DESAFÍOS DE LA TECNOLOGÍA 5G EN EL ÁMBITO DE LA CIBERSEGURIDAD

Challenges of 5G technology in the field of cybersecurity

MAY. Juan Pablo Nieny Hodar*

Resumen: En plena *Cuarta Revolución Industrial* (4RI), la tecnología avanza a una velocidad que supera la capacidad de los estados para adaptarse. En ese sentido, la implementación de la tecnología 5G en Chile, prevista para inicios del 2022, presenta amplias oportunidades para muchas áreas, como el teletrabajo, la telemedicina, la modernización del Estado, el desarrollo de capacidades estratégicas, las ciudades inteligentes, el aumento de la productividad, el internet de las cosas (IoT), el e-commerce, entre otras; sin embargo, los desafíos son insospechados. Por consiguiente, los estados no solo deben asumir que existirán riesgos, sino también potenciales problemas de seguridad. El presente artículo revisarán los desafíos que se generan a partir de la implementación de la tecnología 5G en el ámbito de la ciberseguridad.

Palabras claves: 5G, ciberseguridad, desafíos

Abstract: In the midst of the *Fourth Industrial Revolution* (4IR), technology is advancing at a speed that exceeds the ability of states to adapt. Accordingly, the implementation of 5G technology in Chile, scheduled for early 2022, presents opportunities for many areas, such as teleworking, telemedicine, modernization of the State, the development of strategic capacities, smart cities, increased productivity, the internet of things (IoT) and e-commerce, among others. However, these opportunities present unsuspected challenges. Therefore, States must not only assume that there will be risks, but also challenges to national security. The article will revise these security challenges arising from the implementation of 5G technology in the area of cybersecurity.

* Oficial del Arma de Caballería Blindada. Magíster en Ciencias Militares con mención en Gestión Estratégica. Actualmente es alumno del Tercer año del Curso Regular de Estado Mayor en la Academia de Guerra del Ejército de Chile. ✉juan.nieny@acague.cl

***Key words**:* 5G, cybersecurity, challenges

INTRODUCCIÓN

La comunicación ha sido una de las características centrales de la sociedad, desde el hombre primigenio hasta nuestros días. Niklas Luhmann, sociólogo alemán, explica en su teoría general de sistemas que la comunicación permite que el *sistema social*[1] trascienda y se perpetúe (Luhmann, 2012). En otras palabras, la sociedad es un sistema de comunicaciones per se. Dado lo anterior, la comunicación cobra aún mayor valor en medio de la era de la Información.

El fenómeno de la *Cuarta Revolución Industrial* (4RI), que habría comenzado a inicios del siglo XXI, ha generado cambios profundos en todos los sectores de la sociedad y ha permitido un elevado desarrollo de aquellas herramientas vinculadas a la transmisión, procesamiento y almacenamiento de datos digitales. Es así como la informática se ha visto sometida a una evolución que pareciera no tener límites, configurando un mundo híper-conectado.

Por otra parte, Klaus Schwab indica que la 4RI tendrá un profundo impacto en la naturaleza de las relaciones internacionales y dedica especial atención a ello en su obra:

> De todas las transformaciones importantes vinculadas a la cuarta revolución industrial, la seguridad es una [cuestión][2] insuficientemente discutida en el dominio público y en los sectores fuera de los gobiernos y la industria de la defensa. (Schwab, 2016, p. 67)

En ese orden de ideas, la implementación de la tecnología 5G en Chile se transforma en un desafío para el Estado, ya que existen una serie de riesgos asociados a esta nueva generación de comunicaciones inalámbricas. Diversos medios coinciden en señalar que la tecnología 5G permitirá aumentar diez veces la velocidad de navegación en internet. Además, disminuirá drásticamente la tasa

[1] Niklas Luhmann considera tres sistemas en su teoría general de sistemas: el sistema vivo, el sistema psíquico y el sistema social.

[2] Palabra sugerida por el autor, debido a que el texto original no la contiene.

de latencia[3], lo que se traducirá en la posibilidad de incrementar dispositivos conectados a una red, facilitando el denominado el *internet de las cosas* o *internet of things* (IoT), como lo fue en su momento el internet móvil para la tecnología 4G.

Al mismo tiempo, países como Estados Unidos, Inglaterra, entre otros, han alertado al mundo sobre los riesgos que supone que ciertos proveedores participen en la implementación de infraestructura y servicios asociados a la tecnología 5G, principalmente por riesgos a la seguridad por acciones como espionaje, vigilancia cibernética y apagones informáticos (BBC, 2020). Por otra parte, las ventajas del 5G abren también la posibilidad a las ciberamenazas, las que ponen el foco en el robo de datos, ciberataques y otras actividades de cibercrimen.

En consecuencia, con un horizonte proyectado al 2022 para la implementación del 5G en el país y considerando que ya se han adoptado medidas concretas al respecto, conviene revisar las implicancias de la adopción de esta nueva generación de conectividad inalámbrica para gestionar, conectar y organizar el propio Estado.

Al respecto, el presente artículo busca responder a la interrogante ¿Cuáles son los desafíos de la tecnología 5G en el ámbito de la Ciberseguridad? Para abordarla, inicialmente se contextualiza en relación a la 4RI y a la aceleración tecnológica; posteriormente, se entregan algunos detalles técnicos sobre el 5G, sus ventajas y beneficios; seguidamente, se reflexiona sobre los riesgos asociados a esta nueva tecnología; y, finalmente, se exponen algunos desafíos vinculados a la adopción del 5G. Lo anterior, considerando un contexto, que busca transformar a algunos estados en países ciber-resilientes[4].

---

[3] La latencia es el tiempo que demora en transmitirse un paquete de datos en una red. Corresponde a una unidad de medida de tiempo, expresada en milisegundos. No debe confundirse con la velocidad de conexión que dice relación con la cantidad de información enviada y/o recibida.

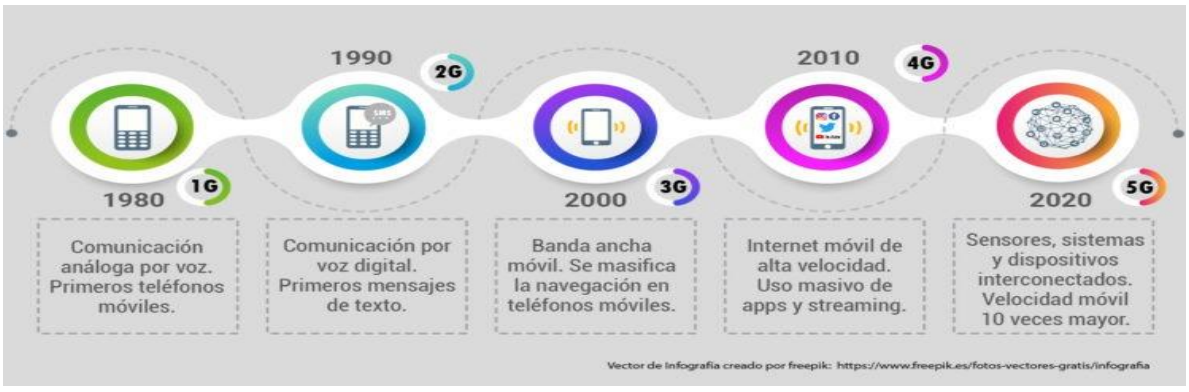
[4] Existen múltiples definiciones para el concepto de ciber-resiliencia (cyber resiliency o cyber resilience). La organización norteamericana The MITRE Corporation, por ejemplo, la define como la capacidad de anticipar, resistir, recuperarse de, y adaptarse a condiciones adversas, estrés, ataques o compromisos en los recursos cibernéticos. Asimismo, el Instituto Nacional de

LA CUARTA REVOLUCIÓN INDUSTRIAL Y EL ACELERADO DESARROLLO TECNOLÓGICO

Es comentado que el mundo actualmente se encuentra experimentando la cuarta revolución industrial, en la que existe un desarrollo exponencial de la tecnología. Según Klaus Schwab, fundador del Foro Económico Mundial y autor del libro *La Cuarta Revolución Industrial*, esta "...se basa en la revolución digital. Se caracteriza por un internet más ubicuo y móvil, por sensores más pequeños y potentes que son cada vez más baratos, y por la inteligencia artificial y el aprendizaje de la máquina" (Schwab, 2016, p. 14). En este contexto se enmarcan las redes de comunicaciones de quinta generación o 5G, tecnología que permitirá incrementar ostensiblemente la velocidad de conexión inalámbrica entre aparatos y desde estos hacia la red Internet. En lo referido a la industria de telefonía móvil, desde la aparición del celular con tecnología de primera generación (1G), la aceleración tecnológica, casualidad o no, ha permitido la renovación generacional cada 10 años (Ver Figura 1). Es dable esperar, por lo tanto, que antes del 2030 ya se esté hablando de la sexta generación (6G).

Figura 1

Evolución de las generaciones de telefonía celular



Nota. Adaptado de Juan Carlos Mena, "Ventajas, desventajas y mitos de la tecnología 5G" (https://www.uao.edu.co/ingenieria/ventajas-desventajas-y-mitos-de-la-tecnologia-5g/).

Ciberseguridad Español (INCIBE) hace referencia a la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes.

¿QUÉ ES EL 5G?

La tecnología 5G corresponde a la quinta generación de tecnología de comunicaciones inalámbrica para celulares, por tanto es la más avanzada tecnología de redes de datos. Técnicamente, se señala que la experiencia de navegación de un usuario promedio de internet, aumentará 10 veces o más en comparación a las actuales redes de datos 4G. Pero no solo eso, la nueva tecnología permitirá aumentar ostensiblemente la cantidad de aparatos que se conectan a una determinada red y la interacción entre ellos, permitiendo un salto significativo para el denominado *internet de las cosas* (IoT) y para la comunicación máquina a máquina (M2M), ampliando la gama de nuevos usos y produciendo un gran impacto sobre la forma en que vivimos.

En los próximos años, el mundo será testigo de cómo se conectan y controlan remotamente una infinidad de dispositivos (robots, drones, servidores, automóviles, tablets, smartphones, electrodomésticos, cámaras de vigilancia, etc.), con múltiples propósitos como la telemedicina, el teletrabajo, el control productivo, la conducción autónoma, el cloud computing, el big data, el entretenimiento, entre otros. Así, las ciudades deberán migrar hacia el concepto de ciudad inteligente o *smart city*, como una evolución del concepto de ciudad digital.

Dado que el 5G utiliza ondas de frecuencia más altas que las redes 4G y que estas ondas recorren menos distancia, consecuentemente, una de las caraterísticas de las smart cities será la proliferación de antenas que permitan el acceso ininterrumpido de los dispositivos (ver desventajas en Cuadro 1). Considerando estas y otras características “las antenas 5G serán un nuevo tipo de antenas que estarán altamente integradas, admitirán una configuración flexible de todas las bandas y permitirán la gestión de haces en situaciones específicas”[5] (Huawei, 2019, p. 7).

[5] Traducción del autor.

Si bien en el año 2008 se creó un proyecto surcoreano llamado *5G mobile communication systems based on beam-division multiple access and relays with group cooperation*, según la 3GPP[6] la quinta generación de redes móviles nace el año 2018 de manera oficial. En comparación a su predecesora, la tecnología 5G presenta ventajas y desventajas que conviene resaltar:

Cuadro 1

Ventajas y desventajas de la tecnología 5G

Ventajas	Desventajas
Aumento de la velocidad de usuario en 10 veces. Es decir, si la tecnología 4G contaba con 10 MB/sec (Megabit por segundo), la 5G aumenta hasta 100 MB/sec.	El 5G al utilizar frecuencias de radio más altas, tendrá un rango de cobertura menor. Por tanto, los operadores necesitarán instalar más nodos (antenas) en el país, lo que tomará más tiempo para dar cobertura total.
Mayor movilidad. El 4G había definido velocidades hasta de 300 km/h, a velocidades mayores ya no cumplía el estándar. 5G aplica incluso para velocidades de hasta 500 km/h, esto significa que con esta red se podrá tener buena comunicación incluso en aeronaves.	Requiere de nueva infraestructura (CW), nuevos equipos de radio (NR) donde integra las 3 tecnologías de radio (RAT 2G, 3G y 4G), con mayor potencia con las nuevas bandas de operación de 5G.
Menor latencia. En 4G teníamos latencias de hasta 10 milisegundos, en 5G de hasta un milisegundo. Las áreas más beneficiadas serán la de los carros autónomos y la salud.	Usuarios deberán adquirir nuevos equipos como teléfonos, tabletas, computadores, etc.
Densidad de conexión mayor. En 4G era una densidad por km^2 de hasta 100 mil dispositivos, en 5G podremos tener hasta un millón de conexiones por km^2.	

[6] Organización que reúne a un grupo de asociaciones de telecomunicaciones de distintas partes del mundo con el propósito de definir especificaciones y estándares para la industria de la telefonía celular.

Mayor eficiencia energética de la red. Las antenas van a consumir menos potencia, lo que genera un ahorro de energía de hasta 100 veces en una estación base. Las baterías de los celulares tendrán una eficiencia de energía de hasta 100 veces más que la actual.	
La capacidad de tráfico por área será de 10 MB/sec x m^2, mientras en 4G no alcanzaba ni a los 0.1 MB.	
Se tendrán velocidades de hasta 20 GB/sec.	

Nota. Adaptado de Juan Carlos Mena, "Ventajas, desventajas y mitos de la tecnología 5G" (https://www.uao.edu.co/ingenieria/ventajas-desventajas-y-mitos-de-la-tecnologia-5g/).

NUEVAS TECNOLOGÍAS, NUEVO ENTORNO

En Chile y en diversos países de la región, existe un gran entusiasmo respecto de los avances tecnológicos y lo que ofrece la tecnología 5G. Sin embargo, en el ámbito de la tecnología y de la información, existe preocupación por los riesgos que ella podría presentar para la seguridad. Y esto como resultado de una simple lógica: a mayor conectividad, mayores puntos de acceso y oportunidades para explotar de manera maliciosa las vulnerabilidades de las redes. Si tomamos en cuenta que la tecnología 5G expandirá el uso del IoT, los riesgos a la seguridad aumentarán enormemente.

Grandes potencias ya lo han advertido y las preocupaciones por espionaje o interrupción de comunicaciones son las razones aducidas.

A lo anterior, se podrían agregar otros factores. Y es que el 5G no solo supone el aumento de riesgos de robo de información digital, espionaje o apagones, sino que también de daño masivo a infraestructura. Esto debido a que en un mundo hiperconectado, muchos procesos serán controlados y dependerán de redes informáticas para su funcionamiento.

Como comentan Purdy, Yordanov y Kler, el año 2013 la empresa Target, una de las cadenas de retail más importantes de Estados Unidos, sufrió un ciberataque que le costó US$292 millones solamente en compensaciones legales, sin contar

costos de ventas y otros perjuicios. El ataque se produjo a través de un proveedor de servicios de climatización que tenía autorización para acceder a sus servidores y monitorear remotamente la temperatura y consumo de energía de sus tiendas (Purdy et al., 2020, p. 117).

Una experiencia de esas características, supondría el fin de muchas empresas, por la incapacidad de soportar los perjuicios. El artículo, titulado *Don't Trust Anyone,* sugiere que las posibilidades de sufrir un ataque se diversifican con la tecnología 5G, y es categórico en señalar que no se puede confiar en nadie. Además, plantea que mientras algunos adversarios de Estados Unidos estarían desarrollando capacidades para apagar remotamente las redes inalámbricas, otros, podrían utilizar sus capacidades submarinas para, literalmente "cortar los cables" de las redes 5G (Purdy et al., 2020, p. 119). Estas ideas dan cuenta de los daños potenciales y los efectos que podrían tener sobre los gobiernos, empresas, industrias y público en general.

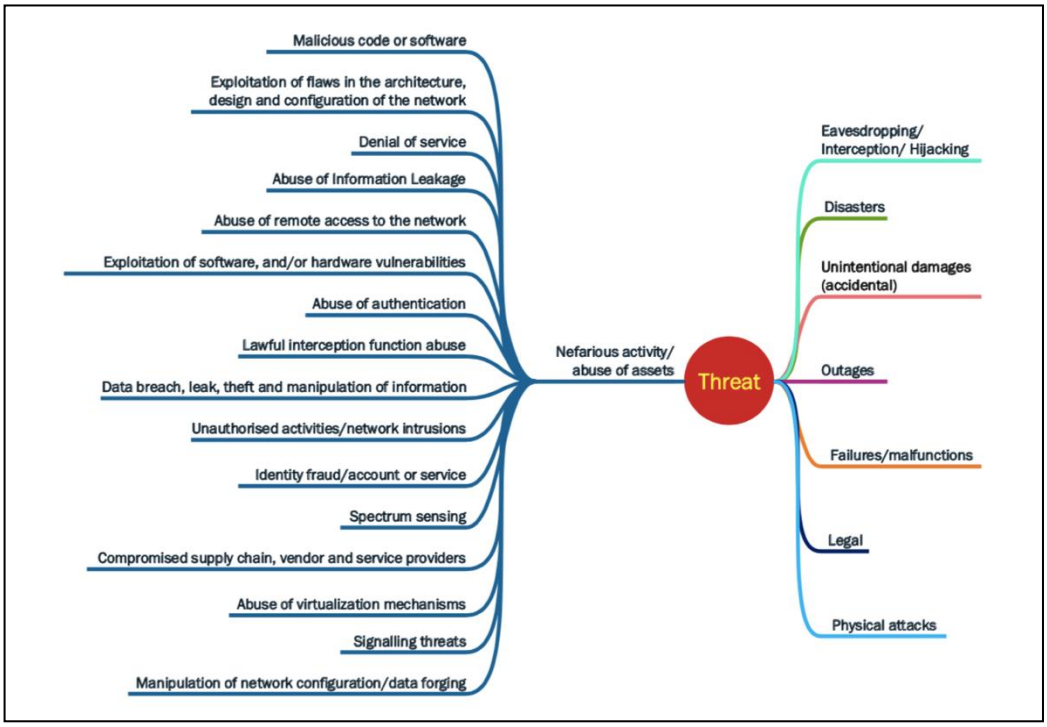
Por lo anterior y un cúmulo de otros ejemplos, se evidenciaría que IoT continuará siendo un desafío y foco de amenazas para la red 5G, sobretodo porque la mayoría de los dispositivos que podrán interconectarse a redes inalámbricas 5G.

Por otra parte, la Unión Europea también ha abordado la problemática de la seguridad de las redes 5G. La Agencia de la Unión Europea para la Ciberseguridad (ENISA), publicó en noviembre de 2019 un reporte titulado *ENISA Threat Landscape For 5G Networks*[7]*.* En el documento, se busca identificar aquellos componentes más críticos de las redes 5G y que pueden quedar expuestos a las ciberamenazas. Además presenta una interesante taxonomía de amenazas para las redes 5G (ver Figura 2). Coincidiendo con muchas voces expertas en relación con esta tecnología, señala que "los riesgos y amenazas aún no se han entendido por completo" (ENISA, 2019, p. 54).

[7] El reporte *ENISA Threat Landscape For 5G Networks,* puede ser consultado en https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Figura 2

Taxonomía de amenazas según ENISA



Nota. European Union Agency for Cibersecurity, (2019), “ENISA Threat Landscape For 5G Networks”, p. 64.

La reflexión que se hace es coincidente con el planteamiento del fundador del Foro Económico Mundial sobre la 4RI respecto a que “tenemos solo una comprensión limitada del máximo potencial de la nuevas tecnologías y de lo que vendrá en el futuro” (Schwab, 2016, p. 71). Estas ideas refuerzan la premisa de que la ciberseguridad debe ser un imperativo para los Estados.

Las 58 amenazas que detalla el reporte, además de las 8 categorías de agentes responsables de las ciberamenazas (cibercriminales, actores internos o insiders, Estados-Naciones, ciberguerreros, hacktivistas, corporaciones, ciberterroristas y script kiddies) permiten comprender lo vulnerable que será la sociedad internacional para cuando la tecnología 5G esté completamente implementada.

En 2003, Kirk Bailey, jefe de la oficina de seguridad de la información de la Universidad de Washington, introducía el concepto de *asumir la brecha* en materias de ciberseguridad (citado por Purdy et al., 2020, p. 122). Con los

actuales avances en tecnología y los que llegarán en el mediano plazo de la mano del 5G, un ataque informático ya no debe abordarse en términos de una posibilidad, sino que de una certeza, quedando solo pendiente conocer "cuándo" este ocurrirá. Esta filosofía ha ayudado a todos los sectores a estar más preparados para las ciberamenazas. Lo anterior nos advierte sobre el cambio en los paradigmas de ciberseguridad hacia la aceptación de vulnerabilidades.

Pero ¿Qué pueden hacer los estados al respecto? Ciertamente, existe mucho entusiasmo de los gobiernos para no quedar atrás en la implementación del 5G. El caso chileno ha sido destacado por la hoja de ruta que ha sido trazada sobre la materia. Evidencias de ello son el plan de Matriz Digital 2018-2022, la Agenda Digital, la difusión durante el año pasado del lanzamiento de la primera licitación nacional para redes 5G, el impulso de carreteras digitales a través de fibra óptica para sectores aislados del país, la firma de diversos memorándum de entendimiento (MoU) con países como España, Israel, Colombia, Ecuador, Reino Unido y Estonia, entre otras iniciativas orientadas al aprovechamiento de las oportunidades que ofrece el mejoramiento de las redes inalámbricas.

No obstante ¿Qué hay en materia de ciberseguridad? De acuerdo con el reporte del Foro Económico Mundial, *The Global Risks Report 2021*[8]*,* publicado en enero del presente año, los riesgos de tipo tecnológico (fraude o robo de datos y ciberataques) han ocupado entre el 2do y 3er lugar en el ranking de los mayores riesgos globales en términos de probabilidad de ocurrencia en los cuatro últimos años (2018, 2019, 2020 y 2021), después de los riesgos del medio ambiente los tres primeros años y en 2021 por detrás de los riesgos sociales que implican las enfermedades infecciosas (WEF, 2021).

Chile, a pesar de los avances logrados en materias de telecomunicaciones y a diferencia de lo que normalmente piensa el común de las personas, estaría igualmente expuesto. Y es que mayor desarrollo no implica necesariamente mayor seguridad.

[8] El reporte *The Global Risks Report 2021* y otras versiones anteriores, puede ser consultado en https://www.weforum.org/reports.

Según Eduardo Parada, Gerente de Ingeniería de la Consultora TI Vector, en entrevista realizada por el portal de noticias Emol.com (2017), "el país ocupa el quinto lugar latinoamericano con más usuarios afectados por ciberataques, con un 20,6%, por detrás de Brasil (30%), Honduras (23,5%), Panamá (22,6%) y Guatemala (21,6%)".

Por otra parte, el sitio *Threat Intelligence Insider Latin America* de Fortinet, señala que Chile fue objeto de 525 millones de intentos de ciberataques durante la primera mitad del año 2020 (RoiPress, 2020). El sitio advierte que en el contexto de la pandemia por COVID-19, los ataques han aumentado y han incrementado el grado de sofisticación, tendencia que podría mantenerse durante los próximos años (Fortinet, 2020).

Contrario a los datos expuestos, y a modo de contrargumento, se podría sostener que Chile es un país ciber seguro y que los datos utilizados en la mayoría de los reportes apuntan a empresas civiles y no a entidades de gobierno. De igual manera, es conveniente recordar que ciertas entidades públicas también han sido objeto de ciberataques, lo que da cuenta de estándares de ciberseguridad similares para el sector público y el privado. Evidencia de lo anterior, son los ciberataques sufridos por Banco Estado durante junio y septiembre del 2020, siendo el último de ellos presumiblemente provocado por hackers (La Nación, 2020). Además, se infiere que la mayoría de las motivaciones para llevar a cabo los ciberataques a empresas privadas y/o instituciones financieras, obedecen a motivaciones criminales para la obtención de dinero, lo cual durante la pandemia y de acuerdo a diversos medios se ha ido incrementando. Sin embargo, si las motivaciones fueran políticas, estos buscarían sitios o infraestructura del Estado.

Y es que el dominio del ciberespacio[9] ofrece una serie de beneficios a la hora de enfrentar a las nuevas amenazas[10] y lograr la iniciativa en la *guerra de la*

[9] Existe consenso entre las fuerzas armadas del mundo en distinguir 5 dominios en el ambiente operacional: el terrestre, el naval, el aéreo, el espacial y el ciberespacio.

[10] Existen diversas conceptualizaciones sobre nuevas amenazas o amenazas emergentes en la literatura. La OEA, por ejemplo, en el año 2003, en la Declaración sobre Seguridad en las Américas, planteaba un enfoque de Seguridad Multidimensional y calificaba como nuevas amenazas al terrorismo, la delincuencia organizada transnacional, la narcoactividad, el tráfico

información (information warfare/IW)[11]. Así lo han entendido las principales potencias mundiales. Estados Unidos, por ejemplo, creó en 2008 el U.S Cyber Command (USCYBERCOM), unidad de comando de nivel estratégico que entró en pleno funcionamiento el 2010, con la responsabilidad de planificar y conducir operaciones militares en el ciberespacio. China, en 1995 iniciaba un plan de IW y en 2000 establecía una unidad estratégica de IW (Ball, 2011).

Si pensamos en la fuerte dependencia que tendrá (o que ya tiene) la sociedad hacia las TICs a propósito de la implementación de la tecnología 5G y, observando las capacidades informáticas que tienen (y que tendrán) las grandes potencias y las relaciones de poder entre ellas, la mayoría ligadas a las principales empresas proveedoras de servicios 5G, entonces no es arriesgado pensar que se pueda generar una suerte de *influencia indirecta* de estados de mayor estatura estratégica hacia los más pequeños, como lo expresa el Coronel el Ejército Español Pedro Baños en su texto orientado a analizar las que considera claves del poder mundial (Baños, 2017, p. 165). Aspectos cualitativos como éstos en el ámbito de las relaciones internacionales, alejados del tecnicismo propio de la tecnología, deberían ser incluidos en los análisis multifactoriales para adoptar definiciones y decisiones sobre la materia.

Ahora bien ¿Qué dicen los indicadores y referencias internacionales respecto de Chile en materia de ciberseguridad? De acuerdo a lo que señala el *National Cyber Security Index*[12], que mide las capacidades de ciberseguridad implementadas por los gobiernos, Chile actualmente ocupa el lugar 39 de un total de 160 países evaluados (NCSI, 2020). En el plano regional, solo Paraguay (nº 38) superó a Chile a partir de la medición de 2020. El resto de los países sudamericanos se ubican en puestos inferiores (entre el 57 y 95).

ilícito de armas, el lavado de activos, los desastres naturales, los desastres de origen antrópico, la trata de personas, los ataques a la seguridad cibernética, entre otros.

[11] Según el académico Milán Vego, reconocido por sus estudios sobre el arte operacional, la guerra de la información corresponde a todas aquellas acciones destinadas a lograr la superioridad de la información negando, explotando, corrompiendo o destruyendo la del enemigo mientras se protege la información y las funciones propias del ataque enemigo.

[12] El ranking del National Cyber Security Index puede ser consultado en https://ncsi.ega.ee/ncsi-index/

A nivel global, destaca Estonia (nº 3), país que el año 2007 sufrió un ciberataque contra organismos estatales e instituciones financieras presumiblemente por parte de hackers rusos. Las consecuencias fueron nefastas generándose una paralización digital del país por semanas (BBC, 2017). Estonia, a la fuerza, aprendió la lección y hoy es un referente en materias de Ciberseguridad y Ciberdefensa. Claramente ningún Estado quiere aprender de esa manera; por ello, se debe sensibilizar a la población y, particularmente, a las autoridades en materias de ciberseguridad, asumiendo por cierto las debilidades del Estado y adoptándose un paradigma de ciber-resiliencia a nivel país.

Otro índice global que conviene observar, es el *Global Cybersecurity Index*, una iniciativa de la International Telecommunication Union (ITU) que ofrece una referencia global para los países en materias de ciberseguridad. El Índice de Ciberseguridad Global (GCI) es un "índice compuesto que combina 25 indicadores en un punto de referencia para monitorear y comparar el nivel de compromiso de ciberseguridad de los países con respecto a los cinco pilares de la Agenda de Ciberseguridad Global (GCA)" (ITU, 2018), detalla el último reporte GCI del año 2018[13]. Chile aparece en el puesto nº 83 a nivel global y nº 9 en América; por debajo de Estados Unidos, Canadá, Uruguay, México, Paraguay, Brasil, Colombia y Cuba, dos puestos más abajo que en el GCI 2014. Al respecto, Carlos Landeros, Director Nacional del CSIRT[14], señalaba en julio de 2019, que la posición de Chile debiera mejorar en las próximas mediciones puesto que se han logrado una serie de avances sustanciales en los últimos años (MININT, 2019). Cabe resaltar que existe una correlación entre los cinco pilares[15] de la GCA y los cinco ejes estratégicos definidos por la Política Nacional de Ciberseguridad 2017-2022: Infraestructura, Legislación, Difusión, Colaboración Internacional y Desarrollo de Industria. En razón de lo anterior, este índice debe ser de particular interés para evaluar la implementación de dicha política.

[13] El ranking del GCI 2018 puede ser consultado en https://ncsi.ega.ee/ncsi-index/

[14] El CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática, del Gobierno de Chile. Pero la sigla es de uso común en la comunidad de seguridad informática y obedece al nombre en inglés para este equipo de respuesta, computer security incident response team.

[15] Los cinco pilares de la GCA son: técnico, legal, organizacional, cooperación y creación de capacidad.

TECNOLOGÍA 5G Y CIBERSEGURIDAD: ALGUNOS DESAFÍOS

Sin duda, la implementación de la tecnología 5G representa un gran desafío para cualquier Estado, puesto que para ello concurren aspectos legales, técnicos, comerciales y otras dimensiones o varibles que podrían condicionar su adopción. En ese sentido, el caso nacional presenta algunas ventajas. En el año 2022, justo cuando se inicie la implementación de la tecnología 5G en Chile, al Estado le corresponderá difundir una actualización de la Política Nacional de Ciberseguridad. En consecuencia, se encontrará en un importante punto de inflexión, que representaría una oportunidad para seguir avanzando sustancialmente en materias de ciberseguridad.

La actual Política Nacional de Ciberseguridad se estructuró considerando 5 objetivos de largo plazo (con horizonte al año 2022) y 41 medidas de política públicas que fueron pensadas para ser ejecutadas en el período 2017-2018, las que contribuyen al logro de los objetivos de largo plazo (MININT, 2017), medidas que se han ido cumpliendo de manera gradual.

De lo anterior se desprende que uno de los mayores desafíos que enfrentan los países, es la formulación de políticas públicas y normas legales que permitan consolidar una institucionalidad en materia de ciberseguridad. Las políticas públicas sobre la materia tienden a orientar la adopción de esta nueva tecnología en sincronía con otras iniciativas públicas (tecnología 5G y transformación digital del Estado, por ejemplo), mientras que una ley marco de ciberseguridad básicamente permite garantizar que la implementación del 5G se realice de acuerdo a los estándares y objetivos que se determinen, que se estructuren sistemas de incidentes informáticos de nivel nacional y se establezcan las responsabilidades en la materia.

El espectro legal vinculado a la tecnología 5G es bastante amplio. En efecto, el desafío para los estados está en articular todos aquellos aspectos que se relacionen con la ciberseguridad y las ventanas de oportunidad que generará el 5G. Así, la legislación sobre delitos informáticos, sobre protección de datos

personales y sobre infraestructura crítica de ciberseguridad, pasan a tener prioridad en las agendas de ciberseguridad.

La rápida evolución tecnológica de las materias que se abordan, su complejidad y especificidad inherente y los riesgos y amenazas a la seguridad nacional que se visualizan, hacen imperativo que la ciberseguridad sea abordada como política integral de largo plazo, una verdadera política de Estado.

Al respecto, conviene revisar lo que propone Elsa Kania en un estudio realizado como parte del proyecto *Securing Our 5G Future*, del Centro para una Nueva Seguridad en América (CNAS) que aborda los desafíos del 5G en un mundo globalizado y competitivo. En su trabajo, la investigadora entrega cinco recomendaciones para el mejoramiento de las políticas relacionadas con el 5G en Estados Unidos, a propósito de las tensiones entre dicho país y China por la materia (Ver Cuadro 2).

Si bien las recomendaciones son específicas para la realidad de Estados Unidos, conviene revisar algunas de ellas y extrapolarlas al caso nacional. Por ejemplo, en el segundo punto se señala que se debe prever que las futuras redes 5G sean seguras por diseño desde el principio. Dado que el año 2022 supone un punto de partida marcado por la implementación de la tecnología 5G y una nueva Política Nacional de Ciberseguridad, la fecha se presentaría como un plazo prudente para asegurar un diseño inicial que permita explotar las potencialidades de las redes 5G, pero protegiendo a sus usuarios y al propio Estado.

En ese sentido, sería factible incluso, ralentizar el avance en la materia si la seguridad así lo demanda.

Cuadro 2

Recomendaciones y consideraciones para políticas públicas

1) Priorizar e invertir en 5G como base para la competitividad.
2) Prever que las futuras redes 5G sean seguramente diseñadas desde el principio.
3) Concurso de liderazgo e innovación tecnológica dentro y más allá de 5G.
4) Buscar una coordinación más estrecha y una innovación colaborativa con aliados y socios.
5) Prepararse para aprovechar las externalidades positivas y mitigar las externalidades negativas del 5G.

Nota. Elaboración propia a partir de la traducción del texto de Elsa B. Kania (2019), *Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy,* pp. 15-22.

Por otra parte, Kania revisa los riesgos y preocupaciones de seguridad asociadas al 5G. Al respecto, se muestra escéptica de los intereses de las empresas chinas proveedoras de los servicios 5G y concluye que "aquellos países que eligen opciones menos seguras o dan prioridad a la facilidad y rapidez de implementación pueden encontrar mayores riesgos y mayores costos en el futuro"[16] (Kania, 2019, p. 13). De su escepticismo y preocupaciones, se desprende que los nuevos riesgos y amenazas que surgen a partir de la tecnología 5G no pueden seguir siendo abordados por los países solo como un avance tecnológico más, y actualizando someramente sus políticas.

Así, las evidentes implicaciones que genera la nueva tecnología 5G para los estados, guardan relación con nuevos riesgos y amenazas a la seguridad de estos.

En línea con lo anterior, otra implicancia relevante de la tecnología 5G, corresponde al desarrollo de capacidades estratégicas de Ciberdefensa y las políticas públicas asociadas. En tal sentido, Chile ha dado un paso importante puesto que la Política Nacional de Ciberdefensa incluye la disposición de creación de un Comando Conjunto de Ciberdefensa dependiente del Jefe del

[16] Traducción del autor.

Estado Mayor Conjunto, con la responsabilidad de la planificación y ejecución de operaciones militares conjuntas de ciberdefensa.

Más aún, la tecnología 5G podría incluso sugerir que los estados formalicen estrategias nacionales de ciberseguridad y/o de ciberdefensa, que permitan articular todos los medios y establecer la manera de lograr los objetivos que la política establezca. La transversalidad de la materia, los múltiples actores que intervienen en la estructura de ciberseguridad del país y la inmediatez de las acciones en el plano informático, harán que los estados pierdan la iniciativa en el ambiente de la información si no logran articular todas sus capacidades frente a los nuevos riesgos y amenazas que se visualizan en el horizonte, algunas incluso insospechadas.

Si bien un conflicto armado interestatal tradicional, al más puro estilo clausewitziano, no se puede descartar, las probabilidades de ocurrencia son menores en comparación con fenómenos como la subversión, el terrorismo, los conflictos de baja intensidad, la insurgencia, la narcoactividad, las guerrillas, el crimen organizado transnacional, entre otros.

En ese plano, pareciera que el paradigma de las guerras industriales entre estados ha cambiado definitivamente. Diversas teorías dan cuenta de ello. De acuerdo a lo que propone Rupert Smith en su obra *The Utility of the Force*, el nuevo paradigma de la guerra entre la gente es el sello de los conflictos modernos (Smith, 2005). Martin Van Creveld coincide con la evolución que plantea Smith y señala, en *La Transformación de la Guerra*, que “los intentos de los estados por mantener el monopolio de la violencia están tambaleándose” (Van Creveld, 2007, p. 261).

La violencia, por tanto, se estaría dirigiendo hacia los civiles y no precisamente hacia aquellos que por años ostentaron el uso legítimo de las armas. Y es aquí donde el ciberespacio cobra relevancia como medio para desarrollar la *guerra de la información*, un fenómeno donde la figura del combatiente tradicional se desdibuja, las fronteras desaparecen y los tiempos se acortan hasta casi la

inmediatez. Las acciones, muchas veces sin elevados recursos, son inmediatas y con efectos catastróficos, incluso con la capacidad de generar daño físico. Así, se estima que el logro de la iniciativa en el ambiente de la información se facilitaría para aquellos estados que hayan apostado por la formulación de una estrategia sobre la materia.

Pero para poder actuar en un ambiente complejo como el que se describe, se evidencian también desafíos para la educación. A partir de las ventajas de la tecnología 5G expuestas, es posible inferir que la población estará expuesta a una enorme cantidad de información y la interacción con aparatos que soporten estas capacidades puede que no siempre sea amigable. En ese contexto, será difícil para las personas poder gestionar la información que les sea útil para su trabajo o para su vida cotidiana. La búsqueda y discriminación entre información real o falsa, o útil e inútil, es algo que se debe educar y que es necesario para la solución de problemas. El campo de batalla futuro representa desafíos similares para los soldados y la gestión de su conocimiento, por lo que la solución de problemas de dicha índole debe adaptarse a las tecnologías disruptivas. Reino Unido, por ejemplo, ha considerado ello y específicamente, en el ámbito de la educación militar, publicó un texto doctrinario conjunto titulado *Understanding and Decision-making* (2016). El documento entrega orientaciones para el logro de un profundo entendimiento individual y luego un entendimiento compartido del ambiente operacional, como paso previo necesario para la toma de decisiones y la solución de problemas. La educación de las personas en general y en las diferentes áreas, en un mundo hiperconectado forma parte del desafío.

De igual manera, uno de los impactos de la tecnología 5G que tendrá efectos sobre la estructura nacional de ciberseguridad, será el aumento de la demanda de profesionales capacitados en el área de la ciberseguridad, lo cual paralelamente es una oportunidad para la fuerza laboral más joven. Un estudio titulado *(ISC)² Cybersecurity Workforce Study (2019)*[17]*,* planteaba que la brecha

[17] El estudio Cybersecurity Workforce Study 2019 de la (ISC)², y otras versiones, pueden ser consultados en https://www.isc2.org/Resource-Center?filter=featured

de profesionales en Latinoamérica es del orden de 600.000 personas, lo que equivale al 15% de la demanda (ISC^2, 2019). En la versión más reciente del mismo estudio se señala que, si bien la demanda ha disminuido producto de los efectos de la pandemia del COVID-19 sobre la economía, la brecha ha aumentado a un 17% para Latinoamérica (ISC^2, 2020). Como se aprecia, la brecha se ha incrementado, manteniéndose la tendencia de los últimos años.

Las especializaciones que más se requieren en el campo de la ciberseguridad, según Excequiel Matamala, Director del Centro de Ciberseguridad de la Asociación Chilena de Empresas de Tecnologías de Información (ACTI), "son seguridad de la información, protección de datos, auditoría de sistemas, gestión de riesgo tecnológico y continuidad operacional, entre otras" (Emol, 2020, p. 1). Por tanto, no es difícil proyectar que habrá problemas para la conformación de equipos de respuesta oportuna si, además, consideramos que los ataques son cada vez más rápidos y la capacidad de respuesta más lenta.

En definitiva, lo que se evidencia un verdadero cambio de paradigma para enfrentar la revolución de la tecnología 5G, debiendo "asumir la brecha actual" y orientar los esfuerzos hacia la ciber-resiliencia.

REFLEXIONES FINALES

En este trabajo se ha reflexionado en torno a las implicancias que podría tener el 5G para la seguridad. Al respecto, se han revisado aspectos de políticas públicas y los desafíos que supone la adopción de la tecnología 5G para los estados y para Chile en particular.

Con la llegada de la tecnología 5G, el mundo espera una verdadera revolución que cambiará la vida y el trabajo de las personas. En ese contexto, propio de la 4RI y particularmente de la revolución digital, no cabe duda que la tecnología 5G permitirá dar un gran paso en materia de conectividad, favoreciendo el desarrollo del Estado y su población.

No obstante, como se ha expuesto, desarrollo no es sinónimo necesariamente de seguridad. En ese sentido, se ha hecho énfasis en exponer los riesgos y

amenazas a los que se estarán expuestos los estados y específicamente lo que ello representa para la seguridad nacional.

A partir de lo anterior, podemos indicar que se ha respondido a la interrogante que orientó el trabajo, estableciéndose que existen implicancias relacionadas con materias jurídicas, educativas y no solo las que atañen directamente a la ciberseguridad, sino que también otras que se relacionan indirectamente con la transformación digital; también, con la necesaria actualización y monitoreo de un panorama de riesgos y amenazas, que se hace difícil de mensurar por la rapidez de los cambios; así como la necesidad de personal capacitado en el área de la cibernética, que tendrá efectos sobre la estructura de ciberseguridad pública y privada del país.

La discusión aquí planteada permite reflexionar respecto de uno de los avances más significativos en materia de TICs que se espera para los próximos años en el marco de la 4RI, que facilita la toma de consciencia por parte de la comunidad académica respecto a esta temática, transitando a un entorno cada vez más ciber-resiliente.

REFERENCIAS

Ball, D. (2011). China's Cyber Warfare Capabilities. *Security Challenges, 7*(2), 81-103. https://www.jstor.org/stable/26461991?seq=1#metadata_info_tab_contents

Baños, P. (2017). *Así se domina el mundo*: desvelando las claves del poder mundial. Madrid, Editorial Ariel.

BBC (2020). *Por qué algunos países prohíben la tecnología del gigante chino.* BBC News. https://www.bbc.com/mundo/noticias-53413017

Carrillo, J., Marco de Lucas, J., Dueñas, J., Cases, F., Cristino, J., González, G. y Pereda, L. (2013). Big Data en los entornos de Defensa y Seguridad. *Documento de investigación 03/2013*. Instituto Español de Estudios

Estratégicos [IEEE]. http://www.ieee.es/Galerias/fichero/docs_investig/DIEEEINV03-2013_Big_Data_Entornos_DefensaSeguridad_CarrilloRuiz.pdf

Centro de Estudios Estratégicos. (2018). *La Ciberguerra, sus impactos y desafíos*. Academia de Guerra del Ejército de Chile.

Corral, D. (2020). 5G, una carrera por la hegemonía y el futuro con muchos beneficios´. *Documento Marco 07/2020*. Instituto Español de Estudios Estratégicos [IEEE]. http://www.ieee.es/Galerias/fichero/docs_marco/2020/DIEEEM07_2020DAVCOR_5G.pdf

Defense Science Board. (2019). *Defense Applications of Fifth Generation Network Technology*. Department of Defense [DoD]. https://www.hsdl.org/?abstract&did=828623

Emol.com. (2017). *¿Estás listo para un cyberataque? Chilenos estamos entre los menos preparados de Latinoamérica.* Portal PYME. Entrevista a Eduardo Parada, Gerente de Ingeniería de la Consultora TI Vector para *Emol.com.* https://pyme.emol.com/9886/estas-listo-cyberataque-chilenos-estamos-los-menos preparados-latinoamerica/

Emol.com. (2020). En Chile hay escasez de capital humano en ciberseguridad. *Ediciones Especiales. Emol.com.* https://seguridaddigital.emol.com/noticias/en-chile-hay-escasez-de-capital-humano-en-ciberseguridad/

European Union Agency for Cibersecurity, (2019), *ENISA Threat Landscape For 5G Networks.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Fortinet. (2020). *Threat Intelligence Insider Latin América, Reporte para Chile, tercer trimestre de 2020.* https://www.fortinetthreatinsiderlat.com/es/Q3-2020/CL/html/trends

Gallardo, M. (2019). Riesgos y amenazas para la seguridad multidimensional. *Transformaciones Estratégicas Globales, Retos y Repercusiones*. Centro de Estudios Estratégicos de la Academia de Guerra, pp. 65-83

Huawei. (2019). *5G Antenna White Paper: New 5G, New Antenna*. Shenzhen, Huawei Technologies Co. Ltd.

ITU. (2018). *Global Cybersecurity Index (GCI) 2018.* Ginebra, Suiza: ITU Publications. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ISC2. (2019). *(ISC) 2 Cybersecurity Workforce Study, 2019.* https://www.isc2.org/Resource-Center?filter=featured

ISC2. (2020). *(ISC) 2 Cybersecurity Workforce Study, 2020.* https://www.isc2.org/Resource-Center?filter=featured

Kania, E. (2019). *Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy*. Center for a New American Security. https://www.cnas.org/publications/reports/securing-our-5g-future

La Nación. (2020). *Ciberataque a Banco Estado habría sido provocado por hackers de Corea del Norte*. http://www.lanacion.cl/ciberataque-a-bancoestado-habria-sido provocado-por-hackers-de-corea-del-norte/

Leiva, R. (2017). Ciberdefensa ¿Hacia un nuevo eje estratégico? *Revista Ensayos Militares, 3* (1), 77-92.

McGuinness, D. (2017). *Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*. BBC Mundo. https://www.bbc.com/mundo/noticias-39800133

Mena, J. (2020). *Ventajas, desventajas y mitos de la tecnología 5G*. Universidad Autónoma de Occidente. https://www.uao.edu.co/ingenieria/ventajas-desventajas-y-mitos-de-la-tecnologia-5g/

Ministerio de Defensa de Chile. (2018). *Política Nacional de Ciberdefensa*. Ministerio de Defensa [MINDEF]. https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Ministerio del Interior. (2017). *Política Nacional de Ciberseguridad*. Ministerio de Interior [MININT]. https://www.ciberseguridad.gob.cl/media/2017/05/PNCS CHILE-FEA.pdf

Ministerio del Interior. (2019). *Fue Publicado el Índice de Ciberseguridad Global (GCI) para 2017-2018*. Ministerio de Interior [MININT]. https://www.ciberseguridad.gob.cl/noticias/fue-publicado-el-indice-de-ciberseguridad global-gci-para-2017-2018/

Ministry of Defense. (2016). Joint Doctrine Publication 04: Understanding and Decision-making. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/584177/doctrine_uk_understanding_jdp_04.pdf

MITRE. (2017). *Cyber Resiliency FAQ*. McLean. The MITRE Corporation. https://www.mitre.org/sites/default/files/PR_17-1434.pdf

NCSI. (2020). *Ranking National Cyber Security Index.* https://ncsi.ega.ee/ncsi index/

Purdy, A., Yordanov, V. y Kler, Y. (2020). Dont't Trust Anyone: The ABCs of Building Resilient Telecommunications Networks. *PRISM, 9* (1), 115-129.

RoiPress. (2020). *Impacto de COVID-19 en el cibercrimen en Chile*. https://roipresscanalnoticias.blogspot.com/2020/09/chile-sufrio-mas-de-525-millones-de.html

Samsung. (2020). *6G. The Next Hyper-Connected Experience for All*. Samsung Research. https://cdn.codeground.org/nsr/downloads/researchareas/6G%20Vision.pdf

Smith, R. (2005). *The Utility of Force, the art of war in the modern world*. Allen Lane.

Schwab, K. (2016). *La Cuarta Revolución Industrial*. Editorial Debate.

Unión Europea. (2019). *ENISA Threat Landscape For 5G Networks.* ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

U.S. Cyber Command. (2020). *U.S. Cyber Command History*. https://www.cybercom.mil/About/History/

Van Creveld, M. (2007). *La Transformación de la Guerra, la más radical reinterpretación del conflicto armado desde Clausewitz*. José Luis Uceda.

Vego, M. (2009). *Joint Operational Warfare: Theory and Practice*. U.S. Naval War College.

World Economic Forum [WEF]. (2021). *The Global Risks Report 2021.*

https://www.weforum.org/reports