# INFRAESTRUCTURA CRÍTICA Y SU RELACIÓN CON LOS CIBERATAQUES: TENDENCIAS INTERNACIONALES

JOHANN GOLSWORTHY MIRANDA[1]
PAULINA CAROCA VALENCIA[2]

***Resumen:*** *Si bien el avance y dependencia de las tecnologías asociadas a la industria 4.0 han propiciado un uso masificado de Internet, como también un avance significativo del bienestar de la sociedad, el uso de estas tecnologías conlleva, a su vez, riesgos y amenazas, siendo uno de ellos los llamados "ciberataques", realizados por diferentes actores y motivaciones, los que incluso por su actuar han llegado a paralizar infraestructuras críticas vitales para la sociedad. En este contexto, este artículo tiene como objetivo analizar los impactos asociados a ciberataques efectuados en el último tiempo, con el propósito de reflexionar acerca de la importancia del desarrollo de una cultura en ciberseguridad que comprenda educación y acción acorde al avance tecnológico.*
***Palabras claves:*** *ataque informático, ciberseguridad, infraestructura crítica, actores, conflicto híbrido.*

***Abstract:*** *Although the progress and dependence on technologies associated with Industry 4.0 have led to a massive use of the Internet, as well as a significant progress in the welfare of society, the use of these technologies entails, in turn, risks and threats, one of them being the so-called "cyber-attacks", carried out by different actors and motivations, which even by their actions have paralyzed critical infrastructures vital to society. In this context, this article aims to analyze the impacts associated with cyber-attacks carried out in recent times, in order to reflect on the importance of developing a culture of cybersecurity that includes education and action in line with technological progress.*
***Keywords:*** *cyber-attack, cybersecurity, critical infrastructure, actors, hybrid conflict.*

---

1 Profesor Civil, Administrador Público de la Universidad de Santiago de Chile (USACH), Magíster en Ciencias Militares mención Gestión Estratégica de la Academia de Guerra del Ejército (ACAGUE). Actualmente se desempeña como Encargado de Planificación Académica de Postgrado y Educación Continua de la Academia Politécnica Militar (ACAPOMIL) del Ejército de Chile. Correo electrónico: jgolsworthy@acapomil.cl. ORCID: https://orcid.org/0000-0001-8062-2472.

2 Personal Civil, Administradora Pública de la Universidad de Santiago de Chile, actualmente se desempeña como Asesor Técnico de Subsistencias en la División de Adquisiciones del Ejército (DIVAE). Correo electrónico: paulina.caroca@usach.cl ORCID: https://orcid.org/0000-0003-4091-9532.

# INTRODUCCIÓN

En la actualidad, la competencia global por el desarrollo tecnológico e innovación que impulsa la industria 4.0: Internet de las cosas (IoT), *cloud computing*, IA, *machine learning*, entre otras,[3] ha propiciado el uso masivo del Internet. En cifras, para el año 2022 existían aproximadamente 5.282[4] millones de usuarios de Internet, a diferencia del año 2007 cuando existían 1.367 millones, mismo año en que ocurrió uno de los primeros ataques informáticos masivos en la historia a un Estado, que transformó a la República de Estonia[5] en uno de los países más desarrollados en el ámbito de la ciberseguridad en nuestros días.

En este orden de ideas, otro caso a destacar fueron los ciberataques a la República Democrática de Georgia en el conflicto bélico con la Federación Rusa en agosto de 2008, el que es considerado el primer ciberataque que coincidió con una acción bélica física, es decir la denominada "Guerra híbrida",[6] o el caso Stuxnet en 2010, el gusano que infectó una planta nuclear de la República Islámica de Irán, haciendo estallar las máquinas de enriquecimiento de Uranio.[7] Respecto a un *ransomware,*[8] el caso de WannaCry en 2017 fue uno de los primeros ciberataques de ámbito global, afectando 150 países del mundo e infectando más de 200 mil computadores mediante la explotación de una falla de Windows.[9]

En este contexto, de ataques informáticos emanados por motivos políticos, conflictos bélicos, sabotaje y *malware* de empleo global, este artículo tiene por objetivo analizar los impactos asociados a ciberataques efectuados en el último tiempo, en miras de reflexionar acerca de la importancia del desarrollo de una cultura en ciberseguridad que comprenda educación y acción acorde al avance tecnológico.

---

3 IBM. ¿Qué es la Industria 4.0? [en línea], [consulta el 01-08-2023]. Disponible en: https://www.ibm.com/mx-es/topics/industry-4-0

4 STATISTAS. Número de usuarios de Internet en el mundo entre 2005 hasta 2022. 2023. [En línea], [consulta el 01-08-2023], disponible en: https://es.statista.com/estadisticas/541434/numero-mundial-de-usuarios-de-internet/

5 En agosto de 2007 la República de Estonia fue objetivo de múltiples ciberataques por 22 días, los que ocurrieron dado un conflicto político entre Estonia y Rusia, el que fue desencadenado por la reubicación de un monumento de la ex Unión Soviética en la ciudad de Tallin. Los ataques principales fueron denegación de servicio DDoS o (DoS) o de denegación de servicio distribuido (DDoS), inyección SQL, entre otros, siendo el objetivo afectar servicios del gobierno, el parlamento, la policía, los bancos, los proveedores de servicios de Internet (ISP). Incluso en Internet se encontraban diferentes instrucciones para que usuarios rusos pudieran adherirse al ataque masivo a diferentes servicios de Estonia. OTTIS, Rain. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. 2007.[En línea], [Consulta el 01-08-2023]. Disponible en: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

6 Son conflictos que emplean estrategias convencionales por un lado y no convencionales, a su vez.

7 Stuxnet fue un *malware* sofisticado que se introdujo mediante una acción de sabotaje (por medio de la utilización de una memoria USB infectada) en una central nuclear iraní, este *malware* realizó una escalada de privilegios en miras de atacar los Sistemas Supervisory Control And Data Acquisition (SCADA) marca Siemens que daba las instrucciones a las centrífugas de uranio iraní, mediante un código complejo. El *malware* contenía cuatro "Zero Days" (vulnerabilidades de sistemas no reconocidas en ese momento), lo que según investigaciones requirió gran mano de obra y recursos para el desarrollo de esta pieza de *malware* considerada como la primera ciberarma. BAEZNER, Marie y ROBI, Patrice. Hotspot Analysis: Stuxnet. 2017. Center for Security Studies (CSS), ETH Zürich. [en línea], [consulta el 02-08-2023]. Disponible en https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

8 Este *ransomware* encripta documentos y extorsiona a sus usuarios a que paguen una suma de dinero, siendo este caso en bitcoins.

9 KASPERSKY. ¿Qué es el ransomware WannaCry? [En línea], [consulta el 02-08-2023]. Disponible en: https://www.kaspersky.es/resource-center/threats/ransomware-wannacry

# INFRAESTRUCTURA CRÍTICA Y RELACIÓN CON LOS CIBERATAQUES

Para entender los casos que se presentan en este artículo, es necesario conocer brevemente qué se entiende por infraestructura crítica[10] de un país. Para la Unión Europea, esta se define como: *"el elemento o sistema esencial para el mantenimiento de las funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar económico o social de la población".*[11] En este contexto, en Chile, mediante la Ley Nº 21.542 que modificó la Constitución Política de la República en el año 2023, se definió en su artículo Nº 32 que:

*"La infraestructura crítica comprende el conjunto de instalaciones, sistemas físicos o servicios esenciales y de utilidad pública, así como aquellos cuya afectación cause un grave daño a la salud o al abastecimiento de la población, a la actividad económica esencial, al medioambiente o a la seguridad del país. Se entiende por este concepto la infraestructura indispensable para la generación, transmisión, transporte, producción, almacenamiento y distribución de los servicios e insumos básicos para la población, tales como energía, gas, agua o telecomunicaciones; la relativa a la conexión vial, aérea, terrestre, marítima, portuaria o ferroviaria, y la correspondiente a servicios de utilidad pública, como los sistemas de asistencia sanitaria o de salud*".[12]

En este contexto, se puede considerar un ataque a la infraestructura crítica[13] un posible ciberataque que paralice los sistemas de transporte subterráneo, por ejemplo, del Metro de Santiago de Chile, que ocasionaría que más de un millón y medio de usuarios diarios[14] no puedan utilizar este medio de transporte, causando caos en el ámbito vial, como también problemas derivados, siendo uno de ellos, por ejemplo, que los servicios de emergencia no puedan trasladarse con rapidez a diferentes incidentes.

Por otro lado, también un ataque informático puede afectar la disponibilidad de los servicios de distribución de electricidad,[15] que, si bien afectaría a los hogares, otras infraestructuras críticas dependientes de este servicio podrían verse comprometidas, por ejemplo, el funcionamiento de

10 La definición de este concepto es a nivel de política de Estado, es decir puede variar.

11 DIRECTIVA. 2008/114/CE. Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. 2008. [En línea], [consulta el 02-08-2023]. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/protecting-critical-infrastructure.html#:~:text=Una%20infraestructura%20cr%C3%ADtica%20europea%20%28ICE%

12 LEY Nº 21.542. Modifica la carta fundamental con el objeto de permitir la protección de infraestructura crítica por parte de las Fuerzas Armadas, en caso de peligro grave o inminente. 2023. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1188583&tipoVersion=0

13 Esto es un ejemplo, ya que aún se debe identificar las infraestructuras críticas, ya sea públicas o privadas, según lo expresado en la Ley Nº 21.542, artículo Nº1, párrafo Nº2: "Una ley regulará las obligaciones a las que estarán sometidos los organismos públicos y entidades privadas a cargo de la infraestructura crítica del país, así como los criterios específicos para la identificación de la misma".

14 Según cifras del Instituto Nacional de Estadísticas (INE), el Metro de Santiago transportó 49,6 millones de personas en abril de 2023, por tanto, diariamente la cantidad aproximada fue de 1,653 millones de usuarios.

15 Situación que ya ha ocurrió, por ejemplo, en Ucrania (2015), donde un ciberataque contra la red eléctrica de dicho país dejó sin suministro eléctrico a 255.000 personas.

hospitales, aeropuertos, transporte eléctrico, entre otros, lo que en algunos casos podría afectar la vida de las personas.


Figura Nº 1: Infraestructura crítica esencial.

Fuente: [en línea], disponible en: https://www.dhs.gov/archive/coronavirus/cybersecurity-and-critical-infrastructure.

En este contexto, un ataque informático que afecte a estas infraestructuras (ver Figura Nº 1) puede representar una amenaza a la paz, como también a la seguridad de un país o grupo de países, entendiendo que existen infraestructuras críticas que traspasan fronteras, como gasoductos, vías de transporte, represas que regulan cursos de agua internacionales, entre otros, tendiendo a que un ataque a estas puede disminuir el bienestar de la sociedad y afectar la seguridad humana, siendo ambas una responsabilidad del Estado.

## ACTORES Y MOTIVACIONES

Entendiendo ya que un ciberataque puede afectar la infraestructura crítica de un Estado, se hace necesario conocer qué tipos de actores podrían realizar estas acciones, como también la motivación o fin asociado a ello (ver Figura Nº 2).

La figura responde a los actores y motivaciones en tiempos de paz, dado que, en un conflicto bélico, por ejemplo, entre dos Estados, los actores señalados pueden tomar bandos al igual que cambiar sus motivaciones iniciales, apoyando, ya sea porque el Estado en conflicto podría solicitar la ayuda de empresas locales, a grupos de *hacktivistas* que podrían aportar al bien común de la defensa.

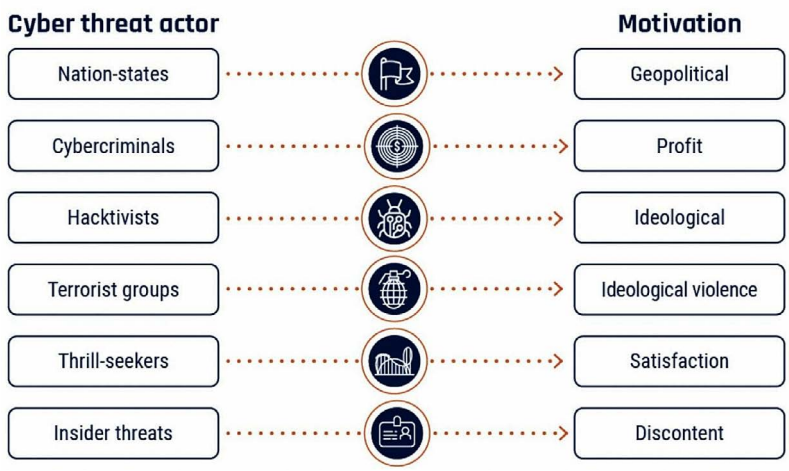


Figura Nº 2: Actores en el ciberespacio.

Fuente: [en línea], disponible en: https://thecyberstory.wordpress.com/2020/04/27/cyber-threat-actors-know-your-enemy/

Desde una perspectiva de los Estados, estos también pueden solicitar ayuda por medios diplomáticos. Un ejemplo de esto ha sido el apoyo en ciberseguridad que han brindado a Ucrania la Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea[16] como también Estados Unidos,[17] entre otros.

Con lo anterior, también es necesario reflexionar sobre el rol de las grandes empresas multinacionales o transnacionales, que, de igual forma como han aportado en la historia de los conflictos tradicionales "con medios físicos", en el conflicto desarrollado en el ciberespacio su apoyo puede ser crucial, específicamente las empresas del área de la tecnología, siendo un ejemplo en la actualidad, el apoyo que están suministrando a Ucrania las empresas: Google, Apple, Microsoft, Oracle, SAP, Nokia, Intel, AMD, CISCO,[18,19] entre otras.

## CASOS INTERNACIONALES DE CIBERATAQUES

A continuación, se presentarán tres casos de ciberataques realizados entre el año 2021-2023 identificando el desarrollo de estos, los actores y cómo aquellos impactaron el bienestar de la so-

16 EUROPEAN UNION. Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue. Diplomatic Service of the European Unión. 2022. [En línea], [consulta el 09-11-2023]. Disponible en: https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en#:~:text=The%20EU%20has%20provided%20%E2%82%AC29%20million%20to%20increase,further%20%E2%82%AC19%20million%20is%20supporting%20resilient%20digital%20transformation.

17 US. DEPARTAMENT OF STATE. U.S. Support for Connectivity and Cybersecurity in Ukraine. 2022 [En línea], [consulta el 09-11-2023]. Disponible en: https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

18 La empresa CISCO ha creado un grupo especial de trabajo en ciberdefensa, con el objeto de proteger a las personas y la infraestructura en Ucrania, mediante un monitoreo continuo, análisis de amenazas y respuesta.

19 CISCO. The War in Ukraine: Supporting our Customers, Partners, and Communities. 2023. [En línea], [consulta el 10-08-2023,]. Disponible en: https://www.cisco.com/c/m/en_us/crisissupport.html

ciedad. Además, se detallarán de forma breve dos casos ocurridos en Chile específicamente en el sector defensa.

## CONFLICTO RUSIA-UCRANIA

Unas pocas horas antes de la invasión a Ucrania ocurrida el 24 de febrero de 2023, se efectuó un ciberataque a la infraestructura terrestre del satélite KA-SAT[20] de la empresa Viasat, que proveía Internet satelital a miles de usuarios ucranianos y miles de decenas de otros clientes de banda ancha fija en toda Europa,[21] incluso otros medios afirmaron que también proveía estos servicios a parte de las defensas ucranianas.

Imagen N° 1: Aerogeneradores afectados.

Fuente: [en línea], disponible en: https://www.handelsblatt.com/unternehmen/energie/erneuerbare-energien-massive-stoerung-der-satellitenverbindung-enercon-meldet-fast-6000-betroffene-windanlagen/28114360.html?ticket=ST-7553140-pIu4EubEVdVLN1eXRJql-ap5

En este ataque, se explotó una configuración incorrecta de un dispositivo VPN para obtener un acceso remoto al segmento de administración de la red KA-SAT. Teniendo el acceso, el atacante procedió a realizar movimientos laterales hasta un segmento de la red específica, la que

20 Está acción se realizó mediante un virus "limpiador" llamado AcidRain, el que atacó los *módems* y enrutadores de la empresa estadounidense y borró todo su sistema.

21 VIASAT, Inc. KA-SAT Network cyber attack overview. 2022. [En línea], [consulta el 10-08-2023], disponible en: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

era utilizada para administrar y operar la red ejecutando comandos de administración legítimos y específicos en una gran cantidad de *módems* residenciales simultáneamente. Los intrusos ejecutaron comandos destructivos que llevaron a sobrescribir datos importantes en la memoria *flash* de los dispositivos *módems*, haciendo que estos no pudieran acceder a la red que proveía el Internet, dejándolos inutilizables.

Parte del impacto de este ataque fueron 5.800 generadores eólicos (ver Imagen Nº 1) de la empresa Enercon en Alemania, los que dejaron de funcionar por utilizar dichos *módems*.[22]

Finalmente, una vez determinada la gravedad de este ataque, rápidamente fue repudiado diplomáticamente por la Unión Europea, Estados Unidos y otros países.[23]

## EL CASO DE ANHALT-BITTERFELD, ALEMANIA Y LA DECLARACIÓN DE ESTADO DE EMERGENCIA

Ante los ciberataques, las decisiones que se tomen por parte de los actores estatales pueden ser múltiples. Sin embargo y en este contexto, existe un caso particular reciente que grafica el nivel de gravedad que podría alcanzar un ataque informático en un país o en una región dentro del mismo y las determinaciones tomadas para mitigarlo. Tal es el caso ocurrido en Anhalt-Bitterfeld, distrito de Sajonia-Anhalt, Alemania, que en el año 2021 sufrió una vulneración de sus sistemas informáticos estatales, paralizando las actividades gubernamentales de la región, a tal punto que impidió el pago oportuno de *"subsidios de vivienda o asistencia social"*,[24] los salarios de los funcionarios públicos, incluso afectando al sector privado, como fue el caso de la inscripción de vehículos comercializados por las concesionarias, las que al no poder registrar las ventas, no pudieron entregarlos a sus nuevos propietarios.

Este ataque significó, además, un retroceso en las labores estatales, pues obligó a los funcionarios públicos y a la ciudadanía a volver a la tramitación "tradicional", ralentizando las actividades públicas y privadas que se podían seguir realizando bajo esta metodología y paralizando por aproximadamente dos semanas[25] aquellas que no podían ejecutarse bajo esta modalidad.

---

22 HOWELL O'NEILL, Patrick. Una hora antes de la invasión, los *hackers* rusos ya habían atacado Ucrania. 2022. [En línea], [consulta el 15-08-2023]. Disponible en: https://www.technologyreview.es/s/14225/una-hora-antes-de-la-invasion-los-hackers-rusos-ya-habian-atacado-ucrania

23 DEUTSCHE WELLE (DW). UE responsabiliza a Rusia por ciberataque antes de la invasión. 2022. [En línea], [ consulta el 20-08-2023]. Disponible en: https://www.dw.com/es/ue-responsabiliza-a-rusia-por-ciberataque-a-red-satelital-antes-de-invasi%C3%B3n-a-ucrania/a-61752931

24 SUEDDEUTSCHE, Zetung. Cyberangriff in Sachsen-Anhalt: Wie Hacker einen Landkreis erpressen. 2021. [En línea], [consulta el 03-09-2023]. Disponible en: https://www.sueddeutsche.de/politik/hacker-anhalt-bitterfeld-1.5353265

25 POLITIK, Erster. Cyber-Katastrophenfall in Deutschland – Landkreis Anhalt-Bitterfeld lahmgelegt. (Primera catástrofe cibernética en Alemania: paralizado el distrito de Anhalt-Bitterfeld). 2021. [En línea], [consulta el 15-09-2023]. Disponible en: https://www.welt.de/politik/deutschland/article232427525/Anhalt-Bitterfeld-Hackerangriff-auf-Landkreis-loest-Katastrophenfall-aus.html

Pero técnicamente, ¿qué fue lo que ocurrió en Anhalt-Bitterfeld? Desde una visión en exceso simplificada y con el propósito de facilitar la comprensión del caso, este ataque se basó en la infección de servidores y equipos con un *malware*[26] llamado *"ransomware"*, que *"bloquea los datos o el dispositivo informático de una víctima y amenaza con mantenerlo bloqueado, o algo peor, a menos que la víctima pague un rescate al atacante"*.

En el caso de Anhalt-Bitterfeld, se infectaron varios servidores y equipos del distrito desde una fuente desconocida, cifrando una cantidad no estimada de archivos que imposibilitó su uso, ante lo cual la reacción de los usuarios fue apagar los equipos, suspender el funcionamiento del correo electrónico y desconectar los sistemas críticos para evitar la propagación del *malware* y la fuga de otros datos, además de los "secuestrados", dejando operativa solamente la red telefónica.[27,28]

Ante la grave situación informática que atravesó el distrito de Anhalt-Bitterfeld e independiente de la gran presión que ejerció el secuestro de información tan relevante, de la cual se desconoce el contenido, pero dada la gravedad del caso, incluso podría incluir datos personales de la ciudadanía, la decisión por parte de las autoridades fue declarar estado de emergencia en vez de "pagar un rescate" –principal objetivo de este tipo de ataques informáticos– para recuperar la información.

Conforme a lo declarado por el administrador del distrito de Anhalt-Bitterfeld, Andy Grabner, esta decisión se tomó como una forma de demostrar a los criminales que, *"como sector público, no nos dejaremos chantajear"*,[29] pese a que esta decisión podría diferir a nivel de gobierno estatal. No obstante, otro de los argumentos que fundamentó esta decisión distrital fue el hecho de que no se podría garantizar que, pagando el rescate, los criminales liberarían la información o no volverían a descifrarla después de recibir el pago y, además, que operar bajo estado de emergencia permitiría reaccionar con mayor celeridad.

¿Y por qué ocurrió este incidente? La debilidad identificada en los sistemas informáticos de Alemania en particular no respondía a un tema desconocido en el país: de hecho, se debe tener

---

26 El *malware* (forma abreviada de *software* malicioso) es un código de *software* que se escribe para dañar o destruir sistemas o redes, o para proporcionar acceso no autorizado a sistemas, redes o datos para usos delictivos o maliciosos. Casi siempre hay una forma de *malware* en la raíz de todos los tipos de ciberataque. Los ciberdelincuentes utilizan el *malware* para: mantener rehenes a usuarios y organizaciones a cambio de grandes sumas de dinero, tomar el control remoto no autorizado de los sistemas o servidores de otras personas, robar datos confidenciales (números de cuenta bancaria y de seguridad social de las personas, propiedad intelectual de las corporaciones, etc.) para fines de usurpación de identidad, ventaja competitiva y otros usos fraudulentos, lanzar ataques paralizantes a los sistemas que se ejecutan en empresas, agencias gubernamentales, empresas públicas u otras instituciones. IBM. ¿Qué es el malware? [En línea], [consulta el 15-09-2023]. Disponible en: https://www.ibm.com/mx-es/topics/malware

27 DEUTSCHE WELLE. Rural German district declares disaster after cyberattack. 2021. [En línea], [consulta el 16-09-2023]. Disponible en: https://www.dw.com/en/rural-german-district-declares-disaster-after-cyberattack/a-58227484

28 DEUTSCH, Víctor. La catástrofe de Anhalt-Bitterfeld y el nuevo modelo de ciberseguridad para administraciones locales. 2021. [En línea], [consulta el 16-09-2023]. Disponible en: https://www.telefonicaempresas.es/grandes-empresas/blog/ciberseguridad-para-administraciones-locales/

29 SUEDDEUTSCHE, *op. cit.*

en cuenta que, a nivel mundial, la infraestructura informática germana –y sobre todo la municipal, centrándose en el caso analizado– es una de las más débiles y, por tanto, franqueable por ciber-criminales.[30] En este sentido y en concordancia con los datos extraídos desde la Encuesta sobre el Futuro Global de la Cibernética del año 2023, elaborada por Deloitte Touche Tohmatsu Limited, Alemania junto con el Reino Unido concentran la mayor cantidad de incidentes informáticos dentro de Europa (ver Figura Nº 3).

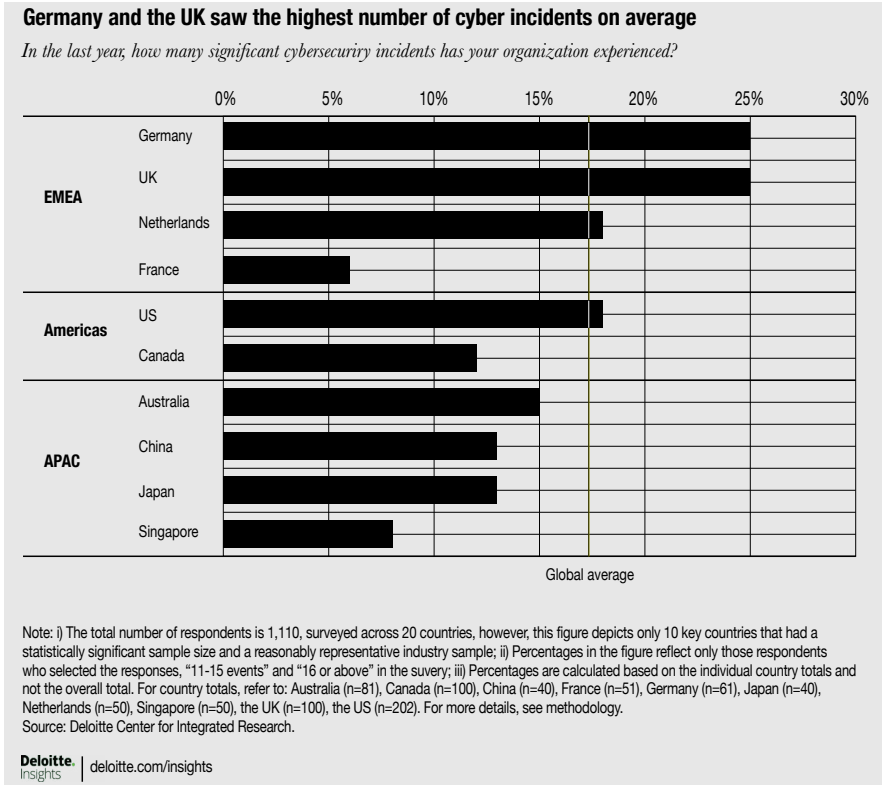


Figura Nº 3: Alemania y el Reino Unido en promedio evidenciaron el mayor número de incidentes informáticos.

Fuente: [en línea], disponible en: https://www2.deloitte.com/uk/en/insights/topics/cyber-risk/global-cybersecurity-threat-trends.html?_x_tr_hist=true

A su vez, Alemania concentra la mayor cantidad de incidentes de *malware* durante el año 2021, lo que se relaciona también con el nivel de preocupación de la región, respecto a los incidentes de *phishing, malware* y *ransomware*, lo cual es coherente con el caso analizado, al evidenciar que la principal amenaza para las organizaciones gubernamentales, como los municipios, podría ser un ataque por *phishing* (ver Figura Nº 4).

30 POLITIK, *op. cit.*

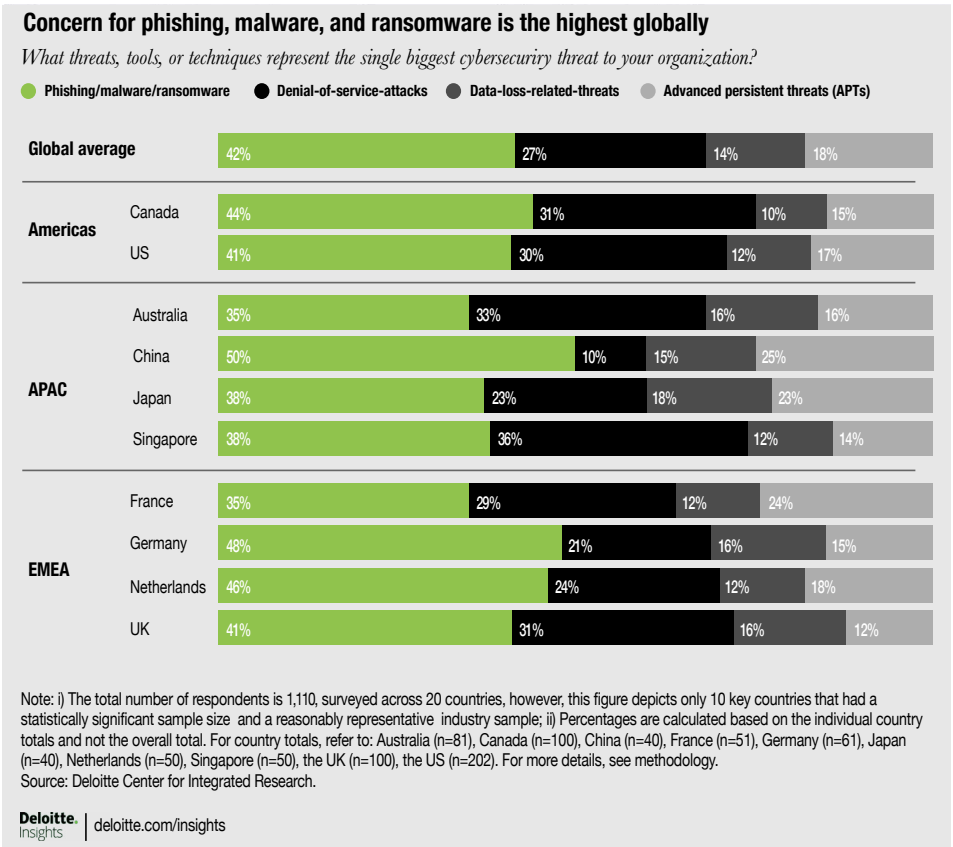


Figura Nº 4: La preocupación por el *phishing*, el *malware* y el *ransomware* es la más alta a nivel mundial.

Fuente: [en línea], disponible: https://www2.deloitte.com/uk/en/insights/topics/cyber-risk/global-cybersecurity-threat-trends.html?_x_tr_hist=true

Ahora bien, retomando el caso de Alemania, presumiblemente el ataque analizado se deba a que, la gran mayoría de las veces, los municipios cuentan con tecnología obsoleta y un departamento de informática que no se encuentra lo suficientemente robustecido y capacitado para enfrentar ataques cibernéticos, lo que a su vez pone en riesgo la información que, a este nivel, se maneja de la ciudadanía. En este mismo orden de ideas, el ataque informático se efectuó bajo el actuar sistemático y constante de cibercriminales que buscaron en Internet y por medio de programas de búsqueda avanzados,[31] denominados *crawlers*,[32] una vulnerabilidad que les permitiese el ingreso a los sistemas informáticos de la administración municipal de Anhalt-Bitterfeld.

31 SUEDDEUTSCHE, *op. cit.*

32 Un *crawler* es un algoritmo programado para recorrer el código HTML de una página web, en miras de recopilar información y almacenarla.

En este sentido, cabe hacer presente que, aun cuando los cibercriminales hayan hecho ingreso a los sistemas informáticos, la decisión tomada por las autoridades permitió responder oportunamente a la crisis, no obstante y de acuerdo a lo señalado por Castillo,[33] una consecuencia de no pagar el rescate que los cibercriminales exigían hizo que estos publicaran finalmente la información recopilada en el ataque, a través de la *dark web*,[34] dejando de público conocimiento información sensible "secuestrada".

Por otro lado, las consecuencias financieras de este ataque se estiman entre 1,7 a 2 millones de euros, presupuesto que, según Castillo,[35] estaba destinada a proyectos de digitalización y modernización de equipos informáticos, de modo que los avances tuvieron que verse retrasados por la reasignación de este presupuesto para otros fines. Sin embargo, la mayor consecuencia negativa corresponde a la merma en la confianza de la ciudadanía en las instituciones públicas y en la seguridad que puedan brindarle a la información que es de su responsabilidad.

Ahora bien, como una manera de afrontar este tipo de ataques, diversos expertos y autoridades alemanas del área de crisis dieron lugar, en septiembre del año 2023, a dos ejercicios de simulación de ciberataque denominado "LÜKEX",[36] cuyo objetivo era atacar al Gobierno y a la administración pública germana.

Este ejercicio no es nuevo, sin embargo y de acuerdo a lo afirmado por Tiesler,[37] jefe de la Oficina Federal de Protección Civil y Gestión de Catástrofes, *"en términos de número de involucrados, se trata del mayor ejercicio LÜKEX jamás realizado"* y, además, *"por primera vez en sus casi 20 años participan todos los estados federados"*, de modo tal que la convocatoria al ejercicio fue significativa. Este ejercicio contempló nuevos escenarios, los cuales no se han dado a conocer para no verse expuesto y contó con la participación de unas 60 autoridades, empresas y un total de 3.000 personas, con el fin de "pasar desapercibido" frente a la población alemana.

---

33 CASTILLO, Ernesto. La ciberdefensa en el Desarrollo y Seguridad Nacional. Cuadernos de Estrategia vol Nº1, Centro de Altos Estudios Nacionales. 2022. [En línea], [consulta el 05-10-2023]. Disponible en: https://caen.edu.pe/wp-content/uploads/2022/11/CUADERNO-DE-ESTRATEGIA-FINAL.pdf

34 La *dark web* es el conjunto oculto de sitios de Internet a los que solo se puede acceder mediante un navegador web especializado. Se utiliza para mantener la actividad de Internet privada y en el anonimato, lo que puede ser útil tanto en aplicaciones legales como ilegales. Si bien algunos la utilizan para evadir la censura del gobierno, también se sabe que se usa para actividades altamente ilegales. KASPERSKY. ¿Qué es la Deep Web y la Dark Web? [En línea], [consulta el 20-09-2023]. Disponible en: https://www.kaspersky.es/resource-center/threats/deep-web

35 CASTILLO, *op. cit.*

36 LÜKEX corresponde a la sigla de Länder- und Ressortübergreifende Krisenmanagementübung (Exercise), que por su traducción al español significa "ejercicio de gestión de crisis entre países y entre servicios".

37 MSN. Alemania comienza simulacro nacional de ciberataque. 2023. [En línea], [consulta el 21-09-2023]. Disponible en https://www.msn.com/es-us/noticias/other/alemania-comienza-simulacro-nacional-de-ciberataque/ar-AA1hl47D

El ejercicio LÜKEX, según la Oficina Federal de Protección Civil y Gestión de Catástrofes, tiene como propósito *"mejorar la gestión conjunta de crisis de los gobiernos federal y de los Estados federados, incluidas las organizaciones de ayuda y las empresas de infraestructura crítica, a nivel estratégico. Para ello, se diseña una situación de crisis ficticia pero realista, que sirve de punto de partida y marco para el ejercicio"*,[38] de modo tal que resulta un excelente ejercicio de proyección y anticipación ante diversos problemas que se dan en la sociedad y que podrían repercutir en los sistemas informáticos.

## IFX NET WORKS EN LA MIRA; EL CASO QUE AFECTÓ A CHILE, COLOMBIA Y OTROS PAÍSES DE AMÉRICA

Un ataque que no ocurrió directamente en Chile, pero que lo afectó de manera indirecta, corresponde al ciberataque que sufrió IFX Networks en el año 2023, multinacional de servicios tecnológicos con presencia en 17 países, distribuidos entre toda América (Norte, Centro y Sur). En el caso de Colombia, afectó a los servicios digitales de 32 entidades del sector público, poniendo en riesgo la información de la ciudadanía, en el ámbito estatal, y de los usuarios y clientes, en el ámbito privado.

Esta fue atacada con un *malware*, del cual se desconoce la potencial vía de ingreso, puesto que, al haber sido atacada la empresa, solo ella puede determinar la forma de *hackeo*, independiente de toda la ayuda que pueda recibir de los Gobiernos de los países a los cuales presta sus servicios, entre los cuales puede estar Colombia, Chile, Ecuador o Panamá, donde también existió un perjuicio ocasionado por el ataque.

En particular para el caso de Colombia, el consejero presidencial para la Transformación Digital de Colombia, Saúl Kattan,[39] señaló a Caracol Radio que *"Es un ataque de ransomware a IFX Networks"*, donde *"secuestraron los datos que tenía IFX en sus servidores (...) hay involucradas entidades importantes como la rama judicial y la rama de salud"*. Tal fue el daño, que obligó a que la rama judicial suspendiera los procesos judiciales en curso y varios portales gubernamentales vieron limitado su acceso y uso.

Por el lado de Colombia, este ataque infundió una gran disconformidad en el Gobierno: el ministro de Tecnologías de la Información y las Comunicaciones, Mauricio Lizcano, señaló que:

38 LÜKEX. Krisenübung für den Bevölkerungsschutz. 2023. [En línea], [consulta el 22-09-2023]. Disponible en: https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/luekex_node.html

39 DEUTSCHE WELLE. Ciberataque afecta a servicios estatales en Colombia y Chile. 2023. [En línea], [consulta el 23-09-2023]. Disponible en https://www.dw.com/es/ciberataque-afecta-a-servicios-estatales-en-colombia-y-chile/a-66818237

*"Este no es un ataque al Gobierno. Es un ataque a una empresa privada que no previó todos los mecanismos de seguridad que se habían puesto, es un fallo de la compañía. Si no se logra resolver el problema para este domingo, invitaré a un comité de expertos internacionales a que lo resuelvan".*[40]

Y este caso, ¿cómo afectó a Chile?

El efecto que conllevó este ataque fue que el portal de adquisiciones del Estado chileno, www.mercadopublico.cl, se viera afectado en cuanto a la disponibilidad en su uso. Por ello, el día 13 de septiembre de 2023, mediante un comunicado oficial[41] entregado por la plataforma, se da a conocer del ataque informático a la empresa IFX Networks, que es el proveedor de la infraestructura tecnológica del portal.

Por su parte, IFX Networks señaló que el ataque habría afectado a la infraestructura colombiana por medio de un *ransomware* y que, pese a lo anterior, *"no se ha evidenciado un compromiso a la integridad de los datos ni de la información de sus clientes y proveedores".*[42]

Ahora bien, ChileCompra y la plataforma de Mercado Público se han recuperado y han habilitado el funcionamiento paulatinamente, encontrándose en la actualidad "operando con normalidad"[43] y, a su vez, enfrentando cualquier eventual incidencia para mantener el funcionamiento habitual de la plataforma y así no generar dificultades a los organismos públicos en sus procesos adquisitivos. Es relevante señalar también que el incidente tardó aproximadamente 15 días corridos en ser superado, recuperando la funcionalidad del portal casi por completo, pues, dada la experiencia de algunos usuarios, la plataforma sigue con funcionamiento intermitente en algunos módulos.

## CASO ESTADO MAYOR CONJUNTO (EMCO)

En 2022, el EMCO fue víctima de un ataque informático realizado por el grupo *hacktivista* Guacamaya. Esta agrupación filtró más de 300 mil archivos en Internet (correos electrónicos). Según las fuentes abiertas, entre los documentos filtrados se encontrarían apreciaciones sobre el estallido social, gastos de las Fuerzas Armadas durante el Estado de Excepción en las regiones

40 SEMANA. El Estado colombiano "cibersecuestrado": 32 entidades están bajo el grave ataque de los *hackers* y aún las consecuencias son inciertas. 2023. [En línea], [consulta el 24-09-2023]. Disponible en https://www.semana.com/politica/articulo/el-estado-colombiano-cibersecuestrado-32-entidades-estan-bajo-el-grave-ataque-de-los-hackers-y-aun-las-consecuencias-son-inciertas/202329/

41 Puede encontrar el comunicado oficial en: https://chilecompra-notifications.s3.amazonaws.com/Indisponibilidad-MercadoPublico/comunicados/2023+09+13+informacion+usuarios+caida+MP+13.53.pdf

42 FUENTES, Sofía. Problemas de ciberseguridad mantienen paralizadas las operaciones de Mercado Público. 2023. [En línea], [consulta el 25-09-2023]. Disponible en: https://www.df.cl/economia-y-politica/laboral-personas/problema-de-ciberseguridad-afecta-a-mercado-publico

43 CHILECOMPRA. ChileCompra informa medidas y comunicaciones tras ciberataque a www.mercadopublico.cl. 2023. [En línea], [consulta el 25-09-2023]. Disponible en: https://www.chilecompra.cl/2023/10/chilecompra-informa-medidas-y-comunicaciones-tras-ciberataque-a/

del Biobío y La Araucanía, entre otros,[44] situación que afecto a la seguridad de la nación, dada su naturaleza de material sensible.

## CASO RHYSIDA: *RANSOMWARE* ATACA A EJÉRCITO DE CHILE

El 27 de mayo de 2023, la red de transmisión de datos del Ejército de Chile fue afectada por el *ransomware* Rhysida,[45] que paralizó diferentes sistemas de la institución. En este contexto, se tomaron diferentes medidas para aislar la red y realizar el trabajo de recuperación.[46]

## IMPORTANCIA DEL DESARROLLO Y EDUCACIÓN EN CIBERSEGURIDAD EN CHILE

De forma breve, en Chile existen diversas iniciativas estatales que han llegado a robustecer la ciberseguridad, siendo algunas de ellas: la implementación del Convenio de Budapest (2016)[47] y segundo protocolo de este,[48] la Política Nacional de Ciberseguridad (2017-2022),[49] la Política Nacional de Ciberdefensa (2018),[50] Política de la Defensa Nacional de Chile (2020),[51] la Ley Nº 21.459, que Establece Normas Sobre Delitos Informáticos (…),[52] la Ley Nº 21.542, que modifica la Carta Fundamental con el objeto de permitir la Protección de Infraestructura Crítica por parte de las Fuerzas Armadas, en caso de Peligro Grave o Inminente (2023),[53] la futura Ley Marco sobre Ciberseguridad e Infraestructura Crítica (En trámite)[54] y la Ley de Protección de Datos Personales (en trámite),[55] entre otras.

Con lo anterior, cabe destacar que el 25 de mayo del 2023 fue presentada la propuesta de Política Nacional de Ciberseguridad (2023-2028),[56] teniendo cinco objetivos estratégicos: "infraestructura

---

44 EL MOSTRADOR. Hackeo al Estado Mayor Conjunto: Monsalve confirma que ciberataque ocurrió en mayo de este año. 2022. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.elmostrador.cl/destacado/2022/09/24/hackeo-al-estado-mayor-conjunto-monsalve-confirma-que-ciberataque-ocurrio-en-mayo-de-este-ano/

45 El informe técnico realizado por el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT), se encuentra disponible en: https://www.csirt.gob.cl/media/2023/07/14TCA23-00011-01.pdf

46 ORTIZ, Florencia. Ejército de Chile descarta que *hackeo* haya afectado sistemas críticos de información. BiobioChile. 2023. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.biobiochile.cl/noticias/nacional/chile/2023/05/29/ejercito-de-chile-descarta-que-hackeo-haya-afectado-sistemas-criticos-de-informacion.shtml

47 [En línea]. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf

48 [En línea]. Disponible en: https://csirt.gob.cl/noticias/chile-firma-segundo-protocolo-budapest/

49 Puede revisar la norma en el siguiente enlace: https://biblioteca.digital.gob.cl/bitstream/handle/123456789/738/Pol%c3%adtica%20Nacional%20de%20Ciberseguridad.pdf?sequence=1&isAllowed=y

50 Puede revisar la política en el siguiente enlace: https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

51 Puede revisar la política en el siguiente enlace: http://163.247.42.118/transparencia/POLDEF/POLDEF2020/POLDEF2020.pdf

52 Puede revisar la norma en el siguiente enlace: https://www.bcn.cl/leychile/navegar?idNorma=1177743

53 Puede revisar la norma en el siguiente enlace: https://www.bcn.cl/leychile/navegar?idNorma=1188583&tipoVersion=0

54 Puede acceder al estado de tramitación de esta Ley en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06

55 Puede acceder al estado de tramitación de esta Ley en: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11092-07

56 CSIRT. Gobierno presentó su propuesta de nueva Política Nacional de Ciberseguridad. 2023. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.ciberseguridad.gob.cl/noticias/gobierno-presento-su-nueva-politica-nacional-de-ciberseguridad/

resiliente", "derechos de las personas", "cultura de ciberseguridad", "coordinación nacional e internacional" y "fomento a la industria y la investigación científica".

En este orden de ideas, resulta claro la cultura en ciberseguridad,[57] que incluye el ámbito de educación: es decir, crear capital humano en ciberseguridad; expertos que cada vez son más demandados en el mercado del trabajo. Esta situación ha sido considerada por la oferta académica del sistema de educación chileno, el cual ha tendido de forma recurrente a ofrecer cursos, diplomados y posgrados en el ámbito, como también instituciones certificadoras de competencias internacionales específicas en ciberseguridad. Ante esto, también cabe recalcar los esfuerzos de las Fuerzas Armadas que, si bien capacitan al personal internamente, desde el ámbito académico se destaca el Ejército de Chile, que impartió el primer programa de Magíster en Ciberdefensa realizado por la Academia Politécnica Militar entre los años 2021-2023,[58] buscando robustecer las capacidades institucionales en la materia y, por ende, fortalecer el bien público de la defensa, ya que, como se puede evidenciar en los conflictos híbridos actuales, el conflicto se traslada a lo digital, con impactos tangibles en la sociedad. Es por esto que resulta fundamental avanzar en el desarrollo de marco legal, medidas técnicas, definición de estructuras de seguridad, cultura en ciberseguridad y la cooperación internacional.[59]

## CONCLUSIONES

Los ataques informáticos analizados en este artículo, realizados por diferentes actores, evidencian cómo estos ocasionan un daño significativo al bienestar de las personas, siendo posible llegar inclusive a un daño físico, afectando la seguridad humana. En este contexto y dada la revisión de casos, se puede apreciar como la guerra híbrida es nuevamente observada en Ucrania en ciberataques días previos a la invasión, siendo este un símil del caso ocurrido en Georgia (2008).

Desde el punto de vista del cibercrimen, cada vez se hacen más comunes los secuestros de información por los denominados *ransomware*, donde una vulnerabilidad detectada es explotada en diferentes instituciones, ya sean públicas o privadas, en búsqueda de beneficios financieros, lo que refleja los casos de WannaCry (2007), Alemania (2021), Colombia (2023), Ejército de Chile (2023), entre otros,[60] evidenciando también la presencia de grupos de *hacktivistas* que filtran información, siendo este el caso de EMCO (2022).

---

57 Este eje se encontraba incluido en la Política de Ciberseguridad año 2017-2022, el que se busca profundizar en la propuesta de política 2023-2028.

58 SUBSECRETARÍA DE DEFENSA. Subsecretario de Defensa inaugura primer Magíster en Ciberdefensa. 2021. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.ssdefensa.cl/n10058_06-08-2021.html

59 MARTÍNEZ, Ricardo. Discurso de apertura del Seminario "Ciberespacio: desafíos para la seguridad y defensa de Chile en el siglo XXI". *Revista Escenarios Actuales*. 2018. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.dropbox.com/sh/skj1xqkh9bkxbwy/AABooEts30YYNejKcYaoDqn_a/6)%202018?dl=0&preview=4_2018.pdf&subfolder_nav_tracking=1

60 Otras instituciones como el Banco Estado (2020) y el Poder Judicial (2022) también fueron víctimas de ataques de *ransomware* con diferentes magnitudes.

Desde la perspectiva de la infraestructura crítica, los ataques presentados conllevan un daño al bienestar de un Estado. Por una parte, el ciberataque a la infraestructura terrestre del satélite KA-SAT (2023) produjo un daño en las comunicaciones de la infraestructura de energía de Alemania y, por otro, el caso de IFX Networks, donde el ataque informático a una empresa privada provocó problemas a sitios web de gestión del Estado.

Con lo anterior, Chile no ha estado ajeno a los riesgos y amenazas presentes en el ciberespacio, ante esto cabe destacar los diferentes esfuerzos en la implementación de las políticas nacionales, tanto de ciberseguridad como de ciberdefensa, siendo estas cruciales para el desarrollo general de la ciberseguridad a nivel de política de Estado perdurable, que permite seguir incentivando la articulación público-privada, la cultura, educación en ciberseguridad, entre otras, entendiendo siempre que un ataque informático no solo afecta el funcionamiento de los sistemas, sino que también podría afectar de manera directa el bienestar de la sociedad.

A modo general, este artículo deja diferentes interrogantes no abarcadas, siendo estas: cómo las tecnologías de la Industria 4.0, (en específico, la Inteligencia Artificial) podrán mejorar los sistemas de ciberseguridad o cómo en un futuro la computación cuántica afectará los sistemas de cifrado, entre otros desafíos. Pero antes de investigar el futuro es necesario reflexionar las siguientes palabras de Bill Gates: *"Internet se está convirtiendo en la plaza del pueblo de la aldea global del mañana"*[61] y ante este enunciado, ¿realmente logramos entender el rol de la seguridad en la plaza del pueblo?

## BIBLIOGRAFÍA

BAEZNER, Marie y ROBI, Patrice. Hotspot Analysis: Stuxnet. Center for Security Studies (CSS), ETH Zürich. 2017. [En línea], [consulta el 02-08-2023]. Disponible en: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

CASTILLO, Ernesto. "La Ciberdefensa en el Desarrollo y Seguridad Nacional". *Cuadernos de Estrategia* vol. Nº 1, Centro de Altos Estudios Nacionales. 2022. [En línea], [consulta el 05-10-2023]. Disponible en: https://caen.edu.pe/wp-content/uploads/2022/11/CUADERNO-DE-ESTRATEGIA-FINAL.pdf

CHILECOMPRA. ChileCompra informa medidas y comunicaciones tras ciberataque a www.mercadopublico.cl. 2023. [En línea], [consulta el 25-09-2023]. Disponible en: https://www.chilecompra.cl/2023/10/chilecompra-informa-medidas-y-comunicaciones-tras-ciberataque-a/

61 GATES, Bill. Business @ The Speed of Thought. 1999. [En línea], [consulta el 03-11-2023]. Disponible en: https://onlinelibrary.wiley.com/doi/abs/10.1111/1467-8616.00097

CISCO. The War in Ukraine: Supporting our Customers, Partners, and Communities. 2023. [En línea], [consulta el 10-08-2023]. Disponible en: https://www.cisco.com/c/m/en_us/crisissupport.html

CSIRT. Gobierno presentó su propuesta de nueva Política Nacional de Ciberseguridad. 2023. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.ciberseguridad.gob.cl/noticias/gobierno-presento-su-nueva-politica-nacional-de-ciberseguridad/

DEUTSCH, Víctor. La catástrofe de Anhalt-Bitterfeld y el nuevo modelo de ciberseguridad para administraciones locales. 2021. [En línea], [consulta el 16-09-2023]. Disponible en: https://www.telefonicaempresas.es/grandes-empresas/blog/ciberseguridad-para-administraciones-locales/

DIRECTIVA. 2008/114/CE. Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. 2008. [En línea], [consulta el 02-08-2023]. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/protecting-critical-infrastructure.html#:~:text=Una%20infraestructura%20cr%C3%ADtica%20europea%20%28ICE%

DEUTSCHE WELLE. Ciberataque afecta a servicios estatales en Colombia y Chile. 2023. [En línea], [consulta el 23-09-2023]. Disponible en: https://www.dw.com/es/ciberataque-afecta-a-servicios-estatales-en-colombia-y-chile/a-66818237

DEUTSCHE WELLE. Rural German district declares disaster after cyberattack. 2021. [En línea], [consulta el 16-09-2023]. Disponible en: https://www.dw.com/en/rural-german-district-declares-disaster-after-cyberattack/a-58227484

DEUTSCHE WELLE. UE responsabiliza a Rusia por ciberataque antes de invasión. 2022. [En línea], [consulta el 20-08-2023]. Disponible en: https://www.dw.com/es/ue-responsabiliza-a-rusia-por-ciberataque-a-red-satelital-antes-de-invasi%C3%B3n-a-ucrania/a-6175293

EL MOSTRADOR. Hackeo al Estado Mayor Conjunto: Monsalve confirma que ciberataque ocurrió en mayo de este año. 2022. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.elmostrador.cl/destacado/2022/09/24/hackeo-al-estado-mayor-conjunto-monsalve-confirma-que-ciberataque-ocurrio-en-mayo-de-este-ano/

EUROPEAN UNION. Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue. Diplomatic Service of the European Unión. 2022. [En línea], [consulta el 09-11-2023]. Disponible en: https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-

FUENTES, Sofía. Problemas de ciberseguridad mantienen paralizadas las operaciones de Mercado Público. 2023. [En línea], [consulta el 25-09-2023]. Disponible en: https://www.df.cl/economia-y-politica/laboral-personas/problema-de-ciberseguridad-afecta-a-mercado-publico

GATES, Bill. Business @ The Speed of Thought. 1999. [En línea], [consulta el 03-11-2023]. Disponible en: https://onlinelibrary.wiley.com/doi/abs/10.1111/1467-8616.00097

HOWELL O'NEILL, Patrick. Una hora antes de la invasión, los hackers rusos ya habían atacado Ucrania. 2022. [En línea], [consulta el 15-08-2023]. Disponible en: https://www.technologyreview.es/s/14225/una-hora-antes-de-la-invasion-los-hackers-rusos-ya-habian-atacado-ucrania

IBM. ¿Qué es el malware? [En línea], [consulta el 15-09-2023]. Disponible en: https://www.ibm.com/mx-es/topics/malware

IBM. ¿Qué es la Industria 4.0? [En línea], [consulta el 01-08-2023]. Disponible en: https://www.ibm.com/mx-es/topics/industry-4-0

KASPERSKY. ¿Qué es el ransomware WannaCry? [En línea], [consulta el 02-08-2023]. Disponible en: https://www.kaspersky.es/resource-center/threats/ransomware-wannacry

KASPERSKY. ¿Qué es la Deep Web y la Dark Web? [En línea], [consulta el 20-09-2023]. Disponible en: https://www.kaspersky.es/resource-center/threats/deep-web

LEY 21.542. Modifica la carta fundamental con el objeto de permitir la protección de infraestructura crítica por parte de las Fuerzas Armadas, en caso de peligro grave o inminente. 2023. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1188583&tipoVersion=0

LÜKEX. Krisenübung für den Bevölkerungsschutz. 2023. [En línea], [consulta el 22-09-2023]. Disponible en: https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/luekex_node.html

MARTÍNEZ, Ricardo. Discurso de apertura del Seminario "Ciberespacio: desafíos para la seguridad y defensa de Chile en el siglo XXI". Revista *Escenarios Actuales*. 2018. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.dropbox.com/sh/skj1xqkh9bkxbwy/AABooEts30YYNejKcYaoDqn_a/6)%202018?dl=0&preview=4_2018.pdf&subfolder_nav_tracking=1

MSN. Alemania comienza simulacro nacional de ciberataque. 2023. [En línea], [consulta el 21-09-2023]. Disponible en: https://www.msn.com/es-us/noticias/other/alemania-comienza-simulacro-nacional-de-ciberataque/ar-AA1hl47D

ORTIZ, Florencia. Ejército de Chile descarta que hackeo haya afectado sistemas críticos de información. BiobioChile. 2023. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.biobiochile.cl/noticias/nacional/chile/2023/05/29/ejercito-de-chile-descarta-que-hackeo-haya-afectado-sistemas-criticos-de-informacion.shtml

OTTIS, Rain. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. 2007. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. [En línea], [consulta el 01-08-2023]. Disponible en: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

POLITIK, Erster. Cyber-Katastrophenfall in Deutschland – Landkreis Anhalt-Bitterfeld lahmgelegt. (Primera catástrofe cibernética en Alemania: paralizado el distrito de Anhalt-Bitterfeld). 2021. [En línea], [consulta el 15-09-2023]. Disponible en: https://www.welt.de/politik/deutschland/article232427525/Anhalt-Bitterfeld-Hackerangriff-auf-Landkreis-loest-Katastrophenfall-aus.html

SEMANA. El Estado colombiano "cibersecuestrado": 32 entidades están bajo el grave ataque de los hackers y aún las consecuencias son inciertas. 2023. [En línea], [consulta el 24-09-2023]. Disponible en: https://www.semana.com/politica/articulo/el-estado-colombiano-cibersecuestrado-32-entidades-estan-bajo-el-grave-ataque-de-los-hackers-y-aun-las-consecuencias-son-inciertas/202329/

STATISTAS. Número de usuarios de Internet en el mundo entre 2005 hasta 2022. 2023. [En línea], [consulta el 01-08-2023]. Disponible en: https://es.statista.com/estadisticas/541434/numero-mundial-de-usuarios-de-internet/

SUBSECRETARÍA DE DEFENSA. Subsecretario de Defensa inaugura primer Magíster en Ciberdefensa. 2021. [En línea], [consulta el 11-11-2023]. Disponible en: https://www.ssdefensa.cl/n10058_06-08-2021.html

SUEDDEUTSCHE, Zetung. Cyberangriff in Sachsen-Anhalt: Wie Hacker einen Landkreis erpressen. 2021. [En línea], [consulta el 03-09-2023]. Disponible en: https://www.sueddeutsche.de/politik/hacker-anhalt-bitterfeld-1.5353265

US. DEPARTAMENT OF STATE. U.S. Support for Connectivity and Cybersecurity in Ukraine. 2022 [En línea], [consulta el 09-11-2023]. Disponible en: https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

VIASAT, Inc. KA-SAT Network cyber attack overview. 2022. [En línea], [consulta el 10-08-2023]. Disponible en: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview