DIPUTADOS
ARGENTINA

INFORME PARLAMENTARIO

n°01
Octubre 2019

Ciberterrorismo y Ciberseguridad

El ciberterrorismo es una amenaza que se manifiesta cada vez con mayor frecuencia a nivel mundial. Este informe define y describe este fenómeno y las maneras de prevenir, luchar y desalentar sus prácticas a través de la ciberseguridad.

Antecedentes

Hacia fines de 2018 el 51,2% de los habitantes del mundo eran usuarios de Internet[1]. En la región de América Latina Argentina es el país con mayor cantidad de usuarios activos sobre el total de su población (93%)[2]. Las tecnologías de Internet crean infinitas oportunidades, pero a la vez traen aparejados riesgos como el ciberterrorismo y la difusión de radicalizaciones violentas[3, 4, 5]. El terrorismo, a través de acciones delictivas, persigue aterrorizar a la población u obligar a un gobierno o a una organización internacional a realizar un acto o abstenerse de hacerlo[6]. Se denomina ciberterrorismo al desarrollo de esa conducta en el ámbito del ciberespacio, donde se busca afectar el control de las infraestructuras críticas, la seguridad de la información estratégica y los datos personales[7]. Se conoce a este tipo de crímenes como "ciberataque", aunque la expresión se refiere en términos generales a diversos tipos de ataques que podrían no involucrar acciones terroristas (ver "Ciberataques"). Argentina se ubica en segundo lugar en la región en materia de *phishing*[8] (ver caja 1), con 1 de cada 1.448 usuarios implicados.

El G20, en su reunión de 2019 en Osaka[9], Japón, ha hecho un llamamiento a las plataformas digitales a sumarse a la lucha contra el ciberterrorismo y las expresiones de extremismos violentos que conducen al terrorismo en las plataformas digitales (en inglés *'Violent Extremism Conducive to Terrorism'* o VECT)[10]. Así, mediante una declaración conjunta, se insta a las plataformas a no permitir su uso para facilitar el terrorismo y los VECT, y a crear términos y condiciones para detectarlos y prevenirlos[11]. Según el Ministerio de Defensa de la República Argentina, el desafío demanda una rápida adaptación de los sistemas de defensa y el desarrollo de capacidades específicas en este singular ámbito[12].

Este informe se enfoca en los riesgos asociados a la explotación de Internet con fines ilícitos por parte del terrorismo, y explora alternativas para fortalecer la prevención y la lucha contra este flagelo. Asimismo, incluye precisiones sobre la ciberseguridad y la ciberdefensa.

RESUMEN

• Internet, a la que actualmente accede más del 50% de la población mundial, ha revolucionado las comunicaciones y el estilo de vida de la gente a nivel global.

• Sin embargo, también conlleva riesgos, siendo el ciberterrorismo uno de los más notorios.

• Los ciberataques incluyen desde el robo de credenciales al uso de software malicioso para comprometer la operación de un sistema (malware) (ver caja 1)

• El ciberterrorismo permite a los victimarios desarrollar propaganda, financiar sus actividades y adiestrar a terroristas en forma virtual.

• Una manera de luchar contra este grave flagelo es adoptar medidas preventivas y detectivas que contribuyan a aumentar la ciberseguridad, lo que incluye poner en práctica herramientas, políticas y acciones que protejan la infraestructura conectada.

• Los especialistas propician como principales soluciones la promoción de la cooperación internacional y de la cooperación público-privada, así como el desarrollo de legislación específica.

• Sin embargo, esos mismos expertos consideran necesario promover medidas adicionales para desalentar al ciberterrorismo.

Ciberseguridad y Ciberdefensa

Existen distintas acepciones del término "ciberseguridad". La Secretaría de Modernización de Argentina (SM), basada en la norma ISO/IEC 27032:2012, la define como la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio13. El Libro Blanco del Ministerio de Defensa, como el conjunto de herramientas, políticas y acciones posibles que se utiliza para proteger la disponibilidad, integridad y confidencialidad de los activos de información de los gobiernos en el ciberespacio. Entre estos activos, se cuentan los dispositivos informáticos conectados, el personal y la infraestructura, los servicios y sistemas de telecomunicaciones, así como las aplicaciones y datos14. Este informe utiliza la definición de la SM.

La "ciberdefensa", por su parte, se entiende como la capacidad estatal de protección y utilización soberana de las cuotas de ciberespacio esenciales, vitales o necesarias para el funcionamiento del instrumento militar, los componentes del sistema de defensa y las infraestructuras críticas con las que cuenta cada Estado15.

Los ciudadanos tienen derecho al debido proceso y la custodia de los derechos fundamentales plasmados en la Constitución Nacional, lo que al mismo tiempo supone la obligación del Estado de velar por su seguridad en todo sentido, incluyendo la protección de las infraestructuras críticas y de los servicios públicos, la custodia apropiada de los datos, y los recaudos fundamentales para que no se vulneren los derechos de la ciudadanía16. Son "infraestructuras críticas" aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad como la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado17. Las "infraestructuras críticas de información", por su parte, son aquellas tecnologías de la información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las "infraestructuras críticas"18.

Los conceptos de ciberseguridad y ciberdefensa son complementarios entre sí. La ciberdefensa comprende un subconjunto operativo dentro de las capacidades de ciberseguridad. Analógicamente la Defensa es una parte operativa de la Seguridad Nacional.

Ciberataques

Definición de ciberataque.

La Secretaría de Modernización define al ciberataque como la acción que se produce en el ciberespacio arriesgando la disponibilidad, integridad y confidencialidad de la información al comprometer los sistemas de información, las telecomunicaciones o las infraestructuras que los soportan[19]. La Organización de las Naciones Unidas (ONU), en una definición más amplia, lo explica como la explotación deliberada de redes informáticas como medio para lanzar un ataque[20].

Los ciberataques pueden o no ser incidentes causados por terroristas, al igual que estar asociados o no al ciber-lavado de activos[21, 22] al ciberdelito o cibercrimen, al ciber-espionaje o al *hacktivismo* (activismo político realizado por movimientos políticos desde sitios web[23, 24]).

Los diferentes tipos de ciberataques (ver caja 1) pueden ocurrir en diferentes ciber-locaciones, tanto en la Internet superficial como en la Internet profunda (ver caja 2)[25].

Los ciberataques son perpetrados por los propios ciberdelincuentes o utilizando las facilidades del ciberespacio a través de redes de computadoras zombis llamadas *"botnets"*, comprometidas para satisfacer las necesidades del hacker sin el conocimiento de los usuarios y con el fin de lograr un objetivo colectivo[26].

Caja 1. ***Diferentes tipos de ciberataques.***

Los tipos de ataques definidos por el Glosario de Términos en Ciberseguridad de Argentina27 incluyen:

Malware: código malicioso/dañino. Es un software que compromete la operación de un sistema al realizar una función o proceso no autorizado, diseñado específicamente para dañar o interrumpir un sistema sin conocimiento ni consentimiento del propietario.

Phishing: método o técnica de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño, suplantando la identidad digital de la víctima.

Troyano: tipo de malware o software malicioso que se presenta al usuario como aparentemente legítimo, basado en un correo electrónico o navegador sin capacidad de autorreplicación. Se utiliza usualmente para robar datos y reclutar botnets.

Gusano (worm): tipo de malware que tiene la propiedad de duplicarse a sí mismo, propagándose e infectando a otros ordenadores, pero a diferencia de un virus, sin la ayuda de una persona.

Root-kit: tipo de malware instalado en una computadora que le da acceso privilegiado a un atacante como si fuera el administrador del equipo. Permite ocultar actividades ilegítimas en un sistema.

Denegación de servicio distribuida (DDoS): ataque que se realiza utilizando múltiples puntos de ataque simultáneamente, enviando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino. Las instalaciones de la red se sobrecargan hasta el punto de rechazar conexiones legítimas.

Caja 2. ***Diferencias entre "Internet superficial" e "Internet profunda".***

Los especialistas subdividen a la Internet en dos basándose en la accesibilidad y el propósito.

Internet superficial: es lo que el público en general entiende por Internet y es usada para navegar online, acceder a redes sociales y compras virtuales. Este tipo de contenido es todo lo que está indexado por motores de búsqueda típicos como Google, Bing o Yahoo, rastreable a través de las direcciones IP (Protocolo de Internet) representadas por un nombre amigable para el usuario[28]. En su conjunto representa el 10% de la totalidad de Internet.

Internet profunda: es un conjunto no visible de contenidos no indexables, difíciles de acceder desde motores de búsqueda convencionales. Se estima que el tamaño de la Internet profunda comprende alrededor del 90% del volumen de la totalidad de Internet[29]. Puede ser un lugar de refugio para mantener la privacidad en línea o para acceder al mercado negro, donde se realizan transacciones ilegales. En los últimos años ha aumentado la presencia de los Estados en la Internet profunda con el fin de erradicar las redes de crimen organizado, pedofilia, tráfico de armas y organizaciones extremistas.

La Internet profunda se encuentra subdividida en dos categorías:

'***Deep web***', también conocida como "Web Invisible" u "Oculta", que engloba a toda la información que está online a la que no se puede acceder de forma pública. Constituye una web de acceso restringido intencional, a la que se accede por contraseñas o páginas dinámicas que se generan al consultar bases de datos.

'***Dark web***', conforma una ínfima parte de la Internet profunda a la que sólo se accede con softwares especiales. Así como la *Deep Web* supone en torno al 90% del contenido de la *World Wide Web*, la *Dark Web* ocuparía únicamente el 0,1% de esta última[30]. Es la parte de Internet más conocida por actividades ilícitas y por el anonimato, garantizado a través de softwares especiales como el buscador Tor[31].

Razones por las cuales hay ciberataques.

Los ciberataques se han convertido en un potente instrumento de agresión contra particulares, actores gubernamentales y entidades privadas[32]. Tienen bajo costo y mínimo riesgo para el ciberdelincuente. Además, su empleo puede resultar muy fácil, así como su efectividad y accesibilidad. Estos factores explican la extensión del fenómeno[33]. Los ciberataques proceden de grupos terroristas, redes de crimen organizado, empresas, Estados o individuos aislados.

Modos de usar internet para promover actos de terrorismo.

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) ha adoptado un enfoque funcional para clasificar a los medios que comúnmente se utilizan en Internet para promover actos de terrorismo[34]. Distingue seis categorías, que suelen superponerse:

1.- Propaganda. Diversos estudios indican que la propaganda constituye uno de los principales fines del uso de Internet por parte de terroristas y grupos VECT. A través de comunicaciones de audio y video en todo tipo de plataformas digitales no solo se promueven actividades terroristas, sino, además, se imparten instrucciones ideológicas o prácticas y se justifican los hechos cometidos[35, 36]. En 2010 existían alrededor de 10.000 sitios web dedicados a la difusión de material violento y terrorista [37]. Progresivamente, Internet aumenta en forma exponencial el número de personas que puede verse afectado[38]. Los contenidos pueden distribuirse mediante sitios web especiales, salas virtuales de charla y foros, revistas en línea, plataformas de redes sociales como Twitter y Facebook, o sitios web populares de videos como YouTube[39, 40]. Diferenciar entre actividad prohibida como la propaganda terrorista y la promoción legitima de un punto de vista constituye un desafío. Entre los objetivos de la propaganda terrorista encontramos el reclutamiento[41], la radicalización y la incitación al terrorismo (Ver caja 3).

2.- Financiación. Las organizaciones criminales tradicionales se han mudado al ciberespacio dada la rentabilidad que supone Internet. Se estima que obtienen 800 % más de ganancias con la piratería en el ciberespacio que con el tráfico de drogas.[42] El uso de las facilidades de Internet ya mencionadas ha intensificado el financiamiento del terrorismo. Algunos expertos sostienen que el ciber financiamiento del terrorismo y el ciber lavado transnacional de activos, desde el punto de vista tecnológico-instrumental, son delitos "parientes cercanos"[43]. Según el Grupo de Acción Financiera Internacional (GAFI) las tecnologías modernas, particularmente las redes sociales, se utilizan no sólo para llegar a simpatizantes sino también para atraer donantes[44].

3.- Adiestramiento. Los extremismos violentos y los grupos terroristas utilizan las plataformas digitales como campamento alternativo de adiestramiento de terroristas[45]. Así los terroristas aprenden a fabricar bombas[46] u otras armas de fuego, a planificar y ejecutar ataques, incluyendo a los ciberataques. Además, comparten técnicas o conocimientos operacionales específicos para perpetrar actos terroristas[47].

4.- Planificación. Las plataformas digitales sirven a los terroristas para comunicar la planificación de ataques o ciberataques sin importar las distancias que los separen[48], traspasando fronteras.

5.- Ejecución. Las plataformas digitales ofrecen a los terroristas una herramienta propicia para facilitar la perpetración de sus actos, ya que pueden, a modo enunciativo, ofrecer ventajas logísticas, reducir las probabilidades de detección, y encubrir la identidad de los responsables. Según los expertos, el motivo por el cual Internet brinda una ventaja tan clara es porque no hay forma de atribuir un ataque, y en consecuencia los ciberterroristas gozan de anonimato[49].

6.- Ciberataques. Incluyen desde interferir en el funcionamiento del sistema financiero y de los bancos al *phishing,* la propagación de virus informáticos como *malware, trojans, worms, root-kit, DDoS* (ver caja 1), amenazas avanzadas, comprometer la información, entre otros[50]. Un típico ejemplo es el *malware* "Gauss", que en 2012 infectó a 2.500 sistemas en todo el mundo[51]. Otro la sustracción de 10 millones de dólares al Banco de Chile mediante un ataque informático[52].

Caja 3. ***Modalidades de manifestaciones Terroristas en Internet.***

1.- Reclutamiento. La propaganda terrorista distribuida a través de sitios web protegidos por contraseña, y los foros y las salas de charla de Internet de acceso restringido sirven como medios de reclutamiento clandestino. Estas metodologías hacen que sea cada vez más difícil para los gobiernos y los grupos de inteligencia hacerles seguimiento y entender quién entra y sale de las organizaciones terroristas[53].

2.- Incitación. La ciber propaganda sirve para incitar a cometer actos de terrorismo o para glorificarlos. Es una estrategia que utilizan comúnmente los terroristas para aumentar el apoyo a su causa y llamar a la acción violenta[54]. La prevención y disuasión de la incitación al terrorismo a fin de proteger la seguridad nacional y el orden público son razones legítimas para restringir el derecho a la libertad de expresión[55].

3.- Radicalización. Es el proceso de adoctrinamiento que suele acompañar a la transformación de los reclutas en personas decididas a actuar con violencia, inspiradas por ideologías extremistas. A menudo implica el uso de propaganda, comúnmente difundida a través de Internet[56].

Marco Legal

Los expertos acuerdan que la lucha contra el ciberterrorismo es compleja dado que representa una tarea que atraviesa a los gobiernos y, dentro de cada país, a diferentes reparticiones, como es el caso de la Argentina (Ver caja 4). La legislación y las responsabilidades se encuentran presentes tanto a nivel nacional como internacional.

Tratados internacionales.

La cooperación internacional es un componente fundamental de cualquier estrategia de ciberseguridad[57]. De acuerdo con las recomendaciones de Naciones Unidas a través de su Centro contra el Terrorismo[58], la cooperación entre Estados es un terreno en el que debe armonizarse la protección de la soberanía, los derechos de los ciudadanos y el patrimonio nacional con el intercambio necesario de información y recursos para prevenir y combatir posibles actos de terrorismo y VECT[59].

Argentina forma parte de diversos instrumentos internacionales que se vinculan con estas cuestiones. Hay acuerdos multilaterales generales sobre la lucha contra el terrorismo que contienen disposiciones específicas sobre control de amenazas en el ciberespacio tales como:

• la *"Estrategia Interamericana Integral de Seguridad Cibernética"* de la Organización de Estados Americanos (OEA)[60];

• la *"Agenda sobre Ciberseguridad Global"* lanzada en 2007 por la Unión Internacional de Telecomunicaciones (UIT)[61];

• el Convenio de Budapest sobre Ciberdelito[62]; y

• otros instrumentos firmados[63] en el marco de la ONU[64] y la OEA[65] en materia de seguridad internacional y lucha contra el terrorismo que pueden tener aspectos aplicables en este terreno.

También resultan relevantes los acuerdos bilaterales firmados por Argentina en materia de ciberseguridad con otras naciones como, por ejemplo, con Chile[66], Israel[67], los Estados Unidos de América[68] y el Reino Unido[69].

Legislación específica de Argentina.

La Constitución dispone el compromiso irrenunciable del Estado con la defensa y la seguridad. Las leyes que integran el marco normativo son las relativas a la Defensa Nacional70, Seguridad Interior71 y a la de Inteligencia y sus modificatorias72.

Los esfuerzos para enfrentar estas nuevas amenazas de manera coordinada entre los distintos organismos del Estado y con participación de diferentes actores de la sociedad civil se vieron cristalizados en el dictado de leyes más sofisticadas, ya que, con la expansión global del uso de Internet, ha crecido la preocupación de los Estados por mitigar los efectos de las conductas ilícitas relacionados con los ciberdelitos.

Ante el constante incremento de delitos informáticos se promueve en Argentina la construcción de un marco jurídico para las TIC que incluya reformas al Código Penal73 y a la ley sobre protección de datos personales74. Sin embargo, a la fecha de este informe un proyecto de ley enviado al Congreso por el Poder Ejecutivo Nacional en 2018 aún no había sido tratado.

En 2019 se aprobó la Estrategia Nacional de Ciberseguridad que recoge entre sus principios rectores y objetivos estratégicos la integración y la cooperación internacional75.

Caja 4. ***Responsabilidad en Ciberseguridad y Ciberdefensa en Argentina.***

La Dirección Nacional de Ciberseguridad dependiente de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros tiene como responsabilidad primaria entender en todos los aspectos relativos a la ciberseguridad y protección de las infraestructuras críticas de información, comprendiendo la generación de capacidades de detección, defensa, respuestas y recupero ante incidentes del Sector Público Nacional[76]. Cuenta a esos efectos con una Dirección de Infraestructuras Críticas de Información[77].

El Ministerio de Defensa cuenta entre su estructura con la Subsecretaría de Ciberdefensa[78].

El Ministerio de Seguridad cuenta con un Comité de Respuesta de Incidentes de Seguridad Informática[79].

Por decreto del PEN Nº 577/17 se creó un Comité de Ciberseguridad integrado por los Ministerios de Defensa, Seguridad y el entonces Ministerio de Modernización (actual Secretaría), asignándoles la responsabilidad de elaborar la "Estrategia Nacional de Ciberseguridad"[80]. Con posterioridad el comité se amplió mediante la incorporación de los ministerios de Justicia y Derechos Humanos, Relaciones Exteriores y Culto y la Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete[81].

Fortalecimiento de la ciberseguridad y ciberdefensa

Los expertos sugieren varias formas de fortalecer la ciberseguridad y la ciberdefensa en Argentina:

- Mapeo de la infraestructura crítica. Algunos coinciden en que es fundamental conocer aquello que se quiere proteger[82], dado que la definición de la infraestructura crítica puede asegurar el éxito de la estrategia en ciberseguridad. Diferentes países han tenido éxito con sus programas de mapeo de infraestructura (caja 5). Esos mismos expertos proponen adoptar como ejemplo a seguir las acciones tomadas por esos países[83] para profundizar el mapeo que ya existe en Argentina.

- Cooperación Internacional. Hay consenso entre los expertos en considerar a la cooperación, tanto internacional como dentro de las instituciones y organismos de gobierno, fundamental y esencial en la lucha contra el terrorismo[84, 85, 86]. Los desafíos planteados, coinciden, requieren de esfuerzos diplomáticos mancomunados, dado que ninguna nación por sí sola puede asegurar adecuadamente sus redes[87], ya que el ciberespacio trasciende fronteras económicas, sociales y geográficas[88]. Un grupo de expertos sugiere que se deberían multiplicar las acciones cooperativas contra las ciber-amenazas[89] reforzando la participación de Argentina en forma más activa en los foros a los que pertenece y en los equipos de trabajo a los que recientemente se ha incorporado, como los grupos especializados de Naciones Unidas que trabajan en esta temática[90, 91, 92].

- Cooperación Público-Privada. El ciberterrorismo atraviesa no solo el ámbito público sino también al sector privado. Por ende, tal como manifiestan los expertos, la cooperación para combatirlo debería ser un esfuerzo colectivo. Estos sugieren que la cooperación público-privada sigue siendo una de las mejores herramientas para acelerar la respuesta frente a ciberataques, así como para lograr un mayor flujo de denuncias e intercambio de información, y mayor confianza por parte del público hacia ambos sectores[93,94,95]. Los expertos reconocen también la necesidad de trabajar en cooperación con el sector privado para obtener mejores leyes e innovación tecnológica, así como para el intercambio de información y datos para fortalecer la lucha contra el ciberterrorismo.

- Desarrollo de la legislación. Diversas áreas dentro del Estado Argentino tienen asignadas responsabilidades sobre la estrategia de ciberseguridad nacional (ver caja 4). Si bien ya existe cierta legislación sobre la materia, los expertos sugieren que debería desarrollarse nueva legislación en las áreas de la educación digital, la colaboración de los privados respecto del control de sus infraestructuras cuando estas sean críticas, los estándares mínimos que debe cumplir todo producto capaz de afectar infraestructuras críticas, y la responsabilidad de los proveedores de Internet (ISP por sus siglas en inglés) 96. En diferentes países, ya existe legislación en la temática (ver caja 5). Algunos expertos proponen tomar los ejemplos de esos países 97, como el caso de Singapur, sugiriendo que se instaure la obligación de todo ISP de entregar la información que un juez solicite sin importar donde se encuentre alojada.

- Desarrollo de capacitaciones. Durante 2019, 150 empleados de 17 gobiernos provinciales participaron de una capacitación virtual sobre ciberseguridad dictada a través de la plataforma del Instituto Nacional de la Administración Pública (INAP), cuyos materiales fueron aportados por la Dirección Nacional de Ciberseguridad 98. Por otra parte, 339 empleados municipales terminaron el módulo de ciberseguridad de una capacitación creada a partir de material elaborado por esa repartición pública 99. Los expertos entienden que estas capacitaciones deben extenderse y profundizarse dentro de un plan integral de capacitación estratégico para todos los empleados de la Administración Pública 100, a fin de capacitarlos sobre los diferentes tipos de ciberataques mencionados (ver más arriba, Caja 4). Asimismo, existen carreras de posgrado y otros programas que abarcan la materia, como la maestría que ofrece la Universidad de Buenos Aires (UBA).

- Campañas de concientización. Los expertos consideran que deberían realizarse mayores esfuerzos en materia de educación. En 16 países, más de mil millones de adultos han sido víctimas de algún tipo de ciberdelito, 800 millones solo en 2018 101. Casi 2 de cada 3 personas (64%) creen que es probable que se conviertan en víctimas de cibercrimen durante el corriente año. De los que fueron víctimas de cibercrimen en el último año, el 38% sufrió una pérdida financiera y pasó 6 horas en promedio resolviendo el crimen 102. Por ello, los expertos sugieren diseñar campañas de concientización dirigidas a la ciudadanía y a las empresas, orientadas a la prevención del cibercrimen, así como a detectar las distintas manifestaciones del terrorismo y los extremismos violentos en plataformas digitales 103, 104, 105.

- Estrategia de desaliento del ciberterrorismo. Algunos expertos indican que los gobiernos deberían calificar a los terroristas como extremistas adoptando esta estrategia para limitar su atractivo y aumentar así el "efecto de desgaste" de la violencia terrorista, es decir, el rechazo que ésta genera en los ciudadanos106. Asimismo, expertos sugieren que los gobiernos deberían comprender qué comportamientos, de los descriptos, realmente son útiles para los perpetradores, concentrando sus esfuerzos en la frustración de estos últimos 107.

Preocupaciones.

Algunas organizaciones de la Sociedad Civil cuya misión es la defensa de los derechos fundamentales de los ciudadanos en el entorno digital han expresado preocupación acerca de la violación de esos derechos y la conceptualización, uso y alcances del término "ciberterrorismo" en el país. Esas mismas organizaciones y algunos expertos se han expresado además sumamente críticos sobre el rol actual del Estado argentino en la materia 108.

Caja 5. ***Ejemplos de países más avanzados en ciberseguridad.***

Existe un ranking en Ciberseguridad Global que lleva adelante la Unión Internacional de Telecomunicaciones dentro del cual, para 2018, la Argentina se ubica en el puesto 94 de un total de 175 a nivel mundial y en el 11 a nivel regional109. Varios expertos han señalado el éxito de las iniciativas de algunos países, lo que incluye:

Reino Unido: En el 1º lugar del ranking del Índice de Ciberseguridad Global (GCI). El Reino Unido creó en 2009 una Oficina en Ciberseguridad y un Centro de Operaciones en Ciberseguridad (CSOC). En 2011 estableció el Programa Nacional en Ciberseguridad y en 2016 lanzó el Centro de Ciberseguridad Nacional, que proporciona un único punto de contacto para Pequeñas y Medianas Empresas (PYMEs), empresas, organismos gubernamentales, y público en general, trabajando en colaboración con fuerzas de inteligencia de todo el país. Estos esfuerzos llevaron al Reino Unido a prevenir miles de ataques y a reducir el tiempo promedio que un sitio de phishing está online, de 27 horas a una hora 110.

Singapur: En el 6º lugar del ranking. En lugar de crear organismos, Singapur desarrolló legislación como la "Ley de Ciberseguridad", que establece un marco legal para la supervisión y el mantenimiento de la ciberseguridad nacional, fortaleciendo la protección de la Infraestructura de Información Crítica contra los ciberataques, autorizando a la Agencia de Ciberseguridad a prevenir y responder amenazas, estableciendo un marco para compartir información de seguridad cibernética y para los ISP 111.

España: En el 7º lugar del ranking, España creó dentro del Ministerio del Interior, el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), órgano que impulsa y coordina todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad. Asimismo, el Instituto Nacional de Ciberseguridad de España (INCIBE) se consolida como entidad de referencia para el desarrollo de la ciberseguridad. En 2019, España fue el primer país de la Unión Europea en elaborar una Guía Nacional de Notificación y Gestión de ciber incidentes 112.

Además de iniciativas nacionales, existen iniciativas desarrolladas por uniones regionales. Por ejemplo, la Unión Europea ha avanzado con el lanzamiento del Reglamento General de Protección de Datos (RGPD)113, norma que establece la protección de datos y privacidad para todos los ciudadanos de la Unión. También, recientemente, creó el Reglamento Europeo de Ciberseguridad 114, que establece los objetivos, tareas y aspectos organizacionales de la Agencia Europea en materia de Ciberseguridad, así como da soporte al marco para la creación de esquemas europeos de certificación de la ciberseguridad.

NOTAS AL FINAL

1 International Telecommunication Union (ITU) Global Cybersecurity Index 2018, ISBN 978-92-61-28201-1 (Electronic version)

2 Statista (2019) Active internet users as percentage of the total population in selected countries in Latin America as of January 2019

3 Gerstenfeld, P; Grant, D.; Chiang, C. (2003) Hate Online: A Content Analysis of Extremist Internet Sites https://doi.org/10.1111/j.1530-2415.2003.00013.x

4 Ashour, O (2010). "Online De-Radicalization? Countering Violent Extremist Narratives: Message, Messenger and Media Strategy." Perspectives on Terrorism, vol. 4, no. 6, 2010, pp. 15–19. JSTOR www.jstor.org/stable/26298491.

5 Conway, M (2012) From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a New Form of Violent Radical Dublin City University

6 Ley 26.268, Modificación del Código Penal.

7 Libro Blanco de la Defensa 2015, p. 25.

8 Symantec (2019) 2019 Internet Security Threat Report.

9 G20 (2019) G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT) Osaka, Japan, June 29, 2019.

10 ONU (2006) Resolución 60/288, 2006 de la Asamblea General de las Naciones Unidas

11 G20 (2019) G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT) Osaka, Japan, June 29, 2019.

12 Libro Blanco de la Defensa 2015, p. 25

13 Secretaría de Gobierno de Modernización, de la Jefatura de Gabinete de Ministros de la República Argentina (2019) Glosario de Términos de Ciberseguridad, Anexo II a la Resolución 1523/2019

14 Libro Blanco de la Defensa 2015, p. 25

15 Libro Blanco de la Defensa 2015.

16 Fundación Vía Libre, comunicación directa: https://www.vialibre.org.ar/

17 Secretaría de Gobierno de Modernización, de la Jefatura de Gabinete de Ministros de la República Argentina (2019) Glosario de Términos de Ciberseguridad, Anexo II a la Resolución 1523/2019

18 Secretaría de Gobierno de Modernización, de la Jefatura de Gabinete de Ministros de la República Argentina (2019) Glosario de Términos de Ciberseguridad, Anexo II a la Resolución 1523/2019

19 Secretaría de Gobierno de Modernización, de la Jefatura de Gabinete de Ministros de la República Argentina (2019) Glosario de Términos de Ciberseguridad, Anexo II a la Resolución 1523/2019

20 Oficina de las Naciones Unidas contra la Droga y el Delito (2013) El uso de internet con fines terroristas. Sección de Servicios en Inglés, Publicaciones y Biblioteca, Oficina de las Naciones Unidas en Viena.

21 Uzal, R. (2017) "Paradigmas y cambios para un efectivo combate al ciberdelito". Iniciativa del Parlamento, Cámara de Diputados de Argentina.

22 Uzal, R., Dr., Riesco, D., Montejano, G., Agüero, W. y Baieli, C. (2015). Presentación en el SIE 2015, 9º Simposio de Informática en el Estado. Lavado Transnacional de Activos en el Ciberespacio. Presentación del contexto, planteo del problema y formulación de propuestas.

23 Lechón Gómez, D. & Mena Farrera, R. (2019) El Hacktivismo e Internet como Territorio en Disputa. Estudios Políticos, Universidad Nacional Autónoma de México.

24 Avogadro, M. (2011). Hacktivism: entramado invisible del Ciberpoder. Revista Razón y Palabra, número 77, año 16, México, Instituto Tecnológico y de Estudios Superiores de Monterrey del Estado de México.

25 Decreto 703/2018 Anexo I.

26 Ministerio de Defensa de España (2011) Cuaderno de Estrategia 149: Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. ISBN: 978-84-9781-622-9

27 Secretaría de Gobierno de Modernización, de la Jefatura de Gabinete de Ministros de la República Argentina (2019) Glosario de Términos de Ciberseguridad, Anexo II a la Resolución 1523/2019

28 Bright planet (2014) Clearing Up Confusion – Deep Web vs. Dark Web

29 Stupples, D. (2013) ICITST-2013: Keynote speaker 2: Security challenge of TOR and the deep web. 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), London, 2013

30 Xataca (2019) Deep Web, Dark Web y Darknet: éstas son las diferencias

31 Bright planet (2014) Clearing Up Confusion – Deep Web vs. Dark Web

32 Amich Elias, C. y Velázquez Ortiz, P (2014) La ciberdefensa y sus dimensiones global y específica en la estrategia de seguridad nacional española.

33 S. Nye, J. Jr. (2010) Cyber Power. Belfer Center for Science and International Affairs. Harvard Kennedy School

34 Oficina de las Naciones Unidas contra la Droga y el Delito en colaboración con el Equipo Especial Sobre La Ejecución De La Lucha Contra El Terrorismo (2013) El uso de Internet con fines terroristas. Austria, Naciones Unidas.

35 Sanchez Medero, G (2010) La nueva estrategia comunicativa de los grupos terroristas. Universidad Complutense de Madrid.

36 Oficina de las Naciones Unidas contra la Droga y el Delito en colaboración con el Equipo Especial Sobre La Ejecución De La Lucha Contra El Terrorismo (2013) El uso de Internet con fines terroristas. Austria, Naciones Unidas.

37 Sanchez Medero, G. (2015) El Ciberterrorismo: de la web 2.0 al internet profundo. Revista Abaco, V 3 N. 85. ISSN: 0213-6252

38 Denning D (2001) Chapter 8 Networks and Netwars: The Future of Terror, Crime, and Militancy: Activism, Hacktivism and Cyberterrorism. National Defense Research Institute

39 Sanchez Medero, G. (2015) El Ciberterrorismo: de la web 2.0 al internet profundo. Revista Abaco, V 3 N. 85. ISSN: 0213-6252

40 Oficina de las Naciones Unidas contra la Droga y el Delito en colaboración con el Equipo Especial Sobre La Ejecución De La Lucha Contra El Terrorismo (2013) El uso de Internet con fines terroristas. Austria, Naciones Unidas.

41 Gerwehr, S. y Daly, S (2006) Al-Qaida: terrorist selection and recruitment. The McGraw-Hill Homeland Security Handbook, David Kamien, ed. (Nueva York, McGraw-Hill)

42 McClarkin E (2012) Thematic Paper on Organised Crime: Cybercrime - New Investigation Strategies and New Technologies. Special Committee on Organised Crime, Corruption and Money Laundering (CRIM) 2012-2013

43 Uzal, R. y otros (2015) Lavado transnacional de activos en el ciberespacio Presentación del contexto, planteo del problema y formulación de propuestas http://sedici.unlp.edu.ar/handle/10915/56183

44 GAFI (2018) Financiamiento del Reclutamiento con Propósitos Terroristas. GAFI, París.

45 Morán Blanco, S. (2017) La Ciberseguridad y el Uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. Revista Española de Derecho Internacional. ISSN: 0034-9380.

46 Weimann, G (sin año) Terrorismo e Internet. Ética Net, Número 3. Granada, España.

47 Asamblea General ONU (2006) Estrategia Global de las Naciones Unidas contra el Terrorismo. Oficina de Lucha Contra el Terrorismo, Equipo Especial.

48 Oficina de las Naciones Unidas contra la Droga y el Delito (2013). El uso de internet con fines terroristas. ONU.

49 Weimann, G. (2006) Terror on the Internet: The New Arena, the New Challenges.

50 POSTNote 389 (2011) Cyber Security in the UK. House of Parliament, Reino Unido.

51 Morelli, A. (sin fecha) Apuntes para una charla sobre la administración del conflicto internacional en el ciberespacio. Consejo Argentino para las Relaciones Internacionales (CARI)

52 El Publimetro (2018) https://www.publimetro.cl/cl/noticias/2018/06/09/banco-chile-sufrio-robo-10-millones-dolares-tras-ataque-informatico.html

53 Gerwehr, S. y Dal, S., (2006) "Al-Qaida: terrorist selection and recruitment", The McGraw-Hill Homeland Security Handbook, David Kamien, ed. (Nueva York, McGraw-Hill, 2006), pág. 83

54 Oficina del alto comisionado de las Naciones Unidas para los Derechos Humanos (2008) Los derechos humanos el terrorismo y la lucha contra el terrorismo. Ginebra. Suiza.

55 Pacto Internacional de Derechos Civiles y Políticos, Artículo 19, párrafo 3.

56 Jalloul Muro, H. (2018) Realidad, Ideología y Terminología: entre la Radicalización, la Violencia Política y el Terrorismo Yihadista. Revista de Estudios en Seguridad Internacional.

57 Carlini, A. (2016) Ciberseguridad, un nuevo desafío para la comunidad internacional

58 Centro de la ONU contra el Terrorismo (2019) Temas y Prioridades

59 Oficina de Lucha contra el Terrorismo, Naciones Unidas (2006) Estrategia Global De Las Naciones Unidas Contra El Terrorismo

60 OEA (2004) Resolución AG/RES 2004 (XXXIV-O/04)

61 Unión Internacional de Telecomunicaciones (sin fecha) La Agenda sobre Ciberseguridad Global.

62 Aprobación del Convenio sobre Ciberdelito. Ley 27.411 de la República Argentina

63 Tratados y otros instrumentos internacionales de la Argentina

64 Naciones Unidas, Oficina de Lucha contra el Terrorismo (sin fecha) Instrumentos Jurídicos Internacionales

65 OEA (2003) Convención Interamericana contra el Terrorismo

66 Memorándum de Entendimiento sobre Cooperación en Materia de Ciberseguridad, Ciberdelito y Ciberdefensa suscripto con Chile en 2018

67 Acuerdo con Israel sobre Cooperación en Asuntos de Seguridad Pública e Interior de 2017

68 Acuerdo entre el Ministerio de Seguridad de la República Argentina y el Departamento de Justicia y el Departamento de Seguridad Nacional de los Estados Unidos de América sobre Incremento de la Cooperación para Prevenir y Combatir el Crimen Grave (art. 11 "Entrega de datos personales y otra información para prevenir crímenes graves y de terrorismo")

69 Memorando de Entendimiento entre el Ministerio de Seguridad de la República Argentina y el Ministerio del Interior del Reino Unido de Gran Bretaña e Irlanda del Norte de 2018

70 Ley 23.554 de Defensa Nacional

71 Ley 24.059 de Seguridad Interior

72 Ley 25.520 de Inteligencia Nacional, modificada por la Ley 27.126 de creación de la Agencia Federal de Inteligencia.

73 Ley 26.388, modificación al Código Penal de la Nación Argentina.

74 Ley N. 25.326 de protección de datos personales.

75 Resolución de la Secretaría de Gobierno de Modernización 829/2019 Estrategia Nacional de Ciberseguridad

76 Decisión Administrativa 103/2019 de la Secretaría de Gobierno de Modernización

77 Decisión Administrativa 103/2019 de la Secretaría de Gobierno de Modernización

78 Decisión Administrativa 546/16 del Ministerio de Defensa

79 Resolución 1107-E/17 del Ministerio de Seguridad

80 Resolución 829/19 de la Secretaría de Gobierno de Modernización

81 Decreto 480/19 – Comité de Ciberseguridad

82 Del Río, M. (2014) La importancia de conocer el entorno a proteger. Blog Incibe

83 Cessario, A. & Torres M.; Fernandez, D., Del Rio, M., Monastersky, D. Comunicación Directa

84 De Arístegui, G (1997). Estudios de Política Exterior S. A.

85 Huster, S. (sin fecha) Terrorismo Y Derechos Fundamentales. Fundación Coloquio Jurídico Europeo

86 Perotti, J. (2009) La cooperación Argentina en la lucha contra el terrorismo en el contexto Internacional e interamericano

Universidad Complutense de Madrid, ISSN: 1696-2206

87 Observatorio de la Ciberseguridad en América Latina y el Caribe (2016) Informe Ciberseguridad 2016.

88 McClarkin E (2012) Thematic Paper on Organised Crime: Cybercrime - New Investigation Strategies and New Technologies. Special Committee on Organised Crime, Corruption and Money Laundering (CRIM) 2012-2013

89 Morelli, A. (sin fecha) Apuntes para una charla sobre la administración del conflicto internacional en el ciberespacio. Consejo Argentino para las Relaciones Internacionales (CARI)

90 Del Rio, M. (2014) La importancia de conocer el entorno a proteger. Blog Incibe

91 Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA), Grupo de Expertos Gubernamentales

92 Geneva Internet Platform, Digital Watch Observatory (2019) UN GGE and OEWG

93 Sánchez Gómez, F. & López Parra, J. (2017) Cooperación público-privada en la protección de infraestructuras críticas

94 Cessario, A. & Torres M.; Fernandez, D., Del Rio, M., Monastersky, D. Comunicación Directa

95 Alfredo Morelli, Ciberespacio Dfendible, Comité de Ciberseguridad (Buenos Aires), Comunicación Directa.

96 Fernández, D., M. del Río, M. y Monastersky, D. Comunicación Directa.

97 Fernández, D., M. del Río, M. y Monastersky, D. Comunicación Directa

98 Datos proporcionados por la Dirección Nacional de Ciberseguridad, Secretaría de Gobierno de Modernización

99 Datos proporcionados por la Dirección Nacional de Ciberseguridad, Secretaría de Gobierno de Modernización

100 Cessario, A. & Torres, M. Comunicación Directa

101 Norton Cyber Crime Report 2018

102 Norton Cyber Crime Report 2018

103 Páez, C. y Rocío A. (sin fecha) Amenazas de seguridad informática y el manejo de datos en las empresas

104 Torres Pedraza, J. (2015) Análisis de la influencia del fenómeno del ciberterrorismo en las dinámicas de seguridad de la Unión Europea

105 Cessario, A. & Torres, M. Comunicación Directa

106 Abrahms, M. (2012) "The Political Effectiveness of Terrorism Revisited." Comparative Political Studies 45, no. 3: 366-393.

107 Abrahms, M (2018) Rules for Rebels. The Science of Victory in Militant History.

108 Fundación Vía Libre: https://www.vialibre.org.ar/

109 International Telecommunication Union (ITU) Global Cybersecurity Index 2018, ISBN 978-92-61-28201-1 (Electronic version)

110 National Cyber Security Centre (2017) The 2017 Annual Review

111 International Telecommunication Union (ITU) Global Cybersecurity Index 2018, ISBN 978-92-61-28201-1 (Electronic version)

112 Gobierno de España – Presidencia de Gobierno (2019) España, primer país de la Unión Europea que desarrolla una Guía Nacional de Notificación y Gestión de Ciberincidentes. La Moncloa

113 Reglamento General de Protección de Datos de la Unión Europea (2016).

114 Reglamento de Ciberseguridad de la Unión Europea (2017)

Este informe fue realizado por profesionales de la Honorable Cámara de Diputados de la Nación siguiendo la metodología de UK POST (United Kingdom Parliamentary Office of Science and Technology). La metodología se orienta a proporcionar un análisis independiente y equilibrado de diversas cuestiones sobre la base de la ciencia y la tecnología, para lo cual se consulta bibliografía y literatura sobre la materia y se realizan entrevistas a una variedad de partes interesadas. Para obtener más información, comuníquese con la coordinadora y co-autora, Dra. Gabriela Commatteo, y el revisor y co-autor del informe, Dr. Juan de Dios Cincunegui a ciberseguridad.mpost@hcdn.gob.ar.

EXPERTOS CONSULTADOS

Max Abrahms, PhD: profesor de ciencias políticas en la Northeastern University. La investigación del Dr. Max Abrahms se centra en las consecuencias del terrorismo, sus motivos y las implicaciones para la estrategia antiterrorista. Es un analista frecuente en materia de terrorismo para los principales medios de comunicación y se ha posicionado como uno de los expertos en terrorismo y contraterrorismo más influyentes del mundo.

Ingeniero Ariel Cessario: especialista en ciberseguridad, consultor y desarrollador en el sector público y privado

Mariano M. del Río: Consultor en Ciberseguridad y Compliance, Fundador de SecureTech #HacerLasCosasBien.

Dr. Diego Fernandez: Socio de Marval, O'Farrel & Mairal, en el departamento de Propiedad Intelectual, Tecnología de la Información y Privacidad, presidente del Comité de Latinoamérica de la International Technology Law Association (ITechLaw), vicepresidente del capítulo Buenos Aires KnowledgeNet de la International Association of Privacy Professionals (IAPP). Profesor del curso de Educación Ejecutiva en Protección de Datos Personales de Universidad Torcuato Di Tella.

Emma McClarkin: miembro del Parlamento Europeo, especialista en comercio digital, tecnológico e internacional.

Dr. Daniel Monastersky: Abogado especializado en Delitos Informaticos, Proteccion de datos y delitos que afectan la reputación online. Director del Posgrado de Gestión y Estrategia en Ciberseguridad UCEMA

Embajador Alfredo Morelli: Experto argentino en el Grupo de Expertos de Naciones Unidas, Primera Comisión, dedicado a temas de guerra cibernética y al uso de las TICS (2013). Miembro del Comité Nacional de Ciberseguridad que diseño la Estrategia Nacional de Ciberseguridad

Martin Torres: especialista en ciberseguridad

Dr. Roberto Uzal: Director de la Maestría en Ciberdefensa y Ciberseguridad - UBA y del Doctorado en Ingeniería Informática – UNSL

Secretaría de Gobierno de Modernización – Dirección de Ciberseguridad

Fundación Vía Libre

EQUIPO

Coordinadora: Dra. Gabriela Alejandra Commatteo

Dr. Juan de Dios Cincunegui

Lic. Ricardo Reisin

Dr. Fernando Ruiz Magadan

La Honorable Cámara de Diputados de la Nación agradece a los entrevistados y revisores por amablemente haber dedicado su tiempo durante la preparación de este informe. Un especial reconocimiento a UK Post en las personas de los Doctores Grant Hill-Cawthorne, Lydia Harriss, Rowena Bermingham y Sarah Foxen. Adicionalmente, se agradece a la Dirección de Información Parlamentaria, a la Dirección General de Diplomacia Parlamentaria, Cooperación Internacional y Culto Departamento de Diseño de la Dirección de Prensa y Comunicación de la Honorable Cámara de Diputados de la Nación

Para ver la versión digital con las referencias completas

Para ediciones anteriores: *Espacio para link/código QR*

www.diputados.gov.ar
Seguinos en nuestras redes sociales