Capítulo 2

Infraestructura crítica vulnerable a la ciberguerra

Hernán Díaz Mardones[*]

Introducción

Las ventajas y oportunidades que hoy se presentan con los avances en los ámbitos de la informática y de las telecomunicaciones, conocidas como TIC (tecnologías de la información y comunicación), permiten el acceso, producción, comunicación, integración y trabajo de información bajo diferentes formas o códigos, como imágenes, textos, sonido, etc., constituyendo la Internet una red global de comunicaciones interconectadas que permite una conectividad integral. Es posible señalar que ya han pasado más de veinte años desde el surgimiento de la Internet, después de su origen militar en EE.UU., oportunidad en la que se dio un gran salto cualitativo, que cambió y redefinió los modos de conocer y relacionarse del hombre. A lo anterior, y en forma inseparable, se suma el desarrollo de los computadores y *software*, junto con los aparatos móviles de comunicaciones de grandes capacidades, siendo estos últimos en la actualidad los principales medios por los que se accede a la Internet.

Este desarrollo tecnológico ha traído consigo acceso a grandes cantidades de *data*, transmisión de archivos, correos electrónicos, mensajería instantánea, etc., incluyendo el acceso a información general, privada, incluso de tipo

* Hernán Díaz Mardones es Coronel (r) del Ejército de Chile. Master of Business Administration, MBA in International Business, Universidad Gabriela Mistral; Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica, Academia de Guerra del Ejército de Chile; Ingeniero Comercial, mención en marketing, UDLA; Oficial de Estado Mayor del Ejército de Chile y de la Fuerza Aérea de Chile, Certificado en MBTI-Myers and Briggs Type Indicator, otorgado por HDS, México. hdiazm@acague.cl

personal, lo que facilita y simplifica la vida tanto en los ámbitos personal como profesional. De esta forma, todas las organizaciones, públicas como privadas, empresas, servicios de diferentes tipos, industrias, etc., han tomado como una de sus principales herramientas el uso de la Internet para mejorar y hacer más eficientes sus propias funciones, optimizando sus propios recursos y a la vez obtener las retribuciones económicas que traen consigo. Para facilitar o gestionar lo anterior, se han creado sistemas de redes, almacenamiento y distribución de megadatos, comunicaciones y otra variedad de infraestructuras que dan sustento al "negocio" de cada una de estas organizaciones en pos de sus fines.

Pero así como se facilita y se hace más expedito todo nuestro quehacer, también se hace más vulnerable, surgiendo riesgos que pueden llegar a convertirse en serias amenazas, afectando particularmente los servicios, organizaciones y estructuras que tienen un rol vital en el desarrollo de las actividades esenciales del ser humano del mundo moderno, las que en particular se denominan infraestructuras críticas (IC), cuyo daño o afección puede tener graves efectos en los intereses esenciales y la seguridad de cualquier país. Estos riesgos provienen de múltiples fuentes y se manifiestan mediante actividades de espionaje, sabotaje, fraudes o ciberataques realizados por otros países, por grupos organizados o por particulares, entre otros, surgiendo las denominadas ciberamenazas.

De ahí es que resulta imprescindible el crear soluciones para prevenir y controlar esos posibles riesgos y amenazas que implica el uso del ciberespacio, cuyo empleo con fines de causar daño a las IC pudiese efectuarse mediante una expresión extrema con la ciberguerra.

En ese contexto, resulta necesario establecer la relación entre la ciberguerra y las infraestructuras críticas, visualizando cuáles de estas pueden tener una mayor vulnerabilidad a las acciones de la ciberguerra, tomando como referencia a los principales actores del mundo en el tema, como lo son Estados Unidos y Europa, particularmente el caso de España y las acciones que han establecido para enfrentar este fenómeno. A su vez, realizar una aproximación a los roles que cumplen en esta relación las entidades públicas y privadas y las necesidades que surgen de ello.

Antecedentes y el conocimiento existente

La preocupación por la protección de la infraestructura crítica en muchos países se refleja mediante programas, planes, medidas legislativas, etc., tal es el ejemplo de los programas y acciones presentados por los presidentes Bill Clinton, George W. Bush y Barack Obama. Por su parte, el rey Juan Carlos I

de España promulga el 2011 la Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011), complementada por el Real Decreto 704/2011. Todos ellos con el claro fin de protegerlas, junto con sus activos claves de alto valor, que pueden convertirse en objetivos para sus adversarios potenciales.

Los aspectos claves en la formulación de una eventual estrategia de ciberguerra y la normativa para el uso de las armas cibernéticas son un tema que requiere análisis e investigación debido al escaso conocimiento y experiencia existente al respecto, donde se destaca el aporte documental de los conflictos cibernéticos entre naciones y el Manual de Derecho Internacional de Tallin (Tallinn Manual on the International Law Applicable to Cyber Warfare).

Este manual[1] fue publicado en el 2013 por el Centro de Excelencia para la Ciberdefensa Cooperativa de OTAN (CCD COE), que se aboca a un tópico emergente a nivel mundial, por lo que todo lo relacionado con el ciberespacio seguirá cambiando, aumentando su importancia y junto con ello la necesidad para las definiciones y desarrollo de normas. Es en ese contexto, pareciera ser, que surge la pregunta acerca de la importancia de contar con una estrategia global en el tema de la seguridad cibernética, lo que se comprueba con el debate que han comenzado de los aspectos jurídicos por Estados Unidos, las Naciones Unidas, la Organización del Tratado del Atlántico Norte y la Unión Europea, como respuesta al creciente problema de los ataques cibernéticos, la ausencia de políticas adecuadas y aspectos de orden legal[2].

Definiendo la infraestructura crítica

Cada Estado define y determina lo que constituye su infraestructura crítica, algunos autores definen la infraestructura crítica como "las capacidades básicas, los sistemas técnicos y las organizaciones responsables de la provisión de activos"[3]. La Comisión Europea define la infraestructura crítica como un "activo o sistema que es esencial para el mantenimiento de las funciones vitales de la sociedad"[4].

La ya citada Ley de Protección de Infraestructuras Críticas de España define como infraestructuras críticas aquellas "cuyo funcionamiento es

1 Documento que examina cómo poder aplicar las normas existentes de derecho internacional a la nueva Ciberguerra.

2 Thomas A. Johnson, *Cyber-Security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare,* Boca Raton; Florida EE.UU., CRC Press Taylor & Francis Group, 2015, preface.

3 Emery Roe and Paul R. Schulman, *Reliability and Risk: The Challenge of Managing Interconnected Infraestructures*, California, Standford University Press, 2016.

4 European Commission, Critical Infraestructure (2013). Bajo: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (Jun 12 2017).

indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales para el desarrollo normal de las actividades y la vida de las personas". En ese contexto, los servicios esenciales se constituyen como aquellos necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas. Por otra parte, también se define como infraestructuras estratégicas a las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información en las que descansa el funcionamiento de los servicios esenciales[5], generándose una interrelación entre las organizaciones que cumplen una determinada función calificada como esencial y el sistema tecnológico que la soporta y hace posible acceder a ellas.

Lo que es común en todas las definiciones es lo referido a los componentes de la infraestructura crítica, que puede incluir comunicaciones, servicios de emergencia, energía, represas, finanzas, alimentos, servicios públicos, industria, salud, transporte, gas, comunicaciones públicas, radio y televisión, tecnologías de la información, instalaciones comerciales, sector químico y nuclear, y agua. Muchos países dependen cada vez más de la infraestructura crítica, particularmente por los servicios que prestan, actividades y funciones que en general desarrollan, cuya afectación tiene importantes consecuencias y en las que tienen poco o ningún control, ya que normalmente se encuentran parcial o totalmente fuera de su jurisdicción.

Lo anterior se debe a que la infraestructura crítica en su gran mayoría es propiedad del sector privado, estimándose que más del 80 por ciento de ella en los países occidentales es operada y de propiedad de dicho sector[6]. En consecuencia, dondequiera que se encuentre la mencionada infraestructura, el Estado puede no estar en condiciones de garantizar la seguridad integral de ellas y puede depender en gran parte de las medidas, acciones e inversiones del sector privado para este fin. De ello surge como lógico que una alianza estratégica entre los sectores público y privado sea fundamental para una política de protección de la infraestructura crítica.

5 Boletín Oficial del Estado de España Nº 102, *Ley de Protección de Infraestructuras Críticas PIC 8/2011, Real Decreto 704/2011*, 29 de abril 2011, p. 4.

6 United Nations Security Council, Counter-Terrorism Committee, Executive Directorate, *Physical protection of Critical Infrastructure against terrorist attacks, CTDE Trends Report*, 8 marzo 2017, p. 2.

Algunos antecedentes de la infraestructura crítica en Estados Unidos y Europa

La Directiva de Política Presidencial de EE.UU., PPD-21, se orienta a mejorar y fortalecer los esfuerzos para mantener y asegurar las infraestructuras críticas. En esa misma directiva se reconoce que ella es diversa y compleja, incluyendo la distribución de sus redes, las diferentes estructuras organizacionales y los diferentes modelos operativos que funcionan tanto en el espacio físico como en el ciberespacio, siendo estas gubernamentales, privadas o multinacionales.

En esta Directiva presidencial, EE.UU. declara que su infraestructura crítica debe ser segura, capaz de resistir y recuperarse rápidamente de los peligros y amenazas, para ello deben proveerse de prevención, protección, mitigación, respuesta y recuperación, mediante planes y programas para reducir las vulnerabilidades, minimizar las consecuencias, identificar e interrumpir las amenazas e incrementar los esfuerzos de respuesta y recuperación de esta. Para lo anterior se le asigna la responsabilidad al Secretario del Departamento de Seguridad Nacional para promover la seguridad y resiliencia de las infraestructuras críticas del país. En función de ello debe identificar y priorizar las vulnerabilidades tanto físicas como las cibernéticas, en coordinación con las demás agencias sectoriales. En el mismo contexto, se le dispone mantener dos centros nacionales de infraestructura crítica, los que son operados por el departamento de Seguridad Nacional, uno para la infraestructura física y otro para la infraestructura cibernética, funcionando ambos en forma integrada[7].

Además, asigna la responsabilidad del desarrollo de la Fuerza de Tarea Conjunta Nacional de Investigación Cibernética (NCIJTF), operada por el FBI, con el objeto de coordinar, integrar y compartir información pertinente relacionada con ciberamenazas. Este equipo tiene representación del Departamento de Seguridad Nacional, la comunidad de inteligencia, el Departamento de Defensa y otras agencias, según corresponda; el Procurador General y el Secretario del Departamento de Seguridad Nacional colaborarán para llevar a cabo sus respectivas misiones de infraestructura crítica. La directiva presidencial incluye en materia de investigación y desarrollo (I+D) las actividades financiadas con fondos federales que buscan fortalecer la seguridad y la resistencia de la infraestructura crítica del país.

7 EE.UU., Presidential Policy Directive (PPD-21) on Critical Infrastructure Security and Resilience, Feb. 12, 2013.

La directiva presidencial, PPD-21, identificó los siguientes 16 sectores de infraestructura crítica y las Agencias del Sector Específico (SSAs, Sector Specific Agencies) a cargo de cada una de ellas:

1. Química: SSA: Departamento de Seguridad Nacional.
2. Instalaciones comerciales: SSA: Department of Homeland Security.
3. Comunicaciones: SSA: Departamento de Seguridad Nacional.
4. Fabricación Crítica (Critical Manufacturing): SSA: Departamento de Seguridad Nacional.
5. Represas: SSA: Departamento de Seguridad Nacional.
6. Defensa Industrial Base: SSA: Departamento de Defensa.
7. Servicios de Emergencia: SSA: Department of Homeland Security.
8. Energía: SSA: Departamento de Energía.
9. Servicios Financieros: SSA: Departamento de Hacienda.
10. Alimentación y Agricultura: Co-SSAs: Departamento de Agricultura de los Estados Unidos y Departamento de Salud y Servicios Humanos.
11. Instalaciones gubernamentales: Co-SSAs: Departamento de Seguridad Nacional y Administración de Servicios Generales.
12. Salud y Salud Pública: SSA: Departamento de Salud y Servicios Humanos.
13. Tecnología de la Información: SSA: Department of Homeland Security.
14. Reactores nucleares, materiales y desechos: SSA: Department of Homeland Security.
15. Sistemas de Transporte: Co-SSAs: Departamento de Seguridad Nacional y Departamento de Transporte.
16. Sistemas de agua y alcantarillado: SSA: Agencia de Protección Ambiental.

Las 16 infraestructuras críticas mencionadas, por una parte, son para EE.UU. la base de lo que han convertido a dicho país en una potencia mundial, pero también pasan a constituir vulnerabilidades si se convierten en blanco de un ataque. Al analizarlas se puede establecer que no todas las 16 infraestructuras críticas definidas en esta directiva presidencial son vulnerables a un ataque cibernético; sin embargo, las que efectivamente lo son forman parte de los recursos más críticos de esa nación.

En Europa, gran parte de los países de la Unión Europea han elaborado una Estrategia Nacional de Seguridad Cibernética, documento clave que incluye las medidas que se deben adoptar para hacer frente a los riesgos cibernéticos. Cada país tiene un enfoque propio respecto del tema, el que es diverso y de acuerdo con sus requerimientos nacionales, es decir, algunos países han desarrollado Planes de Acción Específicos, otros han creado grupos de trabajo por sector crítico para enfocarse en la protección de la

infraestructura crítica de la información y en el organismo responsable de la ciberseguridad nacional[8].

Desde el 2012 la European Union Agency for Network and Information Security (ENISA) ha estado apoyando a los países miembros, siendo su punto de partida en ello la realización de un balance de las actividades de ciberseguridad en Europa, analizando las tendencias y entregando recomendaciones para que los países diseñen, apliquen y evalúen una estrategia. El objetivo de esas estrategias nacionales de seguridad cibernética es garantizar que los Estados miembros estén preparados para afrontar riesgos graves, sean conscientes de sus consecuencias y prestos para responder adecuadamente. Sin embargo, se señala que existen inconvenientes en cuanto a las capacidades nacionales de coordinación en casos de incidentes transfronterizos y en términos de participación y preparación del sector privado. Basado en ello es que la Estrategia de Seguridad Cibernética de la UE de 2013 (EUCSS) pide a ENISA que "fomente las buenas prácticas en materia de seguridad de la información y de las redes para asistir y apoyar a los Estados miembros en el desarrollo de capacidades nacionales de ciberseguridad y la infraestructura energética"[9].

Por su parte España, como se mencionó, publica en abril del 2011 la Ley 8/2011, Protección de la Infraestructura Crítica (Ley PIC), definiendo las infraestructuras críticas, estableciendo cuáles servicios la conforman y los sistemas, tecnología y redes que las soportan, calificándolas como estratégicas[10].

Los dos grandes objetivos de esta norma son: 1) Catalogar el conjunto de infraestructuras que prestan servicios esenciales a nuestra sociedad, y 2) Diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

Respecto de la protección de las infraestructuras críticas, la Ley 8/2011 la define como el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del

8 European Union Agency for Network and Information Security (ENISA), Critical *Information Infrastructures Protection approaches in EU*, 2015, pp. 1-3.

9 Jefatura de Estado "BOE (Boletín Oficial del Estado)", Nº 102 de 29 de abril 2011, referencia: BOE-A-2011-7630, "Medidas de Protección de Infraestructuras Críticas", España (29 abril 2011).

10 Jefatura de Estado "BOE", Nº 102, 2011.

ámbito de su respectiva competencia. De igual modo, esta ley ha establecido las siguientes infraestructuras críticas: administración, agua, alimentación, energía, espacio, industria química, industria nuclear, instalaciones de investigación, salud, sistema financiero y tributario, tecnologías de la información y las comunicaciones y transportes.

Se puede deducir que los principales aportes de esta ley son la creación del Sistema Nacional de Protección de Infraestructuras Críticas, establecer las bases para el Sistema de Planificación PIC, generar el Catálogo Nacional de Infraestructuras Estratégicas y establecer el CERT (Equipo de Respuesta ante Emergencias Informáticas, del inglés Computer Emergency Response Team) para la gestión de incidentes de ciberseguridad.

Al respecto, se visualiza que una política que incluya la ciberseguridad de infraestructuras críticas deberá contener un esquema acabado de áreas, funciones y entidades estatales responsables que servirán para identificar y delimitar el nivel de impacto de cada sector. Además, deberá señalar qué órganos técnicos serán los encargados de ejecutar las medidas que se deriven de esa política, considerando aquellos estándares especiales de ciberseguridad, atendiendo a los particulares niveles de madurez de las IC, especialmente respecto de sus procesos esenciales. En este sentido, se aprecia que las seleccionadas como las más relevantes en EE.UU. son aquellas catalogadas como las más críticas sobre la base de su impacto de interdependencia con las otras definidas como tales, estas son: energía y la red eléctrica, transportes y telecomunicaciones[11]. Por su parte, España tiene similitud en sus propias IC, siendo la del "espacio" la única diferente a las especificadas por EE.UU., pero en general están contenidas tanto por uno como por otros en sus respectivas leyes o políticas.

La ciberguerra y la infraestructura crítica

En el nivel estratégico y con relación a la afectación de las infraestructuras críticas ya mencionadas anteriormente, se asigna como la primera ciberguerra al conflicto de la Estonia rusa el 2007, debido al ataque masivo denominado ataque distribuido de denegación de servicio (distributed denial-of-service (DDoS) en contra de Estonia. El motivo de asignar a este evento como la primera guerra cibernética o ciberguerra se debe al compromiso real de la Organización del Tratado del Atlántico Norte (OTAN) en el establecimiento de un Centro de Defensa Cibernética en el 2008 en Tallin, Estonia. Otra razón

11 Thomas A. Johnson, 2015, p. 43.

está en el hecho de que este fue el ataque DDoS más grande jamás visto, con más de un millón de computadoras dirigidas a las infraestructuras críticas del área de la economía, el comercio y las comunicaciones de Estonia a nivel nacional. Ello se tradujo en que los usuarios estonios no pudieron usar sus tarjetas de crédito, realizar operaciones bancarias, recibir noticias y comunicarse mediante los canales normales de comunicación. Este ataque duró semanas y obligó a Estonia a considerarlo como un acto de guerra, y como miembro de la OTAN, solicitaron ayuda al Consejo del Atlántico Norte de la Alianza Militar de la Organización. El hecho que la OTAN estableciera un Centro de Defensa Cibernética en Tallin se marca como un hito al ser la primera vez que se adopta esta acción; por otra parte, los expertos en ciberseguridad rastrearon la actividad cibernética estableciendo que estaban bajo el control de Rusia, sin embargo, este lo negó declarando que falsificaron sus sitios[12].

Un ataque distribuido de denegación de servicio (DDoS) es un ataque en el que múltiples sistemas informáticos comprometidos atacan a un objetivo, como un servidor, un sitio *web* u otro recurso de red y causan una denegación del servicio para los usuarios del recurso de destino. Su principal característica es la inundación de mensajes entrantes, solicitudes de conexión o paquetes con malformaciones dirigidos al sistema de destino, lo que obliga a disminuir la velocidad o incluso a bloquearse y apagarse, negando así el servicio del sistema a los usuarios legítimos[13]. Por otra parte, los paquetes con malformaciones (malformed packets) se refieren a cualquier ataque que utiliza paquetes no estándar para causar denegación de servicio, estos ataques generalmente explotan errores en el protocolo de control de transmisión y protocolo de internet (TCP / IP) inundando el sistema de la víctima mediante el envío de paquetes con formato atípico[14].

A nivel de empleo de las fuerzas, uno de los hechos que dan cuenta de los comienzos de la ciberguerra ocurrió en 1990 y 1991, en circunstancias que EE.UU. enfrentaba a Irak en la denominada "primera guerra del Golfo", ocasión en la que cinco piratas informáticos de origen holandés penetraron en sistemas informáticos de 34 sitios militares norteamericanos por medio de Internet. De este hecho se obtuvo información de la planificación militar de EE.UU. para la Operación Tormenta del Desierto, dentro de la que se encontraban detalles acerca de la ubicación exacta de tropas, armas y movimiento de buques de guerra en la región del golfo. Estos antecedentes se

12 Thomas A. Johnson, 2015, pp. 177-178.

13 Search Security Techtarget, "Distributed denial of service (DDoS) attack", 2017. goo.gl/k7217h (consultado 14 de junio 2017).

14 Ebscohost Connection, "Malformed Packet Attack", marzo 2007. goo.gl/bQtgan (consultado 14 de junio 2017).

traspasaron a las autoridades iraquíes, pero estos la desecharon por estimar que se trataba de información falsa, y que formaba parte de una operación de decepción o engaño, lo que en realidad no fue así[15].

Por otra parte, dentro de las operaciones en el contexto de la ciberguerra, en la misma Guerra del Golfo mencionada anteriormente está el hecho del desarrollo de operaciones ofensivas por parte de EE.UU. Un ejemplo de ello es la realizada al inicio de este conflicto y que precedió a la invasión por las fuerzas de la coalición, que tuvo como resultado dejar fuera de servicio la mitad de los sistemas computacionales de las fuerzas militares de Irak, lo anterior se realizó mediante la instalación de virus en dispositivos (*hadware*) en Francia y enviados a Irak por intermedio de Jordania, los que estaban diseñados para desactivar las computadoras Windows y el computador central[16].

Otro hecho importante de destacar en relación con la ciberguerra y los efectos de esta en las infraestructuras críticas, es el caso de China. Después de las guerras del Golfo, con las experiencias y aprendizajes derivados de ese conflicto, China efectuó un cambio significativo dando un paso trascendente en el desempeño de sus medios militares y de las acciones relacionadas con la ciberguerra, ello después de observar al ejército iraquí enfrentar a EE.UU. y sus aliados utilizando sistemas de armas soviéticos y chinos, similares a los usados por sus propias fuerzas, con los que fueron derrotados en 42 días debido a la tecnología avanzada y a la estrategia de guerra de información de EE.UU. Con esta experiencia llegaron a la conclusión de que la guerra tradicional se cambiaría para siempre debido al uso de sistemas de información y tecnología avanzada y a la integración de estos, definiéndolos como fundamentales para los cambios y avances necesarios para un nuevo y moderno ejército chino[17]. Con esas nuevas características, la nueva doctrina china se enfocaría a las capacidades de tipo ofensiva y dirigida a la infraestructura del enemigo, así como la infraestructura bancaria, los sistemas de redes eléctricas y otras infraestructuras críticas, centrándose en los aspectos de la fuente de poder de una sociedad determinada, que inevitablemente son los sistemas económicos y los sistemas esenciales, con el fin de debilitar a la nación enemiga hasta el punto de que la guerra regular entre militares no sería necesaria[18].

El actual grado de capacidades chinas para desarrollar acciones de ciberguerra, según EE.UU., se sostiene en el robo de propiedad intelectual de corporaciones norteamericanas, laboratorios de investigación, contratistas de

15 Thomas A. Johnson, 2015, p. 156.
16 Thomas A. Johnson, 2015, p. 156.
17 Thomas A. Johnson, 2015, p. 179.
18 Jennifer Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington: Georgetown University Press), 2005.

defensa y los propios militares, obteniéndolas mediante el ciberespionaje. Según investigaciones, se han obtenido por ese medio cientos de datos e informaciones de 141 organizaciones y compañías que involucran a 20 industrias importantes, mediante ataques que se centran no en hacer daño, sino en la exfiltración de datos y permanecer ocultos en los sistemas de información de la organización objetivo durante el mayor tiempo posible. Dentro de las revelaciones conocidas, existen algunos diseños de armas obtenidos por las mencionadas actividades de ciberespionaje de China, entre ellas destacan los diseños para el sistema avanzado Patriot Missile-Pac-3, el terminal High Altitude Defense para disparar misiles, Aegis de la Armada sistema de defensa de misiles balísticos, el avión de combate F/A-18, el helicóptero Black Hawk, el nuevo buque de combate del litoral de la marina y el F-35 Joint Strike Fighter. La obtención ilegal de estos diseños de sistemas de armas representa miles de millones de dólares de ventajas de combate para China y un ahorro para ellos de al menos 25 años de investigación y desarrollo. El 2014 el Departamento de Justicia norteamericano reunió pruebas suficientes para acusar a cinco grandes entidades chinas de múltiples cargos de espionaje cibernético ilegal[19].

Teniendo consideración de lo anterior, se puede establecer que existe una clara y directa relación entre la ciberguerra y las infraestructuras críticas, ello debido a que las últimas pasan a conformar objetivos, mediante estos, quien quiera afectar una determinada área esencial de una nación, lo puede lograr mediante la anulación, interrupción, destrucción de una determinada IC.

Como nota interesante derivada de los antecedentes descritos está la importancia que el Teniente General Adjunto Qi Jianguo atribuye a la toma y el mantenimiento de la superioridad en el ciberespacio, porque cree que hoy apoderarse del ciberespacio es más importante que el dominio del espacio marítimo y del aire, que en su momento lo tuvo durante la Segunda Guerra Mundial.

Reflexiones finales

Las acciones ofensivas en una ciberguerra se pueden lanzar virtualmente desde cualquier rincón del mundo, por cualquier país, organización o incluso individuos, razón por la que la necesidad de crear estrategias de defensa para proteger las infraestructuras críticas es más que fundamental. Sin lugar a dudas, considerando las diferentes estrategias, políticas y acciones

19 Thomas A. Johnson, 2015, pp. 179-183.

que diferentes países se han propuesto con ese fin, el diseño, preparación e implementación de estrategias defensivas que tengan como punto de partida la prevención, advertencias de intrusión y detección, disuasión, y otros mecanismos de defensa, son fundamentales para evitar vulnerabilidades y adelantarse a las amenazas. Enseguida, algunas medidas relacionadas a ataques de características contraofensivas como parte de la estrategia defensiva, constituirán el siguiente paso y dependerá en gran medida del desarrollo tecnológico asociado a las capacidades que las infraestructuras críticas, tanto de origen privado como públicas, sean capaces de integrar, teniendo cubierto de la mejor manera posible sus medidas defensivas como base para este desarrollo.

Las infraestructuras críticas, como ya se mencionó en los diferentes países tomados como ejemplo, son definidas en forma general como instalaciones, redes, servicios y equipos físicos y de tecnología de la información, siendo un aspecto relevante el que sean consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales y cuya afectación pudiera comprometer la Seguridad Nacional. Sin embargo, resulta importante la definición de detalle de cada una de las IC, con el fin de desarrollar las estrategias de protección y la ciberdefensa de sus componentes. Entre ellas y de acuerdo con las experiencias de los principales países expuestos, en Chile se pueden desde ya considerar diferentes áreas, entre las que se encuentran las empresas que manejan las aguas, como presas, tratamiento y redes de distribución; otras en centrales de energía eléctrica; del sector salud, incluyendo hospitales; las relacionadas con el transporte, entre ellas los aeropuertos, terminales de autobuses; las relacionadas con la industria química, incluyendo el transporte de elementos de alto riesgo como materiales químicos, biológicos y radiológicos; también el sistema financiero, incluyendo en este los bancos, bolsas de valores, recaudación de impuestos, etcétera.

Con ese fin, lo planteado por la directiva presidencial de EE.UU., PPD-21, en relación con las capacidades que deben desarrollar las IC: "ser segura, capaz de resistir y recuperarse rápidamente de los peligros y amenazas, para ello deben proveerse de prevención, protección, mitigación, respuesta y recuperación, mediante planes y programas para reducir las vulnerabilidades, minimizar las consecuencias, identificar e interrumpir las amenazas e incrementar los esfuerzos de respuesta y recuperación", resultan, bajo las experiencias descritas, de la mayor relevancia, resultando más que conveniente que el trabajo que se genere de cualquier país para la promulgación de una política o estrategia nacional de ciberseguridad, relacionado con las políticas específicas de ciberdefensa, las tengan en consideración.

Como se deduce, en las diferentes áreas que pueden integrar las IC se encuentran involucrados organismos y entidades, pertenecientes al sector

público y privado, por tanto resulta importante establecer la necesidad de que ambas áreas del quehacer estén integradas y coordinadas para que los efectos de las diferentes estrategias sean los apropiados y exitosos, ya sea mediante alianzas estratégicas entre ambos sectores, la colaboración formal e informal entre ellos, las asociaciones público-privadas, en algunos casos mediante procedimientos legales, con el fin de asegurar que las partes interesadas participen en la protección de las IC, todas estas estrategias, acciones o medidas deberán amoldarse a las diferentes IC en particular, ya que resulta poco probable que un modelo único sea aplicable a diferentes entidades.

Además, del hecho mismo de la necesidad de integración y coordinación, otro aspecto importante de incluir en los análisis para los efectos antes mencionados, es la conformación por sobre las diferentes IC de un ente integrador y coordinador, que permita un adecuado cumplimiento de funciones, intercambio de información, adopción de estrategias, difundir experiencias, mejora de capacidades, capacitación y estudio del panorama internacional y ataques ocurridos a las IC en diferentes lugares del mundo para que junto con tomar conciencia ayude a diseñar proyectos de protección, normativa, etc. En ese contexto, la educación continua de todos los integrantes componentes de una IC acerca de las ciberamenazas y las prácticas de seguridad fundamentales, son esenciales para ayudar a reducir el riesgo de error y para fortalecer las áreas de colaboración. En síntesis, una arquitectura de carácter integral en seguridad que actúe sobre las funciones de protección, detección y mejora continua, mejorando la gestión de los riesgos, la combinación y fortalecimiento de nuevas herramientas.

Como se puede deducir, la relación de la ciberguerra con las infraestructuras críticas es de carácter directo, ya que constituyen los objetivos reales mediante los cuales quien quiera ejercer efectos nocivos en una determinada área de las que componen dichas infraestructuras, pueden paralizar una nación por un tiempo determinado, logrando aprovechar las vulnerabilidades mediante ataques desde cualquier parte del mundo. Estas acciones y efectos pueden darse en diferentes niveles, siendo lo normal por las experiencias descritas que sucedan en niveles de orden nacional.

Respecto de las que tengan mayor vulnerabilidad a las acciones de la ciberguerra, se puede afirmar que están en general aquellas relacionadas con las instalaciones, redes, servicios y equipos físicos, todos ellos asociados y sustentados en la tecnología de la información, particularmente con acceso a Internet, destacando principalmente las relacionadas con energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, protección civil y defensa, siendo característico su consideración como estratégicas, por su relación con las actividades esenciales y prestación

de servicios públicos fundamentales y cuyas consecuencias pudiera comprometer la Seguridad Nacional.

Bibliografía

Council of the European Union. "Identification and designation of European critical infrastructures and the assessment of the need to improve their protection", *Official Journal of the European Union*, Nº 114/EC (diciembre 2008).

Ebscohost Connection. "Malformed Packet Attack" (marzo 2007).

Edgar Vásquez Cruz. "Proteger la infraestructura crítica, una tarea fundamental en ciberseguridad nacional", McAfee Securing Tomorrow (Documento en línea, 6 de junio 2016) (https://securingtomorrow.mcafee.com/author/edgar-vasquez-cruz/). [Consultado 19 de julio 2017].

Emery Roe and Paul R. Schulman. *Reliability and Risk: The Challenge of Managing Interconnected Infraestructures*, California: Standford University Press, 2016.

European Union. "Critical Information Infrastructures Protection approaches in EU", Agency for Network and Information Security (ENISA), 2015.

Gobierno de España. "Ley de Protección de Infraestructuras Críticas PIC 8/2011", Boletín Oficial del Estado de España Nº 102, Real Decreto 704/2011, 29 de abril 2011.

http://connection.ebscohost.com/c/reference-entries/31667776/malformed-packet-attack (Documento en línea) [consultado 14 de junio 2017].

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (Documento en línea) [consultado el 18 de junio 2017].

Jennifer Sims and Burton Gerber. *Transforming U.S. Intelligence,* Washington: Georgetown University Press), 2005.

Johnson, Thomas A. *Ciber-Security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, Boca Raton, Florida: CRC Press, Taylor & Francis Group, 2015.

Jorge Kamlofsky, Hugo Colombo, Matías Sliafertas, Juan Pedernera. *"Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas"*, CAETI - Universidad Abierta Interamericana, Buenos Aires, Argentina, noviembre 2015.

Manuel Sánchez. "*Infraestructuras Críticas y Ciberseguridad"*, Director para Europa de la World Security Federation (WSF), julio 2011.

Search Security Techtarget. "Distributed denial of service (DDoS) attack" (2017), http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack (Documento en línea) [consultado 14 de junio 2017].

U.S. Government. Presidential Policy Directive (PPD-21) "On Critical Infrastructure Security and Resilience", EE.UU., Feb. 12, 2013.

United Nations Security Council. "Physical protection of Critical Infrastructure against terrorist attacks", CTDE Trends Report, Counter-Terrorism Committee, Executive Directorate, 8 marzo 2017.