importancia la ejecución de una gestión cíclica, es decir, que se incluyan y apliquen procesos de retroalimentación de los datos obtenidos, lo cual permita una oportuna identificación de debilidades que puedan ser abordadas, o bien renovar tecnologías y técnicas que estén ingresando al periodo de obsolescencia. Lo anterior es posible ejemplificarlo desde la perspectiva de ciclo constante, que considera la metodología PDCA (Plan-Do-Check-Act), donde se emplean estrategias de mejora continua[38], cuyo esquema se aprecia en la figura 6.

Figura N°6 Ciclo de retroalimentación PDCA

Fuente: Asq.org.

[38] TAGUE, N , The Quality Toolbox. Second Edition, ASQ Quality Press, 2004, pp. 390-392.

VIII.CIBEROPERACIONES

Las operaciones en el ciberespacio (ciberoperaciones) constituyen el empleo de las capacidades, con el propósito de lograr un objetivo empleándose este entorno virtual[39], cuya función simboliza el cerebro de la organización, es decir, dónde se efectúa la toma de decisiones.

Las ciberoperaciones deben contemplar el conjunto total de riesgos y amenazas, o sea, situaciones potenciales y reales dibujadas sobre el tablero de la planificación[40].

"... constituyen el empleo de las capacidades, con el propósito de lograr un objetivo empleándose este entorno virtual...

Resulta interesante observar el caso de Argentina, con la promulgación de la Resolución N° 350 del año 2014, donde por primera vez se incorpora al Instrumento Militar (FF.AA.) como integrante de la estrategia de defensa cibernética nacional. En este sentido, se instruye al Jefe del Estado Mayor Conjunto de las Fuerzas Armadas para que

> "disponga las medidas necesarias a los efectos de desarrollar capacidades militares para realizar operaciones de ciberdefensa, a los efectos de únicamente garantizar la defensa contra aquellos ciberataques que pretendan obstaculizar las operaciones militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal" y contra aquellos ciberataques "que dirigidos a afectar los objetivos de valor estratégico que el Ministerio de Defensa establezca expresamente"[41].

En esta misma línea, el Mando Conjunto de Ciberdefensa español señala que *en un futuro inmediato* las operaciones en el ciberespacio podrían prevenir guerras y, si esto no fuera posible, igualmente ayudarían a reducir el costo (humano y económico) de las mismas, o incluso llevar a la victoria.

Asimismo, las operaciones se desarrollarán en un entorno multidominio, es decir, que todo va a estar interrelacionado y, por tanto, el dominio del ciberespacio será imprescindible para el control del espacio; "*El control del espacio para alcanzar el control del aire. Quien controle el aire, controlará la superficie*"[42].

Asimismo, una mirada particular de las ciberoperaciones es la que aporta Klimburg[43]; según este autor, hay una obviedad evidente de que la defensa en el ámbito del ciberespacio se puede topar con la disyuntiva de alcanzar una capacidad operativa adecuada sobre la base de aceptar ciertas prácticas no siempre deseables. Lograr capacidad de defensa puede incluso conllevar a la aceptación de algunas formas no claramente aceptables.

[39] CJCS, JOINT CHIEFS OF STAFF, 2018, JP 3-12. Loc. Cit.

[40] LEÓN, José Domínguez. La ciberguerra como realidad posible contemplada desde la prospectiva. Revista de Pensamiento Estratégico y Seguridad CISDE, 2016, vol. 1, no 1, pp. 18-32.

[41] JUSTRIBÓ, Candela. Loc. Cit.

[42] LÓPEZ, J. D. Loc. Cit.

[43] KLIMBURG, Alexander (ed.). National cyber security framework manual. NATO Cooperative Cyber Defense Center of Excellence, 2012.

IX. CIBERSEGURIDAD

El concepto de ciberseguridad figura como una realidad complementaria de la ciberdefensa[44] la que abarca el todo, tal como se expone en la figura 7, siendo un estado deseado a alcanzar, cuya estrategia debe considerar todos los frentes, inclusive aquellos que abarca la perspectiva militar[45].

Figura N°7 Relación contextual del ciber espacio, la ciber seguridad y conceptos relacionados

Fuente: Elaboración propia.

X.CIBERGUERRA

La ciberguerra es asimétrica. El bajo costo de los equipos informáticos puede implicar que los eventuales adversarios no tengan necesidad de fabricar armamento sofisticado y de altos costos para suponer una amenaza significativa a las capacidades militares, ya sea afectando la planificación operacional o anulando los sistemas de inteligencia, de mando y control[46].

Junto a la ciberguerra se establece todo un panel de amenazas cibernéticas que hacen plausible, viable, y probable, como un Pearl Harbor cibernético. Esto implica un riesgo cuyo origen (país u organización) no será posible conocer. De lo que no cabe la menor duda es que el riesgo es real, y que, como ocurriera en un día, en la forma de un ataque aéreo, pueda trasladarse a otro tipo de ataque, por sorpresa, con la abierta intención de producir daño.

[44] CANO, Jeimy. Loc. City.
[45] LÓPEZ, J. D. Loc. Cit.
[46] DÍAZ DEL RÍO, J. Loc. Cit

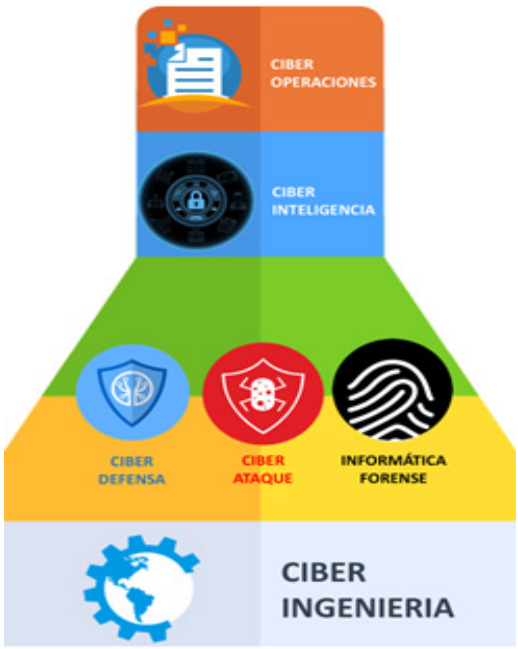
Luego, cabe pensar que una operación de ciberataque de una envergadura considerable puede conllevar importantes riesgos para quien las vaya a sufrir[47]. Esta es la razón de que los países se preparen con la creación de estructuras orgánicas, como es el caso de Alemania, que el 1 de abril del 2017, dio inicio al funcionamiento oficial de su *Cyber and Information Space Command* (CIR), el cual constituye una fuerza de trabajo mixta entre civiles y militares, compuesta por aproximadamente 13.500 personas[48].

XI. ESTRUCTURA Y SENTIDO ORGANIZACIONAL

Para el lector recién iniciado en estos tópicos del ciberespacio puede no resultar evidente la relación estructural de todos los términos anteriormente explicados. En consideración de que esta propuesta está pensada para ser integrada de forma fluida en distintos tipos de organizaciones, la capacidad de incorporar este modelo en cualquier contexto jerárquico es fundamental.

Para facilitar este entendimiento, se provee una arquitectura de funcionamiento y jerarquización de referencia, plasmada en la figura 8, que incluye las distintas áreas que debiesen cumplir cada una de las funciones propuestas.

Figura N°8 Estructura funcional de ciberseguridad propuesta



Fuente: Elaboración propia.

[47] LEÓN, José Domínguez. Loc. Cit.

[48] WERKHÄUSER, Nina. German Army Launches New Cyber Command. Deutsche Welle, april, 2017, vol. 1.

En términos de la ocurrencia en el tiempo de cada función, se resume el contexto de cada una en la tabla 1.

Tabla 1: Ocurrencia en el tiempo de las distintas funciones de la ciber seguridad.

Funciones Permanentes	Funciones Temporales (antes, durante, después)
Ciberoperaciones	Ciberdefensa
Ciberinteligencia	Defensa Activa
Ciberingeniería	Informática Forense

Fuente: Elaboración propia.

XII. NEC Y AUTARQUÍA TECNOLÓGICA

En el contexto militar, NEC o Network Enabled Capability, corresponde a "*la capacidad de integrar todos los componentes del medio operativo (sensores, elementos de decisión y plataformas de armas) desde el nivel político-estratégico hasta el nivel táctico, a través de una infraestructura de información y redes*"[49].

Este concepto, según señala el autor Díaz del Río, evidencia el importante rol que los medios tecnológicos cumplen a la hora de facilitar y posibilitar operaciones militares o ciberoperaciones, además de permitir una rápida distribución de información precisa, fiable, pertinente y oportuna entre los distintos niveles de la toma de decisiones.

También sostiene que esta capacidad permite generar una percepción compartida de la situación a la cual se debe enfrentar el personal, lo cual incrementa la agilidad y velocidad de las acciones, ya que permite la colaboración, sincronización y mejora de las decisiones en diferentes niveles jerárquicos, citando el ejemplo de la OTAN, quienes poseen su propia implementación del NEC, conocida como NNEC (NATO Network Enabled Capability).

Este es el espíritu que busca esta propuesta de ciberseguridad: entregar una visión multifuncional pero coordinada de todos los niveles e integre los conceptos y funciones del ciberespacio que son atingentes a la toma de decisiones, mediante un uso integrado y controlado de las tecnologías.

[49] DEL RÍO Durán, Juan Díaz. La ciberseguridad en el ámbito militar. Cuadernos de estrategia, 2011, no 149, pp. 215-256.

En relación al uso de la tecnologías, es importante realizar un análisis crítico del uso de productos de software y hardware en redes de Mando y Control que almacenan y/o transmiten información clasificada. En concordancia con lo que menciona Díaz del Río, es relevante entender que los sistemas operativos, y gran parte de las aplicaciones compradas a externos (tipo COTS, o Commercial Off The Shelf) requieren de la descarga e instalación de actualizaciones (o "parches"), para corregir errores de programación, mejorar funciones y, lo más importante en este contexto, solucionar problemas de seguridad de los mismos.

Esta situación tiene dos aristas clave. Por un lado, supone una amenaza a aquellos entornos y sistemas que, por su naturaleza, deben permanecer aislados de Internet, por cuanto obliga a que el sistema utilice software que mantendrá las vulnerabilidades que son corregidas en versiones posteriores a la utilizada al momento de la instalación (o forzando a que se realice una conexión a Internet para su actualización); mientras que, por otro lado, es usual que las actualizaciones a instalar consten de una gran cantidad de líneas de código y/o que el fabricante simplemente no revele cuáles modificaciones han sido realizadas al software, lo que en términos simples quiere decir que son ingresadas líneas de programación ajenas y sin supervisión a nuestros sistemas.

Desde la perspectiva del hardware los procesadores que se incluyen en los diversos dispositivos que son empleados, especialmente computadores, poseen código propio (el firmware) que puede contener instrucciones maliciosas cuya detección es altamente compleja.

Finalmente, resulta fundamental reflexionar respecto del gran potencial que las tecnologías nos ofrecen, pero también pueden ser empleadas en nuestra contra, si se continúa dependiendo de externos que provean de software y hardware a utilizar en las organizaciones o como usuarios. La Defensa de cada país debiese encaminarse hacia una modernización autónoma, actuando con una velocidad acorde a los tiempos actuales, pero teniendo como norte la autarquía tecnológica de sus instituciones.

"... resulta fundamental reflexionar respecto del gran potencial que las tecnologías nos ofrecen, pero también pueden ser empleadas en nuestra contra, si se continúa dependiendo de externos que provean de software y hardware a utilizar en las organizaciones o como usuarios.

XIII. CONCLUSIONES

La tendencia mundial apunta a un fortalecimiento de las capacidades de ciberoperaciones en el ciberespacio, incluyendo estructuras que converjan esfuerzos civiles y militares. Una comprensión clara de todos estos conceptos con prefijo ciber es crucial para poder dirigir y dar sentido a estos esfuerzos, permitiendo además su integración en estructuras tradicionales existentes.

En la presente investigación se ha propuesto la individualización de estos conceptos en base a funciones, las cuales se ejecutan en distintas instancias en relación a un incidente informático. Cada una de estas funciones requiere de personal que se especialice en la realización de tareas técnicas y de gestión afines, lo cual ha motivado a las potencias mundiales en captar y capacitar capital humano tanto en contextos de la academia, industria y estado.

Sin duda lo antes expuesto debe ir acompañado de una política nacional que busque generar una cultura de uso responsable y seguro del ciberespacio, por cuanto la efectividad de las medidas tomadas será siempre dependiente del

eslabón más débil de la cadena. La experiencia señala que ese eslabón son las personas, lo cual deja en evidencia que la ciberseguridad debe ser una tarea de todos.

Las tecnologías y el mundo digital en general han transformado todos los aspectos del quehacer humano, proporcionando facilidades y oportunidades que hubiesen sido impensables hace no muchos años atrás. Sin embargo, la madurez de ciertos elementos del ciberespacio (especialmente Internet) ha facilitado también la aparición y perfeccionamiento técnico de ciberamenazas que se sirven de este ambiente digital para cometer delitos de diversa índole.

"Por muy sofisticadas que sean las tecnologías por implementar, por muy diligente que sea el recurso humano, por muy holístico que sea el enfoque estratégico, no debe caerse jamás en el error de pensar que los sistemas son seguros..

Estas ciberamenazas a veces son completamente inherentes al ciberespacio, como también en ocasiones solo se sirven de él a conveniencia. Cualquiera sea el caso, resulta importante conocer sus riesgos y vulnerabilidades e implementar las medidas que permitan hacer frente a estas nuevas condiciones de la manera más eficiente posible.

En este contexto es de suma importancia que tanto personas como instituciones entiendan que no existen sistemas inviolables. Por muy sofisticadas que sean las tecnologías por implementar, por muy diligente que sea el recurso humano, por muy holístico que sea el enfoque estratégico, no debe caerse jamás en el error de pensar que los sistemas son seguros. Dicho de otro modo, todos los sistemas fiables.

Por tanto, como tarde o temprano el ataque alcanzará su propósito, ello implica que debe pensarse en la estructura de momentos. Si la barrera del antes y la del durante han sido sobrepasadas, la barrera del después debe contemplar la recuperación de las prestaciones —las que fueren— afectadas por el ciberataque.

Esta planificación de recuperación ante incidentes debe poseer el carácter de omnipresente en los distintos puntos de la estrategia de ciberseguridad, de modo tal que incluso ante ciberataques de los que no se tenga conocimiento previo (y que probablemente resulten ser los más dañinos), se genere la capacidad para contener sus efectos de la mejor forma posible, y, no menos importante, de aprender de ellos por medio de la informática forense. Solo así será posible robustecer las defensas y mitigar los riesgos.

La ciberseguridad debe entenderse como un esfuerzo constante y cíclico, en cuyo progreso es deseable que participen todos los actores. Esto es algo que ya ha sido comprendido por las grandes potencias internacionales y Chile no debe quedarse atrás.

Bibliografía

About Cyber Geography Research [online]. [Accessed 13 November 2018]. Available from: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/about.html

ALEXANDER, Keith B. Warfighting in cyberspace. national defense univ washington dc inst for national strategic studies, 2007.

ANABALÓN, Juan y DONDERS, Eric. Una revisión de ciberdefensa de infraestructura crítica. ESD, 2014, p. 131.

CANO, Jeimy. Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. Sistemas (asociación colombiana de ingenieros de sistemas)(0119), 4-7. 2011

CJCS, JOINT CHIEFS OF STAFF, 2018, JP 3-12. “Cyberspace Operations”. Federation of American Scientists, Intelligence Resource Program, Department of Defense of the United States of America.

Computer Forensics, 2008. [En línea] [último acceso: 29/10/2018] Disponible en: https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

DEL RÍO Durán, Juan Díaz. La ciberseguridad en el ámbito militar. Cuadernos de estrategia, 2011, N° 149. pp. 215-256.

DENNING, Peter J. y DENNING, Dorothy E. Discussing cyber attack. Communications of the ACM, 2010, vol. 53, no 9, pp. 29-31.

DÍAZ del río, J. “Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio” Capítulo V: “La ciberseguridad en el ámbito militar.”, ISSN 1697-6924, Nº. 149, 2011.

EI-ISAC™ Cybersecurity Spotlight – CIA Triad. CIS Control 20: Penetration Tests and Red Team Exercises [online]. [Accessed 13 november 2018]. Available from: https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/

FARWELL, James P. y ROHOZINSKI, Rafal. Stuxnet and the future of cyber war. Survival, 2011, vol. 53, N° 1, pp. 23-40.

GOEL, Sanjay. Cyberwarfare: connecting the dots in cyber intelligence. Communications of the ACM, 2011, vol. 54, N° 8, pp. 132-140.

HOLMNER, Marlene Amanda, “et al”. A critical analysis of information and knowledge societies with

specific reference to the interaction between local and global knowledge systems. 2008. Tesis Doctoral. University of Pretoria.

JOYANES, A. “Big Data Análisis de grandes volúmenes de datos en organizaciones”, 1era. Edición, México, AlfaOmega, ISBN-10: 8426720811, 2013.

JUSTRIBÓ, Candela. Ciberdefensa: una visión desde la UNASUR. En: VII

Congreso del IRI/I Congreso del CoFEI/II Congreso de la FLAEI (La Plata, 2014). 2014.

KLIMBURG, Alexander (ed.) National cybersecurity framework manual. NATO

Cooperative Cyber Defense Center of Excellence, 2012.

KUEHL, Daniel T. From cyberspace to cyberpower: Defining the problem. Cyberpower and national security, 2009, vol. 30.

LEÓN, José Domínguez. La ciberguerra como realidad posible contemplada desde la prospectiva. Revista de Pensamiento Estratégico y Seguridad CISDE, 2016, vol. 1, no 1, pp.18-32.

LEWIS, James A. Computer Espionage, Titan Rain and China. Center for Strategic and International Studies-Technology and Public Policy Program, 2005, vol. 1.

LIBICKI, Martin C. Cyberspace is not a warfighting domain. ISJLP, 2012, vol. 8, p. 321.

LÓPEZ, J. D. "III jornadas de ciberdefensa del mando conjunto de ciberdefensa." [En línea] [Último acceso: 29/10/2018] Disponible en: https://jornadasciberdefensa.es/

MAHMOOD, Tariq y AFZAL, Uzma. Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. En Information assurance (ncia), 2013 2nd national conference on. IEEE, 2013. pp. 129-134.

MORUECO, MIGUEL. El ciberespacio como nuevo espacio político: notas para una ontología política nómada. [online]. UAM. [Accessed 29 october 2018]. Available from: http://www.uibcongres.org/imgdb/archivo_dpo1785.pdf

OWASP, Top. TOP 10–2017: The ten most critical web application security risks. The Open Web Application Security Project, 2017.

RUUS, Kertu. Cyber war I: Estonia attacked from Russia. European Affairs, 2008, vol. 9, no 1-2.

TAGUE, N , The Quality Toolbox. Second Edition, ASQ Quality Press, 2004. pp. 390-392.

TANKARD, Colin. Advanced persistent threats and how to monitor and deter them. Network security, 2011, vol. 2011, N° 8. pp. 16-19.

TASCÓN, M. y COULLAUT, A. (2016) "Big Data y el internet de las cosas", Catarata, ISBN:9788490970744, 2016

THORNBURGH, Nathan. Inside the Chinese Hack Attack. Times, august, 2005, vol. 25.

WAXMAN, Matthew C. Cyber-attacks and the use of force: Back to the future of article 2 (4). Yale J. Int'l L., 2011, vol. 36, p. 421.

WERKHÄUSER, Nina. German Army Launches New Cyber Command. Deutsche Welle, april, 2017, vol. 1.

WHITE, SARAH, 2018, Understanding Cyberwarfare: Lessons from the Russia-Georgia War. Modern War Institute (MWI) at West Point.

DIRECCIÓN DE LA REVISTA

DIRECTOR

CONSEJO EDITORIAL


CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL