IMPORTANCIA DE LA INFRAESTRUCTURA CRÍTICA, LAS REDES 5G Y SUS IMPLICACIONES PARA LA REGIÓN LATINOAMERICANA

*The importance of critical infrastructure, 5G networks and its
implications for the Latin American region*

YELYZAVETA OMELCHENKO¹

Resumen: En el presente ensayo se busca explicar el significado del concepto de infraestructura crítica, los diferentes sectores que la componen, y cuál es su importancia para la seguridad de una nación. Con este fin se describe a los organismos que fueron creados para controlar todos los aspectos relacionados a ella: en Estados Unidos, la Agencia de Ciberseguridad y Seguridad de la Infraestructura Crítica, y, en Argentina, a una escala menor, el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Profundizando en la importancia de la infraestructura crítica se tratará la introducción de las tecnologías 5G en el mercado latinoamericano y los desafíos, oportunidades y amenazas que esto representa para la región: su implementación podría significar un importante salto en la productividad, llevando a mejoras en el aspecto socioeconómico, pero también un mayor riesgo para la seguridad de las

1. Estudiante avanzada de las carreras de Relaciones Internacionales y Ciencias Políticas de la Universidad Católica Argentina. Mientras continúa formándose en su área de interés, se desempeña como intérprete y traductora de su idioma nativo, el ruso. Su ocupación también le ha impulsado a iniciar la carrera de Traductor Público en la Universidad de Buenos Aires con el fin de profundizar su conocimiento del idioma.

infraestructuras críticas, tanto públicas como privadas, lo que es de vital importancia para el seguro desarrollo de las actividades de una nación. Finalmente, se tratará lo que sucede con el caso argentino dentro del contexto latinoamericano y la disputa entre China y los Estados Unidos por el control del mercado 5G de la región y, por lo tanto, de las infraestructuras y de la información que los atraviesen.

Palabras clave: Infraestructura crítica, 5G, Argentina, Estados Unidos, China.

Abstract: This essay seeks to explain the meaning of the concept of Critical Infrastructure, the different sectors that compose it, and what is its importance to the security of a nation. To this end, it describes the agencies that were created to control all aspects related to this: in the United States, the Agency for Cybersecurity and Security of Critical Infrastructure and in Argentina, on a smaller scale, the National Program of Critical Information Infrastructures and Cybersecurity. In order to better understand the importance of Critical Infrastructure, this paper will approach the introduction of 5G technologies into the Latin American market and the challenges, opportunities and threats this poses to the region: its implementation could mean a significant leap in productivity leading to improvements in the socio-economic aspect, but also an increased risk to the security of critical infrastructures, both public and private, which is vitally important for the safe development of a nation's activities. Finally, this paper will address what happens with Argentina, within the Latin American context and the dispute between China and the United States for the control of the 5G market of the region and, therefore, of the infrastructures and all the information that will go through them.

Keywords: Critical Infrastructure, 5G, Argentina, United States, China.

¿Qué es la infraestructura crítica?

Por infraestructura crítica se entiende a todos aquellos sistemas básicos necesarios para la supervivencia de una organización o

nación. Estos sistemas abarcan todos los aspectos de la actividad humana, proveen los servicios necesarios para el funcionamiento de la economía, salud y seguridad de un país: desde la electricidad que consumimos en nuestros hogares, hasta el agua que ingerimos, los sistemas de comunicación que nos mantienen en contacto con nuestros amigos y familiares, y el transporte que utilizamos. Una alteración o interrupción en su funcionamiento por causas naturales o provocadas por el hombre podría conllevar graves consecuencias.

A lo largo de este trabajo buscaré comparar el caso argentino con el caso norteamericano. Sus definiciones, organismos y marco legal. También desarrollaré una de las cuestiones relacionadas con la infraestructura crítica, que estuvo generando muchos debates durante los últimos años: las tecnologías 5G, que representan una gran oportunidad para el crecimiento socioeconómico de la región, pero a su vez son un riesgo para la seguridad pública y privada de no ser manejadas y controladas correctamente. Por último, describiré la competencia entre dos actores principales por introducir sus tecnologías en Latinoamérica: China y Estados Unidos. Está de más decir, que quien logre controlar el mercado, podrá controlar el flujo de información que circule a través de ellas.

Ahora, para comprender la importancia de lo que significa la infraestructura crítica, adopté dos definiciones, una propuesta por la República Argentina, y la otra, por los Estados Unidos.

Argentina

La Resolución N° 1.523 de la ex Secretaría de Gobierno de Modernización de la República Argentina, de fecha 12 de septiembre de 2019, define infraestructuras críticas como “aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente”. Además, dicha Resolución agrega el concepto de infraestructuras críticas de información y las define como aquellas tecnologías de información, operación y comunica-

ción, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las infraestructuras críticas.

Estados Unidos

Es tal la importancia del significado de este concepto, que fue incluido y definido en la *USA Patriot Act* (cuyas siglas en inglés significan “*Uniting and Srengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*”, o en español, “Ley para unir y fortalecer América proveyendo las herramientas apropiadas, requeridas para impedir y obstaculizar el terrorismo”), ley federal promulgada por George W. Bush el 26 de octubre de 2001, luego de los sucesos del 11 de septiembre de 2001.

En una versión más actualizada, el Departamento de Seguridad Nacional de los Estados Unidos define a la infraestructura crítica como aquella que “describe a los sistemas físicos y cibernéticos y a los activos que son tan vitales para los Estados Unidos que su incapacidad o destrucción tendría un impacto debilitante sobre nuestra seguridad física o económica o sobre la salud pública o seguridad. La infraestructura crítica de la nación provee los servicios esenciales que sustentan a la sociedad (norte)americana”.

Organismos reguladores y marco legal

Argentina

En la República Argentina, mediante la Resolución de la Jefatura de Gabinete de Ministros (JGM) N° 580, de fecha 28 de julio de 2011, se creó el “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad” (en adelante, “ICIC”) en el ámbito de la Oficina Nacional de Tecnologías de Información, con el fin de elaborar un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas, públicas y privadas.

Con este fin, mediante la Disposición de la Oficina Nacional de Tecnologías de Información N° 2, de fecha de agosto de 2013, se

crearon distintos Grupos de Trabajo, de los cuales solo se encuentra activo el “ICIC-CERT” (*Computer Emergency Response Team*), que mantiene estrechos vínculos de cooperación con centros internacionales análogos, en el marco de la OEA (Organización de los Estados Americanos), con el fin de contribuir a la construcción de un ciberespacio seguro. Desde la creación de este grupo de trabajo, dentro del país han surgido otros equipos especializados de similar naturaleza, cuyo accionar era necesario articular a nivel nacional y, para ello, mediante la Decisión Administrativa N° 1.865, de fecha 14 de octubre de 2020, se aprobó la creación de la Dirección Nacional de Ciberseguridad, en el ámbito de la Secretaría de Innovación Pública dependiente de la JGM, cuya función gira en torno a: “Entender en los aspectos relativos a la ciberseguridad y la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de prevención, detección, defensa, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional”, además de diseñar políticas de ciberseguridad, implementar los objetivos fijados en la Estrategia Nacional de Ciberseguridad y “entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT Nacional)”.

Dada la más intensa utilización de las plataformas tecnológicas, especialmente dentro del Sector Público Nacional, y considerando la notable expansión en el uso de las herramientas generales de la población, resalta que se ha producido un aumento considerable de los riesgos y amenazas a la seguridad de la información. Siguiendo la recomendación de “Establecer a nivel nacional un equipo de respuesta ante emergencias informáticas o un equipo de respuesta a incidentes de seguridad informática”, del Informe UNGGE (Grupo de Expertos Gubernamentales de la Organización de las Naciones Unidas), aprobado por la Resolución AG N° 70/237 de las Naciones Unidas, el Director Nacional de Ciberseguridad, mediante Disposición N° 1/2021, creó en el ámbito de la Dirección Nacional de Ciberseguridad el Centro Nacional de Respuesta a Incidentes Informáticos (CERT.ar.), con el objetivo de “coordinar la gestión de incidentes de seguridad a nivel nacional y prestar asistencia en aquellos que afecten a las entidades y jurisdicciones del Sector Público Nacional definidas en el inciso a) del artículo 8° de la Ley

Nº 24.156 y sus modificatorios y a las Infraestructuras Críticas de Información, declaradas como tales”.

En el proyecto de intervención de la delegación argentina en la segunda sesión plenaria de la XIX reunión del CICTE (Comité Interamericano contra el Terrorismo), sobre la infraestructura crítica se menciona lo siguiente: “Con relación a la Declaración ‘Protección de Infraestructura Crítica ante las amenazas emergentes’ del año 2015, permítaseme reseñar brevemente que la República Argentina, a través de su Ministerio de Seguridad, protege la infraestructura física crítica mediante el trabajo del personal de la Gendarmería Nacional Argentina, que es responsable de la protección de puentes, represas, instalaciones nucleares y otros objetivos estratégicos; de la Prefectura Naval Argentina, que aplica de manera efectiva el Código para la Protección de los Buques y de las Instalaciones Portuarias (PBIP) en todo el litoral marítimo y fluvial, y de la Policía de Seguridad Aeroportuaria, que es responsable de la aplicación del Convenio de Chicago de 1944 sobre ‘Seguridad y Protección de la Aviación Civil Internacional contra los Actos de Interferencia Ilícita’ de la Organización Internacional de Aviación Civil (OACI). El personal de las fuerzas de seguridad mencionadas ha recibido entrenamiento relativo a la protección física de instalaciones nucleares y se han tomado medidas para el control efectivo y eficaz de materiales sujetos a proliferación, en colaboración con expertos de distintos países”.

Estados Unidos

En noviembre de 2018, el presidente Donald Trump promulgó la Ley que creó la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA - *Cybersecurity and Infrastructure Security Agency*), cuyo objetivo es “coordinar la seguridad y los esfuerzos de recuperación mediante el uso de asociaciones de confianza dentro del sector público y privado y suministrar la asistencia técnica y asesoramiento a los *stakeholders* federales, así como también a los propietarios y operadores de la infraestructura a lo largo del país”, según el sitio oficial de CISA.

Dicha agencia queda bajo la supervisión del Departamento de Seguridad Nacional de los Estados Unidos. Se crea como conti-

nuación de las actividades del *National Protection and Programs Directorate* (NPPD). Cumple la función de articular todos los recursos nacionales, tanto públicos como privados, para enfrentar ciberataques, proveer herramientas de ciberseguridad, servicios de respuesta a incidentes y capacidades de evaluación para proteger las redes “.gov” que sustentan las operaciones esenciales de los demás departamentos y agencias del sistema federal estadounidense. Nota como crucial la cooperación con los distintos *stakeholders* de todo el país para poder comunicar y responder ante eventuales desastres naturales, ataques terroristas u otros desastres provocados por el hombre.

Dentro de CISA funciona el Centro Nacional de Gestión de Riesgos o NRMC (*National Risk Management Center*), cuyo fin es identificar y abordar los riesgos más significativos para la infraestructura crítica del país.

Sectores que comprende la infraestructura crítica

Las necesidades, los recursos y el nivel de desarrollo de cada país en particular son muy distintos, lo cual define las diferencias en la práctica de las infraestructuras críticas.

En el caso norteamericano, retomando la definición de infraestructura crítica que se utiliza en la *USA Patriot Act*, existen distintos sectores de infraestructura crítica cuyos activos, sistemas y redes, ya sea físicos o virtuales, son considerados tan vitales para los Estados Unidos que su incapacidad o destrucción tendría un efecto debilitante sobre la seguridad, seguridad económica nacional, salud pública nacional o seguridad, o cualquier combinación de ellos.

Los 16 sectores de infraestructura que considera CISA comprenden los siguientes: Químico; Infraestructura Comercial; Comunicaciones; Manufacturas Críticas; Represas; Industria Base de Defensa; Servicios de Emergencia; Energético; Servicios Financieros; Alimentos y Agricultura; Infraestructura Gubernamental; Sanitario y Salud Pública; Tecnologías de la Información; Reactores, Materiales y Residuos Nucleares; Sistemas de Transporte; Sistemas de Aguas y Aguas Residuales.

Más detalladamente:

1. Sector Químico

El Sector Químico es un componente integral de la economía estadounidense que manufactura, almacena, utiliza y transporta químicos potencialmente peligrosos, de los cuales, a su vez, dependen otros sectores de la infraestructura crítica. Resulta crucial la defensa de este sector contra cualquier tipo de amenazas mediante la cooperación entre el sector público y privado.

2. Sector de Infraestructura Comercial

Este sector abarca en su mayoría a aquellas infraestructuras privadas a las que puede acceder el público general con el fin de realizar actividades relacionadas a las compras, negocios, entretenimiento y alojamiento.

Se conforma por ocho subsectores: Entretenimiento y Medios, Juego (casinos), Alojamiento, Eventos al aire libre (parques temáticos), Reunión Pública (estadios), Inmuebles, Centros Comerciales, Ligas de Deportes.

3. Sector de Comunicaciones

Se considera como uno de los sectores más críticos ya que permite el funcionamiento de todos los sectores de infraestructura crítica y afecta muy de cerca a las operaciones de todos los negocios, organizaciones de seguridad pública y del gobierno. Es uno de los sectores que más ha crecido en los últimos veinticinco años.

Afecta principalmente al Sector Energético, que requiere de las comunicaciones para controlar y monitorear el suministro de energía para el funcionamiento de las torres de celulares, y demás; al Sector de Tecnologías de la Información, que depende de las comunicaciones para proveer y distribuir sus servicios; al Sector de Servicios Financieros, que requiere de las comunicaciones para la transmisión de las transacciones y operaciones de los mercados financieros; al Sector de Servicios de Emergencia, que

depende de las comunicaciones para direccionar recursos, coordinar respuestas, operar los sistemas de alerta pública y para recibir los llamados al 911; y finalmente, al Sector de los Sistemas de Transporte, que provee el combustible necesario para los generadores de energía auxiliares y que depende de las comunicaciones para monitorear y controlar el flujo del tráfico aéreo, marítimo y terrestre.

4. Sector de Manufacturas Críticas

Los productos de las industrias que componen el sector son esenciales para la mayoría de los demás sectores de infraestructura crítica. Este sector se enfoca en la identificación, evaluación, priorización y protección de las industrias nacionales vitales que pueden ser susceptibles a desastres naturales y a aquellos provocados por el hombre. Entre estas industrias podemos identificar a la manufactura de metales primarios, máquinas, equipamiento eléctrico y de transporte.

5. Sector de Represas

Provee la retención crítica de agua y controla los servicios de producción de energía hidroeléctrica, suministro de agua municipal e industrial, control de inundaciones, etc.

6. Sector de la Industria Base de Defensa

Se encarga de la investigación, desarrollo, diseño, producción, suministro y mantenimiento de los sistemas, subsistemas y componentes y partes de armamento militares para cumplir con los requerimientos de las Fuerzas Armadas norteamericanas. El sector provee productos y servicios esenciales para la movilización, despliegue y sustento de las operaciones militares.

7. Sector de Servicios de Emergencia

Este sector provee servicios de prevención, preparación, respuesta y rescate en los incidentes del día a día. Se encuentra presente en cada uno de los niveles de la organización geográfica de los sectores del gobierno norteamericano. Abarca a los distintos departamentos policiales, bomberos, etc. También incluye a los recursos del sector privado, tales como las organizaciones de seguridad privada, proveedores de servicios médicos de emergencia, entre otros.

8. Sector Energético

Sector únicamente crítico ya que permite el funcionamiento de los demás sectores de infraestructura crítica. Se debe proveer energía de manera estable para no comprometer a la salud y bienestar de la población. CISA lo define como el motor de la economía del siglo.

9. Sector de Servicios Financieros

El sector incluye bancos, proveedores de productos de inversión, aseguradoras y a los proveedores de los servicios que mantienen en funcionamiento al sector. Necesita ser protegido de los cortes de suministro energético a gran escala, desastres naturales y del aumento y la sofisticación de los ciberataques.

10. Sector de Alimentos y Agricultura

Este sector, en su mayoría, es privado y se compone de granjas, restaurantes y unidades de almacenamiento de productos. Representa una quinta parte de la actividad económica de los Estados Unidos.

11. Sector de Infraestructura Gubernamental

Son los edificios gubernamentales dentro de los Estados Unidos y en el extranjero. Algunos de ellos son de acceso público, pero

otros manejan información, materiales, procesos y equipamiento sensible. Además de las estructuras físicas, el sector incluye elementos cibernéticos que contribuyen a la protección de los activos del sector y a los individuos que cumplen funciones esenciales.

12. Sector Sanitario y Salud Pública

Protege a todos los sectores de la economía de peligros tales como el terrorismo, enfermedades contagiosas y desastres naturales. Aquí la cooperación entre el sector público y privado se vuelve crucial, ya que en su mayoría estos proveedores son privados.

13. Sector de Tecnologías de la Información

Produce y provee el *hardware*, *software*, los sistemas y servicios de tecnología de la información y en colaboración con el Sector de Comunicaciones, Internet. La infraestructura de este sector presenta algunos desafíos debido a su interdependencia e interconexión, pero también oportunidades para abordar y coordinar las respuestas del sector público y privado ante amenazas.

14. Sector de Reactores, Materiales y Residuos Nucleares

Abarca los reactores energéticos que proveen energía a los norteamericanos, isótopos utilizados en los tratamientos médicos, etc. Se encarga de coordinar la seguridad del Sector Nuclear.

15. Sector de Sistemas de Transporte

Transporta de manera rápida y segura a la población y a los bienes dentro del país y en el extranjero. Se compone por la aviación, vehículos a motor, transporte marítimo, transportes de pasajeros, sistemas de tuberías, líneas ferroviarias de cargas, correo y envío de cargas.

16. Sector de Sistemas de Aguas y Aguas Residuales

El correcto tratamiento del agua para el consumo es esencial para la salud pública y para todas las actividades humanas. Dentro de Estados Unidos hay más de 153.000 sistemas de consumo de agua potable. Es crucial la protección de cada uno de ellos de ataques por contaminación con componentes mortales, ataques físicos y ciberataques. El sector también es vulnerable ante desastres naturales.

Cada uno de estos sectores se encuentra al cuidado de distintas agencias específicas, tales como el Departamento de Seguridad Nacional de los Estados Unidos, Defensa, Energía, Tesoro, Agricultura, Salud, entre otros.

Tecnologías 5G: desafíos, amenazas y oportunidades

Las tecnologías de la quinta generación o 5G representan un importante avance de nuestros tiempos. Servirán de base para el funcionamiento de tecnologías como IoT (Internet de las Cosas), big data, AI (Inteligencia Artificial), y el aprendizaje automático de las máquinas.

Este avance significa una gran oportunidad para el desarrollo socioeconómico, pero a su vez, representa un nuevo riesgo y una mayor proliferación de amenazas relacionadas con la ciberseguridad y la seguridad de las infraestructuras críticas que expliqué anteriormente. Dentro de los sectores de infraestructura crítica definidos por CISA, a estas tecnologías se las podría ubicar en el Sector de Comunicaciones y Tecnologías de la Información.

La topología de la red 5G es diferente a las topologías de las generaciones anteriores ya que se necesitan muchas más antenas y estaciones radio base. Por lo tanto, la inversión requerida será mucho mayor que para las redes de generaciones anteriores.

Para estas tecnologías se ha creado *5G New Radio* (5G NR), que es una nueva interfaz aérea especialmente desarrollada para funcionar como soporte de la gran variedad de servicios, dispositivos y despliegues que abarcarán las tecnologías 5G. Una interfaz aérea es la “porción de la frecuencia de radio del circuito entre del disposi-

tivo móvil y la estación base activa”, la cual se modifica a medida que el usuario se desplaza.

Esto claramente conlleva nuevos desafíos en cuanto a la privacidad y protección de datos personales, ya que el uso de estas redes generaría una entrega de gran cantidad de datos y se debe proteger al consumidor del uso y abuso de la información personal. El riesgo principal de las redes 5G está relacionado con la cantidad de dispositivos que estarán conectados a ella, lo que las convertirá en objetivos más atractivos y cuyas vulnerabilidades podrían tener un impacto mayor al antes visto.

Para los países menos desarrollados, como los latinoamericanos, resulta más indispensable que nunca fortalecer sus sistemas de ciberseguridad y seguridad de la infraestructura crítica. Sin embargo, la tecnología 5G es clave para una nueva revolución en la productividad (que requiere de la seguridad como herramienta principal para su éxito). Según Omdia, la introducción de las tecnologías 5G en Latinoamérica podría significar un importante salto en la productividad entre 2029-35. Esto representa una gran oportunidad para el crecimiento socioeconómico de la región. Se estima que el potencial económico y el valor social del 5G en América Latina será de \$3,3 trillones para 2035.

A partir de un minucioso análisis de la región, en el estudio realizado por Omdia, se menciona que Argentina tiene un gran potencial en términos de 5G para ser uno de los primeros en adoptar e implementar esta tecnología, lo que tendría un gran impacto en el sector manufacturero y en el sector de servicios –sería la única forma de mantenerse competitivos en el mercado. Entre los potenciales sectores beneficiados se destaca el sector agropecuario, el automotriz y el energético.

Respecto de este último sector, en el Reporte de Nokia sobre el porqué del 5G en América Latina se menciona lo siguiente: “Actualmente alrededor de treinta compañías poseen concesiones en Vaca Muerta, de las cuales YPF, ahora controlada por el Estado argentino, tiene el mayor número. Vaca Muerta tiene el segundo play más grande (área de grandes acumulaciones de hidrocarburo) de gas no convencional y el cuarto más grande de petróleo de este tipo, en donde el 5G juega un rol diferencial para la productividad y la seguridad. La mayor parte de la conectividad requerida para estas

grandes áreas sigue pendiente, lo que representa una oportunidad aún no explorada para un despliegue temprano de las redes 5G”.

Alan Weissberger, especialista en telecomunicaciones y tecnologías de redes empresariales, en su artículo publicado en el Blog del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), el 30 de agosto de 2020, cuestiona el pronóstico optimista de Omnia sobre este posible salto productivo que podría generarse en América Latina por la implementación del 5G, ya que aún no se ha podido identificar ningún caso de uso real del 5G en la región: “Los operadores latinoamericanos han estado relativamente silenciosos, dejando de lado algunas pruebas, una implementación en Uruguay, y recientes lanzamientos suaves utilizando DSS (compartición dinámica de espectro) en Brasil. Su precaución es entendible, considerando la tardía adopción del 4G. Omdia estima que el 4G en América Latina es aproximadamente el 52 % de las líneas y que el 3G es aproximadamente del tercio (a fines de 2019). Incluso el 2G continúa siendo importante con un 13 %, y que no va a desaparecer hasta después de 2024”.

Agrega que “es muy temprano para saber definitivamente cómo el COVID-19 cambiará las conductas y los patrones de adopción de la 5G en América Latina” y que, “debido a la pandemia, existe una clara necesidad de digitalizar los sectores esenciales, tales como el sector de la salud, servicios de emergencia, manufacturas y de las cadenas de suministro”.

Por otro lado, Emmanuel Jaffrot, Doctor en Telecomunicaciones de la “Ecole Nationale Supérieure des Telecommunications” de París, magíster en Procesamiento de Señales e Imágenes e Ingeniero en Electrónica, en su artículo publicado en la Revista *Fibra*, el 16 de mayo de 2016, describe el proceso de estandarización de las tecnologías 5G impulsado por la Unión Internacional de Telecomunicaciones (UIT) –organismo dependiente de la Organización de las Naciones Unidas (ONU)–, que, a su vez, condujo a la creación de organismos regionales encargados de llevar a cabo estas definiciones tecnológicas: “En nuestro continente, se creó 5G Americas, basado en Estados Unidos, que apunta a agrupar los actores del sector, en particular de Estados Unidos, América Latina y el Caribe. América Móvil, AT&T, Cable & Wireless, Cisco, Commscope, Entel Uruguay, Ericsson, Hewlett Packard, Intel,

Mitel, Nokia, Qualcomm, Sprint, T-Mobile y Telefónica aparecen como los líderes de esta región”. Jaffrot agrega que la 5G tiene todas las posibilidades de ser una tecnología disruptiva y que es la primera vez que, a diferencia de la implementación de las tecnologías 3G y 4G, se encuentran muy presentes las consideraciones geopolíticas, ya que el continente asiático está muy presente en el proceso, especialmente China y sus principales actores del sector de telecomunicaciones: China Mobile, Huawei, China Telecom, China Unicom, ZTE, Datang Telecom Technology & Industry Group, así como la Academia China de Investigación en Telecomunicaciones del Ministerio de Industria y de las Tecnologías de la Información.

El actor que logre imponer su modelo será quien controle el mercado, la infraestructura y tenga acceso a todos los datos y desarrollos de esta tecnología. De hecho, según datos aportados por Emmanuel Jaffrot, en su entrevista publicada por la Revista *Iproup* el 23 de enero de 2020, señaló que para ese entonces a nivel global Huawei ya había firmado más de 60 contratos, mientras que Nokia 63 y Ericsson 32. Agregó que “la compañía asiática posee un interés muy fuerte por entrar con su red de 5G en América Latina. En el caso particular de la Argentina, ya efectuó tres pruebas ambientales reales con Telecom Personal y, durante este año, las repetirá con Claro y Telefónica” y que, “según datos de mercado, la tecnológica asiática es responsable del 70 % de la red nacional de Telecom y del 100 % de la de fibra óptica que el prestador posee en Capital y GBA”. “El core de la red de Movistar es 100 % Huawei. Claro y Arsat también cuentan con equipamiento de esta compañía”.

En el informe del Observatorio de Política Internacional del Senado Argentino, titulado “EE. UU. - China: Hegemonía Geopolítica y Carrera Tecnológica”, de agosto de 2020, se analiza la disputa entre los dos países por el control del 5G, y más específicamente, la carrera por el dominio tecnológico mundial y la hegemonía geopolítica, además de la ampliación de la capacidad militar de China. En este contexto se puede comprender la referencia a una “guerra comercial” que hacían las distintas publicaciones académicas y periodísticas durante los últimos años. En marzo de 2018, Estados Unidos impuso una serie de sanciones sobre productos importados desde China y, a su vez, “inició una ofensiva estratégica contra algunas empresas del rubro *high-tech*, como Huawei y ZTE,

vinculándolas al Ejército Popular de Liberación y presentándolas, por lo tanto, como una amenaza a la seguridad nacional”. Incluso,

“el país del norte boicoteó el despliegue chino de redes 5G con misiones a los países que vienen negociando su implementación con Huawei. Los gobiernos de Australia, Nueva Zelanda, Canadá y Japón (recientemente se les sumó Reino Unido) fueron los primeros en alinearse con Estados Unidos y tomar medidas para excluir a los proveedores de 5G chinos de aquellos países. Pero Estados Unidos no tiene una estrategia verosímil para el despliegue rápido de 5G. Las empresas estadounidenses carecen de una oferta alternativa a la ofrecida por China ya que, si bien producen algunos de los *softwares* 5G más avanzados, no fabrican gran parte del *hardware* necesario para construir las infraestructuras digitales, lo cual limita su competitividad global. A lo sumo, proveedores de redes como la multinacional estadounidense AT&T han implementado bajo una etiqueta engañosa lo que han dado a conocer como red ‘5GE’, que no es más que una versión mejorada de la actual tecnología 4G LTE”.

Omdia, en su estudio sobre el 5G en América Latina, recomienda a los formuladores de políticas públicas:

- Terminar de asignar el espectro radioeléctrico (son las “autopistas del aire” por las que viajan las distintas señales) del 4G. En los últimos años, se han logrado grandes avances en todos los países, pero el 5G requiere grandes cantidades de espectro y no sólo en las llamadas frecuencias 5G.
- Desarrollar una hoja de ruta clara de política de espectro. Un espectro armonizado global y regionalmente permitiría precios más bajos a través de economías globales de escala, una adopción más rápida y un despliegue de redes más rentable. Tal hoja de ruta debe tener en cuenta el espectro sin licencia y planificar las redes privadas que Omdia cree que será un motor clave de la empresa 5G.
- Desarrollar proactivamente una política de infraestructura para alentar y facilitar que el sector privado invierta en redes 5G. Promover un marco que simplifique y facilite el despliegue de infraestructuras en un proceso de planificación nacional coherente; agilizar los procesos de aprobación para el des-

pliegue de la red, armonizando y simplificando la obtención de permisos locales; definir los requisitos razonables y procedimientos eficientes y transparentes; y establecer un tiempo máximo de respuesta y aprobación automática en caso de que no se promueva ninguna respuesta de los municipios.

- Promover el intercambio de infraestructuras de todo tipo de redes e infraestructuras en términos comercial y técnicamente acordados. Esto podría resultar en ahorros sustanciales de costos y hacer que la inversión sea más atractiva: 5G requerirá una densificación significativa (incluidas las células pequeñas), y el hecho de compartir podría ser la única manera de superar la resistencia de la comunidad a la instalación de más sitios (por ejemplo, torres).
- Desarrollar un plan nacional de transformación digital. Un plan integral de estrategia nacional de transformación digital que incluya un cronograma, objetivos y metas con el 5G como facilitador de la economía digital, que debería ser una prioridad para los responsables de la formulación de políticas públicas en Latinoamérica.

La realidad es que América Latina requiere de grandes inversiones para poder implementar esta tecnología. El origen de los fondos de estas inversiones determinará quién tendrá una mayor influencia en la región: China o Estados Unidos. No hay que olvidar que esta nueva tecnología significa también una mayor interdependencia de todos los sistemas que proveen los servicios necesarios para el funcionamiento de la economía, salud y seguridad de un país: desde la electricidad que consumimos en nuestros hogares, hasta el agua que ingerimos, los sistemas de comunicación que nos mantienen en contacto con nuestros amigos y familiares, y el transporte que utilizamos –es decir, la infraestructura crítica. Garantizar su seguridad resulta de vital importancia para las naciones, y más aún para la vulnerable región latinoamericana.

Esta nueva tecnología atravesará todos los aspectos de la vida cotidiana de las personas, y afectará a todos los sectores de la infraestructura crítica. Inclusive, ya se ha comenzado a hablar de la red 6G, que podría ser hasta cien veces más rápida que la velocidad máxima del 5G, en el desarrollo de la cual China lleva una amplia ventaja. El

reciente logro de los científicos chinos de haber alcanzado la supremacía cuántica no es un hecho menor, ya que permite realizar tareas que una supercomputadora tradicional no podría. Entonces, se trata de establecer qué actor tendrá el control de las tecnologías del siglo XXI y será el líder de la cuarta revolución industrial.

Bibliografía

- Bracken, B., “Chinese Breakthrough in Quantum Computing a Warning for Security Teams”, 2020. Recuperado de: <https://threatpost.com/chinese-quantum-computing-warning-security/161935/>
- Departamento de Seguridad Nacional de los Estados Unidos: Infraestructura Crítica. Recuperado de: <https://www.cisa.gov/infrastructure-security>
- Disposición N° 1/2021. DI-2021-1-APN-DNCIB#JGM. Recuperado de: <https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-1-2021-347311/texto#:~:text=Que%2C%20por%20la%20Resoluci%C3%B3n%20N,determinaci%C3%B3n%20de%20los%20sectores%20alcanzados.>
- Drincovich, S., “La nueva guerra comercial mundial que involucra a la Argentina: un solo número, una sola letra”, en Iproup, 2002. Recuperado de: <https://www.iproup.com/innovacion/10626-5g-definicion-que-es-y-la-guerra-tecnologica-que-afecta-a-argentina>
- Intervención de la Delegación Argentina – OEA, 2018. Recuperado de: <http://scm.oas.org/pdfs/2019/CICTE01301A.pdf>
- Jaffrot, E., “La definición del estándar 5G”, en revista Fibra, 2016. Recuperado de: <http://papel.revistafibra.info/la-definicion-del-estandar-5g/>
- Kavanagh, S., “What is 5G New Radio”, en 5G.co, 2020. Recuperado de: <https://5g.co.uk/guides/what-is-5g-new-radio/>
- Ley de Ciberseguridad y Seguridad de la Infraestructura, 2018. Recuperado de: <https://www.govinfo.gov/content/pkg/PLAW-115publ278/pdf/PLAW-115publ278.pdf>
- Observatorio de Política Internacional del Senado Argentino, 2020. “EE. UU. - China: Hegemonía Geopolítica y Carrera Tecnológica”. Recuperado de: <https://www.senado.gob.ar/bundles/senadomicrositios/pdf/internacionales/publicaciones/eeuuchina2020.pdf>
- Resolución N° 1.523/2019. Secretaría de Gobierno de Modernización de la República Argentina. Definición de Infraestructuras Críticas.

Recuperado de: <https://www.argentina.gob.ar/normativa/nacional/reso-luci%C3%B3n-1523-2019-328599>

Swaing, Lopes, Agnese, “Why 5G in Latin America? A call to action for Latin American operators and policymakers, 2020. Recuperado de: https://news.america-digital.com/wp-content/uploads/2020/08/Nokia_Why_5G_in_Latin_America_Report_ES.pdf

USA Patriot Act, 2001. Recuperado de: <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>

Weissberger, A., “Nokia & Omdia: 5G could bring up to \$3.3 trillion to Latin America by 2035 – vs. 13% of mobile subs in 2025?”, en Technology Blog, 2020. Recuperado de: <https://techblog.comsoc.org/2020/08/30/nokia-omdia-5g-could-bring-up-to-3-3-trillion-to-latin-america-by-2035-more-pie-in-the-sky/>