# LOS CIBERATAQUES COMO AMENAZAS A LAS INFRAESTRUCTURAS Y RECURSOS CRÍTICOS DE UN ESTADO

Gustavo Vila[1]


## RESUMEN

Las Tecnologías de la Información y Comunicaciones (TIC) son una de las fuerzas más poderosas que se hallan detrás de la evolución de las sociedades contemporáneas. A su vez, los Estados dependen del funcionamiento confiable de sus infraestructuras críticas para el logro de sus Objetivos Nacionales (OONN). En la actualidad, distintos tipos de ciberamenazas explotan la creciente complejidad y conectividad de los sistemas de infraestructura crítica, colocando a éstos en una posición de vulnerabilidad y riesgo. Debido al rol protagónico de aquellos en la vida diaria de todas las personas, se hace necesario lograr un adecuado marco de seguridad en el ciberespacio, como una forma de contribuir decisivamente a la seguridad nacional.


Palabras clave: Infraestructura crítica, Terrorismo, Ciberseguridad, Amenazas, Defensa Nacional.

## 1 - Introducción

En el mes de Junio de 1982, un satélite de reconocimiento de EEUU detectó una enorme explosión en un gasoducto de Siberia. La causa fue una falla en el sistema de control informático del gasoducto, el cual había sido robado por espías soviéticos de una compañía de Canadá. Los soviéticos desconocían que la CIA había manipulado el software para que, luego de un tiempo, el sistema se resetease y permitiese la generación de presiones insoportables para las uniones y soldaduras de las tuberías, sin que se disparasen las alarmas del sistema. Esta puede ser considerada la primera demostración de los efectos de una "bomba lógica" en una infraestructura crítica (The Economist, 2010).

Las TIC son una de las fuerzas más poderosas que se hallan detrás de la evolución de las sociedades contemporáneas y los Estados dependen del funcionamiento confiable de sus infraestructuras críticas para el logro de sus Objetivos Nacionales (OONN) e Internet fue

[1] El Magister Gustavo Vila es un Coronel retirado del Arma de Infantería del Ejército Nacional. Es Oficial Diplomado de Estado Mayor, egresado del Curso de Altos Estudios Nacionales (CALEN), Licenciado en Ciencias Militares con orientación en Estrategia (IMES), y Magister en Estrategia Nacional.

diseñado para la comodidad y fiabilidad, no para la seguridad. Sin embargo en un mundo interconectado, Internet brinda a la par oportunidades y amenazas en relación con las infraestructuras críticas: ningún pasaporte es necesario en el ciberespacio, un dominio que constituye un bien público mundial impuro[2]. Las ciberamenazas explotan la creciente complejidad y conectividad de los sistemas de infraestructura crítica, colocando a los mismos en una posición de vulnerabilidad y riesgo. Debido a su rol protagónico en la vida diaria de las personas, se hace necesario lograr un adecuado marco de seguridad en el ciberespacio, como una forma de contribuir decisivamente a la seguridad nacional. Un ejemplo de lo anterior lo constituye la situación caótica que supondría la interrupción de la energía eléctrica o anomalías en el sistema económico-financiero, mediante ataques informáticos desarrollados por Estados, organizaciones o personas (Saavedra, 2015) (Sancho, 2016). Si bien las computadoras e Internet han transformado la economía y han dado grandes ventajas cualitativas a los ejércitos de las grandes potencias, no es menos cierto que la tecnología digital tiene su contracara: los riesgos a ciberataques por parte de actores estatales y no estatales, constituyendo una amenaza compleja, difusa y potencialmente muy peligrosa[3] (Martin, 2016).

# 2 - Desarrollo

## 2.1 – Globalización, terrorismo y nuevas amenazas

El ciberespacio es un dominio virtual donde se llevan adelante complejas actividades "on line" asociadas al proceso de globalización en el que nos hallamos insertos; este quinto dominio ha sido generado por las TIC y en él coexisten las personas y las computadoras, y constituye el campo de batalla de la ciberguerra. En el ciberespacio no hay un límite geográfico claro y el teatro de operaciones son las redes globales interconectadas (Sancho, 2016). Este dominio se caracteriza por permitir ocultar la identidad y ubicación de las personas, en tanto que es omnipresente en algunos lugares e inexistente en otros, permitiendo aumentar la velocidad, volumen y alcance de los Estados y las personas, requiriéndose para su acceso de medios de tratamiento automático de información y conexiones de datos. La Junta de Estado Mayor Conjunta de los EEUU define al ciberespacio como "Un dominio global dentro del entorno de información consistente en las redes interdependientes de tecnología de información, infraestructura y datos, incluidos Internet, las redes de telecomunicaciones, los sistemas informáticos, así como los procesadores y controladores allí insertados" (DoD, 2016, p. 58).

[2] Los bienes públicos mundiales pueden ser puros e impuros. Un bien público mundial puro es aquel donde hay imposibilidad que exista rivalidad y exclusión en su uso o consumo. Uno impuro en cambio, es aquel en el cual existe rivalidad y/o exclusión en su uso o consumo. El ciberespacio encaja en esta última categoría," […] presentando deficiencias en cuanto a su oferta, cobertura, disponibilidad, calidad y seguridad. […] las autoridades nacionales tienen una importante responsabilidad en la regulación de la existencia, uso, y condiciones de funcionamiento del ciberespacio…" (Santo, 2016, P 48).

[3] Existen muchas "áreas oscuras" y a diferencia de la guerra convencional, no hay una normativa específica al respecto. En el caso de la OTAN, el vacío pretendió ser llenado con el llamado "Manual de Tallin", el cual en sus 302 páginas, proporciona 95 "reglas" a partir de la legislación que aplica a los conflictos convencionales, adaptados al ciberespacio y a la ciberguerra. Bajo esta óptica un hacker puede ser considerado un blanco legítimo si representa una amenaza para el país que sufre la agresión cibernética, ante la posibilidad que cause lesiones o muerte de personas, o bien daños o destrucción de infraestructura crítica, pudiendo en consecuencia ser objeto de ataques para su neutralización (El Mundo, 2013).

La actual globalización supone tanto ventajas como riesgos[4]. Al hablar de actores hostiles en el ciberespacio se debe hablar de Estados y organizaciones, y dentro de éstas adquieren especial significación las organizaciones terroristas. Hoy el ciberespacio es uno de los campos de batalla en la guerra contra el terrorismo y las infraestructuras críticas constituyen blancos altamente redituables; a su vez las TIC pueden llegar a constituirse en armas de destrucción y desinformación masiva. El ciberterrorismo ya está entre nosotros y resulta posible y altamente probable que las TIC sigan siendo utilizadas por actores no estatales para alcanzar sus objetivos (Martin, 2016). El empleo del ciberespacio por organizaciones terroristas ha dado origen al término "ciberterrorismo" el cual es definido por el Ministerio de Defensa de España (2010) como "un ciberataque para causar la inutilización o interrupción de redes de ordenadores o comunicaciones para generar temor o intimidar a la sociedad con un objetivo ideológico" (p. 348).

Hoy los grupos terroristas utilizan Internet para llegar a sus seguidores y difundir su mensaje, pero sus capacidades para lanzar ciberataques sobre infraestructuras y recursos críticos siguen siendo muy limitadas. Esta ausencia de ciberataques por organizaciones terroristas puede interpretarse como el resultado de la falta de habilidades técnicas apropiadas dentro de los grupos para desarrollar virus informáticos o la incapacidad para infiltrar agentes en las infraestructuras críticas, pero esta circunstancia puede cambiar muy rápidamente. Actualmente se han detectado una serie de grupos de hackers que trabajan para diferentes organizaciones terroristas, así como un sinnúmero de amenazas[5] (Europol, 2018). Si bien las organizaciones terroristas no disponen de capacidades creíbles para lanzar un ciberataque masivo, algunos

[4] Desde el punto de vista de las TIC la globalización puede ser considerada a partir de tres aspectos: la conectividad, la fiabilidad y la vulnerabilidad. En relación con la conectividad, Saavedra (2016) señala que personas dispersas por todo el mundo pueden reunirse virtualmente como nunca antes; si bien las ventajas del mundo on line son muy frecuentemente rescatadas, no es menos cierto que a la par de las ventajas existen una serie de debilidades. Nuestra sociedad y los servicios públicos esenciales (SSPPEE) que constituyen la infraestructura crítica y permiten nuestra vida cotidiana sin sobresaltos, son cada vez más "on line-dependientes". La creciente conectividad a través de una Internet insegura multiplica las vías para un ciberataque; a su vez, la creciente dependencia en las computadoras aumenta el daño que pueden causar (The Economist, 2010). En este contexto, la fiabilidad está dada por la capacidad de las organizaciones que habiendo detectado una vulnerabilidad en sus sistemas, rápidamente aplica parches y medidas defensivas. El problema es que el grado de fiabilidad es variable: existen organizaciones que reparan y refuerzan sus sistemas rápidamente, otras no son capaces de darse cuenta que están utilizando un software vulnerable, en tanto que otras ni siquiera son capaces de bajar las actualizaciones de seguridad del software que utilizan. En lo que refiere a la vulnerabilidad, esta se incrementa proporcionalmente a la reducción de las barreras de acceso al ciberespacio al existir dispositivos de muy bajo costo que combinan comunicaciones, acceso a la web, así como capacidades de video. Esta conectividad, a través de la Internet de las Cosas (IoT), ofrece un sinnúmero de oportunidades a personas y organizaciones con las habilidades y medios técnicos adecuados. Mayor conectividad significa mayor vulnerabilidad, resultando particularmente expuestos las redes eléctricas, instalaciones nucleares, los oleoductos de gas y petróleo, y los bancos y el sistema financiero en general (The Economist, 2010).

[5] El Estado Islámico (EI) disponía de la Hacking División, también conocida por la denominación de Ciber Califato, la cual incorporaba a cualquier grupo hacker que se identificase con la organización terrorista. En un momento la Hacking División llegó a contar con varias organizaciones, siendo las más importantes el Ciber Ejército del Califato (Caliphate Cyber Army), el Ciber Ejército Islámico (Islamic Cyber Army) y los Hijos del Ejército del Califato (Sons of the Caliphate Army). Estas organizaciones trabajaban en el ciberespacio atacando websites, recopilando información sobre los sistemas de energía eléctrica y las industrias, y realizando reclutamiento en Facebook y Twitter.

estudios sugieren que estos grupos pueden estar tratando de "tercerizar" estas capacidades. Para ello,

> en lugar de tratar de desarrollar su propia capacidad y herramientas, algunos grupos terroristas ahora se orientan hacia mercados criminales en línea, utilizando los servicios de la industria del crimen para comprar el acceso a las capacidades que ellos mismos carecen. Si esto es cierto, es probable que la efectividad de los grupos ciberterroristas aumente, tal vez en el corto plazo (Europol, 2018, p. 15).

A los efectos de amplificar los efectos sobre la opinión pública, debido al poco impacto que genera un ciberataque en el mundo virtual (el cual muchas veces es ocultado por quién lo recibe), es posible amplificar los efectos de aquel conduciendo al mismo tiempo un ciberataque contra infraestructuras críticas que produzcan efectos en el mundo real, en lo que se denomina un "ataque híbrido", pudiendo afectar alguno de los servicios públicos esenciales (SSPPEE) como ser el agua potable, la energía eléctrica, las represas o los sistemas de comunicaciones (Europol, 2018).

## 2.2 – La guerra cibernética y las ciberamenazas

Dentro de las llamadas "nuevas amenazas"[6] encontramos **la guerra cibernética o ciberguerra,** la cual es un conflicto en el ciberespacio. Ésta puede ser definida como "el uso de capacidades basadas en la red de un Estado, para interrumpir, denegar, degradar, manipular o destruir información residente en computadores y redes de ellos, o los propios ordenadores y las redes de otro Estado" (Leiva, 2018, p. 27).[7] Debido a ello, en la ciberguerra no proteger las redes propias equivale a dejar abierta la puerta de calle de nuestra casa; la securitización de una red en cambio equivale a cerrar con llave: no impide los robos, pero los dificulta.

Asociados con el concepto de ciberguerra se encuentran los conceptos de ciberseguridad y ciberdefensa.

- **Ciberseguridad.** Puede definirse como "Prevención de daños, protección y restauración de equipos, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicación alámbrica y comunicación electrónica, incluyendo la información contenida en el mismo, para asegurar la disponibilidad, integridad, autenticación, confidencialidad y no rechazo" (DoD, 2016, p. 57). Ella es un proceso mediante el cual se protege a través de la prevención, detección y respuesta contra los diferentes tipos de amenazas a las infraestructuras críticas, los sistemas de información y de comunicaciones, negándole su uso a terceros. La seguridad

[6] El Decreto 105/14 Política de Defensa Nacional de la ROU señala como obstáculos que podrían devenir en amenazas al deterioro del medio ambiente; las pandemias; el Crimen Organizado (y dentro de éste la modalidad de crimen cibernético); el terrorismo; la materialización del espionaje y los ataques cibernéticos; la inestabilidad democrática en la región; el surgimiento de guerras extracontinentales; el agravamiento de conflictos regionales; las crisis económicas; y la apropiación y el control indebido de los recursos estratégicos (Poder Ejecutivo, 2014).

[7] La diferencia entre la ciberguerra y la guerra convencional en lo que a efectos sobre el adversario refiere, es ínfima. Una de las principales diferencias la constituye el medio ambiente operacional, que en este caso lo constituye el ciberespacio. En este tipo de conflicto el soldado es el *cracker*, quién busca vulnerabilidades en nuestros dispositivos y sistemas, del mismo modo que el comandante enemigo busca las vulnerabilidades en nuestro despliegue, o el ladrón busca las vulnerabilidades en nuestros domicilios.

informática se lleva adelante con tres objetivos: asegurar la disponibilidad, confidencialidad e integridad de los sistemas y la información (Saavedra, 2015).

- **Ciberdefensa.** Es la "aplicación de medidas de seguridad para proteger las los diferentes componentes de los sistemas de información y comunicaciones de un ciberataque" (Ministerio de Defensa, 2010). Comprende tanto medidas de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras organizaciones.

En función de lo anterior, y tal como lo señala Camps (2016), podemos atribuirle a la ciberseguridad un carácter más preventivo, es decir evitar que se produzca el ciberataque, en tanto que la ciberdefensa tiene un carácter más reactivo, es decir la reacción una vez producido al ataque.

Los actores capaces de materializar un ataque informático son variados y García et al. (2016) señalan que el ataque puede ser realizado por una variedad de elementos hostiles que incluyen crackers, delincuentes comunes, atacantes internos, personal descontento, personal realizando actividades no autorizadas (acceso a Internet), servicios de inteligencia extranjeros, crimen organizado, terroristas, entre otros. Por ello una **ciberamenaza** es:

> Cualquier circunstancia o evento con el potencial de impactar negativamente sobre las operaciones de la organización (incluyendo su misión, funciones, imagen o reputación), recursos, y otras organizaciones a través de Tecnología de la Información (TI) y/o un Sistema de Control Industrial (SCI), a través del acceso, destrucción, divulgación, modificación de información o denegación de servicio, de forma no autorizada (DoE, 2012).

En el Anexo 3 se realiza una caracterización de las amenazas.

Las TIC han generado el ciberespacio, el quinto dominio de interacción humana[8], y a partir de 1998[9] un nuevo campo de batalla de dimensiones planetarias. Este nuevo dominio ha inducido la aparición de nuevas amenazas materializadas por individuos, organizaciones o Estados que buscan defender sus intereses a través de herramientas cibernéticas (Camps, 2016). Por su parte Santo (2016) y Parraguez (2017), señalan que una cantidad creciente de países identifican los ataques cibernéticos como una amenaza igual o mayor que la representada por un ataque terrorista debido a sus afectaciones a la seguridad nacional y sus implicaciones en todos los campos de poder nacional. Un ciberataque (o ataque cibernético) es definido por el Ministerio de Defensa (2010) de España como una "forma de ciberguerra/ciberterrorismo donde combinado con un ataque físico o no se intenta impedir el empleo de los sistemas de información del adversario o el acceso la misma".

[8] El primer dominio lo constituye la tierra, el segundo el mar, el tercero el aire, el cuarto el espacio, y el quinto el ciberespacio.

[9] En 1998, la organización insurgente Ejército de Liberación Tigres de Tamil Ealam (LTTE – Liberation Tigers of Tamil Ealam, también conocida como los "*Tigres Tamiles*") que operaba en Sri Lanka, atacó con correos masivos sedes diplomáticas del gobierno de Sri Lanka con un promedio de 800 correos diarios, a lo largo de dos semanas, saturando sus redes. El mensaje decía "Somos los Tigres Negros de Internet y estamos haciendo esto para desorganizar sus comunicaciones" (Martin, 2016). Esta acción fue el primer ciberataque por parte de una organización irregular contra el sistema informático de un país.

## 2.3 – Los Activos Críticos Nacionales (ACN) como objetivos potenciales.

### 2.3.1 – Qué son las Infraestructuras y Recursos Críticos (IRRC) y los ACN?

Cada Estado y dentro de éste, cada organización debe definir y determinar aquellas **Infraestructuras y Recursos Críticos (IRRC)** que constituyen sus **Activos Críticos Nacionales (ACN).** La legislación de Perú a este respecto, resulta muy ilustrativa acerca del vínculo entre IRRC y ACN.

- El Decreto Supremo N° 106-2017-PCM define la infraestructura como "Conjunto de estructuras, instalaciones u obras que componen un Activo Crítico Nacional – ACN, que son esenciales e imprescindibles para el normal desarrollo o funcionamiento de un país." (Poder Ejecutivo del Perú, 2017).
- El mismo decreto anterior define los recursos como "Conjunto de elementos tangibles o intangibles, disponibles de una Nación, que componen un Activo Crítico Nacional – ACN, permiten atender una necesidad o alcanzar un objetivo y son esenciales e imprescindibles para el normal desarrollo o funcionamiento de un país" (Poder Ejecutivo del Perú, 2017).
- Finalmente se define un ACN como:

  recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales, o que están destinados a cumplir dicho fin. La afectación, perturbación o destrucción de dichos activos no permite soluciones alternativas inmediatas, generando grave perjuicio a la Nación. (Poder Ejecutivo, 2017).

Cada Estado debe determinar cuáles son los ACN a ser protegidos y establecer políticas o estrategias para la protección de los mismos. España, por ejemplo, definió las bases de su política de protección de infraestructura crítica a través de la Ley de Protección de Infraestructuras Críticas PIC 8/2011, Real Decreto 704/2011. Allí son definidos doce sectores estratégicos en donde cada organismo encargado de sector debe identificar los correspondientes ACN. Estos sectores incluyen Administración, Espacio, Industria Nuclear, Industria Química, Instalaciones de Investigación, Agua, Energía, Salud, Tecnologías de la Información y Comunicaciones, Transporte, Alimentación, Sistema Económico y Financiero. A su vez España divide sus ACN como infraestructuras estratégicas y críticas.

- Infraestructura estratégica son las instalaciones, redes, sistemas, equipos físicos y tecnología de la información de los que depende el funcionamiento de los SSPPEE.
- Infraestructura crítica son aquellas instalaciones estratégicas cuya operatividad resulta indispensable y no permite otras alternativas, para el funcionamiento de los SSPPEE (BOE, 2018).

### 2.3.2 – Las agresiones a los ACN y los posibles agresores

Como señala Uzal (2017), "los componentes de la Infraestructura Crítica de un estado nación constituyen blancos potenciales y altamente valorados por diversos tipos de organizaciones ciberterroristas." Las plantas e instalaciones modernas disponen de sistemas de

producción y de control automatizados, resultando fundamental el papel que cumplen los Controladores de Lógica Programable (PLC[10], por su sigla en inglés) y los Sistemas de Supervisión, Control y Adquisición de Datos (SCADA[11], por su sigla en inglés), los cuales a su vez constituyen elementos vulnerables dentro de las infraestructuras críticas.

- Un PLC es una computadora de uso específico, la cual es empleada para el control en los procesos automatizados de naturaleza electromecánica (por ejemplo el control de la maquinaria de una instalación o en líneas de montaje).
- Un SCADA es un software de control de producción, el que intercomunicado con los diferentes componentes de la instalación, permite el control de todo el proceso, brindando información en tiempo real a los operadores.

Ambos interactúan entre sí, permitiendo el SCADA el gerenciamiento integral de una instalación a partir de los datos provenientes de los PLC instalados.

Los ciberataques buscan afectar el funcionamiento normal de los PLC y los SCADA[12]. Mediante la modificación de los programas de los PLC de una instalación se logra distorsionar el funcionamiento de determinados componentes electromecánicos de la misma (por ejemplo calderas, centrifugadoras, transformadores, etc.) sometiéndolos a condiciones de funcionamiento anormales que lleven a su explosión, rotura, incendio o cualquier otra forma de degradación. Esta acción hostil sobre los PLC se complementa con una acción similar sobre los SCADA, de forma que el sistema de información muestre en sus pantallas datos falsos, que oculten el ataque que está teniendo lugar, y en cambio simulen que el funcionamiento de la instalación se está realizando en condiciones operativas normales[13] (Uzal, 2017) (The Economist, 2010).

[10] Programmable Logic Controller.

[11] Supervisory Control and Data Adquisition.

[12] Si bien los ciberataques a los ACN no pueden impedirse, Uzal (2017) señala que es posible mitigar sus efectos a través de la adopción de una serie de medidas como ser *firewalls*, *honey pots*, o Sistemas de Detección de Intrusiones (IDS). El *firewall* es un filtro que controla las comunicaciones que pasan de una red a otra, y que en virtud de su configuración, permite o impide el paso del flujo. Una subred que ha sido aislada por firewalls recibe el nombre de Zona Desmilitarizada (DMZ, por su sigla en inglés) y en ella se ubican los servidores críticos de la instalación. Los *honey pots* son sistemas de información falsos (también llamados "*sistemas señuelos*") que buscan confundir a los agresores acerca de la ubicación de los verdaderos sistemas de información, atrayendo los ciberataques y facilitando su detección y eventual identificación de los perpetradores. Los IDS se ubican en la Intranet del ACN (también llamada Red de Área Local o LAN) con la finalidad de monitorear todo el tráfico en la red, buscando detectar patrones anormales o sospechosos y dar una alerta temprana, logrando reducir el riesgo de ataques.

[13] Un ejemplo típico del desarrollo y los riesgos de un ciberataque sobre ACN lo constituyó el ataque del año 2010 con virus Stuxnet sobre la infraestructura nuclear de Irán. Inicialmente el virus fue introducido por una persona, utilizando un pen drive USB, en una o varias de las computadoras de las instalaciones del programa nuclear iraní. Una vez dentro del sistema, el virus escaneó todas las computadoras con sistema operativo Windows que estaban conectadas a la red en busca de los PLC que controlaban las centrifugadoras. En este caso, el PLC que fue blanco del ataque, era aquel que controlaba la velocidad de las centrifugadoras. Luego de infectar los PLC, el virus permaneció latente e indetectable durante casi un mes, replicándose a sí mismo y permitiendo a los hackers hacerse con el control de las centrifugadoras y obtener información acerca de la operación normal del sistema. Con las centrifugadoras fuera de control, Stuxnet reprodujo los datos de su funcionamiento normal en el SCADA, engañando a los operadores iraníes acerca del funcionamiento real de los sistemas. Así el virus permaneció indetectado durante meses para los operadores de la fábrica, en tanto que las centrifugadoras se autodestruían gradualmente. Stuxnet resultó tan bien diseñado que incluso cuando los operadores de las centrifugadoras se percataron de que las cosas estaban fuera de control, un código les impidió el apagado de las máquinas. Finalmente y luego de varios meses, debido a las tensiones extremas

En la actualidad, los vacíos legales en lo relacionado con el uso del ciberespacio, así como la indefinición respecto de las actividades criminales,

> […] es aprovechado por países o grupos con un gran desarrollo en cuestión de cibercomandos, ciberguerra y ciberespionaje, para que desde el anonimato y a través del ciberespionaje o ciberataques, tomen información sensible de países u organismos antagónicos o causen daño a la infraestructura crítica para obtener o incrementar su poder económico, tecnológico o militar (García et al, 2016, p. 201).

Hoy el ciberespacio es un campo de batalla más[14].

## 2.4 – La defensa de los ACN contra los ciberataques

La defensa informática debe tener como principal objetivo la defensa de los datos, los cuales se hallan en toda la infraestructura crítica pública y privada, debido a los serios trastornos a la seguridad nacional en los diferentes planos que puede generar su afectación (Artiga, 2016). En teoría cada Estado se da sus propios estándares de ciberseguridad, los cuales son determinados por la legislación aplicable a través de directivas, políticas, normas, instrucciones, regulaciones y procedimientos para asegurar la preservación de los datos cumpliendo con los requisitos de confidencialidad, integridad y disponibilidad de la información.[15] Actualmente en el campo de la protección de los ACN, lo difícil es determinar qué defender más que cómo defenderlo, de ahí la necesidad de determinar cuál es la infraestructura crítica que resulta vital para el normal funcionamiento del país.

Los bajos estándares en los procedimientos de ciberseguridad en un entorno complejo de redes y comunicaciones amplio y abierto facilitan que un equipo de hackers competente, trabajando para un Estado u organización, tengan altas probabilidades de éxito, particularmente cuando el blanco son por ejemplo, las redes de energía eléctrica (Saavedra, 2016). El sector energético en general, y particularmente las plantas de generación y las redes de distribución eléctrica, constituyen tal vez el sector más sensible de cualquier sociedad moderna, debido a los efectos en cascada que cualquier disfunción puede llegar a generar. En caso de ocurrencia de un ataque de estas características el mismo supondrá una afectación mayor a la seguridad nacional caracterizada por pérdidas humanas, distorsiones en la vida de las personas por la paralización o degradación de los SSPPEE, problemas de seguridad pública y enormes perjuicios a las actividades económico-financieras y productivas.

---

a que fueron sometidas, cerca de 1.000 centrifugadoras del programa nuclear de Irán se desintegraron. Todavía hoy se desconoce con certeza quién o quiénes fueron responsables de la creación de Stuxnet, pero las pruebas apuntan a grupos de hackers trabajando para Israel y los EEUU. La empresa de seguridad Symantec considera que se habrían utilizado entre 5 y 10 expertos en software, durante un período de aproximadamente 6 meses (Holloway, 2015) (BBC, 2015) (ABC, 2017).

[14] Actualmente cualquier operación militar es precedida y se realiza simultáneamente con actividades de ciberespionaje y una serie de ciberataques a los sistemas de comando, comunicaciones, control e inteligencia y a la infraestructura crítica del enemigo, buscando afectar su capacidad de combatir y la moral de su población.

[15] Confidencialidad para preservar las restricciones establecidas en restricciones de acceso y divulgación de la información, incluyendo medios para la protección de la propiedad y confidencialidad de la información. Integridad para proteger la información contra la modificación y/o destrucción no autorizada y garantizar la autenticidad de la misma. Disponibilidad buscando asegurar el acceso seguro, confiable y a tiempo a la información y al uso de la misma (DoE, 2012).

Todavía no existe conciencia cabal de los riesgos que suponen los diferentes tipos de ciberamenazas a la seguridad nacional. Los cambios en el medio ambiente estratégico y en el campo de las TIC han sido tan grandes y acelerados que los actores públicos y privados no han evaluado sus efectos ni medido sus consecuencias. La defensa contra un ciberataque es una tarea que debe ser desarrollada en forma conjunta por el Gobierno Nacional y el sector privado de la sociedad y las estrategias de ciberseguridad "apuntan tanto a la protección de la sociedad contra las ciberamenazas perjudiciales, como al refuerzo del desarrollo social y económico, a partir de un entorno seguro de tecnologías de la información y comunicaciones" (Parraguez, 2017).

## 2.5 – Caso de la ROU: una breve aproximación

### 2.5.1 – El marco jurídico-legal

En el año 2010 fue aprobada la Ley 18.650, Ley Marco de Defensa Nacional (LMDN) de nuestro país. La misma fue complementada en el año 2014, por el Decreto 105/014, el cual aprobó la Política de Defensa Nacional (PDN). Este último documento define el escenario estratégico actual y el futuro, determina los Intereses Nacionales (IINN), y a partir de éstos incluye los objetivos permanentes y estratégicos de la Defensa Nacional (DN) y los posibles obstáculos a enfrentar en su materialización. Dentro de los obstáculos se menciona el Crimen Organizado y dentro de éste se incluyen:

> […] delitos como el narcotráfico, tráfico ilegal de armas, el lavado de activos, la trata de personas, la corrupción y los ataques cibernéticos, entre otros". Posteriormente se establece como obstáculo para los objetivos de la DN la "materialización del espionaje y los ataques cibernéticos (Poder Ejecutivo, 2014).

También se establece a texto expreso que:

> En la actualidad se da en forma reiterada el espionaje por parte de Empresas, Organismos o estados extra-regionales a los gobiernos de la región, las empresas públicas, así como a empresas privadas u organismos de la sociedad civil con el fin de captar ilícitamente información para obtener ventajas económicas y el control político, militar o social, en el plano estratégico de los países (Poder Ejecutivo, 2014).

Finalmente, en el mismo sentido, este decreto establece como lineamiento estratégico "Proteger al Uruguay de ataques cibernéticos y preservar la reserva de datos producto de la gestión estatal y privada, tanto a nivel nacional como regional, en cuanto esta última corresponda" (Poder Ejecutivo, 2014).

### 2.5.2 – La arquitectura de ciberseguridad de la ROU

La responsabilidad de la conducción de la ciberseguridad en nuestro país recae en la Presidencia de la República, y dentro de ella, específicamente en la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC)[16]. Su brazo operativo lo constituye el

[16] La estructura comprende un Consejo Directivo Honorario, una Dirección Ejecutiva (conformada por el Director Ejecutivo y la Directora Adjunta) del cual dependen cinco Consejos Asesores. Por debajo existen cinco áreas operativas (Seguridad de la Información; Organismos y Procesos; Servicios de Apoyo; Ciudadanía Digital; Tecnología y una Secretaría General (Poder Ejecutivo, 2006). El organismo fue creado en el año 2005 a través de la Ley 17.930 y reglamentado por el Decreto en el año 2006 por el Decreto 205/006 (Camps, 2016) (Poder Legislativo, 2005). Este

Centro de Respuesta de Incidentes de Seguridad Informática del Uruguay (CERTuy), el cual tiene por misión "Proteger los activos de información críticos del Estado y promover el conocimiento en seguridad de la información de manera de prevenir y responder a incidentes de seguridad" (CERTuy, 2018a).[17] Dependiendo del CERTuy se hallan los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT - *Computer Security Incident Response Team*). [18]

En lo que refiere a incidentes informáticos, en el primer semestre de 2017 se atendieron un total de 457, lo que supone un incremento del 9% respecto de igual período del año anterior. El aumento de los incidentes pudo haberse debido a la existencia de nuevos sistemas de detección, y al aumento en la confianza en el CERTuy por parte de los miembros de las comunidades objetivo (CERTuy, 2018b). El siguiente gráfico representa los porcentajes por categorías de los incidentes.

organismo participa en la formulación de políticas en materia información, conocimiento y desarrollo informático, liderando la estrategia de implementación de Gobierno Electrónico como base de un estado eficiente y centrado en el ciudadano, impulsando la sociedad de la información y del conocimiento y el buen uso de las TIC (Poder Legislativo, 2006). AGESIC realiza diversas actividades de capacitación teniendo como brazo operativo en ciberseguridad al Centro de Respuesta de Incidentes de Seguridad Informática del Uruguay (CERTuy - *Computer Emergency Response Team – Uruguay)*

[17] Dentro de las tareas del CERTuy se destacan el prevenir y responder a incidentes de seguridad informática; proponer y asesorar normas y procedimientos de seguridad; brindar alertas informáticos; coordinar los planes de recuperación y realizar los análisis post ataques; fomentar las buenas prácticas y la creación de Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT); interacción con organismos similares de otros Estados (Poder Ejecutivo, 2009a) (Poder Ejecutivo, 2009b) (CERTuy, 2018a). Este centro está conformado por un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Dentro de la comunidad objetivo del CERTuy se encuentran el gobierno, salud, orden público, servicios de emergencia, energía, telecomunicaciones, transporte, suministro de agua potable, ecología y ambiente, agro-industria, banca y servicios financieros, y en general cualquier sector que afecte a más de un 30% de la población (CERTuy, 2018a).

[18] Los CSIRT corresponden a las diferentes comunidades objetivo, y dentro de sus servicios hallamos algunos de naturaleza reactiva (alertas y manejo de incidentes) y otros proactivos (anuncios, detección de incidentes, y desarrollo de técnicas y herramientas); asimismo, brindan capacitación y entrenamiento, análisis de riesgos, consultorías en seguridad y actividades de concientización de la comunidad en temas de seguridad informática (CSIRT-ANTEL, 2018). En función de su misión, en caso de incidentes informáticos, el CERTuy coordina con el CSIRT – ANTEL, el CSIRT del Ministerio de Defensa Nacional (MDN) o con otros equipos de respuesta del sector público o privado (Camps, 2016).

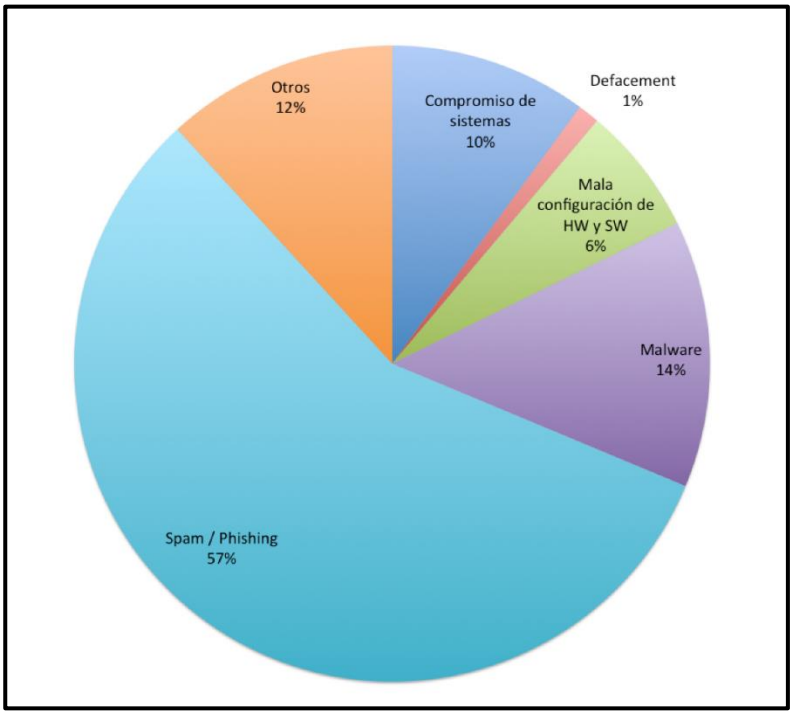


*Figura 1* Discriminación de incidentes informáticos en la ROU durante el primer semestre del año 2017. CERTuy

## 2.5.3 – Planes y estado del arte en ciberseguridad y protección de ACN

La ROU incluyó a la ciberseguridad/ciberdefensa en su PDN aprobada en el año 2014, pero comenzó a desarrollar la estructura organizacional para poder enfrentar incidentes informáticos a partir del año 2008 con la creación del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)[19]. Actualmente no se posee una Estrategia Nacional de Ciberseguridad, pero se está trabajando en ella, existiendo los recursos humanos, los organismos y los marcos legales para poder desarrollarla[20].

[19] El CERTuy fue creado en el año 2008 a través de la Ley 18.362. Dicha ley le asigna las tareas de prevención y respuesta en caso de incidentes informáticos. Con posterioridad, en el año 2009 el Decreto 451/009 reglamenta la citada ley y define las responsabilidades del CERTuy (Camps, 2016).

[20] A los efectos de poder desarrollar el Plan Estratégico de Protección de ACN capaz de integrarse a una Estrategia Nacional de Ciberseguridad, existe una serie de actividades mínimas a ser desarrolladas:

- Creación de un Centro Nacional para la Protección de los ACN.
- Definir los ACN y su grado de importancia crítica desde el punto de vista de la seguridad nacional.
- Realizar un Estudio de Seguridad de cada ACN.
- Designación de un Responsable de Seguridad y Enlace por cada ACN.
- Determinar las amenazas, vulnerabilidades y riesgos de cada ACN.
- Desarrollar planes generales y de contingencia en los diferentes niveles para la actuación antes, durante y después de una crisis. Como mínimo los planes deberían comprender:

Recientemente el Banco Interamericano de Desarrollo (BID) llevó a cabo un estudio sobre el estado de la madurez en seguridad cibernética en América Latina y el Caribe, sobre la base de cinco áreas y cuarenta y nueve indicadores. Las cinco áreas incluyeron: política y estrategia de seguridad cibernética; cultura cibernética y sociedad; educación, formación y competencias en seguridad cibernética; marco jurídico y reglamentario; normas, organizaciones y tecnologías.

Cada uno de los indicadores fue evaluado individualmente para cada país de la región, contando con cinco niveles de madurez: inicial, formativo, establecido, estratégico y dinámico, siendo puntuados de 1 a 5. En este estudio del BID la ROU fue muy bien evaluada en las diferentes áreas, siendo uno de los países pioneros de la región a este respecto, presentando una serie de vulnerabilidades que deberían ser corregidas a la brevedad es especial en lo que respecta a:

- Desarrollo de la correspondiente estrategia nacional, con énfasis en lo que refiere a contenidos y a la estrategia de defensa cibernética.
- En materia legal, en lo que se relaciona con el derecho sustantivo y procesal de ciberdelincuencia, donde existen carencias importantes.
- Adhesión a las normas, poniendo especial atención en lo que refiere a su aplicación por los operadores y a la existencia de un conjunto de normas y prácticas mínimas aceptables.
- Protección de infraestructura crítica, destacándose todo lo relacionado con la identificación, organización, coordinación y gestión de riesgos.
- Gestión de crisis, poniendo acento en la planificación (donde existen vacíos importantes) y evaluación.
- Mejoramiento de las tecnologías de seguridad cibernética.

La ROU debe determinar en primer lugar cuáles son sus ACN necesarios para su seguridad nacional, y en segundo lugar, desarrollar la necesaria planificación estratégica que contemple aquello que debe ser protegido y que acciones deben ser realizadas en caso de ataque. Como señala Camps (2016), si bien la ROU carece de:

> una estrategia de ciberseguridad nacional, ha sido evaluado positivamente en un reciente informe conjunto del Banco Interamericano de Desarrollo y la Organización de Estados Americanos. De igual forma se carece de una organización conjunta a nivel Fuerzas Armadas que tenga como cometido específico repeler ataques cibernéticos que afectan la seguridad nacional o eventualmente realizarlos como respuesta a un ataque anterior (p. 276).

# 3 – Conclusiones

La tecnología informática nos ha dado la posibilidad de resolver un sinfín de tareas cotidianas de una manera práctica y veloz, ocupando cada vez mayores espacios en la vida comunitaria. Esta "*sociedad de la información*" a la par de generar oportunidades, genera

- Plan Estratégico de Protección de ACN.
- Planes Estratégicos Sectoriales.
- Planes de Seguridad del Operador.
- Planes de Protección Específicos a cada ACN.
- Planes de Crisis y de Apoyo Operativo para cada ACN.

riesgos y amenazas, los cuales son directamente proporcionales al grado de dependencia digital de esa sociedad. Es en este entorno donde se llevan a cabo actividades ilícitas de naturaliza diversa por parte de actores estatales, organizaciones e individuos que pueden afectar los ACN, vulnerando nuestra seguridad nacional y generando perjuicios de diferente naturaleza y gravedad a la sociedad. Los conflictos actuales se han caracterizado por el empleo cada vez más frecuente del ciberespacio como un campo de batalla. Es debido a estas ciberamenazas que los Estados deben adecuar su normativa jurídico-legal, sus organizaciones, capacidades y estrategias a los nuevos tiempos marcados por la aceleración de la globalización y un sistema internacional anárquico.

No puede existir seguridad de los ACN si no existe una política pública de ciberseguridad y no podrá existir una política pública de ciberseguridad si no existe una Cultura de Seguridad y Defensa en la sociedad. En la ROU, si bien la responsabilidad política en materia de ciberseguridad recae en los tres poderes del Estado, se destacan especialmente los roles del Ministerio del Interior y Ministerio de Defensa Nacional, tal cual lo establece el Decreto 105/014 que determina la Política de Defensa Nacional de la República, alineado con la LMDN Nro. 18.650.

En lo que refiere específicamente a nuestro país, se desprenden una serie de consideraciones. En primer lugar, la ROU, aún con las carencias constatadas, se encuentra mucho mejor preparada en materia de protección de ACN/IRRC que la mayoría de los países de la región. En segundo lugar, para mantener y consolidar la anterior condición se estima necesario:

- Incrementar la formación de recursos humanos altamente especializados para trabajar en el campo de las TIC.
- Incrementar la formación de los niños y jóvenes en su paso por el Sistema Educativo Nacional (SEN) en el dominio de las habilidades y destrezas informáticas.
- Actualizar y completar la legislación vigente.
- Continuar desarrollando la infraestructura nacional de comunicaciones e informática.
- Potenciar los mecanismos de ciberseguridad de los ACN y de respuesta ante incidentes informáticos.

En tercer lugar, a partir de los recursos humanos, materiales y económicos a disposición de los actores públicos y privados, es necesario proceder a la formulación de políticas, programas y proyectos que permitan diseñar una Estrategia Nacional de Ciberseguridad integral, capaz de prevenir o minimizar las vulnerabilidades señaladas en los obstáculos y amenazas a los OONN definidos por la Política de Defensa Nacional.

Con el tiempo necesario, recursos económicos, contactos personales y adecuada motivación, un adversario decidido siempre será capaz de penetrar cualquier sistema. Si bien hasta el momento los grupos terroristas han utilizado las TIC fundamentalmente para propaganda y comunicaciones, y por incapacidad o por decisión propia no han llevado a cabo ciberataques contra ACN, esta situación podría variar en el corto o mediano plazo en virtud de la óptima ecuación costo-beneficio que supone un ataque de esta naturaleza.

# Referencias

ABC. (2017, 13 de Mayo). The internet of hacked things. Recuperado de http://www.abc.net.au/news/2015-10-07/four-corners-internet-of-hacked-things/7778954

Artiga, R. (2016). El Ciberespacio y la Seguridad Nacional en El Salvador. En J. Rodriguez Pinto (Ed), *Ciberdefesa e Ciberseguranca: Novas Ameacas a Seguranca Nacional*. (P 99-129). Río de Janeiro, Brasil: ESG.

Baltodano, E. (2010). Malware: Software malicioso. En J. Villasuso (Ed). *Ciberseguridad en Costa Rica.* (P 268-274) San Jose, Costa Rica: Universidad de Costa Rica.

BBC. (2015, 11 de Octubre). El virus que tomó el control de mil máquinas y les ordenó autodestruirse. Recuperado de https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

BID (2016). *Ciberseguridad: ¿estamos preparados en América Latina y el Caribe?* Recuperado de https://www.agesic.gub.uy/innovaportal/file/5396/1/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe.pdf

Boletín Oficial del Estado (BOE) de España (2018). *Ley de Protección de Infraestructuras Críticas PIC 8/2011, Real Decreto 704/2011*.

Recuperado de https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

Camps, P. (2016). Ciberdefensa y Ciberseguridad: Nuevas Amenazas a la Seguridad Nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito. En J. Rodriguez Pinto (Ed). *Ciberdefesa e Ciberseguranca: Novas Ameacas a Seguranca Nacional*. (P 265-278). Río de Janeiro, Brasil: ESG.

Carozo, E. (2013). Centro de respuesta de incidentes informáticos. ¿Para qué? *Revista de Seguridad*.

Recuperado de https://revista.seguridad.unam.mx/numero-16/centro-de-respuesta-incidentes-inform%C3%A1ticos-para-qu%C3%A9

Carozo, E., Martínez, C. , Vidal, L. , Betarte, G. , Blanco, A. , Cota, E. , Pérez, J. (2006). *CERTuy: Hacia un CSIRT Nacional*.

Recuperado de https://iie.fing.edu.uy/eventos/telcom2006/trabajos/mvdtelcom-013.pdf

Centro Argentino para las Relaciones Internacionales (CARI). (2013). *Ciberdefensa-Ciberseguridad. Riesgos y amenazas.*

Recuperado de http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

CERTuy (2018a). *Qué es el CERTuy?*

Recuperado de https://www.cert.uy/inicio/institucional/que_es_el_cert/

CERTuy (2018b). *Estadisticas de incidentes en el primer semestre de 2017*.

Recperado de

https://www.cert.uy/inicio/novedades/alertas_y_vulnerabilidades/estadisticas+de+incidentes+en+el+primer+semestre+de+2017

CSIRT-ANTEL (2018). *Servicios del CSIRT de ANTEL*.

Recuperado de http://www.csirt-antel.com.uy/node/4

Department of Defense (DoD) (2015). *The DoD Cyber Strategy*. Washington, USA: Autor.

Department of Defense.(DoD) ( (2016). *JP 1-02 Dictionary of Military and Associated Terms*. Washington, USA: Autor.

Department of Energy (DoE). (2012). *DOE/OE-0003 Electricity Subsector Cybersecurity Risk Management Process*.

Recuperado de https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

Diaz, H (2018). Capítulo 2: Infraestructura crítica vulnerable a la ciberguerra. En Centro de Estudios Estrategicos de la Academia de Guerra de Chile (Ed), *La Ciberguerra. Sus impactos y desafíos*. (P 45-59). Santiago de Chile, Chile: Academia de Guerra.

El Comercio (2018, 19 de Setiembre). ¿Cuál es la diferencia entre un hacker y un cracker?

Recuperado de https://elcomercio.pe/tecnologia/actualidad/diferencia-hacker-cracker-noticia-490674

El Mundo (2013, 20 de Marzo). La OTAN pone en su punto de mira a los 'hacktivistas' como objetivos militares.

Recuperado de http://www.elmundo.es/elmundo/2013/03/20/navegante/1363780082.html

El Observador (2017, 16 de Mayo). Detectan posible vínculo de Corea del Norte con ciberataques masivos. Recuperado de https://www.elobservador.com.uy/detectan-posible-vinculo-corea-del-norte-ciberataques-masivos-n1071692

Europol (2018). *Terrorism Situation and Trend Report*.

Recuperado de https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018

García, J. y Mondragón, J. (2016). La Ciberseguridad y Ciberdefensa en el contexto de México. En J. Rodriguez Pinto (Ed). *Ciberdefesa e Ciberseguranca: Novas Ameacas a Seguranca Nacional*. (P 178-206). Río de Janeiro, Brasil: ESG.

Hirane, C. (2016). Ciberespacio. Bien Publico Mundial en tiempos de globalización: Política pública de ciberseguridaduna necesidad imperiosa y la Ciberdefensa como desafío del Siglo XXI. En J. Rodriguez Pinto (Ed). *Ciberdefesa e Ciberseguranca: Novas Ameacas a Seguranca Nacional*. (P 41-79). Río de Janeiro, Brasil: ESG.Holloway, M. (2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities*.

Recuperado de http://large.stanford.edu/courses/2015/ph241/holloway1/

Homeland Security (2018a). *Critical Infrastructure Sectors*.

Recuperado de https://www.dhs.gov/critical-infrastructure-sectors

Homeland Security. (2018b). *National Infrastructure Protection Plan*.

Recuperado de https://www.dhs.gov/national-infrastructure-protection-plan

IMPO. (2006). *Decreto 205/006 Funcionamiento de la AGESIC*.

Recuperado de https://www.impo.com.uy/bases/decretos/205-2006

Interpol (2016). *Informe Anual de 2016*. Recuperado de https://www.interpol.int/es/Centro-de-prensa/Publicaciones2/Informes-anuales/2016

Joint Chief of Staff (2018). *JP 3-12 Cyberspace Operations*. Washington DC, USA: Autor.

Joyanes, L. (2010). Introducción. Estado del Arte de la Ciberseguridad. En Ministerio de Defensa (Ed). *Cuaderno de Estrategia Nro 149. Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el Ciberespacio*. (P 13-46). Madrid, España: Ministerio de Defensa.

Koble, M. (2018). *La diferencia entre el phishing y spoofing*.

Recuperado de https://techlandia.com/diferencia-phishing-spoofing-info_241711/

Leiva, R (2018). Capítulo 1: Aparece la Ciberguerra. En Centro de Estudios Estrategicos de la Academia de Guerra de Chile (Ed), *La Ciberguerra. Sus impactos y desafíos*. (P 23-44). Santiago de Chile, Chile: Academia de Guerra.

Marowsky, C. (2018). Capítulo 5: Efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica. En Centro de Estudios Estrategicos de la Academia de Guerra de Chile (Ed), *La Ciberguerra. Sus impactos y desafíos*. (P 107-128). Santiago de Chile, Chile: Academia de Guerra.

Martin, G. (2016). *Understanding Terrorism. Challenges, Perspectives, and Issues*. London, United Kingdom: Sage.

Martin, P. (2015). *Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos*.

Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf

McAfee (2018). *Threat Landscape Dashboard*.

Recuperado de https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard.html

Ministerio de Defensa (2010). *Cuaderno de Estrategia Nro 149. Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el Ciberespacio.* Madrid, España: Autor.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*.

Recuperado de https://doi.org/10.6028/NIST.CSWP.04162018

OWASP. (2016). *Ingeniería social: hacking psicológico*.

Recuperado de https://www.owasp.org/images/2/27/02_INGENIER%C3%8DA_SOCIAL.pdf

Parraguez, L. (2017). *The State of Cybersecurity in Mexico: An Overview*.

Recuperado de https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview

Poder Ejecutivo. (2017). *Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN). Nro 106-2017-PCM*.

Recuperado de https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-para-la-identifica-decreto-supremo-n-106-2017-pcm-1585361-1/

Poder Ejecutivo. (2014). *Decreto 105/014. Política de Defensa Nacional*.

Recuperado de https://www.impo.com.uy/bases/decretos/105-2014

Poder Ejecutivo (2009a). *Decreto 451/009 Funcionamiento y organización del CERTuy*. Recuperado de https://www.agesic.gub.uy/innovaportal/v/298/1/agesic/decreto-n%C2%B0-451_009-del-28-de-setiembre-de-2009.html

Poder Ejecutivo (2009b). *Decreto 452/009. Política de Seguridad de la Información*. Recuperado de https://www.agesic.gub.uy/innovaportal/v/299/1/agesic/decreto-n%C2%B0-452_009-de-28-de-setiembre-de-2009.html

Poder Legislativo (2010). *Ley 18.650. Ley Marco de Defensa Nacional*.

Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp6292733.htm

Poder Legislativo (2005) *Ley 17.930. Creación de AGESIC*.

Recuperado de http://agesic.gub.uy/innovaportal/v/700/1/agesic/creacion_de_agesic.html

Saavedra, B (2017). *Big Data. Too big to ignore for Latin America and the Caribbean*. Washington DC, USA: CHDS.

Saavedra, B. (2016). *Critical infrastructure in Latin America: connected, dependent, and vulnerable*. Washington DC, USA: CHDS.

Saavedra, B. (2015). *Cybersecurity in Latin America and the Caribbean: the state of readiness for the defefnse of cyberspace.* Washington DC, USA: CHDS.

Symantec. (2018). *Resumen Ejecutivo. Informe Sobre Amenazas para la Seguridad en Internet.*

Recuperado de https://www.symantec.com/content/dam/symantec/mx/docs/reports/istr-23-executive-summary-mx.pdf

The Economist (2010). War in the Fifth Domain. *Autor*.

Recuperado de https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

The White House. (2018). *Presidential Policy Directive / PPD-21-- Critical Infrastructure Security and Resilience.* Recuperado de https://obamawhitehouse.archives.gov/the-

press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience

The White House (2013). *Executive Order 13636 of February 12, 2013 Improving Critical Infrastructure Cybersecurity.*

Recuperado de https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

Uzal, R. (2017). *Ciberterrorismo: Aportes para la protección de infraestructura crítica*. Recuperado de http://espacioestrategico.blogspot.com/2017/03/ciberterrorismo-aportes-para-la.html

Uzal, R. (2015). *El Problema de la Ciber Atribución: Aportes para una estrategia de Ciber Defensa*.

Recuperado de http://www.cari.org.ar/pdf/boletin61.pdf

Wikipedia. (2018a) *Rootkit.* Recuperado de https://es.wikipedia.org/wiki/Rootkit

Wikipedia. (2018b) *Programa espía*.

Recuperado de https://es.wikipedia.org/wiki/Programa_esp%C3%ADa

Wikipedia. (2018c). *Cookies (informática).*

Recuperado de https://es.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)

Wikipedia. (2018d). *Phising*. Recuperado de https://es.wikipedia.org/wiki/Phishing

Wikipedia (2018e). Suplantación.

Recuperado de https://es.wikipedia.org/wiki/Suplantaci%C3%B3n

Wikipedia. (2018f). *Ataque de denegación de servicios*.

Recuperado de https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio