Revista de Administración Pública

INAP

# La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio

*Anahiby Becerril Gil*

*Resumen*: Las amenazas y riesgos en el ciberespacio se desarrollan en un espacio común global. En los últimos años hemos sido testigos de cómo las acciones negativas o el uso malicioso del ciberespacio han aumentado en su impacto, sofisticación y alcance y en un futuro no muy lejano podrían traer consecuencias humanitarias devastadoras. Ante este panorama la pregunta ya no es el por qué preocuparnos por el ciberespacio y la ciberseguridad, sino ¿cómo enfrentar los riesgos y retos que trae consigo el uso malicioso del ciberespacio a nuestra seguridad nacional? Los bits y las leyes deben trabajar juntos. Con este artículo se tiene el objetivo de llamar la atención y poner en la mesa la necesidad de desarrollar una Estrategia de Ciberseguridad para la Seguridad Nacional que considere las amenazas y retos que el ciberespacio y el empleo malicioso de las TIC traen consigo.

*Palabras Clave*: ciberespacio, ciberseguridad, ciberguerra, ciberataque, ciberarmas

# Cybersecurity in National Security: threats and challenges in cyberspace

*Abstract*: Threats and risks in cyberspace develop in a global common space. In recent years we have witnessed

how negative actions or malicious use of cyberspace have increased in their impact, sophistication and scope and in the not too distant future could bring devastating humanitarian consequences. Against this background, the question is no longer the reason to worry about cyberspace and cybersecurity, but how to face the risks and challenges that the malicious use of cyberspace brings to our national security? Bits and laws must work together. This article aims to draw attention and put on the table the need to develop a Cybersecurity Strategy for National Security that considers the threats and challenges that cyberspace and the malicious use of ICTs bring.

*Keywords*: cyberspace, cybersecurity, cyberwar, cyber-attack, cyber weapons

Fecha de recepción: 10 de enero de 2019
Fecha de aceptación: 5 de febrero de 2019

Revista de Administración Pública

INAP

# La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio

**Anahiby Becerril Gil***

## La compleja realidad del ciberespacio

Las amenazas y riesgos en el ciberespacio se desarrollan en un espacio común global[1]. Las redes están tan interconectadas[2] que puede ser difícil limitar los efectos de un ataque contra una parte del sistema sin dañar otras o interrumpirlo del todo. Nuestros activos de información fluyen por igual en el ciberespacio. El intercambio y la salvaguardia de éstos hoy en día resultan críticos para proteger los intereses públicos y privados en el área de la seguridad, el desarrollo, la protección de los derechos humanos y la economía.

* Licenciada en Derecho por la Universidad de las Américas, Puebla (UDLAP). Doctora en Derecho y Globalización. Especialista en Gobernanza, Derechos Humanos y Cultura de Paz (UCLM, España). Investigadora en el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, INFOTEC. Miembro del Sistema Nacional de Investigadores (SNI de CONACYT). Miembro de *Internet Society* (ISOC) y de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI).

1 Otros son: el espacio marítimo, aéreo y ultraterrestre.

2 Situación que ha sido materia de preocupación en el seno de la Asamblea General de la ONU donde se ha reconocido "que esa creciente interdependencia tecnológica se basa en una red completa de componentes de las infraestructuras de información esenciales"; *Cfr.* Preámbulo Resolución A/RES/58/199 de fecha 30 de enero 2004, disponible en: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (Consultado el 28 de enero de 2019).

Si consideramos la cada vez mayor dependencia tecnológica a través de la cual las sociedades, individuos, empresas y países desarrollamos gran parte de nuestras actividades diarias, desde hace tiempo deberíamos ya habernos preguntado sobre nuestra seguridad personal, la pública y la seguridad nacional en el ciberespacio.

En gran medida, la tecnología ha premiado la interconectividad en detrimento de la seguridad[3]. En los últimos años hemos sido testigos de cómo las acciones negativas o el uso malicioso del ciberespacio han aumentado. Lo anterior consecuencia de la accesibilidad a las herramientas, así como mejoras en las metodologías y capacidades técnicas de ataque[4], lo que permite la sofisticación de los actores empeñados en causar estragos o interrupciones. Sus efectos también se han incrementado y en un futuro no muy lejano podrían traer consecuencias humanitarias devastadoras[5].

En mayo del año 2017, el *ransomware WannaCry* impactó a 150 países y cientos de miles de sistemas, paralizando la atención médica, las instalaciones de producción y las telecomunicaciones. En el año 2018 se expusieron nuevas debilidades del hardware y se sumaron violaciones masivas

3 Presidencia de Gobierno, "Estrategia de Seguridad Nacional 2017", España, 2017, p. 34, disponible en: http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (Consultado el 27 de enero de 2019)

4 "*... the attack tools and methodologies are becoming widely available and the technical capability and sophistication of users bent on causing havoc or disruption is improving*" (Traducción libre); *Cfr. United States National Strategy to Secure Cyberspace*, 2003, p. 6, disponible en: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Consultado el 28 de enero de 2019)

5 El Comité Internacional de la Cruz Roja ya ha alertado sobre el uso de operaciones cibernéticas en conflictos armados y las consecuencias humanitarias devastadoras que pueden traer consigo; *Cfr.* Cordula Droege (ICRC Legal Adviser), "No legal vacuum in cyber space," Interview on 16 Aug. 2011, *ICRC Resource Centre*, disponible en: https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (Consultado el 28 de enero de 2019)

de datos: en India, Aadhaar[6], considerado el sistema de identificación biométrica más grande del mundo, sufrió violaciones que comprometieron los datos de los 1.100 millones de ciudadanos registrados; en septiembre, Facebook notificó a sus usuarios la violación masiva de datos más grande que ha sufrido, la cual afectaría a más de 50 millones de personas[7]. Y este año 2019 lo iniciamos con el "peor ataque de piratería informática"[8] que ha sufrido Alemania; documentos y mensajes personales, números telefónicos móviles, información de tarjetas de crédito, direcciones, correos (entre otros), se encuentran dentro de esta *große Datenleck*[9], algunas de las víctimas son la Canciller Alemana, el Presidente Alemán Frank-Walter Steinmeier, así como partidos políticos, periodistas y artistas entre otros[10].

La *European Union Agency For Network and Information Security*[11] (en adelante ENISA) reconoció como las

6 Aadhaar es la base de datos gestionada por la *Unique Identification Authority* (UIDAI) de la India. Proporciona un número aleatorio de 12 dígitos emitido por la UIDAI a los residentes de la India después de cumplir con el proceso de verificación establecido por la misma. Además de contener datos personales y demográficos contiene también información biométrica (diez huellas digitales, escáner del iris de ambos ojos y una fotografía facial). De conformidad con el Gobierno: "*La plataforma de identidad Aadhaar es uno de los pilares clave de la "India digital", en donde cada residente del país cuenta con una identidad única. El programa Aadhaar ya ha alcanzado varios hitos y es, con diferencia, el sistema de identificación biométrico más grande del mundo*"; *Cfr.* Unique Identification Authority of India, "*What is Aadhaar?*", Government of India, disponible en: https://uidai.gov.in/what-is-aadhaar.html (Consultado el 28 de enero de 2019)

7 De conformidad con Facebook, la violación habría sucedido en la tarde del 25 de septiembre. Los atacantes explotaron una función en el código de Facebook para obtener acceso a las cuentas de usuario y posiblemente tomar control de ellas; *Cfr.* Isaac Mike and Frenkel,Sheera, "Facebook Security Breach Exposes ccounts of 50 Millon Users", *The New York Times*, 28 de septiembre 2018, disponible en: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (Consultado el 28 de enero de 2019)

8 Enrique Müller, "Alemania Sufre el mayor "hackeo" de su historia con la filtración de datos personales de centenares de políticos", *El País Internacional*, 04 de enero de 2019, disponible en: https://elpais.com/internacional/2019/01/04/actualidad/1546595085_679572.html (Consulado el 20 de enero 2019)

9 Gran fuga de datos.

10 Markus Reuter, "Alles außer AfD: Was wir über das große Datenleck wissen", *Netzpolitik.com*, 04 de enero 2019, disponible en: https://netzpolitik.org/2019/alles-ausser-afd-was-wir-ueber-das-grosse-datenleck-wissen/ (Consultado el 20 de enero de 2019)

11 Agencia Europea de Seguridad de las Redes y de la Información

principales tendencias dentro en panorama de amenazas cibernéticas del 2018[12] las siguientes:

*Figura I*
*Visión general y comparación del panorama actual de amenazas 2018 con el de 2017, ENISA*[13]

| Top Threats 2017 | Assessed Trends 2017 | Top Threats 2018 | Assessed Trends 2018 | Change in ranking |
|---|---|---|---|---|
| 1. Malware | ➲ | 1. Malware | ➲ | → |
| 2. Web Based Attacks | ↑ | 2. Web Based Attacks | ↑ | → |
| 3. Web Application Attacks | ↑ | 3. Web Application Attacks | ➲ | → |
| 4. Phishing | ↑ | 4. Phishing | ↑ | → |
| 5. Spam | ↑ | 5. Denial of Service | ↑ | ↑ |
| 6. Denial of Service | ↑ | 6. Spam | ➲ | ↓ |
| 7. Ransomware | ↑ | 7. Botnets | ↑ | ↑ |
| 8. Botnets | ↑ | 8. Data Breaches | ↑ | ↑ |
| 9. Insider threat | ➲ | 9. Insider Threat | ↓ | → |
| 10. Physical manipulation/ damage/ theft/loss | ➲ | 10. Physical manipulation/ damage/ theft/loss | ➲ | → |
| 11. Data Breaches | ↑ | 11. Information Leakage | ↑ | ↑ |
| 12. Identity Theft | ↑ | 12. Identity Theft | ↑ | → |
| 13. Information Leakage | ↑ | 13. Cryptojacking | ↑ | NEW |
| 14. Exploit Kits | ↓ | 14. Ransomware | ↓ | ↓ |
| 15. Cyber Espionage | ↑ | 15. Cyber Espionage | ↓ | → |

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

12 En el documento "Analysis of the European R&D Priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe", ENISA, hace referencia a las "existential threats", entendidas como las amenazas, que en caso de llegar a ocurrir "tienen el potencial de destruir la parte directamente afectada de la sociedad, la industria o las empresas" (*Those threats that if enacted have potential to destroy the directly impacted part of society, industry and business*); *Cfr.* European Union Agency for Network and Information Security ENISA, *Analysis of the European R&D Priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe*, European Union Agency For Network and Information Security, 2018, disponible en: https://www.enisa.europa.eu (Consultado el 24 de enero 2019)

13 European Union Agency for Network and Information Security, "ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends", European Union Agency For Network and Information Security, 2019, p. 09, disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (Consultado el 28 de enero 2019)

De este panorama destacan los mensajes de correo electrónico y el denominado *phishing* como en el principal vector de infección de *malware*. Además se presenta un incremento en DDos *(Denial of service)*, *botnets*, fugas de información y violaciones de datos. Y se suma una nueva amenaza, que ejemplifica el *cybercrime-as-a-service* (CaaS): el *cryptohacking*[14]. ENISA estimó que durante la primera mitad de 2018 los *cyptominers* habían monetizado para sus usuarios más de 2.5 mil millones de dólares americanos.

Las predicciones para este año 2019 no son muy alentadoras. El Foro Económico Mundial (en adelante FEM), recientemente publicó su informe "*The Global Risks Report 2019*"[15], en donde sitúa al robo o fraude de datos y a los ciberataques dentro de los primeros 5[16] lugares en su "Encuesta de Percepción de Riesgos Globales" (*Global Risks Perception Survey*, GRPS), consolidando su posición junto con los riesgos medioambientales en el cuadrante de alto impacto y probabilidad del panorama de riesgos globales[17]. Para el caso de los ciberataques, tuvo un aumento de 82%, a nivel global. Dentro del informe el FEM también reconoció que el año pasado proporcionó evidencia adicional de los riesgos que los ciberataques plantean para la infraestructura crítica de los países.

Los ciberataques amenazan al mundo y nuestra seguridad. Es por lo que la ciberseguridad se ha vuelto una preocupa-

14 De conformidad con ENSIA, el *cryptohacking* o *cryptomining* es un ejemplo del funcionamiento del cibercrimen como servicio (*Cybercrime-as-a Service)*, conpetualizando así a los programas que emplean el poder del procesamiento de dispositivos de la víctima para extraer criptomonedas sin consentimiento, para más tarde obtener dinero en el mundo real, monetizado después de intercambios y transacciones legales. Este poder se utiliza para resolver rompecabezas criptográficos que se registran en la cadena de bloques; *Cfr.* European Union Agency for Network and Information Security, "ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends", European Union Agency For Network and Information Security, 2019, p. 09, disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (Consultado el 28 de enero 2019)

15 Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, p. 5, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado el 29 de enero de 2019)

16 En primer lugar se encuentran los acontecimientos climáticos extremos, seguido de el fracaso de la mitigación y adaptación al cambio climático y en tercero los desastres naturales.

17 Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, p. 16, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado el 29 de enero de 2019)

ción para la comunidad internacional. La Organización de Naciones Unidas (en adelante ONU) ha emitido diversas recomendaciones en donde enfatiza que "la difusión y el uso de las tecnologías y los medios de la información afectan los intereses de toda la comunidad internacional"[18], reconociendo que las tecnologías "también pueden ser empleadas con finalidades distintas de los objetivos de mantener la estabilidad internacional y la seguridad"[19].

A lo anterior debemos sumar una falta de ciberconfianza (*cybertrust*) global en el uso y desarrollo de capacidades y habilidades que los diversos *stakeholders* desarrollan dentro del ciberespacio.

Ante este panorama la pregunta ya no es el por qué preocuparnos por el ciberespacio y la ciberseguridad, sino ¿cómo enfrentar los riesgos y retos que trae consigo el uso malicioso del ciberespacio a nuestra seguridad nacional? Asegurar la ciberseguridad del Estado es uno de los desafíos clave de nuestro tiempo. Y debe ser una prioridad, tanto en el Plan Nacional de Desarrollo, como en la política exterior de nuestro país, así como en el seguimiento a la Estrategia Nacional de Ciberseguridad bajo sus tres principios: respeto de los Derechos Humanos, gestión de riesgos y un enfoque multidisciplinario y *multistakeholder*.

En este artículo no hablaremos del cibercrimen u operaciones en contra de la confidencialidad, disponibilidad e integridad de la información y los sistemas, amenazas que son principalmente tratadas bajo las leyes nacionales penales, tampoco nos referiremos al ciberterrorismo. Haremos mención de los diversos riesgos y retos que se presentan

18 "*... the dissemination and use of information technologies and means affect the interests of the entire international community*"; *Cfr.* Asamblea General de Naciones Unidas, Preámbulos de las Resoluciones A/RES/55/28 de 20 de Noviembre del año 2000; A/RES/56/19 de 29 de noviembre de 2001; A/RES/59/61 de 3 de diciembre de 2004; A/RES/60/45 de 8 de diciembre de 2005; A/RES/61/54 de 6 de Diciembre de 2006; A/RES/62/17 de 05 de diciembre de 2007; A/RES/63/37 de 2 de diciembre de 2008; A/RES/64/25 de 2 de diciembre de 2009.

19 Preámbulos de las Resoluciones A/RES/58/32 de 08 de diciembre de 2003; A/RES/59/61 de 3 de diciembre de 2004; A/RES/60/45 de 8 de diciembre de 2005; A/RES/61/54 de 6 de diciembre de 2006; A/RES/62/17 de 5 de diciembre de 2007; A/RES/63/37 de 2 de diciembre de 2008; A/RES/64/25 de 2 de diciembre de 2009.

en la ciberseguridad en materia de seguridad nacional (en adelante SN).

Esta contribución tiene como objetivo el hacer un llamado y poner en la mesa la necesidad de desarrollar una Estrategia de Ciberseguridad para la Seguridad Nacional que considere las amenazas y retos que el ciberespacio y el empleo malicioso de las TIC traen consigo.

## 2. El entorno "ciber-": consenso sobre el no consenso

Uno de los primeros retos a los que nos enfrentamos al entender este nuevo espacio, es la falta de un término único para los conceptos "ciberespacio", "ciberseguridad", ciberamenazas". Casi todas las palabras que emplean "ciber-", traen consigo falta de uniformidad.

Si bien en este artículo no pretendemos definir al ciberespacio y la ciberseguridad como conceptos unitarios, consideramos importante entender los efectos que tiene la falta de una terminología común para el ciberespacio, y cómo afecta esto a la búsqueda de la seguridad y estabilidad internacional.

### *2.1. El ciberespacio*

Este espacio de realidades abstractas, ideas, información y sistemas lógicos, abarca cuestiones políticas, tecnológicas y sociales, fomentado por Internet es una creación humana que poco entendemos. Algunos países y organismos internacionales han reconocido a Internet como una herramienta para el ejercicio de los Derechos Humanos, en específico la libertad de expresión y acceso a la información[20], en otros este espacio constituye una amenaza. En

20 La Resolución A/HRC/20/L.132 del Consejo de Derechos Humanos de la Organización de Naciones Unidas: intitulada "Promoción, protección y disfrute de los derechos humanos en Internet", reconoció, en lenguaje de Derechos Humanos, una serie de derechos de acceso y empleo del Internet para todas las personas. En este sentido, en la Resolución se afirma que los DDHH de las personas deben ser reconocidos y garantizados en el mundo *offline*, así como en el *online*. Adicionalmente, se exhorta a los Estados para que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países; *Cfr.* Consejo de Derechos Humanos de Naciones Unidas, Resolución A/HRC/20/L.13, "Promoción, protección y disfrute de los derechos humanos en Internet", de 29 de junio el 2012, disponible en: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf (Consultado el 20 de enero de 2019)

la visión China, por ejemplo, Internet tiene la capacidad de manipular la información, la verdad y el estado moral y psicológico de sus ciudadanos.[21]

El ciberespacio es definido por la *Estrategia Militar Nacional de Estados Unidos para Operaciones del Ciberespacio* como un "dominio caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas en red e infraestructuras físicas asociadas"[22]. Por su parte la Unión Internacional de Telecomunicaciones (en adelante UIT) hace referencia al ciberentorno, para describir a "usuarios, redes, dispositivos, todo el *software*, procesos, información almacenada que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes"[23].

El ciberespacio es un mundo electrónico, un espacio común global en donde las personas se encuentran unidas para intercambiar ideas, servicios e incluso amistad[24]. Constituye un sistema nervioso, el cual controla a los países y la infraestructura crítica que los sostiene. Su funcionamiento saludable es esencial para la economía y la seguridad nacional[25]. Es un entono digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas, permitiendo el

21 Thimoty L. Thomas, "Information Security Thinking: A Comparation of U.S., Russian and China Concepts, Foreign Miltary Studies Office, julio, 2001, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Consultado el 20 de enero de 2019)

22 "*domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and Exchange data via networked systems and associated physical infrastuctures*" (Traducción libre); *Cfr.* United States Department of Defense (DoD), *The National Military Strategy for Cyberspace Operatios*, diciembre 2006, p. ix, disponible en: https://www.hsdl.org/?view&did=35693 (Consultado el 20 de enero de 2019)

23 Unión Internacional de Telecomunicaciones, UIT-T X.1205, disponible en: https://www.itu.int/rec/T-REC-X.1205-200804-I/es (Consultado el 20 de enero 2019)

24 Gobierno de Canadá, "Canada´s Cybersecurity Strategy. For a stronger and more prosperous Canada," 2010, disponible en: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx (Consultado el 27 de febrero 2019).

25 United States Government, "Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009, disponible en: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (Consultado el 27 de febrero 2019).

ejercicio de sus derechos y libertades, de la misma forma que lo hacen en el mundo físico[26]. La definición que se otorgue respecto al ciberespacio atiende en gran medida al uso que se le otorgue.

El ciberespacio como una función o dominio separado no forma parte de la concepción rusa. Para este país el concepto clave constituye la información, la cual puede ser almacenada en cualquier lugar y transmitida por cualquier medio. El Gobierno Ruso hace referencia a las "operaciones de red informática" (*computer network operations*, CNO), del "*information space*" (espacio de información)[27]. Este útlimo término es empleado para referirse a lo que el occidente conocemos como el ciberespacio. El término incluye el procesamiento informático y humano de la información (motivo por el cual la *information war* incluye el dominio cognitivo humano).[28]

Este entendimiento del espacio de información quedó plasmado en la propuesta para un "Código Internacional de Conducta para la Seguridad de la Información"[29], presentado por la Organización de Cooperación de Shanghai[30] a la Asamblea General de Naciones Unidas en el año 2011[31]. Además del proyecto propio elaborado por Rusia sobre una "Convención sobre Seguridad de la Información

26 Gobierno de México, "Estrategia Nacional de Ciberseguridad", México, 2017, disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (Consultado el 27 de febrero 2019).

27 Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, pp. 7-8.

28 Thimoty L. Thomas, "Information Security Thinking: A Comparation of U.S., Russian and China Concepts", *Foreign Miltary Studies Office*, julio, 2001, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Consultado el 20 de enero de 2019)

29 Shanghai Cooperation Organization, "International Code of Conduct For Information Security (SCO)", 2011, disponible en: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609563C11.pdf (Consultado el 29 de enero 2019)

30 La también conocida SCO, por las siglas en inglés para *Shanghai Cooperation Organization* se encuentra conformada por los siguientes 8 países: Rusia, China, Kazajistán, Kirguistán, Tayikistán, Uzbekistán, India, Pakistán.

31 Asamblea General de Naciones Unidas, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)*, 14 de septiembre 2011, disponible en: http://undocs.org/A/66/359 (Consultado el 18 de diciembre de 2019)

Internacional"[32]. El Código de Coducta propuesto contenía la definición del "espacio de información" (*information space*), como:

> "la esfera de actividad relacionada con la formación, creación, conversión, transferencia, uso y almacenamiento de información y que tiene un efecto en la conciencia individual y social, la infraestructura de información y la información en sí". [33]

Esta definición tiene algunas similitudes con la idea occidental del ciberespacio, además del enfoque sobre los efectos en la conciencia individual y social, como se había referido. Mientras que el concepto de "*information warfare*" (guerra de información) hace referencia a lo siguiente:

> "conflicto entre dos o más Estados en el espacio de información con el objetivo de infligir daños a los sistemas, procesos y recursos de información, así como a estructuras de importancia crítica y otras estructuras; socavando los sistemas políticos, económicos y sociales; llevar a cabo campañas psicológicas masivas contra la población de un Estado para desestabilizar a la sociedad y al gobierno; así como obligar a un Estado a tomar decisiones en interés de sus oponentes".[34]

En ambas definiciones de sostiene la idea de una esfera social dentro de los datos e información.

Lograr un consenso en el entendimiento de lo que se pretende proteger, representa uno de los principales problemas

32 Ministerio de Asuntos Exteriores de Rusia, *Convention on International Information Security*, 22 de septiembre 2011, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (Consultado el 27 de enero de 2019).

33 Shanghai Cooperation Organization, "International Code of Conduct For Information Security (SCO)", 2011, disponible en: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609563C11.pdf (Consultado el 29 de enero 2019)

34 Shanghai Cooperation Organization, "International Code of Conduct For Information Security (SCO)", 2011, disponible en: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609563C11.pdf (Consultado el 29 de enero 2019)

en el consenso para la adopción de normas y principios para regular a este nuevo dominio.

### *2.2. La ciberseguridad*

Debemos considerar que el ciberespacio constituye este cuarto dominio en donde se realiza gran parte de las actividades del gobierno, además de que a través de él se desarrolla el flujo de información, tanto crítica como estratégica de los países, instituciones y empresas. Dada su importancia, el ciberespacio debería situarse dentro de la Estrategia Global de Seguridad Nacional.

La ciberseguridad ayuda a identificar, evaluar y abordar las amenazas en el ciberespacio, para reducir ciber-riesgos y eliminar el impacto de los ciberataques, el cibercrimen, ciberterrorismo, ciberespionaje, en el sentido de fortalecer la confidencialidad, integridad y disponibilidad de datos, sistemas y otros elementos de la infraestructura de información y comunicación.

Por ejemplo, dentro de su Estrategia de Seguridad Nacional, España[35] reconoce que el ciberespacio está asociado a nuevas amenazas y que, al igual que espacios comunes como el espacio marítimo, el aéreo y ultraterrestre, resultado de sus características de fácil acceso y débil regulación, lo que permite que fácilmente puedan convertirse en escenario de confrontaciones.

Mientras que el gobierno ruso se refiere a la ciberseguridad como "seguridad de la información" (*information security*), para incluir también temas relacionados con el contenido en línea.[36]

35 Gobierno de España, "Estrategia de Seguridad Nacional. Un proyecto compartido de todos para todos", Presidencia del Gobierno, España, 2017, p. 65, disponible en: http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (Consultado el 27 de enero de 2019)

36 Kleir Giles, Keir, "Russia's public stance on cyberspace issues", 2012, pp. 1-13, disponible en: https://www.researchgate.net/publication/261044707_Russia's_public_stance_on_cyberspace_issues (Consultado el 20 de enero 2019)

En nuestro país, la seguridad nacional[37] dentro del ciberespacio comprende el desarrollo de capacidades para "prevenir riesgos y amenazas en el ciberespacio que puedan afectar la independencia, integridad y soberanía nacional, afectando el desarrollo y los interesas nacionales"[38].

La ciberseguridad va a tratar de la seguridad de este ciberespacio. Podemos interpretar el término atendiendo a los conceptos otorgados por la comunidad técnica, y por los empleados por los documentos nacionales de ciberseguridad. Sin embargo, consideramos que la definición que la UIT[39] emitió en su Recomendación ITU-T X.1209 (12/2019), resulta adecuada al explicar el concepto, a saber:

> "3.2.5. ciberseguridad [b-ITU-T X.1205]: el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno".

37 La Seguridad Nacional (SN), de conformidad con el artículo 3 de la Ley en la materia, constituyen las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven entre otras a: *I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país; II. La preservación de la soberanía e independencia nacionales y la defensa del territorio; III. El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno; IV. El mantenimiento de la unidad de las partes integrantes de la Federación señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos; V. La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional; VI. La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes.*

38 Gobierno de México, "Estrategia Nacional de Ciberseguridad", 2017, p. 18, disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (Consultado el 29 de enero de 2019)

39 El texto refiere: *"Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*"; *Cfr.* Union Internacional de Telecomunicaciones (UIT), Rec. ITU-T X.1209 (12/2019), Capabilities and their context scenarios for cybersecurity information sharing and exchange, ITU-T X-Series Recommendations, UIT, 2010, p. 1.

Identificando como los "activos" a los "dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedia, así como la totalidad de la información transmitida y/o almacenada en el ciberentorno. Reconociendo que la ciberseguridad garantiza se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Refiriendo a las propiedades de la ciberseguridad las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y la confidencialidad.

La falta de una definición consensuada sobre lo que es el ciberespacio impacta sobre lo que, a través de la ciberseguridad, necesitamos proteger. Lo que también dificulta la aclaración de roles y atribuciones para los diferentes *stakeholders*.

## 3. El reconocimiento de las amenazas de ciberseguridad

Si bien las ciberamenazas pueden presentarse en la forma de ciberataques, también pueden ser el resultado de errores o incluso desastres naturales. En este apartado nos enfocaremos a los primeros, ejemplificando diversos modelos y métodos para causar daño asociados al ciberespacio.

### *3.1. Cyberarmas*

Las armas son instrumentos de daño, las ciberarmas no son la excepción. Son patrones abstractos de *bits*[40]. Se conforman de "0" y "1", programados para causar daño, al igual que las armas tradicionales.

Para lograr su objetivo, utilizan primordialmente software[41]. Constituyen códigos de computadora que se em-

40 Neil, Rowe, "Distinctive ethical challenges of cyberweapons", in Tsagourias, Buchan, Russell, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, Massachusetts, 2017, p. 310. (307-326)

41 Neil Rowe, "Distinctive ethical challenges of cyberweapons", in Tsagourias, Buchan, Russell, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, Massachusetts, 2017, p. 309. (307-326)

plean o son diseñados para ser utilizados con el objetivo de amenazar o causar daño, lo que no les diferencia del armamento tradicional. Son instrumentos que se emplean, o están diseñados para ser utilizados, con el objetivo de amenazar o causar daños físicos, funcionales o mentales a estructuras, sistemas o seres vivos.[42]

Éstas pueden presentarse en la forma de programas modificados para controlar computadoras y otros dispositivos. Sus usos pueden ir desde evitar la respuesta o adecuado funcionamiento de un sistema de defensa de misiles, hasta borrar los programas de datos clave de un sistema informático para que no pueda realizar tareas, o bien podría bloquear el acceso a la red para que un sistema no pueda comunicarse con otros. Pueden incluso ocasionar un "apagón" masivo de sistemas críticos.

Constituyen armas especificas que pueden ser empleadas dentro de los ciberataques. Algunas son controladas por medios remotos a través de Internet empleando técnicas de "botnets" donde "la máquina del atacante envía ordenes a la máquina de la víctima" con fines de espionaje o sabotaje".[43] En los casos en que el objetivo no se encuentre en Internet, se pueden emplear mecanismos de tiempo o especificaciones de eventos desencadenantes para controlarlo[44].

Para Rowe, las características de las ciberarmas son las siguientes:

42 Thomas Rid & Peter McBurney, "Cyber-Weapons", *The RUSI Journal*, 157;1, 2012, 6-1, disponible en: https://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354 (Consultado el 29 de enero de 2019)

43 Christopher Elisan, *Malware, Rootkits, and Botnets: A Beginner,s Guide*, McGraw Hill, 2013.

44 Randall Dipert, "Other-tahn-Internet (OTI) cyberwarfare: challenges for ethics, law and policy", *Journal of Military Ethics*, 12(1), abril, 2013, disponible en: https://www.researchgate.net/publication/263529399_Other-than-internet_oti_cyberwarfare_Challenges_for_ethics_law_and_policy (Consultado el 27 de enero de 2019)

*Cuadro 1*
*Características de las ciberarmas*[45]

| | |
|---|---|
| Ciberarmas | No requieren proximidad física del atacante a la víctima, ya que los ataques se pueden realizar a través de Internet, o bien se pueden plantar bien en el avance del ataque (como "caballos de Troya") y se activan cuando el atacante ya no está. |
| | Son fáciles de ocultar, incluso más fáciles que las armas biológicas, ya que son solo patrones abstractos de bits. También pueden operar muy rápidamente y luego destruir toda evidencia de su presencia. |
| | Los ataques cibernéticos pueden ser muy difíciles de atribuir al actor atacante (estatal o no estatal) ... En una guerra cibernética pura, no acompañada por ataques tradicionales, es prácticamente imposible de justificar en el ciberespacio de acuerdo con los estándares de prueba exigidos por la ley de guerra. |
| | Las armas cibernéticas requieren fallas en su víctima o no funcionan en absoluto. |
| | Son considerablemente más variadas que las municiones convencionales. Las armas cibernéticas pueden sabotear las operaciones de los sistemas informáticos de muchas maneras diferentes, algunas bastante sutiles. |
| | Tienden a tener consecuencias inesperadas. Esto se debe a que los sistemas informáticos dependen de miles de millones de instrucciones de componentes que funcionan constantemente cada vez que se usan, y solo un error puede alterar la cadena de instrucciones de los agujeros, a menos que se tomen precauciones inusuales, como agregar funcionalidad redundante. |

Finalmente, apunta el autor, las armas cibernéticas no tienen usos legítimos. Por lo tanto, encontrar ciberarmas es una evidencia *prima facie* de intención ofensiva.

45 Neil Rowe, "Distinctive ethical challenges of cyberweapons", in Tsagourias, Buchan, Russell, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, Massachusetts, 2017, pp. 310-311. (307-326)

Las ciberarmas pueden facilitar que individuos inocentes se conviertan en objetivos, consecuencia de la "ventaja" que le da el anonimato a través del control remoto que en algunos casos puede ejercer el atacante, como ha sucedido en los casos del empleo de drones para ataques militares.

Otro reto lo constituyen las tecnologías y servicios de doble uso, consideradas así por que pueden emplearse en el ámbito militar, empero se comercializan para la venta a civiles. En este contexto surge el *Arreglo Wassenaar*. Este constituye un régimen multilateral que establece controles sobre la transferencia de bienes y tecnologías de doble uso (militar y civil), Del cual México es parte desde el año 2012.

Sin embargo, el control de las ciberarmas planeta cuestiones como: conocer sí nos encontramos en el desarrollo de una carrera ciberarmamentista; en caso de que sea afirmativo lo anterior, debemos conocer cuál es el nivel de madurez y la etapa en que nos encontramos dentro de la carrera armamentista que emplea estas tecnologías; si es a través de un tratado internacional, la forma en que puede lograrse un acuerdo sobre el desarrollo, la imprevisibilidad, responsabilidad y atribución en el desarrollo de estas tecnologías. A estas interrogantes debemos sumar las cuestiones éticas en el uso de las ciberarmas. Además, falta realizar más estudios sobre los daños colaterales, psicológicos, además de humanos que pueden causar.

El analista estadounidense Coronel Timothy Thomas señala que hay varios elementos únicos en el enfoque de Rusia en la guerra de información, señalando que una "*information weapon"* o arma de información implica:

> "Un medio dirigido a activar (o bloquear) los procesos del sistema de información en los que el sujeto que usa las armas tiene interés. Un arma de información puede ser cualquier medio o sistema técnico, biológico o social que se utiliza para la producción, el procesamiento, la transmisión, la presentación o el bloqueo de datos y/o procesos que funcionan con los datos."[46]

46 Roland Heickerö, "Emerging Cyber Threats and Russian -views on Information. Warfare and Information Operatios", FOI, Swedish Defence Research Agency, 2010, pp. 13-15, disponible en: http://www.highseclabs.com/data/foir2970.pdf (Consultado el 29 de enero de 2019)

Para el autor el objetivo final del efecto de un arma de información es el conocimiento de un sistema de información específico y el empleo intencional de ese conocimiento para distorsionar el Modelo del mundo de la víctima.

Finalmente se debe considerar que estas armas de información, refería el exjefe adjunto del Estado Mayor Teniente General Aleksander Burutin en el año 2008, pueden ser empleadas de manera eficiente tanto en época de paz como durante la guerra[47].

### *3.2. Ciber ataques o ataques cibernéticos*

> *Un conjunto de ataques maliciosos puede llegar a constituir un arma de destrucción masiva*[48].

Los ataques cibernéticos o ciberataques proporcionan al menos tres ventajas sobre otro tipo de armamento empleado en la guerra. Primero, pueden organizarse de forma relativamente más rápida y sistemática en todo el ciberespacio. Segundo, gracias a la hiperconectividad, ningún objetivo es demasiado remoto para un ataque cibernético. Tercero, los ataques cibernéticos tienen relativamente más opciones de herramientas, tiempo y objetivos de ataque para satisfacer sus objetivos y con costos limitados.[49]

Los ciberataques constituyen actos que se desarrollan en el ciberespacio y que podrían razonablemente causar daño[50]. Un ciberataque puede ser un acto de ciberespionaje, piratería o intento de obtener de forma ilícita contraseñas y preguntas de seguridad para obtener información secreta gubernamental o comercial. También puede constituir el

47 Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, p. 10.

48 BBC, "US launches cyber security plan," 29 mayo 2009, disponible en: http://news.bbc.co.uk/2/hi/americas/8073654.stm (Consultado el 20 de enero de 2019)

49 Chris Demchak, "Economic and Political Coercion and a Rising Cyber Westphalia", *Pacetime Regime for State Activities in Cyberspace*, CCDCOE, pp. 598-602.

50 Michael Robinson & Kevin Jones & Helge Janicke, "Cyber warfare: Issues and challenges", *Computers & Security*, 2015, 49, pp. 70-94, disponible en: https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges (Consultado el 10 de enero de 2019)

bloqueo o desfiguración de un sitio web ya sea directamente o mediante una red de *bots*. Otro caso es el ataque contra la confidencialidad, disponibilidad o integridad de información crítica, o puede ser un acto genuino de guerra cibernética.

Lo que cuenta en el ciberataque, para ser considerado una amenaza de seguridad nacional, es el objetivo. Consideremos que algunas de las técnicas de software que pueden ser empleadas para la guerra cibernética, también lo son para llevar a cabo otro tipo de delitos comunes. Lo que difiere son los objetivos entre los cibercriminales. Si bien este tipo de armas implica la intromisión ilícita a sistemas informáticos, resulta distinto el robar la información personal para acceder a cuentas bancarias, enviar correos *spam* que con fines de sabotaje[51].

Por ello entendemos que, para el caso de seguridad nacional, un ciberataque debe estar encaminado a socavar las funciones de un sistema o red de computadoras con un propósito político o de seguridad nacional.

### *3.3. La ciberguerra (cyber warfare)*

El 27 de abril del año 2007 Estonia fue atacada. Para ese año, el país había instituido un gobierno electrónico en el cual el 90% de los servicios bancarios, incluso sus elecciones parlamentarias, se desarrollaban a través de Internet. En cuestión de horas los portales de los principales bancos del país fueron colapsados. Todos los sitios web de los principales periódicos dejaron de funcionar. Las comunicaciones del Gobierno fueron bloqueadas. Docenas de objetivos estratégicos fueron atacados en todo el país. Aunque las consecuencias pueden ser medibles como efectos de guerra tradicional, un sistema de cómputo fue

51 Entendido como el daño, destrucción, perjuicio o entorpecimiento ilícito de vías de comunicación, servicios públicos, funciones de las dependencias del Estado, organismos públicos descentralizados, empresas de participación estatal, órganos constitucionales autónomos o sus instalaciones; plantas siderúrgicas, eléctricas o de las industrias básicas; centros de producción o distribución de artículos de consumo necesarios, de armas, municiones o implementos bélicos, con el fin de trastornar la vida económica del país o afectar su capacidad de defensa (artículo 140 Código Penal Federal)

responsable de todo[52]. Se contabilizaron al menos 128 ataques únicos *DDos*, dirigidos a los protocolos de Internet en Estonia durante este período[53]. Nunca se había atacado a un país entero en casi todos los frentes digitales a la vez.

Ciberguerra, *cyber warfare*, guerra cibernética, este término se emplea por diversos actores, cada uno con distintos significados. Aunque ha creado interés durante muchos años, carece de una definición generalmente aceptada. Incluso los analistas difieren en cuanto a si la etapa actual del conflicto cibernético puede considerarse como una guerra cibernética.

El concepto de guerra cibernética fue introducido por primera vez por John Arquilla y David Ronfelt en su artículo: "*CYBERWAR IS COMING!*"[54] (1993). En él, los autores describieron la guerra cibernética –distinta a la *netwar*[55]– como una forma de guerra que interrumpe, si no destruye, los sistemas de información y comunicaciones. También argumentaron que debido al cambio en la tecnología o la "revolución de la información[56]", la guerra cibernética se convertiría en un modo dominante de conflicto y guerra.

52 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe", *WIRED MAGAZINE*, agosto 21, 2007, disponible en https://www.wired.com/2007/08/ff-estonia/ (Consultado el 26 de enero de 2019)

53 Sean Kerner, *Estonia Under Russian Cyberattack?*, Security, mayo 18, 2007, disponible en: http://www.internetnews.com/security/article.php/3678606/Estonia+Under+Russian+Cyber+Attack.htm (Consultado el 26 de enero de 2019)

54 John Arquilla y David Ronfeldt, "*CYBERWAR IS COMING!",* RAND, National Security Research División, 1993, disponible en: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

55 Definida como los "conflictos de ideas de nivel social librados en parte a través de los modos de comunicación por Internet" (*societal-level ideational conflicts waged in part through internetted modes of communication*); *Cfr.* John Arquilla y David Ronfeldt, "*CYBERWAR IS COMING!*", RAND, National Security Research División, 1993, p. 27, https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf (Consultado el 25 de enero de 2019)

56 Descrita por los autores como "el reflejo del avance de las tecnologías de información y comunicación computarizadas y las innovaciones relacionadas en la teoría de la organización y la gestión" ("*The information revolution reflects the advance of computerized information and communications technologies and related innovations in organization and management theory"*); *Cfr.* Arquilla, John y Ronfeldt, David, "*CYBERWAR IS COMING!", RAND*, National Security Research División, 1993, p. 25, disponible en: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf (Consultado el 25 de enero de 2019)

Desde el punto de vista del Derecho Internacional Humanitario, el Comité Internacional de la Cruz Roja, define el término –*cyber warfare*– como los "medios y métodos de guerra que consisten en operaciones cibernéticas que representan, o se llevan a cabo en el contexto de, un conflicto armado, en el sentido del Derecho Internacional Humanitario (DIH)"[57]. Es una operación contra una computadora o sistema informático, a través de un flujo de datos cuando se utiliza como medio y método de guerra en el contexto de un conflicto armado (a diferencia de las operaciones físicas y cinéticas o el uso del ciberespacio para la comunicación durante un conflicto armado)[58].

El Departamento de Defensa de Estados Unidos define a la guerra cibernética como "un conflicto armado llevado a cabo en su totalidad o en parte por medios cibernéticos".[59] Rusia, por su parte, emplea el término "*information war*" (IW) para referirse a "una batalla entre estados que involucran el uso exclusivo de armas de información en el ámbito de los modelos de información".[60] Dentro del contexto ruso no hay una diferencia importante entre los términos IW, lucha de información y batalla de información.[61]

Hay una distinción notable entre la psicología que sustenta el uso cibernético ruso y los métodos occidentales. Rusia ha dividido sus operaciones cibernéticas en dos: "información

57 *Cfr.* International Committee of the Red Cross, *Cyberwarfare and international humanitarian law: the ICRC's position*, ICRC, 2006, p. 1, disponible en: https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf (Consultado el 25 de enero de 2019)

58 Cordula Droege (ICRC Legal Adviser), "No legal vacuum in cyber space," entrevista de 16 agosto del año 2011, *ICRC Resource Centre,* disponible en: https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-inter- view-2011-08-16.htm (Consultado el 26 de enero de 2019)

59 "*Cyber Warfare (CW): An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. Includes cyber attack, cyber defense, and cyber enabling operations*" (Traducción libre); *Cfr.* Departamento de Defensa de Estados Unidos de América, *Cyberspace Operations Lexicon*, p. 8, disponible en: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf (Consultado el 26 de enero de 2019)

60 Thimoty L. Thomas, *Comparing Us, Russian, and Chinese Information Operations Concepts*, Foreign Military Studies Office, 2004, p. 6, disponible en: http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Consultado el 20 de enero de 2019)

61 Ibíd.

técnica: ataques cibernéticos y DDoS e información-psicológica, que utiliza el ciberespacio para subvertir a otras sociedades".[62]

El concepto común resulta la información, la cual puede ser almacenada en cualquier lado y transmitida por cualquier medio, así como procesada de forma inmediata.

Existen autores que emplean el término "ciber conflicto" (*cyber conflict*). Para Valeriano y Maness ´éste implica:

> "*the use of computational technologies for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions among states*"[63]

Bajo esta tesitura, los autores consideran que la ciberguerra podría ser una escala mayor dentro del ciberconflicto que incluye la destrucción física y la muerte. Sin brindar una una definición clara de cuándo el conflicto cibernético se convierte en un escenario de guerra cibernética.

### *3.4. Conflictos híbridos*

> *Una atribución de la guerra futura será la confrontación de la información ... la información se está convirtiendo en el mismo tipo de arma que los misiles, bombas, torpedos, etc.*[64]

El crecimiento en los conflictos y en las denominadas "acciones" o "guerras híbridas", han ido evolucionando

62 Mark Laity, Chief of Strategic Communications, Supreme Headquarters Allied Powers Europe (SHAPE), *Russia: Implications for UK defence and security*, House of Commons, Reuno Unido, disponible en: https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/10705.htm (Consultado el 29 de enero de 2019)

63 *El uso de tecnologías computacionales con fines malévolos y destructivos para impactar, cambiar o modificar las interacciones diplomáticas y militares entre los estados* (Traducción libre); *Cfr.* Brandon Valeriano & Bryan C. Maness, "Cyber War Versus Cyber Realities: Cyber Conflict in the International System", Oxford University Press, Oxford, 2015, pp. 3-4.

64 Slipchenko, *Future War (A Prognostic Analysis)*, January 1998, en Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, disponible en: https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Consultado el 25 de enero de 2019)

como amenazas en el ciberespacio con impactos en el mundo físico, que aún distan de conocerse a plenitud.

El potencial de conectividad que tiene Internet ha ayudado a la proliferación en el uso de armas de información masiva. O, mejor dicho, desinformación.

La creciente conectividad, el abaratamiento y accesibilidad de las tecnologías, ha generado un importante traslado de poder hacia actores no estatales. Las amenazas provienen de individuos y grupos que se encuentran emergiendo como actores relevantes, los cuales rápidamente ganan espacios e influencia, resultado de la "viralización" y la hiperconectividad que el ciberespacio nos provee.

Los conflictos que resultan de este tipo de acciones se caracterizan por no estar limitados a tiempo de guerra, ni siquiera se encuentran restringidos a una "fase inicial del conflicto", antes del inicio de hostilidades. Es una actividad continua independiente del estado de las relaciones que tenga el atacante con el Estado afectado.

Bajo el criterio ruso, nos encontramos en una "*informatsionnaya voyna*" (*information war*), donde la información, su intercepción, manipulación, distorsión y robo conforma el "conjunto de sistemas, métodos y tareas para influir en la percepción y el comportamiento del enemigo, la población y la comunidad internacional en todos los niveles".[65]

Los medios empleados en esta guerra de información pueden incluir: "desacreditar el liderazgo del adversario, intimidar al personal militar y a los civiles… falsificación de eventos, desinformación, entre otros"[66]. Todos ellos enfocados en el logro de fines políticos o diplomáticos, influyendo en el liderazgo y la opinión pública de Estados extranjeros, así como de organizaciones regionales e internacionales. La desinformación masiva, se perfila como

65 Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, p. 6, disponible en: https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Consultado el 25 de enero de 2019)

66 Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, p. 12, disponible en: https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Consultado el 25 de enero de 2019)

una amenaza para las sociedades. Debemos comenzar a analizar las consecuencias que pueden traer consigo la influencia en la percepción o decisión que tienen las personas al ser sometidas a campañas de desinformación masivas personificadas, gracias al *profiling* resultado de la información que dejan a través del uso de redes sociales o sus interacciones con otros.

Otra cuestión reside en las consecuencias que el "*affective computing*"[67] puede traer a la estabilidad de los individuos y las sociedades. Aún desconocemos cuales son los efectos que el perfilamiento de los usuarios con fines comerciales o las consecuencias ciertas de las implicaciones de Cambridge Analytica en las elecciones de Estados Unidos de América. Sin embargo, debemos considerar las amenazas que el empleo de algoritmos para conocer y manipular los sentimientos de las personas. Todos estos ingentes volúmenes de flujos de datos personales pueden ser generados por los nodos de IoT (Internet de las cosas, –*Internet of Things*– o por su acrónimo IoT), los cuales se transforman en la obtención de inteligencia, es decir, en información estratégica, útil, para la toma de decisiones y realización de acciones, o incluso, para el empleo de otros dispositivos y a partir de ahí, actuar sobre nosotros y nuestro entorno.

## 4. Los Retos

### *4.1. Algoritmos para la defensa y el ataque*

El año pasado puso en relieve la importancia del uso de la Inteligencia Artificial (en adelante IA), el denominado *machine learning* (aprendizaje automático), y el Internet de las cosas IoT para la economía y los riesgos globales. Este trinomio aumenta los riesgos ya existentes y dan paso al surgimiento de otros.

La IA puede desempeñar un papel importante en la ciberseguridad, la inteligencia en la detección de ciberamenazas, en los análisis para detectar, contener y mitigar los

67 Entendida "cómo con el empleo de la Inteligencia artificial se puede reconocer, responder y manipular las emociones humanas"; *Cfr.* Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado el 29 de enero de 2019)

*advanced persistent threats* (APTs), así como en la lucha y mitigación de actividades maliciosas en el ciberespacio. Un ejemplo de ello son las técnicas de inteligencia artificial empleadas para buscar de forma automática *malware* desconocido o vulnerabilidades de día cero (*zero-day*), en función de ciertas características y comportamientos.

La comprobación tradicional de vulnerabilidades de la red se basa en procesos que requieren mucha mano de obra y gran experiencia, sin embargo, son propensos a errores. El análisis y seguridad de las redes puede beneficiarse de los marcos automatizados basados en razonamiento para obtener una mejor conciencia cibernética del ciberespacio altamente dinámico. Comprender cómo se interconectan los dispositivos de red, cómo se procesa y cómo se almacena, resulta crucial para la conciencia cibernética que requieren las aplicaciones, como el monitoreo proactivo de la seguridad informática. La supervisión proactiva de la seguridad informática depende en gran medida de datos de red precisos, concisos y de calidad. Los sistemas inteligentes proporcionan mecanismos para reducir el impacto de los ataques cibernéticos y, siempre que sea posible, previenen los ataques y gestionan los riesgos de vulnerabilidad a través de la concienciación cibernética en tiempo real.[68]

Sin embargo, las técnicas y herramientas de IA también pueden y son explotadas con propósitos maliciosos. Imaginemos que con el empleo de la IA a la biotecnología se puedan crear patógenos, virus nuevas enfermedades que puedan ser empleados en contra de las personas. Otro ejemplo de ello es el empleo de técnicas de IA para identificar y explotar vulnerabilidades en sistemas y dispositivos. Distinto escenario constituye que un atacante (o grupo de atacantes) diseñe técnicas de IA para identificar y explotar vulnerabilidades en, vehículos autónomos o en drones, para facilitar ataques coordinados en lugares con grandes cantidades de personas o en horas pico. Además, a través de ataques coordinados, las técnicas de IA

68 Leslie F, Sikos, Dean Philp, Catherine Howard, Shaun Voigt, Markus Stumptner, y Wolfang Mayer, *Knowledge Representation of Network Semantics for Reasoning-Pwerd Cyber-situational Awareness*, en Leslie F. Sikos (editor), "AI in Cyberseucirty", Springer, Suiza, 2019, pp. 19-22 (19-46).

pueden explotar vulnerabilidades en infraestructuras de ciudades inteligentes (por ejemplo, sistemas de transporte inteligentes) para maximizar el impacto de dichos ataques, con el objetivo de causar pánico e inquietud en la sociedad. Por lo tanto, también existe la necesidad de defenderse contra los ataques ciberfísicos basados en la IA.

### *4.2. El cómputo cuántico*

Dentro del flujo constante de información, el cifrado de las comunicaciones digitales ha cobrado una gran relevancia. Tal y como lo señaló el Relator Especial David Kaye, en el Informe A/HCR/29/32[69], en la actualidad el cifrado y anonimato son las principales vías de seguridad en línea que ofrecen a las personas un medio para proteger su privacidad, al permitirles elaborar y compartir ideas y opiniones, sin injerencia alguna. De esta forma reconoce las implicaciones sobre el uso del cifrado[70] y el anonimato como una forma de protección de la privacidad en la era digital.

69 David, Kaye, A/HRC/29/92 ,*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Organización de las Naciones Unidas, 2015, disponible en: *http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx* (Consultado el 27 de enero de 2019).

70 El tema del cifrado tomó mayor relevancia en la conciencia pública derivado de la solicitud de FBI (*Federal Bureau of Investigation*) hacia la empresa Apple Inc., para colaborar en la investigación de los ataques terroristas que tuvieron verificativo en diciembre del año 2015 en San Bernardino, California. En esa ocasión el FBI solicitaba a la empresa la creación de una versión del sistema operativo de iPhone, que fuera capaz de evadir los sistemas de seguridad, lo que, bajo el argumento de la empresa, dicho *software* tendría el potencial para desbloquear cualquier dispositivo de esa clase y poner en riesgo la privacidad de sus usuarios. Para entender el contexto, la criptografía presupone la utilización de un método general de cifrado y una clave de cifrado. Mientras que el primero consiste en el sistema para encriptar el texto, la clave es una cadena que selecciona uno de los muchos cifrados disponibles. El cifrado se emplea comúnmente para la elaboración de firmas digitales, con la finalidad de identificar al emisor del mensaje y garantizar el contenido del mismo (como en el caso de la firma electrónica empleada por el Sistema de Administración Tributaria). El cifrado implica la codificación de datos para que sólo los destinatarios deseados puedan acceder a ellos. Derivado de la controversia suscitada entre la empresa Apple Inc., y el FBI y como un reconocimiento a la importancia de proteger la privacidad de los usuarios, aplicaciones como *WhatsApp* han creado un cifrado para proteger las conversaciones.

Mucha de la información que fluye a través del ciberespacio se encuentra cifrada, lo que aporta un elemento mayor de seguridad. Empero, "si alguna vez se construyen computadoras cuánticas a gran escala, podrán romper muchos de los sistemas de cifrado de clave pública que actualmente se encuentran en uso"[71]. Lo anterior comprometería la confidencialidad y la integridad de las comunicaciones digitales que se llevan a cabo a través de Internet y en otros lugares.

En el *Consumer Electronics Show* (CES) 2019, se presentó "IBM Q System One", considerado el primer sistema de computación cuántica de aproximación universal integrado del mundo, diseñado tanto para uso científico como comercial[72]. De esta forma IBM inicia la carrera en el mercado de ordenadores cuánticos con fines comerciales. Si consideramos que muchos de nuestros protocolos de comunicaciones más importantes se basan principalmente en tres funcionalidades criptográficas básicas: cifrado de clave pública, firmas digitales e intercambio de claves.[73] Con el surgimiento del cómputo cuántico comercial se acrecientan los riesgos y amenazas. Consideramos "segura" nuestra información, toda vez que se encuentra cifrada. Empero, el cifrado actual no representa ninguna barrera ante la computación cuántica.

La criptografía post-cuántica o criptografía resistente a la computación cuántica, tiene como objetivo el desarrollo de sistemas criptográficos que sean seguros contra computadoras. El robo de una base de datos que se encuentre cifrada, con la tecnología cuántica, podrá ser conocida. Por ello debemos empezar a trabajar en la investigación y desarrollo de soluciones de cifrado postcuántico que enfrenten los retos que trae aparejado.

71 National Institutoe of Standards and Technology, "Post-Quantum Cryptography", NIST, 2017, disponible en: https://csrc.nist.gov/projects/post-quantum-cryptography (Consultado el 29 de enero de 2019)

72 IBM, "IBM Unveils World's First Integrated Quantum Computing System for Commercial Use", 08 de enero 2019, disponible en: https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use (Consultado el 22 de enero de 2019)

73 National Institute of Standards and Technology, "Report on Post-Quantum Cryptography", NISTIR 8105, 2016, p. 1.

## Conclusiones

> *La ciberseguridad global implica una tremenda gama de problemas económicos, de privacidad y de seguridad nacional.* [74]

¿Entendemos las amenazas? No. A esto le sumamos una falta de unanimidad y claridad respecto a cómo afrontarlas. Igual que cualquier otra tecnología, el ciberespacio, empleado por las manos equivocadas representa un peligro importante para los individuos, las empresas, Estados y sociedades por igual. Empero lo anterior no significa que debamos desconectarnos y asilarnos de las bondades que esta tecnología y las TIC han traído consigo en pro de la humanidad.

Necesitamos emplear un enfoque holístico dentro de la ciberseguridad. Conocer cuáles son las amenazas que enfrenta el Estado y analizarlas. Conocer a los responsables de su planeación y financiación. Entender los riesgos e implementar una adecuada gestión de éstos. La falta de una visión completa de la problemática acrecienta los riesgos y tiene efectos al momento de decidir un curso de acción. toda vez que se carece de una visión de los impactos en el ámbito jurídico, estratégico, económico y político, a largo plazo, de cualquier decisión que se tome.

Otro reto que se presenta son las consideraciones éticas que trae consigo el uso de las ciberarmas y la guerra cibernética en general. Las ciberarmas son una nueva clase de armas, la guerra cibernética es una nueva clase de guerra. Al igual que sucede con la guerra tradicional, existen principios éticos que son seguidos por algunos actores, mientras que otros no tienen el mismo impulso de actuar éticamente. También resulta esencial identificar de manera concreta, las acciones que violen las pautas éticas acordadas en instrumentos internacionales. Esto nos permitirá resaltar el mal comportamiento en el ámbito internacional y responsabilizar a los perpetradores.

74 Martha Finnemore & Duncan B. Hollis, "Constructing Norms for Global Cybersecurity", The American Journal of International Law, Vol. 110, No. 3, 2016, pp. 425-479 (430)

No pueden trasladarse todas las experiencias y estrategias desarrolladas en el mundo físico al ciberespacio. La novedad y constante evolución de la tecnología plantea un serio un problema. Por ello la SN necesita actuar a la velocidad de las redes. El ciberespacio "no es un sistema de soporte aislado sino un ecosistema multidimensional que tiene que funcionar perpetuamente y de manera resistente, libre de amenazas o posibilidades de daño"[75]. Necesitamos crear un ecosistema cibernético resiliente. Podemos automatizar algunas herramientas en la implementación de la ciberseguridad, siempre que la toma de decisiones sea humana. Una ayuda pueden ser los sistemas de IA aplicados al rastreo y mitigación de riesgos. Lo anterior debe ir de la mano con la capacitación constante de la fuerza laboral de ciberseguridad, permitiéndoles adaptarse y responder a las amenazas conocidas y a las desconocidas, las cuales emplean técnicas y procedimientos tácticos aún no creados.

No necesitamos una militarización del ciberespacio. Necesitamos coordinación y colaboración, seguridad y resiliencia. Pero no restricciones arbitrarias ni violatorias de derechos humanos. Este espacio que llamamos ciberespacio es un lugar y herramienta en donde ejercemos nuestros derechos humanos, en especial la libertad de expresión, acceso a la información, pero donde principalmente peligran otros como la privacidad, la protección de nuestra información.

Para España, los esfuerzos por diseñar un sistema eficaz de gobernanza sobre las nuevas tecnologías son la clave para la Seguridad Nacional.[76] En nuestro caso también deberían serlo. La importancia de una Agenda Digital coherente. Coherente con las amenazas, riesgos, políticas y su implementación. Coherente con los *multistakeholders* que conforman el ecosistema del ciberespacio. Reforzados con sistemas fuertes de *accountability* para el gobierno y las empresas en materia de ciberseguridad, lo que podría ayudar a mitigar los riesgos.

75 Paul Cornish, "Cyber Warfare and Homeland Security", en Kostopolous, George, *Cyberspace and Cybersecurity*, Segunda Edición, CRC Press, Florida, p. 175.

76 Presidencia del Gobierno, "Estrategia de Seguridad Nacional 2017", España, 2017, p. 35.

Necesitamos una política clara, conformada por un consenso compartido, formado por una discusión informada y creada por un cuerpo común de conocimiento. No se deben tomar decisiones a la ligera, ni a favor de un solo sector, de las cuales desconocemos sus impactos a mediano y largo plazo.

## BIBLIOGRAFÍA

Arquilla, John & Ronfeldt, David, "CYBERWAR IS COMING!", *RAND*, National Security Research División, 1993, disponible en: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf (Consultado el 29 de enero de 2019)

Asamblea General de Naciones Unidas, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)*, 14 de septiembre 2011, disponible en: http://undocs.org/A/66/359 (Consultado el 18 de diciembre de 2019)

BBC, "US launches cyber security plan," 29 mayo 2009, disponible en: http://news.bbc.co.uk/2/hi/americas/8073654.stm (Consultado el 20 de enero de 2019)

Consejo de Derechos Humanos de la Organización de Naciones Unidas, Resolución A/HRC/20/L.132 de 29 de junio 2012, disponible en: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf (Consultado el 20 de enero de 2019)

Cornich, Paul "Cyber Warfare and Homeland Security", en Kostopolous, George, *Cyberspace and Cybersecurity*, Segunda Edición, CRC Press, Florida, 2017.

Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe", *WIRED MAGAZINE*, agosto 21, 2007, disponible en https://www.wired.com/2007/08/ff-estonia/ (Consultado el 26 de enero de 2019)

Departamento de Defensa de Estados Unidos de América, "Cyberspace Operations Lexicon", disponible en: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf (Consultado el 26 de enero de 2019)

Departamento de Defensa de Estados Unidos de América, "The National Military Strategy for Cyberspace Operatios", diciembre 2006, disponible en: https://www.hsdl.org/?view&did=35693 (Consultado el 20 de enero de 2019)

Demchak, Chris, "Economic and Political Coercion and a Rising Cyber Westphalia", *Pacetime Regime for State Activities in Cyberspace*, CCDCOE NATO, 2013.

Dipert, Randall, "Other-tahn-Internet (OTI) cyberwarfare: challenges for ethics, law and policy", *Journal of Military Ethics*, 12(1), abril, 2013, disponible en: https://www.researchgate.net/publication/263529399_Other-than-internet_oti_cyberwarfare_Challenges_for_ethics_law_and_policy (Consultado el 27 de enero de 2019)

Droege, Cordula (ICRC Legal Adviser), "No legal vacuum in cyber space", entrevista 16 de agosto 2011, *ICRC Resource Centre,* disponible en: https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (Consultado el 28 de enero de 2019)

Elisan, Christopher, "Malware, Rootkits, and Botnets: A Beginner,s Guide", McGraw Hill, 2013.

European Union Agency for Network and Information Security, "Analysis of the European R&D Priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe", European Union Agency for Network and Information Security, 2018, disponible en: https://www.enisa.europa.eu (Consultado el 24 de enero 2019)

European Union Agency for Network and Information Security, "ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends", European Union Agency For Network and Information Security, 2019, disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (Consultado el 28 de enero 2019)

Finnemore, Martha & Hollis, Duncan B., "Constructing Norms for Global Cybersecurity", *The American Journal of International Law*, Vol. 110, No. 3, 2016, pp. 425-479.

Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado el 29 de enero de 2019)

Giles, Keir, "Handbook of Russian Information Warfare", NATO Defense College, Roma, 2016, disponible en:

https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf (Consultado el 25 de enero de 2019)

Gobierno de Canadá, "Canada´s Cybersecurity Strategy. For a stronger and more prosperous Canada", 2010, disponible en: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx (Consultado el 23 de enero de 2019)

Gobierno de Estados Unidos de América, "United States National Strategy to Secure Cyberspace", 2003, disponible en: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Consultado el 28 de enero de 2019)

Heickerö, Roland, "Emerging Cyber Threats and Russian -views on Information. Warfare and Information Operatios", FOI, Swedish Defence Research Agency, 2010, disponible en: http://www.highseclabs.com/data/foir2970.pdf (Consultado el 29 de enero de 2019)

IBM, "IBM Unveils World's First Integrated Quantum Computing System for Commercial Use", 08 de enero 2019, disponible en: https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use (Consultado el 22 de enero de 2019)

International Committee of the Red Cross, *Cyberwarfare and international humanitarian law: the ICRC's position*, ICRC, 2006, disponible en: https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf (Consultado el 25 de enero de 2019)

Isaac, Mike & Frenkel, Sheera, "Facebook Security Breach Exposes ccounts of 50 Millon Users", *The New York Times*, 28 de septiembre 2018, disponible en: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (Consultado el 28 de enero de 2019)

Kerner, Sean, "Estonia Under Russian Cyberattack?", *Security*, mayo 18, 2007, disponible en: http://www.internetnews.com/security/article.php/3678606/Estonia+Under+Russian+Cyber+Attack.htm (Consultado el 26 de enero de 2019)

Laity, Mark, Chief of Strategic Communications, Supreme Headquarters Allied Powers Europe (SHAPE), *Russia: Implications for UK defence and security*, House of Commons, Reino Unido, disponible en: https://publications.parliament.uk/pa/cm201617/cmselect/

cmdfence/107/10705.htm (Consultado el 29 de enero de 2019)

Ministerio de Asuntos Exteriores de Rusia, "Convention on International Information Security", 22 de septiembre 2011, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (Consultado el 27 de enero de 2019).

Müller, Enrique, "Alemania Sufre el mayor "hackeo" de su historia con la filtración. De datos personales de centenares de políticos", *El País Internacional*, 04 de enero de 2019, disponible en: https://elpais.com/internacional/2019/01/04/actualidad/1546595085_679572.html (Consulado el 20 de enero 2019)

National Institute of Standards and Technology, "Post-Quantum Cryptography", NIST, 2017, disponible en: https://csrc.nist.gov/projects/post-quantum-cryptography (Consultado el 29 de enero de 2019)

National Institute of Standards and Technology, "Report on Post-Quantum Cryptography", NISTIR 8105, 2016.

Presidencia de Gobierno, "Estrategia de Seguridad Nacional 2017", España, 2017, disponible en: http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (Consultado el 27 de enero de 2019)

Presidencia de Gobierno, "Estrategia de Seguridad Nacional. Un proyecto compartido de todos para todos", Presidencia del Gobierno, España, 2017, disponible en: http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (Consultado el 27 de enero de 2019)

Rid, Thomas & McBurney, Peter, "Cyber-Weapons", *The RUSI Journal*, 157;1, 2012, disponible en: https://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354 (Consultado el 29 de enero de 2019)

Reuter, Markus, "Alles außer AfD: Was wir über das große Datenleck wissen", *Netzpolitik.com*, 04 de enero 2019, disponible en: https://netzpolitik.org/2019/alles-ausser-afd-was-wir-ueber-das-grosse-datenleck-wissen/ (Consultado el 20 de enero de 2019)

Robinson, Michael & Jones, Kevin & Janicke, Helge "Cyber warfare: Issues and challenges", *Computers & Security*, 2015, 49, pp. 70-94, disponible en: https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges (Consultado el 10 de enero de 2019)

Rowe, Neil "Distinctive ethical challenges of cyberweapons", in Tsagourias, Buchan, Russell, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, Massachusetts, 2017, pp. 307-326

Shanghai Cooperation Organization, "International Code of Conduct For Information Security (SCO)", 2011, disponible en: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609563C11.pdf (Consultado el 29 de enero 2019)

Thomas, Thimoty L., "Information Security Thinking: A Comparation of U.S., Russian and China Concepts", *Foreign Miltary Studies Office*, julio 2001, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Consultado el 20 de enero de 2019)

Union Internacional de Telecomunicaciones (UIT), Rec. ITU-T X.1209 (12/2019), *Capabilities and their context scenarios for cybersecurity information sharing and exchange*, ITU-T X-Series Recommendations, UIT, 2010.

Unique Identification Authority of India, "*What is Aadhaar?*", Government of India, disponible en: https://uidai.gov.in/what-is-aadhaar.html (Consultado el 28 de enero de 2019)

Valeriano, Brandon & Maness, Bryan C., "Cyber War Versus Cyber Realities: Cyber Conflict in the International System", Oxford University Press, Oxford, 2015.

Resoluciones de la Asamblea General de Naciones Unidas
A/RES/55/28 de 20 de noviembre del año 2000
A/RES/56/19 de 29 de noviembre de 2001
A/RES/58/32 de 08 de diciembre de 2003
A/RES/58/199 de fecha 30 de enero 2004
A/RES/59/61 de 3 de diciembre de 2004
A/RES/60/45 de 8 de diciembre de 2005
A/RES/61/54 de 6 de diciembre de 2006
A/RES/62/17 de 05 de diciembre de 2007
A/RES/63/37 de 2 de diciembre de 2008