Revista Política y Estrategia
Nº 138, (2021)

Editada por: **Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) Chile**.

Lugar de edición: Santiago, Chile

Dirección web: http://www.politicayestrategia.cl

ISSN versión digital: 0719-8027

ISSN versión impresa: 0716-7415

DOI: https://doi.org/10.26797/rpye.v1i138.957

Para citar este artículo / To cite this article: TORRIJOS Rivera, Vicente y JIMÉNEZ Salcedo, Daniel: "¿Seguridad sin fronteras, seguridad en abstracto? Tendencias en el estudio de la ciberseguridad y la ciberdefensa".

Revista Política y Estrategia N° 138. 2021. pp. 141-164

DOI: https://doi.org/10.26797/rpye.v1i138.957

Si desea publicar en Política y Estrategia, puede consultar en este enlace las Normas para los autores:

To publish in the journal go to this link:

http://politicayestrategia.cl/index.php/rpye/about/submissions#authorGuidelines

¿SEGURIDAD SIN FRONTERAS, SEGURIDAD EN ABSTRACTO? TENDENCIAS EN EL ESTUDIO DE LA CIBERSEGURIDAD Y LA CIBERDEFENSA ∞

VICENTE TORRIJOS RIVERA*
DANIEL JIMÉNEZ SALCEDO**

RESUMEN

Si bien la tecnología digital aporta importantes beneficios económicos y sociales a gran parte de la población, cuestiones como el acceso desigual a la Internet, la falta de un sistema mundial de gobernanza de la tecnología y la inseguridad cibernética plantean un riesgo importante para la seguridad internacional. La falta de una gobernanza tecnológica mundial y la presencia de puntos ciegos de seguridad cibernética aumentan el riesgo de fragmentación del ciberespacio y de reglamentos tecnológicos que compiten entre sí. Todo esto nos lleva a decir que vivimos en un mundo sin fronteras en términos de ciberseguridad. Debido a esta alarmante situación, trataremos de identificar los principales desafíos de la ciberseguridad, los cuales representan un riesgo alarmante para la paz y la seguridad internacionales. En primer lugar, será abordada la amenaza que suponen los ciberataques, la ciberprivacidad, la ciberdelincuencia y la ciberguerra. Luego se hará énfasis en los riesgos y la resistencia sistémicos, la "seguridad de las cosas/ security of things" y la protección de las infraestructuras críticas. Finalmente, se propone un análisis de las nuevas reglas de colaboración y las implicaciones de las cuestiones de ciberseguridad en el derecho internacional. Todo esto se hará teniendo en cuenta la situación política internacional;

Palabras clave: *Ciberataque; ciberseguridad; ciberguerra; tecnología; resistencia; Seguridad Nacional; relaciones internacionales.*

---

* Analista político, escritor y periodista con especialidad en Opinión Pública, Magíster en Estudios Políticos, postgraduado en Altos Estudios Internacionales. Profesor Titular de la Escuela Superior de Guerra y Profesor Adjunto en la National Defense University / W.J. Perry Center, Washington DC. vicentetorrijos@hotmail.com ORCID: https://orcid.org/0000-0003-3837-6196

** Internacionalista y politólogo con maestría en Política Internacional de Sciences Po Bordeaux. Consultor del Departamento de Relaciones Externas de la Organización de Estados Americanos. danieljsal@gmail.com ORCID: https://orcid.org/0000-0001-6443-157X

∞ Fecha de recepción: 040320 - Fecha de aceptación: 161221.

SECURITY IN ABSTRACT, SECURITY WITHOUT BORDERS? TRENDS IN THE STUDY OF CYBERSECURITY AND CYBERDEFENSE

ABSTRACT

While digital technology brings significant economic and social benefits to much of the population, issues such as unequal access to the Internet, the lack of a global system of technology governance and cyber insecurity pose a significant risk to international security. The lack of global technology governance and the presence of cyber security blind spots increase the risk of fragmented cyberspace and competing technology regulations. All this leads us to say that we live in a world without borders in terms of cybersecurity. Because of this alarming situation, we will try to identify the main cybersecurity challenges, which represent an alarming risk to international peace and security. First, we will address the threat posed by cyberattacks, cyber privacy, cybercrime and cyberwar. We will then move on to systemic risk and resilience, the "security of things" and critical infrastructure protection. Finally, we will analyze the new rules of collaboration and the implications of cybersecurity issues in international law. All of this will be done taking into account the actual international political situation.

Key words: *Cyberattack; cybersecurity; cyberwarfare; technology; resilience; National Security; international relations.*

SEGURANÇA SEM FRONTEIRAS, SEGURANÇA EM ABSTRACTO? TENDÊNCIAS NO ESTUDO DA CIBER-SEGURANÇA E DA CIBERDEFESA

RESUMO

Embora a tecnologia digital traga benefícios econômicos e sociais significativos para grande parte da população, questões como o acesso desigual à Internet, a falta de um sistema global de governança tecnológica e a insegurança cibernética representam um risco significativo para a segurança internacional. A falta de governança global da tecnologia e a presença de pontos cegos de segurança cibernética aumentam o risco de fragmentação do ciberespaço e de regulamentações tecnológicas concorrentes. Tudo isso nos leva a dizer que vivemos num mundo sem fronteiras em termos de segurança cibernética. Devido a esta situação alarmante, vamos tentar identificar os principais desafios da cibersegurança, que representam um risco alarmante para a paz e segurança internacional. Primeiro, abordaremos a ameaça que representam os ataques cibernéticos, a ciberprivacidade, o crime cibernético e a guerra cibernética. Em seguida, passaremos ao

risco sistêmico e à resiliência, à "segurança das coisas" e à proteção da infra-estrutura crítica. Finalmente, analisaremos as novas regras de colaboração e as implicações das questões de segurança cibernética no direito internacional. Tudo isso será feito levando em conta a situação política internacional.

Palavras-chave: *Cyberattack; segurança cibernética; guerra cibernética; tecnologia; resiliência; Segurança Nacional; relações internacionais.*

Introducción

Tradicionalmente, las guerras se han desarrollado por tierra, mar y aire, mirando frente a frente al enemigo y luchando en el mismo tiempo y espacio. Muchos de los conflictos internacionales se han originado por la defensa de las fronteras las cuales han dejado de ser simples líneas imaginarias en un mapa para convertirse en barreras físicas a través de ríos o murallas. Con la llegada de una nueva década vale la pena reflexionar sobre cuáles son los riesgos para que se presente un conflicto internacional y sobre qué dominio de la guerra podría desarrollarse. El avance tecnológico en términos digitales ha llevado a que cualquiera que sea el instrumento que se fuese a utilizar en un conflicto, va a estar ligado con una red, es decir con el ciberespacio. En ese sentido, se puede postular la idea que cualquier futuro conflicto entre actores razonablemente avanzados será un conflicto cibernético. Ningún atacante moderno resistirá destruir, interrumpir o confundir los sensores, las comunicaciones y los circuitos de toma de decisiones del enemigo. Lo que variará es si el conflicto tendrá lugar también en los dominios físicos. Esta percepción cambiará la naturaleza del conflicto de manera fundamental y, posiblemente, reducirá el umbral de la guerra y confundirá la propia distinción entre la guerra y la paz.

La incertidumbre geopolítica y geoeconómica, incluida la posibilidad de que el ciberespacio esté fragmentado, también amenaza con impedir que se desarrolle todo el potencial de las tecnologías de la próxima generación. El reporte global de riesgos 2020, expedido por el foro económico mundial, calificó el "colapso de la infraestructura de la información" como el sexto riesgo más impactante hasta el año 2030[1]. La falta de una gobernanza mundial de la tecnología y la presencia de puntos ciegos de seguridad cibernética aumentan el riesgo de un ciberespacio fragmentado y regulaciones tecnológicas que compiten entre sí. Todo esto nos lleva a afirmar que vivimos en un mundo sin fronteras en materia de ciberseguridad. Debido a esta alarmante situación trataremos de determinar los principales desafíos en materia de ciberseguridad, los cuales representan un alarmante riesgo para la paz y seguridad internacionales. En primer lugar, trataremos la amenaza que representan los ciberataques, la ciber privacidad, el cibercrimen y la ciberguerra. Luego continuaremos con el riesgo sistémico y resistencia, la "seguridad de las cosas/ security of things" y protección de la infraestructura crítica. Finalmente se analizarán las nuevas normas de colaboración y las implicaciones en el derecho internacional de las cuestiones de ciberseguridad. Todo esto teniendo en cuenta la coyuntura política internacional.

1 World Economic Forum**.** *The Global Risks Report.* Geneva : World Economic Forum, 2020.

Los riesgos en una nueva década

De acuerdo con el Global Risks Perception Survey del foro Económico Mundial, la comunidad de actores y los forjadores globales identifican los problemas relacionados con el ciberespacio, como los ciberataques y el fraude o robo de datos, dentro de la lista de los 10 principales riesgos a largo plazo. No es para manos, pues incluso en los más frágiles tiempos de la pandemia del COVID- 19 que ha tenido que afrontar el mundo, los ciberataques y robo de datos han sido recurrentes en la coyuntura internacional.

La Organización Mundial de la Salud (OMS) ha prendido las alertas de la comunidad internacional anunciando que desde el comienzo de la pandemia del COVID-19 ha visto un aumento dramático en el número de ataques cibernéticos dirigidos a su personal y de estafas por correo electrónico dirigidas al público en general[2]. Los estafadores que se hacen pasar por la OMS en los correos electrónicos también se han dirigido cada vez más al público en general para canalizar las donaciones a un fondo ficticio y no al auténtico Fondo de Respuesta Solidaria de COVID-19. El número de ataques cibernéticos es ahora más de cinco veces mayor que el número dirigido a la Organización en el mismo período del año 2019[3].

En este contexto también han surgido tensiones entre los Estados a raíz de supuestos ataques cibernéticos para el robo de información relacionada con el desarrollo de la vacuna contra el coronavirus. El Centro Nacional de Seguridad Cibernética de Gran Bretaña anunció coordinadamente con las autoridades de los Estados Unidos y Canadá que el grupo APT 29, también conocido como Cozy Bear, está atacando a las instituciones de investigación académica y farmacéutica que participan en el desarrollo de la vacuna contra el coronavirus. Este grupo, según las autoridades británicas, hace parte del servicio de inteligencia ruso[4]. Por su parte, el embajador de Rusia ante el Reino Unido declaró que no cree en esa historia y que no ve ninguna razón para usar este tema como un asunto de interferencia[5].

Este tipo de acusaciones se inscriben en un contexto en el que los países de la OTAN han denunciado en múltiples ocasiones a los Estados Miembros de la Organización de Cooperación de Shanghái (OCS), en particular a China y Rusia, de perpetuar ataques en contra de sus agencias gubernamentales u otro tipo de instituciones con información confidencial. Estas acusaciones han sido constantemente rechazadas por los gobiernos de los países de la OCS, como se expondrá más adelante.

La seguridad en el quinto dominio de la guerra

El ciberespacio se ha convertido en el quinto dominio de la guerra, llevando a que los estudios sobre seguridad y defensa internacionales consideren este último como un esce-

2 WHO. World Health Organization. *WHO reports fivefold increase in cyber attacks, urges vigilance.* [Online] 04 2020. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

3 Ibíd.

4 British National Cybersecurity Center. *APT29 targets COVID-19 vaccine development. [Online] 7 2020. https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development*

5 KELIN, Andrei. BBC. *Russia's UK ambassador rejects coronavirus vaccine hacking allegations.* [Online] 07 2020. https://www.bbc.com/news/uk-53458122

nario amenazante para los Estados. Dada la relevancia que ha adquirido este escenario es de señalar el debate académico existente sobre el significado del término seguridad para inscribirlo dentro del marco de lo que se ha llegado a denominar como ciber seguridad. En dicho debate se pueden distinguir dos corrientes principales conocidas como los tradicionalistas y los no tradicionalistas. Los primeros, defienden el concepto tradicional de la seguridad el cual es mucho más estrecho en su concepción en tanto defienden una postura realista sobre el término. En ese sentido sostienen la idea de que, primero, seguridad equivale a la seguridad nacional o del estado de posibles agresiones externas. Y, en segundo lugar, esas agresiones externas "son amenazas de carácter militar y tercero, esas amenazas son identificables y objetivas"[6].

Por el otro lado, están los no tradicionalistas quienes se han preocupado porque el término de seguridad sea mucho más amplio. Las redefiniciones de la seguridad incorporan nuevos temas no militares como el medio ambiente, las drogas ilícitas, la migración, la pobreza entre otros. En ese sentido, gran parte del debate sobre el término de seguridad reside en la tensión respecto a que los primeros no incluyen temas no tradicionales ni actores no estatales mientras que los últimos sí.

En la actualidad, la seguridad como elemento político clave en la escena internacional, se compone de nuevas dimensiones que se suman a las consideradas tradicionales. La difusión masiva que se está produciendo de la información en la nube, ligado a la implantación de las tecnologías de la información y comunicación como las principales herramientas de trabajo, están trayendo grandes beneficios a organizaciones y empresas de todo tipo (tanto en el sector público como privado), pero a la vez están produciendo grandes problemas de seguridad y de protección de datos y privacidad que será preciso afrontar.

Así surge la cuestión de la ciberseguridad como un elemento adicional dentro de los estudios de seguridad tanto a nivel nacional como internacional. El término "ciberseguridad" ha sido objeto de la literatura académica y se utiliza ampliamente dado que sus definiciones son muy variables, vinculadas al contexto, a menudo subjetivas y, a veces, poco informativas. No obstante, la definición propuesta por la Unión Internacional de Telecomunicaciones de las Naciones Unidas (UIT) incluye un conjunto de elementos que permiten señalar las principales características de este concepto. "La seguridad cibernética es el conjunto de instrumentos, políticas, directrices, enfoques de gestión de riesgos, medidas, capacitación, prácticas óptimas, garantías y tecnologías que pueden utilizarse para proteger el entorno cibernético y los activos de la organización y del usuario"[7]. Esta definición alude a los principales temas a tratar cuando se habla de ciber seguridad, pues se hace alusión a estrategias, procesos y métodos con una naturaleza interdisciplinar que requieren de la intervención humana para sacar adelante soluciones tecnológicas que se ven reflejadas en políticas y acciones que buscan la protección en un escenario amenazante.

---

6 ŠULOVIĆ, Vladimir. (2010). "*Meaning of Security and Theory of Securitization*". Belgrade Centre for Security Policy? Retrieved from http://www.bezbednost.org/upload/document/sulovic_(2010)_meaning_of_secu.pdf

7 ITU. Definition of cybersec*urity. ITU. [Online] 2020. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets*

Por su parte, la ciberdefensa se centra en "la prevención, la detección y la respuesta oportuna a los ataques o amenazas para que no se altere ninguna infraestructura o información"[8]. Con el aumento del volumen y la complejidad de los ciberataques, la ciberdefensa es esencial para la mayoría de las entidades a fin de proteger la información sensible y salvaguardar los activos. En ese sentido el termino de ciber defensa está encaminado a la capacidad de respuesta ante la presencia de un ataque en el ámbito del ciberespacio.

El ciberespacio les permite a los atacantes realizar varias agresiones en distintos momentos al mismo tiempo; y esos ataques, a pesar de ser dirigidos en el mundo virtual, afectan lo real. En ese sentido, las ciber amenazas se han convertido, sin lugar a duda, en uno de los principales temas en la agenda de seguridad de todo el mundo. Por ello, la prevención de cualquier ciberataque se convierte en una prioridad en la agenda internacional. Debido al alto grado de dependencia que estos sectores presentan del espacio cibernético y de las tecnologías de la información y de la comunicación, un fallo en la red o una incidencia sobre esta podría suponer una vulnerabilidad y/o amenaza en materia de seguridad en cualquiera de estos sectores. Todo esto destaca la necesidad de realizar acciones que doten a esta nueva realidad de una estrategia de ciberseguridad en la que se identifique el conjunto de amenaza a las cuales el Estado debe responder.

La Conferencia de Plenipotenciarios de la UIT es el foro donde se reúnen los delegados más importantes del sector de las tecnologías y telecomunicaciones en representación tanto del sector privado como de los Estados. En estas conferencias se han confrontado dos visiones sobre la ciber gobernanza global. Por un lado, está la visión de los Estados occidentales los cuales defienden que la web global debe ser manejada por empresas privadas, grupos de la sociedad civil y los usuarios de Internet, mas no por los gobiernos[9].

Por el otro lado está la visión de Estados como China y Rusia los cuales han propuesto un modelo basado en el control del Estado. Esto quiere decir que buscarían aprobar que los gobiernos tengan permiso para llevar el control del contenido y la estructura de la web dentro de sus fronteras. Así mismo, defienden que el Estado esté en la capacidad de restringir el acceso a ciertos portales de internet y llevar un monitoreo sobre los individuos mirando el uso que le dan a la red. A estas propuestas se han sumado varios Estados árabes quienes argumentan que debería existir una identificación universal de los usuarios de internet. Esta multiplicidad de posiciones ha llevado a que la gobernanza sobre el dominio del ciberespacio aún tenga un largo camino por recorrer. La UIT no es aún una organización que unifique el actuar de los Estados sobre este tema, pues como se mencionó anteriormente las tensiones entre los Estados son recurrentes, sumado a que es un escenario donde adjudicar el ataque a un actor en específico representa aún un gran desafío tanto en términos tecnológicos como de jurisprudencia internacional.

8 GALINEC, Darko. Cybersecurity and cyber defence: national level strategic approach. [Online] 2017. https://www.tandfonline.com/doi/full/10.1080/00051144.2017.1407022

9 ITU. ITU NATIONAL Cybersecurity Strategy Guide. [Online] 2020. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

Las ciberamenazas

No se puede negar que posiblemente se está viviendo el momento de mayor interconexión en la historia de la humanidad. A pesar de las ventajas que esto representa, también puede servir como una herramienta usada para generar daño. Así lo plantea Susan Brenner en el artículo "Cyberterrorism: how real is the threat?" cuando argumenta que el espacio cibernético es el más peligroso porque no existen fronteras entre los Estados[10]. Las ciberamenazas se han convertido, sin lugar a duda, en uno de los principales temas en la agenda de seguridad de todo el mundo. Incluso para las grandes potencias como Estados Unidos mantenerse seguro en el ciberespacio se ha convertido en otro de los propósitos planteados con el fin de defender sus intereses nacionales[11]. Esto ocurre dado que en la actualidad el ciberespacio le permite tanto a los Estados como a los actores no estatales la posibilidad de afectar la actividad económica, política y de seguridad de una nación.

Ahora bien, es importante tener en cuenta que los ciberataques no son conducidos únicamente por actores individuales sino también por Estados. Para el gobierno de Estados Unidos los principales perpetradores estatales de ataques cibernéticos en el año 2018 fueron Rusia, China, Irán y Corea del Norte[12]. Los ataques de estos últimos se pueden dar en el marco del espionaje, robo de información, entre otros.

Es por esto que el espacio cibernético se ha convertido en un elemento crítico del cual no solo los sectores económicos y productivos dependen, sino que el Estado mismo debe tener en consideración. Las operaciones bancarias y financieras tanto nacionales como internacionales, la infraestructura, medios de transporte, el sector energético y el sanitario, dependen en gran medida de nuevas tecnologías relacionadas con el uso de internet. Debido al alto grado de dependencia que estos sectores presentan del espacio cibernético y de las tecnologías de la información y de la comunicación, un fallo en la red o una incidencia sobre la misma podría suponer una vulnerabilidad y/o amenaza en materia de seguridad en cualquiera de estos sectores[13]. Todo ello destaca la necesidad de realizar acciones que doten a esta nueva realidad de una estrategia de ciberseguridad.

Ataques cibernéticos se han producido cada vez con mayor frecuencia e impacto. Ya en el 2007 se había dado un ataque a la infraestructura financiera y comercial en Estonia. De igual forma en el 2010 ocurrió el sabotaje a las instalaciones nucleares de Irán por medio del gusano informático Stuxnet[14]. En este caso, el virus informático tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio

10 BRENNER, Susan. Cyberterrorism, how real is the threat? [Online] 05 20, 2016. [Cited: 02 17, 2020.] https://www.tandfonline.com/doi/abs/10.1080/01296612.2002.11726680.10.1080/01296612.2002.11726680

11 The White House**.** National Security Strategy. [Online] 12 2017. http://www.whitehouse.gov/wp-contnt/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

12 MATTIS, Jim. Summary of the National Defense Strategy . [Online] 2018. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

13 DAY, Paul. *Cyberattack.* Londres : Carlton books, 2014. 978178097533.

14 Ibíd.

instrucciones de autodestruirse[15]. Esta fue la primera vez que un ataque cibernético logró dañar la infraestructura nuclear de un Estado marcando así un hito en los temas de ciberseguridad. Más recientemente es importante señalar los casos de ciberataques en Arabia Saudita y Ucrania, los cuales deben prender las alertas del mundo puesto que la capacidad que tienen estos ataques para irrumpir en la cotidianidad de una nación y generar caos en distintos ámbitos de la sociedad significa una amenaza que en cualquier momento cualquier Estado podría sufrir.

El cibercrimen

Las bandas cibercriminales cada vez más organizadas varían sus tácticas, técnicas y procedimientos para evadir los controles de seguridad a nivel micro y la aplicación de la ley a nivel macro. Según cifras del Foro Económico Mundial, el cibercrimen le costó a la economía mundial más de 600.000 millones de dólares en 2017, y los pronósticos para 2018 predijeron 1,5 billones de dólares en pérdidas[16]. Durante los últimos cinco años se ha demostrado que este tipo de ataques solo se está volviendo más sofisticado con el tiempo, incorporando conocimientos técnicos con ingeniería social avanzada para centrar los esquemas en las víctimas que pueden producir mayores beneficios como empresas e individuos de alto valor[17].

Mientras que en años anteriores las bandas operaban como adversarios, ocupaban diferentes territorios e incluso se atacaban mutuamente con programas malignos, a partir de 2018 se conectó a las principales bandas de ciberdelincuentes en una colaboración explícita[18]. Esta tendencia es un signo negativo que pone de relieve cómo los distintos operadores unen sus fuerzas, revelando el factor de resistencia en estas operaciones. Ahora bien, los controles de seguridad adecuados y la educación de los usuarios, así como la respuesta planificada a los incidentes, pueden ayudar a mantener a raya esta amenaza y a contener sus efectos perjudiciales si alguna vez una cuenta es tomada y robada por delincuentes muy experimentados.

Sin embargo, persiste el problema de la atribución de la culpa de los ciberataques, ya que los atacantes pueden usar un proxy para impedir que sea detectado quien perpetúa el ataque. Por lo tanto, gran parte del énfasis hoy en día es mejorar la tecnología de atribución. Sin atribución, no hay represalias ni disuasión. Incluso con la tecnología adecuada, la cuestión de la atribución es delicada: decir todo lo que se sabe podría ser políticamente delicado y podría correr el riesgo de revelar capacidades críticas de inteligencia, lo que a su vez podría comprometer la capacidad de atribuir fuentes en el futuro.

15 Ibíd.

16 KASPERSEN, Anja. World Economic Forum. *Cyberspace: the new frontier in warfare.* [Online] 9 24, 2015. https://www.weforum.org/agenda/2015/09/cyberspace-the-new-frontier-in-warfare/

17 HATHAWAY, Oona A., CROOTOF, Rebecca, PERDUE, William, LEVITZ, Philip, NIX, Haley, NOWLAN, Aileen & SPIEGEL, Julia T*he Law of Cyber-Attack,.* California : 100 California, 2018.

18 KESSEM, Limor. Security Intelligence. *The Business of Organized Cybercrime: Rising Intergang Collaboration in 2018.* [Online] 3 20, 2019. [Cited: 02 16, 2020.] https://securityintelligence.com/the-business-of-organized-cybercrime-rising-intergang-collaboration-in-2018/

Ciberguerra

Es importante aclarar que dentro de los ataques cibernéticos se pueden distinguir dos modalidades. Según lo explica Dorothy Denning[19], por un lado, se puede hablar de la ciberguerra, por el otro, del ciberterrorismo[20]. La ciberguerra se presenta cuando los Estados actúan mediante el uso del ciberespacio para afectar otro Estado. En ese sentido, la ciberguerra es un conflicto informático o de red que involucra ataques de motivación política de un Estado-nación en otro Estado-nación. En este tipo de ataques, los actores del Estado-nación intentan interrumpir en las actividades de las organizaciones o Estados-naciones, especialmente con fines estratégicos o militares y ciberespionaje[21]. El uso de ciberataques como una herramienta de política exterior había sido esporádico a principios de siglo. Sin embargo, Rusia, Irán y Corea del Norte están provocando ataques más agresivos en contra de Estados Unidos[22]. Según cifras de la dirección de inteligencia nacional de Estados Unidos, en el año 2011 alrededor de 10 Estados contaban con capacidad para perpetuar ciberataques, pero para el año 2017 ya más de 30 Estados cuentan con dicha capacidad[23].

Además de eso, es relevante destacar el hecho de que ahora mismo vivimos bajo un espacio anárquico y virtual de Internet. Más de veinte ejércitos nacionales tienen ahora unidades cibernéticas preparándose y luchando en el ciberespacio, y el ritmo de los asaltos a información crítica, sistemas e infraestructura física se está acelerando. Las defensas nacionales de hoy en día dependen de las tecnologías de la información y la conexión a través de Internet o redes. El comercio internacional, la producción de electricidad, e incluso el control de las armas nucleares dependen del ciberespacio[24]. Mientras tanto, el uso de operaciones cibernéticas defensivas está aumentando. Es por ello que se está buscando llegar a un acuerdo internacional de control de armas, dado que las aplicaciones del control de armas a la guerra cibernética se vuelven más claras.

Ciberterrorismo

Por otro lado, está el ciberterrorismo el cual se puede definir como un ataque premeditado, motivado políticamente en contra de información, sistemas y programas informáticos que resultan en violencia en contra de objetivos no combatientes por parte de agentes no nacionales[25]. En ese sentido, esta táctica es utilizada por los grupos terroristas con el fin de perpetuar un ataque dando lugar a la violencia contra personas o propiedades, o al menos causar suficiente daño para generar miedo[26]. El uso del internet se convierte así en una herramienta fundamental pues es la que les permite a los miembros de la organización comunicarse y coordinar eventos, pero también es el medio con el cual pueden irrumpir en

19 DENNING, Dorothy. 2000. *Cyberterrorism.* Information Warfare and Security, pp. 1-10.

20 DENNING, Dorothy. *Cyberwarfare.* s.l. : IEFE, 2011, Vols. Sptember-October.

21 Ibíd.

22 MATTIS, Jim. Loc. Cit.

23 Department of State of the United States. US Department of State. *Country Reports on Terrorism 2018.* [Online] 2018. [Cited: 02 17, 2020.] https://www.state.gov/reports/country-reports-on-terrorism-2018/

24 DAY, Paul. Loc. Cit.

25 Ibíd.

26 DENNING, Dorothy. 2011. Loc. Cit.

la cotidianidad de las personas y generar grandes impactos. Es importante señalar que para 1998 el Departamento de Estado de Estados Unidos apenas registraba en la web a 12 de 30 organizaciones terroristas, mientras que en la actualidad todas ellas tienen actividad en la web[27]. Esto ha provocado que el ciberespacio esté constantemente bajo asalto.

Ciber espías, ladrones y saboteadores irrumpen en los sistemas informáticos para robar datos personales y secretos comerciales, afectar los sitios web, interrumpir servicios, sabotear datos y sistemas, lanzar virus y gusanos informáticos, realizar fraude en transacciones, y hostigar a individuos y compañías. Estos ataques son facilitados con herramientas de software cada vez más potentes y fáciles de usar, que están disponibles de forma gratuita desde miles de sitios web en Internet. Por todo esto se puede decir que el ciberterrorismo ocurre en el ciberespacio, pero tiene repercusiones en el mundo real. Esa afectación del mundo real suele darse sobre la infraestructura crítica. No obstante, esto ha sido motivo de debate puesto que hay quienes argumentan que es posible que exista una mayor probabilidad de que los grupos terroristas se especialicen en este tipo de ataque mientras hay quienes son más escépticos frente a dicha posibilidad. Esto considerando la capacidad técnica y tecnológica que puedan llegar a tener las distintas organizaciones terroristas para poder generar la suficiente incidencia e impacto en el ciberespacio. Pues vale la pena recordar que el fin último de este tipo de ataques es generar repercusiones políticas.

Ahora bien, vale la pena señalar que a pesar de las tecnologías que pueden llegar a adquirir ciertos grupos terroristas, los Estados siguen siendo los actores con mayores y mejores capacidades para realizar acciones en el ciberespacio. Es por ello que los grupos patrocinados por los Estados han sido clasificados como una preocupación primordial para la seguridad de los sistemas informáticos y la infraestructura de los Estados afectados. A fin de explorar esta amenaza, se pueden analizar presuntos grupos patrocinados por Estados que tienen un historial de ataques a entidades gubernamentales, o que tienen un historial de que se les ha encomendado la tarea de reunir información de inteligencia que previsiblemente podría evolucionar hacia el ataque a entidades gubernamentales o intergubernamentales[28].

De acuerdo con reportes del Departamento de Estado de los Estados Unidos, hay una serie de grupos ciberterroristas que se han atribuido de manera creíble el patrocinio de los gobiernos de Rusia, China, Irán y Corea del Norte[29]. Se ha observado que tienen como objetivo los partidos políticos y las entidades gubernamentales de los Estados Unidos, Asia, el Oriente Medio y Europa occidental, además de diversos objetivos de la industria a nivel mundial[30]. Estos grupos han utilizado un gran número de tácticas que van desde ataques de *spear-phishing*, hasta herramientas de malware personalizadas para ganar terreno en sistemas y datos filtrados[31]. El hilo conductor es que los ataques suelen estar bien planeados y dirigidos con precisión.

27 Department of State of the United States. 2018. Loc. Cit.

28 DAY, Paul. Loc. Cit.

29 Department of State of the United States. 2018. Loc. Cit.

30 Ibíd.

31 KESSEM, Limor. Loc. Cit.

Por ejemplo, las amenazas cibernéticas de Rusia se caracterizan por contar con algunos grupos sospechosos patrocinados por el Estado, pero también por una enorme clandestinidad criminal, con docenas de foros de habla rusa con decenas de miles de usuarios[32]. A los grupos patrocinados por el Estado ruso se les ha atribuido una serie de acciones de muy alto perfil en los últimos años, incluidas operaciones para interferir en las elecciones del gobierno federal de los Estados Unidos y ataques a organizaciones gubernamentales de Europa occidental.

Ciberresiliencia y riesgo sistémico

Ante este alarmante panorama, se deben considerar dos elementos clave en las cuestiones de la ciberseguridad, tal y como el riesgo sistémico y la ciberresiliencia. Por un lado, el riesgo sistémico se refiere al riesgo de una avería de todo un sistema en lugar de simplemente la falla de partes individuales. Es por ello que se debe tener en cuenta que el ciberespacio y su infraestructura subyacente son vulnerables a una amplia gama de riesgos derivados de amenazas y peligros tanto físicos como cibernéticos. Por años los estudios de seguridad se habían basado exclusivamente en el estudio de aquellos peligros y riesgos físicos. Sin embargo, gobiernos como el de Estados Unidos vienen trabajando en estrategias que proporcionan al Departamento de Seguridad Nacional un marco para identificar las responsabilidades de seguridad cibernética durante los próximos cinco años[33]. De esta manera se busca mantener el ritmo del panorama de riesgo cibernético en evolución, mediante la reducción de las vulnerabilidades y la creación del concepto de ciberresiliencia. En ese sentido, la ciberresiliencia se puede definir como el mecanismo que busca contrarrestar a los actores maliciosos en el ciberespacio, responder a incidentes, y lograr que el ecosistema cibernético sea más seguro y resistente[34].

Una distinción que es importante realizar es la diferenciación de lo que es un riesgo sistémico y un riesgo sistemático. El primero se enfoca en el reconocimiento de un sistema, como un conjunto de diferentes elementos que se encuentran relacionados entre sí, teniendo una o varias interdependencias con un objetivo en común. En cambio, el riesgo sistemático hace referencia a la metodología de hacer las cosas dado que se analiza e identifica el problema antes de responder con una acción específica. La ciberresiliencia se entiende así como la capacidad de los sistemas para anticipar y adaptarse al potencial de sorpresa y falla, debiendo considerarse en el contexto de sistemas complejos que comprenden no solo los dominios físicos y de información, sino también los dominios cognitivos y sociales, garantizando que la recuperación del sistema ocurra al considerar el *hardware*, el *software* y los componentes de detección interconectados de la infraestructura cibernética[35].

32 Department of State of the United States. 2018. Loc. Cit.

33 MATTIS, Jim. Loc. Cit.

34 GONZALEZ, James. Ciberriesgo desde la perspectiva de riesgo sistémico. [Online] 2019. [Cited: 2 17, 2020.] 10.29236/sistemas.n151a6. Recuperado de: https://sistemas.acis.org.co/index.php/sistemas/article/download/14/12/

35 KOTT, Andrew and LINKOV, Ingrid. 2019 *Ciber resilience of Systems and Networks.* 1 edition, s.l. : Springer Nature, Vols. 4-7.

Security of Things

El Internet de las Cosas o Security of Things (IO) es un concepto que se refiere a nuevos tipos de arquitecturas y protocolos en comparación con las redes tradicionales. La seguridad es un tema extremadamente crítico para la IO que debe ser abordado de manera eficiente. La heterogeneidad, característica inherente a la IO, plantea muchos problemas de seguridad que deben abordarse desde la perspectiva de las nuevas arquitecturas, como las redes definidas por el software, los algoritmos criptográficos y la computación[36].

Una de las definiciones más comunes aceptadas ampliamente para el Internet de las Cosas (IO) es: "Colección de 'cosas' incrustadas con electrónica, software, sensores y actuadores y conectadas a través de Internet para recoger e intercambiar datos entre ellas"[37].

Los dispositivos de IO están equipados con sensores y potencia de procesamiento que les permiten ser desplegados en muchos entornos. Así mismo, el impacto del papel humano se ha minimizado en la IO. Esto dado que la composición de lo que se denomina como el Internet de las cosas consiste de varios elementos dentro de los cuales se pueden destacar: los servicios diarios, casas y ciudades inteligentes, reguladores del consumo de energía, servicios móviles etc.[38].

El Internet de las cosas presenta una amplia gama de nuevos riesgos y desafíos de seguridad para los dispositivos, sus plataformas y sistemas operativos, sus comunicaciones e incluso los sistemas a los que están conectados. El poder del Security of Things reside tanto en el mundo físico como en el mundo virtual. Diferentes tipos de vulnerabilidad producen diferentes amenazas con el potencial de diferentes daños. Al evaluar el valor en riesgo, se pueden tomar decisiones informadas sobre cuando invertir en medidas defensivas.

Infraestructura crítica

Los sectores de la infraestructura que normalmente se consideran críticos incluyen el transporte, la agricultura, la defensa y la seguridad, la salud pública, la producción de combustible y la tecnología de la información[39]. Como la infraestructura crítica es clave para el funcionamiento de una nación, representa un blanco potencial del terrorismo y otras acciones perturbadoras. La infraestructura crítica incluye tanto sistemas físicos como cibernéticos esenciales para el funcionamiento mínimo de la economía y el gobierno. Tras los ataques terroristas del 11 de septiembre de 2001, Estados Unidos dirigió una mayor atención a la protección física de las infraestructuras críticas. En los años transcurridos la política, los programas y la legislación relacionados con la seguridad física de las infraes-

36 YOUSUF, Omerah and MIR, Roohie Naaz. Emerald Insight. *A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures.* [Online] 06 12, 2019. [Cited: 02 17, 2020.] 2056-4961. https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2018-0084/full/html

37 Ibíd.

38 DAY, Paul. Loc. Cit.

39 YATES, Sheldon. *National Critical Infrastructure Policy: Background and Select Cybersecurity Issues.* New York : Nova Science Publishers, 2016. 9781634847568. 9781634847575..

tructuras críticas se han estabilizado en gran medida[40]. Sin embargo, dada la coyuntura actual se ha vuelto a considerar el otro riesgo para la infraestructura crítica el cual se refiere a la seguridad cibernética. Es por ello que la Protección de Infraestructuras Críticas es un programa importante en el que los gobiernos tienen que tomar medidas para hacer frente a las amenazas a esa infraestructura en términos de ciberamenazas.

Hoy en día, casi todos los sectores críticos utilizan sistemas cibernéticos. Los sectores de transporte, banca y finanzas, salud y emergencias, defensa y gobierno usan tecnologías de información convencionales que son vulnerables a un ataque en la red[41]. En ese sentido, la infraestructura crítica se encuentra en riesgo debido a ciertas amenazas que pueden ser clasificadas en cuatro categorías. Por un lado, el hacktivismo, luego el cibercrimen, también el ciberespionaje y finalmente la ciberguerra[42]. En cuanto al hacktivismo podemos mencionar que su principal propósito no es hacer dinero, sino protestar por algo. Por ejemplo, protestan contra las restricciones gubernamentales en Internet y apuntan a los sitios web de organizaciones públicas[43]. Normalmente no intentan afectar un sitio web específico durante mucho tiempo. Más bien, buscan una vulnerabilidad específica en varios sitios web y afectan todos los sitios web dentro de su ámbito de búsqueda que contiene la vulnerabilidad específica.

En cuanto a los cibercriminales, como ya habíamos mencionado anteriormente, buscan afectar el sistema bancario y financiero con el propósito personal de ganar dinero. Se ha estimado que el cibercrimen le cuesta a la economía mundial un billón de dólares al año[44]. Tal vez aún más sorprendente es el hecho de que gran parte de este crimen cibernético se produce en las manos de pequeños grupos de *hackers* que trabajan de forma independiente o en nombre de las naciones rebeldes con pocos recursos.

El ciberespionaje se refiere al acto de robar documentos oficiales de los gobiernos de manera que pierdan su confidencialidad. Según el Departamento de Defensa Estratégica de Estados Unidos, cada año se roba una mayor cantidad de propiedad intelectual a las redes mantenidas por empresas, universidades, departamentos y agencias gubernamentales de los EE.UU. Finalmente, la ciberguerra se refiere al uso de ataques coordinados a sectores críticos específicos de un país. Cada sector crítico es un objetivo potencial de la ciberguerra. La mayoría de los expertos en seguridad cibernética afirman que el virus Stuxnet, descubierto en junio de 2010, fue el comienzo de una verdadera ciberguerra.

Nuevas normas de colaboración y las implicaciones en el derecho internacional

El Secretario General de las Naciones Unidas, Antonio Guterres, ha advertido sobre la importancia y trascendencia de las amenazas cibernéticas en las Relaciones Internacionales al decir “Estoy absolutamente convencido de que, a diferencia de las grandes batallas del pasado, que se iniciaron con un aluvión de artillería o bombardeos aéreos, la próxima gue-

40 MATTIS, Jim. Loc. Cit.

41 DENNING, Dorothy. 2011. Loc. Cit.

42 YATES, Sheldon. Loc. Cit.

43 DAY, Paul. Loc. Cit.

44 World Economic Forum**.** Loc. Cit.

rra comenzará con un ciberataque masivo para destruir la capacidad militar... y paralizar la infraestructura básica como las redes eléctricas". El Secretario General Guterres destacó su temor de tal catástrofe, señalando que el derecho internacional y los sistemas de defensa de las naciones no están preparados y han hecho poco para mitigar la posibilidad de un gran ciberataque:

"Ya existen episodios de guerra cibernética entre los estados. Lo que es peor es que no existe un esquema regulatorio para ese tipo de guerra, no está claro cómo se aplica la Convención de Ginebra o el derecho internacional humanitario".

En la última década, docenas de intentos de tratados y acuerdos sobre seguridad cibernética se han venido abajo. Por ejemplo, el Grupo de Expertos Gubernamentales de las Naciones Unidas celebró una serie de negociaciones desde 2004 hasta finales de 2017 con el objetivo de establecer normas para la seguridad cibernética, frenar la militarización del ciberespacio y proponer sanciones para disuadir los actos de agresión[45]. Sin embargo, los diplomáticos abandonaron las conversaciones de 13 años a finales de agosto de 2018, resolviendo que las diferencias insuperables en las políticas nacionales harían imposible llegar a un acuerdo.

Otro obstáculo importante es la cuestión de la responsabilidad (accountability), ya que a menudo es difícil probar que los *hackers* informáticos responsables de los ataques estaban dirigidos por un gobierno determinado. En conjunto, estas dificultades obligaron a los diplomáticos a descartar más de una década de negociación. Pero como advirtió el Secretario General Guterres en Lisboa, el peligro de un gran ciberataque no ha hecho más que aumentar.

Ante esta situación, en el ámbito del derecho internacional el derecho de recurrir a la legítima defensa es puesto en cuestión. El Artículo 51 de la Carta de Naciones Unidas dice "Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas"[46]. No obstante, el precedente legal ha dejado claro que no todos los usos de la fuerza pueden ser considerados también como ataques armados. De hecho, vale la pena señalar que cuando en el artículo 51 se hace referencia a un "ataque armado", es distinto de la redacción del artículo 2.4 de la Carta de Naciones Unidas, el cual prohíbe la amenaza o el uso de la fuerza. De hecho, en un famoso caso entre Nicaragua y los Estados Unidos, la Corte Internacional de Justicia (CIJ) ha dictaminado que hay amenazas o usos de la fuerza que no se consideran ataques armados y que, por lo tanto, no permiten a la víctima invocar el derecho de legítima defensa[47]. Por ello, ataques armados solo incluyen las "formas más graves del uso de la fuerza". Las intrusiones en la frontera, por ejemplo, se han clasificado como "incidentes fronterizos" no lo suficientemente graves como para desencadenar el artículo 51[48].

45 HATHAWAY, Oona A., CROOTOF, Rebecca, PERDUE, William "et al". Loc. Cit.

46 Naciones Unidas. Carta de las Naciones Unidas. 1945. 1 UNTS XVI.

47 HOLLIS, Duncan. Why States Need an International Law for. s.l. : Lewis & Clark , 2007. 1023.

48 Ibíd.

Tres escuelas de pensamiento han surgido tratando de guiar su enfoque para clasificar los ciberataques. La posición más tradicional es la de los académicos de la Escuela de Derecho de Yale, conocida como el enfoque basado en instrumentos[49]. Este enfoque trata un ciberataque como un ataque armado solo si utiliza armas militares. Por ejemplo, el bombardeo de servidores informáticos o de cables de Internet podría cumplir los requisitos de un ataque armado si el ataque fuera de suficiente gravedad. El enfoque basado en instrumentos, por lo tanto, incluye muy pocos ciberataques como ataques armados. Esto tiene la clara desventaja de que las víctimas de los ciberataques no tienen derecho a la defensa propia, aunque los ciberataques pueden ser mucho más perjudiciales que los bombardeos u otros ataques físicos.

La segunda escuela de pensamiento acude el enfoque basado en objetivos. Sean Condron, uno de los más importantes defensores del enfoque basado en objetivos, ha descrito cuándo los ciberataques deben constituir ataques armados según tal enfoque[50]. Para Condron, cuando el ataque tiene como objetivo la infraestructura crítica del Estado, el Estado debe ser capaz de ejercer medidas de defensa activas. Los Estados que abogan por derechos firmes para defenderse de un ciberataque, en su mayoría Estados industrializados que son los que más tienen que perder en un ciberataque, también tienden a preferir el enfoque basado en objetivos.

El tercer enfoque sobre el derecho a la legítima defensa en el ciberespacio se denomina enfoque basado en los efectos, que es un punto medio entre el enfoque basado en los instrumentos y el basado en los objetivos[51]. En ese sentido, clasifica un ciberataque basado en la gravedad de sus efectos. Michael Schmitt ofreció seis criterios para evaluar la gravedad de los efectos de un ciberataque, incluyendo el momento del ataque, el daño a largo plazo causado, la escala del ataque, etc. Según el enfoque adoptado, los distintos Estados de la comunidad internacional han reaccionado a la cuestión sobre regular o no el ciberespacio en términos de derecho internacional. Actualmente se pueden destacar dos grupos de Estados que han adoptado enfoques distintos sobre esta cuestión. Por un lado, está la Organización de Cooperación de Shanghái (OCS) y por otro está la Organización del Tratado del Atlántico Norte (OTAN).

Los Estados miembros de la OTAN han reconocido que los ciberataques podrían ser tan dañinos para las sociedades como un ataque convencional. Como resultado, la ciberdefensa es reconocida como parte de la tarea central de la OTAN de defensa colectiva. En ese sentido, cabe recalcar que la OTAN adoptó una política y un plan de acción, que fue aprobado por los Estados miembro en la Cumbre de Gales en septiembre de 2014[52]. Desde entonces, los Aliados han aprobado un plan de acción conjunto que fue actualizado en febrero de 2017. La política establece que la ciberdefensa forma parte de la tarea central de la Alianza de defensa colectiva, confirma que el derecho internacional se aplica en el

49 Ibíd.

50 HATHAWAY, Oona A., CROOTOF, Rebecca, PERDUE, William "et al". Loc. Cit.

51 HOLLIS, Duncan. Loc. Cit.

52 NATO. The North Atlantic Treaaty Organization. *Defending against cyber attacks.* [Online] 2017. https://www.nato.int/cps/en/natohq/topics_118663.htm?selectedLocale=en

ciberespacio e intensifica la cooperación de la OTAN con la industria[53]. Así, la máxima prioridad es la protección de los sistemas de comunicaciones que son propiedad de la Alianza y gestionados por ella.

En contraste, durante los últimos años la organización de Cooperación de Shanghái ha prestado especial atención a las cuestiones relacionadas con la ciberseguridad y las normas internacionales al respecto. En 2009, los Estados miembros de la OCS llegaron a un acuerdo de cooperación en el ámbito de la seguridad internacional de la información[54]. En 2011, cuatro de los Estados miembros de las OSC presentaron al Secretario General de las Naciones Unidas una propuesta sobre un Código Internacional de Conducta para la Seguridad de la Información, para su discusión en la reunión de la Asamblea General de las Naciones Unidas[55]. Posteriormente, en 2015, los cinco miembros de la OCS presentaron una versión revisada del Código para su análisis por la Asamblea General de las Naciones Unidas. El objetivo de dicho código, tal como lo propone la OCS, sería identificar los derechos y responsabilidades de los Estados en el espacio de la información, y mejorar su cooperación para hacer frente a las amenazas y desafíos comunes en el ciberespacio[56].

La Organización de Cooperación de Shanghái ha expresado su insatisfacción respecto a las definiciones presentadas por los Estados Unidos y otras naciones de la OTAN sobre los temas relacionados con la ciberseguridad. Los países de la OCS a menudo se han opuesto diametralmente a las políticas cibernéticas de la OTAN, las cuales generalmente exigen definiciones más estrictas y un mayor derecho a represalias. Además, los conflictos en el ciberespacio han enfrentado con frecuencia a una nación de la OCS contra una nación de la OTAN; el virus Stuxnet y la piratería informática a la convención del partido Demócrata en Estados Unidos por parte de Rusia son algunos ejemplos.

Considerando la relevancia que han adquirido las amenazas en el Quinto dominio de la Guerra conocido como el ciberespacio, entre 2009 y 2012, un grupo internacional de expertos jurídicos del Centro para la Excelencia de la Cooperativa de Defensa Cibernética de la OTAN intentó elaborar una definición de ciberataques basada en el consenso. Sin embargo, a pesar de que las naciones de la Organización de Cooperación de Shanghái fueron invitadas y enviaron representantes a las conversaciones, finalmente las abandonaron debido a las diferencias irreconciliables con los funcionarios de la OTAN. Como resultado, el producto final de los expertos, llamado el Manual de Tallin, incorporó las opiniones tanto de la OTAN como de la OCS, pero adoptó principalmente posiciones occidentales sobre las cuestiones más controversiales.

53 NATO. North Atlantic Treaty Organization. *Cyber defense.* [Online] julio 16, 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm

54 The Shanghai Cooperation Organization. SCO. [Online] 2019. https://dig.watch/actors/shanghai-cooperation-organisation

55 The Shanghai Cooperation Organization. SCO responds to cyberchallenges. [Online] junio 09, 2011. http://infoshos.ru/en/?idn=8349

56 SCO. SCO attends international cybersecurity conference in China. [Online] diciembre 20, 2017. http://eng.sectsco.org/news/20171220/368561.html

El Manual abarca un amplio espectro de derecho internacional aplicable a las operaciones cibernéticas, desde regímenes jurídicos en tiempos de paz hasta el derecho de los conflictos armados[57]. Esto le permite referirse a una amplia gama de principios de derecho internacional y regímenes que regulan los acontecimientos en el ciberespacio. A pesar de las múltiples críticas que ha recibido el Manual de Tallin dado que deja ciertos vacíos tanto en términos legales como conceptuales sobre los ciberataques, su relevancia en términos de los avances sobre los temas de ciberseguridad permanece vigente. El proceso del Manual de Tallin continúa con una evaluación legal, técnica, estratégica y operativa de los escenarios cibernéticos, con el objetivo de ser una fuente de referencia práctica para los comandos cibernéticos a nivel internacional.

Conclusiones

Luego de trazar los principales riesgos y desafíos que se presentan en el ciberespacio, se puede afirmar que la cuestión de la seguridad cibernética tiene más relevancia que nunca en el estudio de las relaciones internacionales y la seguridad internacional. Si bien, como se mencionaba al inicio del texto, la seguridad se ha relacionado siempre con eventos físicos que amenazan la integralidad territorial de los Estados, actualmente los riesgos cibernéticos desdibujan esa integralidad territorial, haciendo que las fronteras en el mundo del ciberespacio no conozcan límites y desafiando la concepción tradicional de la seguridad. El mundo del ciberespacio ha visto crecer amenazas de todo tipo que afectan tanto el ámbito económico, como social y político de una nación. Desde pequeños *hackers* que buscan afectar ciertas páginas web, pasando por cibercriminales que solo buscan su propio enriquecimiento, hasta llegar a los más avanzados ciberespías que roban información de entidades gubernamentales, todo se encuentran en un entorno anárquico en el que aún no hay suficiente regulación.

Los estudios de seguridad y defensa por décadas se han enfocado en los eventos reales y tangibles, a los cuales se les afrontaba con una respuesta física en el mundo real. Al incluir un quinto dominio en los escenarios de la guerra, los Estados deben crear y diseñar políticas de defensa y seguridad que respondan a aquellas amenazas que, a pesar de que no se ven en el mundo físico pueden llegar a tener repercusiones en él. En ese sentido se abre la puerta a la reflexión sobre la seguridad en escenarios abstractos, intangibles, que desafían la concepción tradicional de lo que es una amenaza y a la cual se le debe dar una respuesta en ese mismo escenario intangible y abstracto.

Como se ha mencionado a lo largo de este texto, ya son múltiples las modalidades como los actores pueden perpetuar ataques en el ciberespacio. Las ciberamenazas se han convertido sin lugar a duda en otro de los principales temas en la agenda de seguridad. Incluso para los Estados más desarrollados mantenerse seguro en el ciberespacio se ha convertido en otro de los propósitos planteados con el fin de defender sus intereses nacionales. Esto ocurre dado que en la actualidad el ciberespacio le permite tanto a los Estados como a los actores no estatales la posibilidad de afectar la actividad económica, política y

57 TALBOT Jensen, Eric. The tallinn manual 2.0: Highlights and insights. *Georgetown Journal of International law.* [Online] 2017 https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3169202_code812464.pdf?abstractid=2932110&mirid=1

de seguridad de una nación. En ese sentido la prevención de cualquier ciberataque se convierte en una prioridad en la agenda de seguridad internacional.

El ciberespacio les permite a los atacantes realizar varias agresiones en distintos momentos al mismo tiempo y esos ataques a pesar de ser dirigidos en el mundo virtual, afectan lo real. Los recientes casos de ciberataques en Arabia Saudita y Ucrania deben prender las alertas del mundo puesto que la capacidad que tienen estos ataques para irrumpir en la cotidianidad de una nación y generar caos en distintos ámbitos de la sociedad significa una amenaza que en cualquier momento cualquier Estado podría sufrir. Incluso son alarmantes las cifras sobre el aumento del número de Estados con capacidades para ejecutar un ciberataque.

Todo esto nos puede llevar a una situación de ciberguerra o ciberterrorismo según sea el caso y el perpetuador del ataque. Así, llegamos a la conclusión que la ciberguerra es un conflicto informático o de red que involucra ataques de motivación política de un Estado-nación en otro Estado-nación. En este tipo de ataques, los actores del Estado-nación intentan interrumpir en las actividades de las organizaciones o Estados-naciones, especialmente con fines estratégicos o militares y ciberespionaje.

El ciberterrosimo, por su parte, tiene la particularidad de ser un ataque premeditado, motivado políticamente en contra de información, sistemas y programas informáticos que resultan en violencia en contra de objetivos no combatientes por parte de agentes no nacionales. No obstante, como se discutió a lo largo del texto, muchas veces estos grupos terroristas pueden llegar a ser financiados por Estados que tienen algún interés de atacar a otro en el ciberespacio. Esta situación nos lleva a un conflicto sobre la atribución del ataque dado que la inteligencia cibernética difícilmente logra llegar a identificar al actor específico que perpetuó el ataque y, en caso de hacerlo, demostrar el nexo entre tal individuo y una organización o un Estado es un reto aún mayor.

A pesar de las respuestas que ya desde principios de siglo los Estados vienen dando a este fenómeno, creando agencias y secciones especializadas dentro de los ministerios de defensa relacionados con la ciberseguridad, persiste aún un vacío tanto político como jurisprudencial respecto a la cuestión de atribución y proporcionalidad de la respuesta ante un ataque cibernético. Más preocupante aún, no existe si quiera un consenso sobre la definición de lo que es un ciberataque, lo cual demuestra los grandes retos que aun afronta el mundo en cuestión de gobernanza en el ciberespacio. El Manual de Tallin y su versión más actualizada son iniciativas conjuntas por parte de ciertos grupos de académicos por llegar a un consenso sobre las características que tiene un ciberataque, una operación cibernética y la manera como se puede llegar a atribuir y responder ante el mismo. No obstante, este documento carece de obligatoriedad puesto que no es vinculante a ningún Estado en derecho internacional. Esto deja al quinto dominio de la guerra en un escenario de anarquía en el que no se tiene en cuenta el derecho internacional humanitario ni ningún otro tipo de consideración.

A pesar de que la Cruz Roja Internacional participó de las discusiones del Manual de Tallin, y sus disposiciones son tomadas en cuenta por los Estados Miembros de la OTAN, existen posiciones divergentes sobre esta materia en cuestión. Regresamos entonces a la

consideración de que sobre este tema no convencional de la seguridad persiste un componente abstracto que deja a la discreción de cada actor del sistema internacional actuar en un escenario de anarquía. El más reciente ejemplo, la vulnerabilidad de la operación de la Organización Internacional de la Salud durante una época de pandemia deja ver un segundo elemento invisible en este contexto además del virus, como lo son los ciberataques que pueden llegar a afectar la manera como la comunidad internacional afronta la pandemia. Todo esto deja la puerta abierta para reflexionar sobre cómo el avance tecnológico y científico de nuestra era afecta la seguridad internacional en un mundo en el que en el quinto domino de la guerra no existen fronteras.

REFERENCIAS BIBLIOGRÁFICAS

Publicaciones

BLACKWELL, Adam. *Seguridad Multidimensional: Enfrentando Nuevas Amenazas.* 2015, Seguridad, Ciencia y Defensa, pp. 171-176.

BRENNER, Susan. 2002. *Cyberterrorism: how real is the threat?* pp. 149-154.

BUZAN, Barry. *Nex Patterns of global security in the Twenty First Century.* 1991, International Affaires, pp. 431-451.

BUZAN, Barry. *People, States & Fear.* 2007, ecpr press.

Cardenal Juan Pablo, "et al". *Sharp Power Rising Authoritarian Influence.* 2017, National Endowment for Democracy, pp. 1-156.

DAY, Paul. *Cyberattack.* Londres : Carlton books, 2014. 978178097533.

DENNING, Dorothy. 2000. *Cyberterrorism.* Information Warfare and Security. pp. 1-10.

DENNING, Dorothy. 2011.*Cyberwarfare.* s.l. : IEFE, Vols. Sptember-October.

GUELLER, Armando. *The use of complexity-based models in international Relations.* 2011, Cambridge Review of International Affaires, pp. 63-80.

HAFTENDORN, Helga. *The Security Puzzle: Theory-Building and Discipline-Building in International Security.* 1991, International Studies Quarterly, pp. 3-17.

HATHAWAY, Oona A., CROOTOF, Rebecca, PERDUE, William, LEVITZ, Philip, NIX, Haley, NOWLAN, Aileen & SPIEGEL, Julia. *The Law of Cyber-Attack,.* California : 100 California, 2018.

INSULZA, José. *La Seguridad Multidimensional y los retos actuales*2011, OEA, pp. 39-53.

KOTT, Andrew and LINKOV, Ingrid. 2019 *Ciber resilience of Systems and Networks.* 1 edition, s.l. : Springer Nature, Vols. 4-7.

MACKINLAY, John. *Defeating Complex Insurgency.* THE CORNWALLIS GROUP X: ANALYSIS FOR NEW AND EMERGING SOCIETAL CONFLICTS. pp. 22-74.

MAKARENKO, Tamara. *The Crime–Terror Continuum: Tracing the interplay between transnational organizaed crime and terrorism.* 2004, Global Crime, pp. 129-145.

MUGGAH, Robert. The Rise of Citizen Security in Latin America and the Caribbean. [book auth.] Humberto Campodónico, Sergio Tezanos Vázquez Gilles Carbonnier. *Alternative Pathways to Sustainable Development: Lessons from Latin America.* s.l. : Brill, 2017, pp. 291-322.

Naciones Unidas. Carta de las Naciones Unidas. 1945. 1 UNTS XVI.

NIXON, Thomas Homer. *The rise of complex terrorism.* 2002, Foreign Policy, pp. 52-62.

STEIN, Abraham. *El concepto de Seguridad Multidimensional. 2009,* Centrales, pp. 31-37.

ŠULOVIĆ, Vladimir. (2010). **"***Meaning of Security and Theory of Securitization*". Belgrade Centre for Security Policy. Retrieved from

TREVERTON, Gregory F., NEMETH, Erik and SRINIVASAN, Sinduja. *Threats Without Threateners.* 2012, Rand Corporation, pp. 3-12.

World Economic Forum. *The Global Risks Report.* Geneva : World Economic Forum, 2020.

YATES, Sheldon. *National Critical Infrastructure Policy : Background and Select Cybersecurity Issues.* New York : Nova Science Publishers, 2016. 9781634847568. 9781634847575.

YOUNG, Aaron and GRAY, David. *Insurgency, Guerilla Warfare and Terrorism: Conflict and its.* 2011, Global Security Studies, pp. 60-71.

ZANINI, Michele and EDWARDS, Sean. *The Networking of terror in the information age.* Networks and Netwars: The Future of Terror, Crime, and Militancy, pp. 22-60.

Internet

BBC. El virus que tomó control de mil máquinas y les ordenó autodestruirse. [Online] 2015. http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

BRENNER, Susan. Cyberterrorism, how real is the threat? [Online] 05 20, 2016. [Cited: 02 17, 2020.] https://www.tandfonline.com/doi/abs/10.1080/01296612.2002.11726680. 10.1080/01296612.2002.11726680

British National Cybersecurity Center. *APT29 targets COVID-19 vaccine development.* [Online] 07 2020. https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

CCDCOE. The NATO Cooperative Cyber Defence Centre. [Online] 2019. https://ccdcoe.org/

CHIVIS, Christopher and DION, Cynthia. *Why It's So Hard to Stop a Cyberattack and Even Harder to Fight Back.* 2017, Rand Corporation. https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html

Department of State of the United States. US Department of State. *Country Reports on Terrorism 2018.* [Online] 2018. [Cited: 2 17, 2020.] https://www.state.gov/reports/country-reports-on-terrorism-2018/

El Pais. Ciberataques desde el Kremlin. [Online] 2018. https://elpais.com/elpais/2018/02/16/opinion/1518800402_049645.html

GALINEC, Darko. Cybersecurity and cyber defence: national level strategic approach. [Online] 2017. https://www.tandfonline.com/doi/full/10.1080/00051144.2017.1407022

GIDDENS, Anthony. Fate Risk and security. [Online] 2016. https://revisesociology.com/2016/10/05/giddens-fate-risk-and-security/

GONZALEZ, James. Ciberriesgo desde la perspectiva de riesgo sistémico. [Online] 2019. [Cited: 02 17, 2020.] 10.29236/sistemas.n151a6 https://sistemas.acis.org.co/index.php/sistemas/article/download/14/12/

HAPPA, Jassim, GLENCROSS, Mashhuda and STEED, Anthony. Frontiers in ICT. *Cyber Security Threats and Challenges in Collaborative Mixed-Reality.* [Online] 4 09, 2019. https://www.frontiersin.org/articles/10.3389/fict.2019.00005/full

HOLLIS, Duncan. Why States Need an International Law for. s.l. : Lewis & Clark , 2007. 1023. http://www.bezbednost.org/upload/document/sulovic_(2010)_meaning_of_secu.pdf)

ITU. Definition of cybersecurity. *ITU.* [Online] 2020. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets

ITU. ITU NATIONAL. Cybersecurity Strategy Guide. [Online] 2020.http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

KASPERSEN, Anja. World Economic Forum. *Cyberspace: the new frontier in warfare.* [Online] 09 24, 2015. https://www.weforum.org/agenda/2015/09/cyberspace-the-new-frontier-in-warfare/

Kelin, Andrei. BBC. *Russia's UK ambassador rejects coronavirus vaccine hacking allegations.* [Online] 07 2020. https://www.bbc.com/news/uk-53458122

KESSEM, Limor. Security Intelligence. *The Business of Organized Cybercrime: Rising Intergang Collaboration in 2018.* [Online] 03 20, 2019. [Cited: 02 16, 2020.] https://securityintelligence.com/the-business-of-organized-cybercrime-rising-intergang-collaboration-in-2018/

MATTIS, Jim. Summary of the National Defense Strategy. [Online] 2018. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Nato Review Magazine. Nato's role in Cyber space. [Online] febrero 02, 2019. https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm

NATO. North Atlantic Treaty Organization. *Cyber defense.* [Online] Julio 16, 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. North Atlantic Treaty Organization. *Nato Cyber defense.* [Online] Febrero 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

NATO. The North Atlantic Treaaty Organization. *Defending against cyber attacks.* [Online] 2017. https://www.nato.int/cps/en/natohq/topics_118663.htm?selectedLocale=en

NYE, Joseph. Project Syndicate. *China: poder blando y poder punzante.* [Online] 01 04, 2018. https://www.project-syndicate.org/commentary/china-soft-and-sharp-power-by-joseph-s--nye-2018-01/spanish

OEA. Special conference on security. [Online] 2003. https://www.oas.org/en/sms/docs/DECLARATION%20SECURITY%20AMERICAS%20REV%201%20-%2028%20OCT%202003%20CE00339.pdf

RAE**.** Real Academia de la Lengua Española. [Online] 2018. https://www.rae.es/

RUBIN, Michael. The age of hyper-terrorism and 'low cost' terrorism. [Online] 2017. http://www.aei.org/publication/the-age-of-hyper-terrorism-and-low-cost-terrorism/

SCO. SCO attends international cybersecurity conference in China. [Online] Diciembre 20, 2017. http://eng.sectsco.org/news/20171220/368561.html

SCO. SCO Secretary-General Vladimir Norov's news conference at the SCO Secretariat. [Online] marzo 20, 2019. http://eng.sectsco.org/news/20190320/518936.html

Shanghai Cooperation Organization. SCO. [Online] 2019. https://dig.watch/actors/shanghai-cooperation-organisation

TALBOT Jense, Eric. The tallinn manual 2.0; Hihghlights and insights. *Georgetown Journal of International law.* [Online] 2017.

https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3169202_code812464.pdf?abstractid=2932110&mirid=1

The Shanghai Cooperation Organization. SCO responds to cyberchallenges. [Online] junio 09, 2011. http://infoshos.ru/en/?idn=8349

The White House. National Security Strategy. [Online] 12 2017. http://www.whitehouse.gov/wp-contnt/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

WHO**.** World Health Organization. *WHO reports fivefold increase in cyber attacks, urges vigilance.* [Online] 04 2020. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

World Economic Forum. *Informe de riesgos mundiales 2018.* Ginebra : Marsh & Mc Lennan Companies, 2018.Xinhua. Xinhuanet. *SCO countries hold drill targeting cyber-terrorism.* [Online] 2017. http://www.xinhuanet.com/english/2017-12/06/c_136806108.htm

YOUSUF, Omerah and MIR, Roohie Naaz. Emerald Insight. *A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures.* [Online] 06 12, 2019. [Cited: 02 17, 2020.] 2056-4961. https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2018-0084/full/html