Reto postpandemia: Inseguridad cibernética

Post-Pandemic Challenge: Cyber Insecurity

Capitán de Navío Pedro José Pablo Iriarte Chávez. Licenciado en Ciencias Marítimas Navales, graduado de la Escuela Naval del Perú en diciembre del 2000. Cuenta con las calificaciones de Guerra de Superficie y Electrónica & Comunicaciones. Es graduado del Curso de Comando y Estado Mayor Naval en la Escuela Superior de Guerra Naval y del Curso de Comando y Estado Mayor Conjunto en la Escuela Conjunta de las FFAA en Argentina. Posee el grado de Magíster en Ingeniería de Control y Automatización en la Pontificia Universidad Católica del Perú; así como Magíster en Seguridad y Defensa Hemisférica en el Colegio Interamericano de Defensa en los EEUU. Entre los principales cargos, se ha desempeñado como Oficial de Disciplina de la Escuela Naval, Oficial Secretario de la Secretaría de la Comandancia General, Comandante del B.A.P. *Loreto*, Segundo Comandante del B.A.P. *Herrera*, Edecán del Presidente de la República, Jefe de la Sección de Planeamiento y de Operaciones de la Comandancia de la Fuerza de Superficie, Comandante del B.A.P. *Ferré*, Jefe de la Sección de Planeamiento de la Comandancia General de Operaciones del Pacífico, y actualmente se desempeña como Jefe de la Sección de Operaciones de la citada Comandancia General.

Resumen: Las medidas que mitigaron el avance de la pandemia del covid-19 han cambiado la vida de toda la humanidad, generando mayor dependencia digital, volviendo a la nueva normalidad en nuevos hábitos acompañados de avances tecnológicos producidos por la revolución industrial 4.0. Es en este contexto que el ciberespacio surge como el dominio más empleado por las personas en la actualidad, volviéndolas más vulnerables, aumentando las oportunidades para ejecutar ataques cibernéticos, generando miedo e incertidumbre, afectando la seguridad de manera multidimensional en las sociedades. Los Estados, apoyándose con la comunidad internacional, tienen el desafío de implementar políticas y estrategias que permitan contener las amenazas a la ciberseguridad de manera conjunta con sus ciudadanos. En el presente artículo, en base a ejemplos prácticos, se analizará la importancia de difundir las amenazas a la ciberseguridad que tienen todos los ciudadanos, así como también las medidas de mitigación que se deben realizar para evitar riesgos que afecten la seguridad y defensa nacional.

Palabras claves: ciberseguridad, amenazas cibernéticas, ciberdefensa.

Abstract: *The measures that mitigated the advance of the covid-19 pandemic have changed the lives of all humanity, generating greater digital dependence, returning the new normal into new habits accompanied by technological advances produced by the industrial revolution 4.0. It is in this context that*

cyberspace emerges as the domain most used by people today, becoming vulnerable and increasing the opportunities to execute various intrusions and cyberattacks, generating fear and uncertainty that affect security in a multidimensional way. States face the challenge of implementing policies and strategies to contain cybersecurity threats together with their citizens and with the support of the international community. In this article, based on practical examples, we will analyze the importance of disseminating cybersecurity threats that all citizens have, as well as mitigation measures to avoid risks that affect national security and defense.

Keywords: *Cybersecurity, Cyber Threats, Cyber Defense.*

Introducción

La aparición y aceleración tecnológica de la computación, internet e información, dio origen a la llamada ciberseguridad en nuestros días. De los tres eventos, uno de ellos ha cobrado mayor importancia por la facilidad de manejo y acceso: la información. Alvin Toffler nos adelantó que la información iba tener un papel muy importante como pieza de intercambio a todo nivel en las sociedades, argumentando que la *infosfera*[1] iba impactar a todas las personas radicalmente a corto tiempo, reemplazando los elementos de la economía tradicional.

Asimismo, el General Stanley McChrystal, Jefe Militar en la Guerra de Afganistán, mencionó que muchas personas poseen variada información que no tiene ningún valor si no es la persona que pueda hacer algo con ella, por lo que a partir del 2007 surgió un cambio en la cultura organizacional del Departamento de Defensa de los Estados Unidos (EEUU), dónde se tuvo que cambiar la idea sobre la información, migrando del llamado “saber algo es poder" hacia "compartir es poder”. Este *slogan* sería una justificación por la que muchas personas podrían considerar a Edward Snowden, ex empleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA) como un héroe en vez de un villano. De ahí la importancia de la información en estos tiempos.

1 Término empleado en la obra “La tercera ola” de Toffler para argumentar que toda civilización tiene tres esferas, y una de ellas es la infósfera, definida por los canales de comunicación en donde circulan la información necesaria para las sociedades.

Después de la pandemia del covid-19, la población mundial aumentó sustancialmente el empleo del ciberespacio, aumentando significativamente la información en la llamada nube, generándose el uso cotidiano de un sin número de aplicaciones en las sociedades. Este ascendente uso del ciberespacio favoreció, a nivel global, tanto la dimensión como la variedad de las amenazas cibernéticas que vienen afectando la seguridad multidimensional de los Estados.

El manejo de la información en el ciberespacio

La aparición de la revolución industrial 4.0 y su aceleración producto de la pandemia, ha incrementado el uso de internet en las personas, especialmente en lo relacionado al internet de las cosas, calculándose que en la actualidad existe el 59.5% de la población mundial conectada, y como consecuencia, el aumento exponencial del flujo de información en la web.

De acuerdo a Fernando Rey, la carrera tecnológica entre China y EEUU está propiciando que la *big data* sea empleada por millones de empresas, a fin de brindar mejores servicios y productos a las personas; pero a su vez está volviendo más vulnerable la vida de todos; he ahí la importancia de las cinco leyes de ciberseguridad que propone Nick Espinosa: la primera indica que si existe una vulnerabilidad, los ciberdelincuentes la aprovecharán; la segunda es que todas las personas son vulnerables de alguna medida; la tercera es que las personas se fían incluso cuando no deberían fiarse; la cuarta es que con la innovación tecnológica existe siempre la opción de sacar alguna ventaja; y por último la quinta ley indica que, ante la duda de alguna vulnerabilidad, vuelva a la primera ley. Estas leyes son de suma importancia para todas las personas e Instituciones que cuentan con diversas vulnerabilidades en el ciberespacio.

En ese orden de ideas, Rufino Contreras menciona que producto de lo vulnerable que nos hemos vuelto por la necesidad de estar conectados para trabajar, estudiar, comprar, compartir la vida social, etc., han aumentado en un 43% los ataques cibernéticos. Esto principalmente desde la época relacionada a la pandemia del covid-19; empleándose principalmente técnicas de *phishing* y *malware* a distintas organizaciones públicas y privadas, así como a personas naturales.

Kelly Bissell y Larry Ponemon en un estudio sobre criminalidad cibernética mencionan que los cibercriminales, aprovechando el costo oportunidad, constantemente evolucionan sus técnicas de ciberataques, principalmente empleando el eslabón más débil en la ruta del crimen: las personas. Ejemplo

de esto ocurrió en los casos de *carbanak* y *bonet Mirai,* donde las técnicas empleadas fueron afectadas por los mismos individuos de manera involuntaria.[2]

En ese sentido, parte del problema también radica en la implementación de las nuevas normativas para el teletrabajo y teleeducación en las sociedades. Los Estados, después de la pandemia del covid-19, implementaron esta nueva normalidad en distintas organizaciones. Esta tendencia contribuye al empleo excesivo de las computadoras y cámaras web; generando mayor vulnerabilidad en las personas, los cuales muestran sus identidades, sus domicilios, su composición familiar y demás datos personales, de manera involuntaria; pudiendo ser interceptado por agentes externos que empleen estos datos para obtener algún beneficio particular o crear identidades falsas para cometer algún delito.

Acciones para prevenir ciberdelitos

Klaus Schwab, experto en revoluciones tecnológicas, recomienda que para afrontar este momento de revolución tecnológica global se necesita empoderar a las personas a todo nivel, buscando crear conciencia cibernética colectiva. Asimismo, los Estados deben orientar esfuerzos para proteger las infraestructuras críticas y brindar seguridad a los ciudadanos de las amenazas cibernéticas que vulneran sus derechos fundamentales. A su vez, países con un reducido avance tecnológico como el Perú deben orientar esfuerzos de manera continua, mediante un enfoque multidimensional para construir una *cybersociedad resiliente*, empleando políticas y estrategias con los sectores públicos y privados que fomenten una cultura de conciencia cibernética.

Como hemos mencionado, el gran avance tecnológico le viene ganando a la estructura de ciberseguridad global; y la brecha, especialmente en los países en vía de desarrollo, sigue aumentando y exige a los Estados desarrollar una estrategia nacional unida a mecanismos de cooperación internacional. Bajo este esquema Rodrigo Bijou nos plantea que el Estado debe preocuparse solamente de las puertas traseras del ámbito cibernético, siendo los individuos y las empresas los que deban enfocarse en ellos mismos para desarrollar la seguridad cibernética bajo un enfoque libre de interactuar en un mundo digitalizado. Otros expertos como Cardon y McHenry plantean el empleo de la innovación como mecanismo para afrontar la necesidad de ciberseguridad con pocos recursos.

---

2 Carbanak (2014): Caso de empleo de técnica de *phising* para robo de bancos, que pudo haber sido empleado para otros delitos no sólo del sector privado sino también del sector público. Botnet Mirai (2016): Red de bots que eran dispositivos inteligentes caseros que fueron empleados sin saber que estaban empleando sus propios dispositivos.

En la actualidad, imágenes como las vistas en la serie animada Los Supersónicos, serie de dibujos animados creada por William Hanna y Joseph Barbera en el año 1962 donde sus personajes vivían en una ciudad futurista del año 2062; son cada vez más cercanas. Por ejemplo, en China, a través del implementado sistema nacional de crédito social, el dilema seguridad-privacidad se viene llevando a cabo en los ciudadanos chinos, a través del uso por parte de las autoridades de datos de reconocimiento facial y vehicular, *big data* de aplicaciones comerciales, así como de las redes sociales; generando críticas con respecto a vulneración de los derechos humanos ligados a la privacidad. Este sistema ofrece al mundo el desafío de que el Estado proporcione a sus ciudadanos normas de convivencia y vigilancia para una sociedad más segura bajo el paraguas de un bien común como la seguridad.

Los países de América Latina difieren mucho en sus prioridades políticas, especialmente las relacionadas a ciberseguridad. El gran desafío es establecer políticas de Estado a fin de buscar cómo incentivar una cooperación interestatal e interagencial, que permita una sinergia que trascienda fronteras de manera invisible.

Sobre el particular, desde el año 2004 la Organización de Estados Americanos (OEA), mediante la estrategia para combatir las amenazas a la seguridad cibernética, le encargó al Comité Interamericano contra el terrorismo (CICTE), tratar asuntos de seguridad cibernética. Si bien desde su implementación se ha fomentado el desarrollo de una cultura de seguridad cibernética en los países del hemisferio a través de foros, grupos de trabajo y demás mecanismos de cooperación y capacitación, aún faltan muchos países miembros que implementen sus estrategias nacionales de ciberseguridad.

El experto en ciberseguridad, Kevin Newmeyer plantea las "buenas prácticas" basadas en las experiencias de las organizaciones y sus recomendaciones para el desarrollo de las estrategias nacionales de ciberseguridad; presentando tres paradigmas con la que los países podrían afrontan cada estrategia dependiendo del tipo de enfoque que se le quiera dar a la ciberseguridad. Dentro de estos, el enfoque del paradigma de seguridad nacional es el más empleado en los países de América Latina, para lo cual las autoridades políticas y militares son las encargadas de implementar y dictar las políticas de ciberseguridad al respecto, para que todos los Ministerios las apliquen y ejecuten de manera coordinada juntamente con el CSIRT/CERT establecido. Además, a través de planes de ciberseguridad a nivel nacional, se pueden incentivar a las empresas privadas para que inviertan

en seguridad de infraestructuras críticas, y de esta manera evitar el riesgo que existe dentro de este paradigma la falta de compromiso de este sector con el Estado.

En el caso del Perú, el enfoque de ciberseguridad es de seguridad nacional orientada a gestión de riesgos, para evitar ocurrencias de incidentes que pudieran afectar la ejecución de eventos críticos como lo fueron los Juegos Panamericanos Lima 2019. La planificación del citado evento internacional sirvió como experiencia impulsadora para implementar la organización de ciberseguridad y ciberdefensa en el Perú, iniciando la creación de los Comandos de Ciberdefensa de cada Institución Armada y el respectivo Comando Operacional de Ciberdefensa (COCID), el cual tiene en la actualidad la misión de planear, organizar, dirigir y conducir operaciones conjuntas de ciberdefensa, con la finalidad de defender, explotar y responder ante amenazas y ataques realizados a través del ciberespacio que afecten la seguridad digital de las redes, sistemas de información, telecomunicaciones y activos críticos de nuestras fuerzas y medios de alto valor militar. En la actualidad existe el Comando de Ciberdefensa de la Marina de Guerra del Perú, como un órgano de línea operativo que opera de manera transversal en todo el ámbito naval.

Internacionalmente, en lo que respecta al establecimiento de estas estrategias nacionales, la Unión Internacional de Telecomunicaciones (UIT) emitió la Guía de Desarrollo de Ciberseguridad, la cual promueve una mayor cultura cibernética integradora a todo el aparato estatal y sector privado de los países en vía de desarrollo, fomentando la cooperación internacional para reducir los riesgos que se tienen día a día en el ciberespacio, como por ejemplo a través de la adhesión al Convenio de Budapest.

La OEA, a través del CICTE, fortalece este campo, empleando mecanismos cooperativos y eficaces para contrarrestar y apoyar a los países con menos capacidades cibernéticas que a su vez son más vulnerables para ser "cómplices" o "anfitriones" de cibercriminales. En ese sentido, un papel muy importante en materia de ciberseguridad lo tienen la denominada diplomacia cibernética, que según Pawel Herczynski es empleada por la Unión Europea para establecer medidas de política exterior y de seguridad comunes a los países que la conforman.

Finalmente, experiencias internacionales de cooperación y comunicación eficaz para afrontar amenazas cibernéticas se demuestran a través de organizaciones como la Organización Internacional de Policía Criminal

(Interpol), en donde los países miembros colaboran de manera sinérgica con diversa información para enfrentar delitos comunes en esta materia.

A nivel Armadas de la región, en los últimos 10 años se vienen promoviendo y desarrollando ejercicios multinacionales dentro del marco de cooperación internacional como el ejercicio UNITAS, donde se realizan ejercicios prácticos de ciberataques y ciberdefensas entre los miembros de los países participantes.

Conclusiones

El esfuerzo de la OEA por incentivar a los países de la región en desarrollar sus propias estrategias nacionales de ciberseguridad es relevante, pero más aún es la cooperación internacional y comunicación a todo nivel para enfrentar las amenazas que se presentan en el dominio del ciberespacio.

Dentro de nuestro hemisferio se deben fomentar mayores ejercicios multinacionales al respecto, como los realizados por la Unión Europea, donde participen no sólo miembros de las fuerzas militares y de seguridad, sino, también, agencias gubernamentales de distintos países para que entiendan la importancia de la interoperabilidad en este campo.

En ese sentido, la capacitación y entrenamiento son claves para fortalecer las instituciones nacionales e internacionales, reduciendo la vulnerabilidad a las ciberamenazas. Organizaciones multilaterales como la OEA o el Comando Sur de los EE.UU., deben liderar mayores ejercicios que incluyan respuestas eficaces a ciberataques, que al final fomenten más conciencia cibernética, resiliencia y gestión de riesgo al respecto. Todo esto contribuirá al objetivo de la ciberseguridad propuesto por la UIT, y de esta manera favorecer a la preservación de las fuerzas y medios organizativos, humanos, financieros, tecnológicos e informativos de nuestros países y de la comunidad internacional.

Referencias

1. Bissell, K., & Ponemon, L. (2020). *The cost of cybercrime: Ninth annual cost of cybercrime study*. Accenture. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
2. Bijou, R. (2015, junio). *Governments don't understand cyberwarfare. We need hackers*. TED Talk. https://www.ted.com/talks/rodrigo_bijou_governments_don_t_understand_cyber_warfare_we_need_hackers#t-66917
3. Cardon, E., & McHenry, D. (2016). The relevance of culture. *Military Review English Edition, 97*(4), 34-39. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160831_art009.pdf
4. Comité Interamericano contra el Terrorismo. (2021). *¿Qué hacemos?* Organización de Estados Americanos. http://www.oas.org/es/sms/cicte/
5. Contreras, R. (2020, 9 de junio). El ciberterrorismo se viste de phishing. *Computing*. https://www.computing.es/seguridad/noticias/1119115002501/ciberterrorismo-se-viste-de-phishing.1.html
6. Espinosa, N. (2018, 7 de septiembre). *The five laws of cybersecurity*. TED Talk. https://www.ted.com/talks/nick_espinosa_the_five_laws_of_cybersecurity/transcript?language=es
7. Interpol. (2020). *Ciberdelincuencia: efectos de la COVID-19*. https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf?inLanguage=esl-ES
8. McChrystal, S. (2014, marzo). *The military case for sharing knowledge*. TED Talk. https://www.ted.com/talks/stanley_mcchrystal_the_military_case_for_sharing_knowledge
9. Newmeyer, K. (2015). Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal, 1*(3), 9–19.
10. Herczynski, P. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
11. Rey, F. (2020, 26 de enero). El Big Data, o cómo tus datos le han dado más poder a la economía y la política. *El Orden Mundial*. https://elordenmundial.com/big-data-poder-datos-economia-politica/
12. Schwab, K. (2016, 14 de enero). *The Fourth Industrial Revolution: What it means, how to respond*. World Economic Forum. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond
13. Toffler, A. (1980). *La tercera ola*. Plaza & Janes.
14. Unión Internacional de Telecomunicaciones. (2007). *Guía de ciberseguridad para los países en desarrollo*. Unión Internacional de Telecomunicaciones. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-S.pdf
15. Urrutia, F. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf