La pandemia como una amenaza a la vida y a la seguridad del Estado

EL CIBERESPACIO, DURANTE Y DESPUÉS DE LA PANDEMIA COVID-19

Ph. D. Mariano Bartolomé[1] y

Crnl. I. M. André Gustavo Monteiro Lima[2]

RESUMEN

El surgimiento de la pandemia Covid-19, en diciembre de 2019 en China y su posterior expansión a nivel mundial, representó un fuerte impacto en los hábitos de toda la población. Las relaciones sociales virtuales, que ya estaban aumentando, se expandieron y pasaron a formar parte de nuestra rutina, convirtiéndose en un lugar común para el trabajo, la educación, la salud y otros campos de la actividad humana. En el escaso tiempo de un año, la infraestructura cibernética soportó un flujo de información muchas veces más grande que el que teníamos hasta entonces. Este artículo tiene como objetivo evaluar la relación entre la pandemia y el campo de la ciberseguridad durante el año 2020.

Palabras clave: Cibercriminalidad, ciberespacio, ciber-espionaje, ciberterrorismo, Covid-19

ABSTRACT

The emergence of the Covid-19 pandemic, in December 2019 in China and its subsequent expansion worldwide, had a strong impact on the habits of the entire population. Virtual social relationships, which were already increasing, expanded and became part of our routine, becoming a common place for work, education, health and other fields of human activity. In the short time of a year, the cyber infrastructure supported a flow of information many times greater than the one it sustained until then. This article aims to evaluate the relationship between the pandemic and the field of cybersecurity during the year 2020.

Key words: Cybercrime, cyberspace, cyberterrorism, cyber espionage, Covid-19

INVESTIGADOR INDEPENDIENTE

[1] Graduado y Doctor en Relaciones Internacionales, por la Universidad del Salvador. Posee una Maestría en Sociología (UNLZ-IVVVVE/Academia de Ciencias de la República Checa) y realizó estudios posdoctorales en la Universidad Complutense de Madrid. Profesor permanente del Colegio Interamericano de Defensa. De nacionalidad argentina, oriundo de la ciudad de Mar del Plata.

[2] Coronel Ingeniero Militar, nacido en Rio de Janeiro-RJ, Brasil. Egresado del Instituto de Ingeniería Militar (IME) en 1993. Maestro en Ingeniería de Telecomunicaciones por el IME (2000) y Doctor en Ingeniería por la Universidad de Brasilia (UnB) en 2006. Actualmente es profesor del Colegio Interamericano de Defensa.

DOI: https://dx.doi.org/10.24133/age.n14.2021.06

Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 14. Núm. 1 abril 2021. pp. 67 - 76

Introducción

Tomando como eventos referenciales la aparición del microprocesador, comúnmente denominado chip, y la primera transmisión de Internet entre las universidades de California y Standford, ambos hechos sucedidos en 1969, las Tecnologías de la Información y las Comunicaciones (TICs) registraron un enorme salto cualitativo durante el último medio siglo. Como resultado de ese avance suele decirse que la sociedad contemporánea se encuentra globalmente inmersa en un contexto de Big Data, en referencia al enorme volumen de información que la atraviesa y articula, mensurable en centenares de terabytes, la velocidad de su generación y tráfico, y la heterogeneidad de sus fuentes y formatos (Mitchell, Locke, Wilson y Fuller 2012).

Esta novedosa situación ha alcanzado todos los aspectos de la interacción social, configurando un nuevo ámbito para el desarrollo de las actividades humanas: el ciberespacio, entendido como un "dominio global y dinámico compuesto por infraestructuras de TI (incluido Internet), redes, sistemas de información y telecomunicaciones" (Quintana, 2016, pág. 45). La idea de dominio debe ser entendida aquí en consonancia con los llamados *comunes globales*, dominios que no están bajo el control ni bajo la jurisdicción de ningún Estado, pero cuyo acceso y uso es objeto de competencia por parte de actores estatales y no estatales de todo el planeta (Stang, 2013).

Es así que a los cuatro dominios o ámbitos tradicionales de la seguridad y la defensa –terrestre, marítimo, aéreo y aeroespacial– se sumó el cibernético, que los atraviesa. En esta lógica, las amenazas y riesgos que se desarrollan en este quinto dominio, el ciberespacio, constituyen el campo de estudio y actuación de la ciberseguridad. Existen múltiples definiciones de ciberseguridad, más o menos abarcativas, aunque suele ser referencial la que propone la Unión Internacional de Telecomunicaciones (2018, p.13), en los siguientes términos:

> La ciberseguridad es el conjunto de herramientas, políticas, guías de acción, abordajes de gestión de riesgo, acciones, entrenamientos, mejores prácticas, reaseguros y tecnologías que pueden ser empleados para proteger la disponibilidad, integridad y confidencialidad de activos en las infraestructuras interconectadas pertenecientes al gobierno, organizaciones privadas y ciudadanos. Esos activos incluyen equipos de computación, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones e información en el ambiente cibernético.

Las cuestiones de ciberseguridad pueden ser clasificadas desde diferentes puntos de vista, aunque en última instancia esas clasificaciones suelen ser el reflejo de la combinación entre cuatro elementos, a saber: protagonistas de la amenaza o incidente; herramientas o técnicas empleadas por ellos; blancos de la acción e impacto generado (The Hague Centre for Strategic Studies, 2015). Desde la perspectiva de sus protagonistas podemos discriminar entre actores estatales y no estatales, reparando además en el contenido político o no de los objetivos que exhiben sus protagonistas (Baezner, 2018). En este enfoque adquieren relevancia grupos no estatales que realizan actividades ilícitas de cierta gravedad, de manera sostenida en el tiempo, con fines de lucro; o que persiguen metas políticas a través del ejercicio de la violencia. En el primero de estos casos, la referencia es al crimen organizado, mientras el segundo remite básicamente al terrorismo.

A los dos tipos señalados de protagonistas del campo de la ciberseguridad puede agregarse un tercero, conformado por organizaciones que realizan prácticas de espionaje. Aquí, sin embargo, los contornos del fenómeno se vuelven más difusos a la luz de dos circunstancias: por un lado, sus fines pueden ser tanto económicos, como políticos; por otra parte, normalmente está fuertemente limitada la autonomía decisoria del actor no estatal que lleva adelante la actividad, pudiendo ser una organización patrocinada por un Estado (lo que habitualmente se denomina proxy), o incluso una entidad de fachada de este último (Hathaway & Klimburg, 2012). De esta manera, la cibercriminalidad, el ciberterrorismo y el ciber-espionaje son fenómenos que refieren a las formas de expresión en el ciberespacio de la criminalidad organizada, el terrorismo y el espionaje. Y junto con la llamada ciberguerra, cuyo análisis excede los alcances del presente trabajo, constituirían las cuestiones de ciberseguridad más relevantes en la agenda de la Seguridad Internacional contemporánea (Hathaway & Klimburg, 2012; Burton, 2015).

La relevancia de esas tres cuestiones no solo no ha disminuido con la aparición del virus Covid-19, calificado el 11 de marzo del año pasado por la Organización Mundial de la Salud (OMS) como una pandemia. A decir verdad, esa importancia parece haber aumentado en forma directamente proporcional al agravamiento de la situación sanitaria global. Algunos datos respaldan esta apreciación: según el relevamiento efectuado por una respetada empresa de seguridad cibernética, el 90 % de los usuarios aumentaron el uso de dispositivos electrónicos, el 86 % descargó nuevas herramientas virtuales de la red y un 66 % continuó sus obligaciones de manera remota; más de la mitad de estos trabajadores a distancia no recibió por parte de sus empleadores ninguna capacitación ni programas en ciberseguridad, y un 44 % de ese total fue objeto de ataques de phising (Harán, 2020).

En ese sentido, el Covid-19 habría operado como un factor susceptible de reforzar, maximizar o agravar otras fuentes de daño. La literatura reciente refiere a esta cualidad bajo el rótulo de "conductores (drivers) de inseguridad" (Williams, 2013) o "potenciadores de riesgo" (Portero Rodríguez, 2013), entre otros apelativos, cuya lista está dominada por la heterogeneidad: en un listado no exhaustivo podrían incluirse, además del Coronavirus, a la pobreza y

desigualdad socioeconómicas extremas, el cambio climático, las brechas tecnológicas, las ideologías radicales, el crecimiento poblacional, la urbanización masiva y desordenada, la escasez de recursos naturales (particularmente el petróleo), la militarización global y la licuación del poder del Estado en beneficio de formas alternativas de gobierno, entre otras.

Con este contexto, el presente trabajo tiene como objetivo principal describir el rol del Covid-19 como conductor de inseguridad o potenciador de riesgo en el campo de la ciberseguridad. Más específicamente, en materia de cibercriminalidad, el ciberterrorismo y el ciber-espionaje. Con esa meta, en primer lugar se realizará una breve descripción sobre la fisonomía que suelen exhibir estos tres fenómenos, sin referencia al citado virus; segundo, se consignarán algunas novedades registradas en el desarrollo de cada uno de ellos a partir de la irrupción de la pandemia, en las cuales se verifica una nítida relación de causalidad, y en tercer término, se efectuará una breve referencia al desarrollo de los fenómenos identificados en un contexto que hemos denominado "nueva normalidad" y que se caracteriza por la adopción de nuevas prácticas y procedimientos a la luz de la irrupción de la pandemia. Para finalizar, se elaborarán unas breves conclusiones.

I. Algunos comentarios sobre cibercriminalidad, ciberterrorismo y ciber-espionaje

Respecto a la cibercriminalidad, a grandes rasgos podría ser entendida como "formas tradicionales delictivas perpetradas por medio de comunicaciones electrónicas, redes y sistemas de información, además de la publicación ilegal en los medios electrónicos y delitos propios de las redes electrónicas" (Buscaglia, 2015, pág. 59). En esta definición resulta clave la referencia a la cualidad *tradicional* de la actividad ilegal, en el sentido de preexistir a la conformación del ciberespacio. Entonces, abarcaría la gestión en ese entorno virtual de tráficos ilícitos de diverso tipo, por ejemplo, armas, documentación, drogas naturales y sintéticas e incluso personas, entre otros. También incluiría el empleo del ciberespacio para la legalización de activos procedentes de esas acciones comerciales fuera de la ley, actividad usualmente denominada lavado de dinero.

Complementando a la cibercriminalidad asociada a formas delictivas tradicionales, existe otra dimensión conocida como crimen ciberdependiente, entendida como "un crimen que sólo puede ser cometido usando computadoras, redes de computadoras u otras formas de TICs" (Europol, 2019, pág. 14). Entra en este campo el empleo de software malicioso (malware) de diferentes tipos, destacándose los que vedan el acceso del usuario a los datos almacenados en el equipo afectado, solicitándose un "rescate" monetario para su liberación; en algunos casos este tipo de software, conocido como ransomware, es destructivo, generando daños permanentes. Según declaraciones de Catherine De Bolle, Directora Ejecutiva de EUROPOL, durante el año 2019 el ransomware mantuvo su primacía como la forma de ataque más expandida y dañina en el Viejo Continente (Ibid.).

Otras expresiones de crimen ciberdependiente remiten al *phising*, el robo de información personal de un individuo a través de un engaño, por lo general apelando a correos electrónicos o páginas web falsas. Los datos así obtenidos pueden ser empleados para la realización de delitos financieros de diferente tipo, comerciales o bancarios, por parte del grupo que los obtuvo o de otros. O pueden ser usados para efectuar nuevos ciberataques, por ejemplo, con ramsomware. En su último reporte anual, EUROPOL indica que las técnicas de phising fueron responsables de al menos el 90 % de las infecciones por malware, así como del 72 % de las filtraciones de datos en organizaciones (Europol, 2020a).

La llamada denegación distribuida de servicio (DDoS) también integra el inventario de expresiones del crimen ciberdependiente. Consiste en el bloqueo o inhabilitación temporaria de un sistema informático, impidiendo el acceso a él por parte de terceros, de sus operadores, o de ambos. Se realizan mediante peticiones o conexiones simultáneas a ese sistema desde un gran número de ordenadores -millones, eventualmente- infectados con un mismo malware, que operan coordinadamente como "zombies" (bots) y lo saturan. En forma similar a los ciberataques con ransomware, en el caso del DDoS los criminales apuntarían a obtener algún tipo de recompensa monetaria a cambio de la suspensión de la agresión.

Resulta claro que la obtención de cierto consenso en torno al significado de la cibercriminalidad está facilitada por la existencia previa de una definición consensuada a nivel internacional, en torno al crimen organizado. Y esa definición existe desde principios de siglo, cuando tuvo lugar la Convención de Palermo de las Naciones Unidas, actualmente vigente. No es este el caso del terrorismo, fenómeno en torno al cual pujan decenas de abordajes y lecturas alternativas, sin que ninguna de ellas se haya impuesto con nitidez hasta el momento. A pesar de esa limitación, la Unión Internacional de Telecomunicaciones ha podido conceptualizar al ciberterrorismo como "la utilización de la red por organizaciones terroristas para ataques cometidos en la red contra infraestructuras esenciales, así como el uso de TIC e Internet para los fines de propaganda, recopilación de información, preparación de ataques al mundo real, comunicación y financiación de actividades terroristas" (UIT, 2014, pág. 38).

Actualmente, las organizaciones terroristas tienen páginas en Internet, además de participar en redes sociales, comunidades de videos y otros foros para realizar su propaganda. Dichos medios también funcionan como una forma de difundir sus doctrinas, captar adeptos y capacitar sus miembros en diversas técnicas y herramientas utilizadas con el propósito de cometer el terrorismo. No es raro que una persona haya

visto imágenes de videos publicados por estos grupos, ensalzando sus acciones, en todo el planeta. Además, el dominio cibernético ofrece una serie de herramientas de comunicación que pueden utilizarse como medio para planificar o coordinar ataques.

Por otro lado, nunca ha habido tanta información de calidad disponible sobre el mundo como en la actualidad. Desde mapas geográficos, imágenes de satélite, fotografías, comportamiento de personalidades y personas comunes. Todo está disponible en Internet. Esta información puede ser utilizada legalmente por un ciudadano común, pero también es una excelente fuente utilizada por los grupos terroristas para planificar sus actividades. Accesoriamente, otro de los principales beneficios que el entorno cibernético puede ofrecer a estos grupos es la financiación de sus actividades. Ya sea mediante donaciones a cuentas publicadas en sus propias páginas o redes sociales, o simulando comercio electrónico en tiendas online. Estas organizaciones se basan en sistemas legales y de investigación débiles en varios países del mundo, lo que dificulta el seguimiento del dinero y la verificación de las transacciones financieras.

En resumen, los grupos terroristas pueden utilizar cualquier forma de delito cibernético para recaudar fondos para su causa. Este aspecto es otro factor de complicación para la acción de la justicia, dado que las posibilidades legales de investigación y las penas aplicadas a un ciberdelito común tienden a ser más ligeras que las que se utilizarían en el caso de configuración de acción terrorista. A veces, puede resultar difícil configurar un ciberdelito como una acción de este tipo, lo que beneficia a estos grupos.

Finalmente, en el caso del ciber-espionaje, ya se ha indicado que los actores involucrados en esta actividad suelen operar por delegación estatal, o directamente integrar su estructura, formal o informal. Sus blancos pueden ser tanto públicos como privados, e incluso de la sociedad civil. Y en su peligrosidad incide la confluencia de tres factores: enormes capacidades y recursos materiales; bajo riesgo para el actor hostil, y amplio beneficio que puede reportar esta actividad (Centro Criptológico Nacional, 2020). Es precisamente debido a su peligrosidad, que las entidades que protagonizan estas labores suelen ser tipificadas como amenazas persistentes avanzadas (APT, por sus siglas en inglés), resaltando su empleo de sofisticadas técnicas para poder acceder a sistemas y permanecer en ello por largos períodos de tiempo, con consecuencias destructivas (Kaspersky, 2020).

Algunos ejemplos de ciber-espionaje que alcanzaron notoriedad internacional incluyen el ataque perpetrado contra el Bundestag (Parlamento alemán) hace un lustro, cuando varios legisladores recibieron falsos correos electrónicos que implicaron la descarga involuntaria de un malware que posibilitó el robo de gran cantidad de información. Las pesquisas de los servicios de seguridad germanos concluyeron que el responsable de la agresión era un hacker vinculado al servicio de inteligencia militar ruso (Bartolomé, 2020b). Más cerca en el tiempo, por espacio de más de dos meses en 2017 se ejecutó una exfiltración de datos desde la empresa estadounidense Equifax, afectando a 148 millones de personas; es decir, más de la mitad de la población del país. Casi tres años más tarde, como fruto de las actuaciones judiciales y las investigaciones realizadas desde el Poder Ejecutivo (USGAO, 2017) se acusó del hecho a un grupo relacionado con las fuerzas armadas de China (Benner, 2020). Un tercer caso susceptible de ser mencionado tuvo lugar a mediados de 2019, ocasión en que más de medio centenar de universidades en diferentes países fueron víctimas de actividades de espionaje (vía phishing) orientadas al robo de información científica y propiedad intelectual; se identificó como responsable el grupo Cobalt Dickens, ligado al régimen de Irán (Paganini, 2019).

Conviene mencionar que el cibercrimen, el ciberterrorismo y la actividad de los grupos APT comparten, como característica, la inclusión dentro de su inventario de blancos a las llamadas infraestructuras críticas, ya mencionadas en párrafos anteriores como infraestructuras esenciales.

Tomando en cuenta elementos de las definiciones de Quintana (2016) y Burnett (2015) combinados en trabajos anteriores, entendemos como tales a sistemas, máquinas, edificios o instalaciones relacionados con la prestación de servicios esenciales a la población. Esas infraestructuras incluyen los sistemas de procesamiento de información y telecomunicaciones, el software que permite operarlos, y el personal que maneja los sistemas y emplea ese software (Bartolomé, 2020a, pág. 153).

Mediante *ransomwares* que ingresan a través de técnicas de *phishing*, o bloqueos tipo DDoS, los criminales atacan infraestructuras críticas básicamente con fines extorsivos.

En el caso de los terroristas, el objetivo sería generar un daño de magnitud, cuya autoría puedan reivindicar políticamente. Los grupos APT, a su turno, podrían hacerlo no sólo por cuestiones de espionaje, sino también para recolectar información sobre objetivos estratégicos que, eventualmente, podrían ser destruidos o neutralizados. Es necesario tener presente, en este punto, que estas organizaciones pueden llevar adelante acciones ofensivas funcionales a los intereses de los Estados para los cuales operan, o de los que realmente forman parte (Council of Economic Advisers, 2018; Centro Criptológico Nacional, 2020).

Cerrando este apartado, conviene subrayar el uso intensivo que ciberespías, ciberterroristas y cibercriminales hacen de la llamada *Dark Web*, esa porción encriptada de la *Deep Web* donde proliferan los negocios ilegales, a los que se accede de manera anónima con softwares específicos que en sí mismos no son criminales. Las operaciones comerciales que en ella se realizan, usualmente se abonan con criptomonedas, entre ellas el bitcoin. Kumar (2019) estimó en más de

65 mil a los dominios alojados en este sector de Internet de complicada accesibilidad.

II. Efectos del Covid-19 en la cibercriminalidad, el ciberterrorismo y el ciber-espionaje

Ya hemos indicado que las tres cuestiones abordadas en el presente trabajo se mantuvieron vigentes tras la aparición del virus Covid-19 y su expansión a escala global, en los primeros meses del año 2020. En especial la cibercriminalidad y el ciber-espionaje incrementaron cuantitativamente sus acciones, y las volvieron más complejas desde el punto de vista cualitativo. En cuanto al terrorismo, aunque con una intensidad algo menor que los otros fenómenos, su persistencia no ha sido en modo alguno despreciable.

Diversos factores contribuyeron a esa vigencia. Entre ellos, el incremento de la actividad on-line, sobre todo en los campos de educación, salud y comercio. En los términos de una reconocida compañía de seguridad informática,

la implementación del teletrabajo de manera masiva, en lugar de darse de manera paulatina, sucedió de una manera brutal, a las apuradas y mezclándose con una vida cotidiana y una situación social absolutamente convulsionada. A esto se le suma el hecho de que los cibercriminales se adaptan rápido a estas situaciones y buscaron empezar a explotar las oportunidades que la improvisada implementación del teletrabajo le presentaban (ESET, 2020, pág. 3).

Los flujos de información también aumentaron de manera exponencial, no sólo por las actividades antes mencionadas, sino también como un efecto de los altos grados de incertidumbre existentes, que llevaron a la gente a buscar en Internet las respuestas a sus dudas, temores y preocupaciones. Pero ese crecimiento de la actividad on-line fue en buena medida improvisado, razón por la cual estuvo acompañado por accesos remotos no autorizados, el uso indebido de computadoras personales y prácticas deficientes de contraseñas y validación, entre otras debilidades. En algunos casos, pueden vincularse estas flaquezas con la inexistencia de culturas de teletrabajo, o con la decisión de priorizar la continuidad de actividades, antes que subordinarlas a criterios de ciberseguridad.

En materia de terrorismo, las organizaciones Al Qaeda y Daesh (Estado Islámico) intentaron valerse de la pandemia en un doble sentido. Por un lado, procuraron obtener un rédito en materia de difusión de su ideario, enfatizando en que la expansión del virus a escala global no era otra cosa que un castigo divino a las sociedades apóstatas y consumistas de Occidente, o a quienes persiguen y maltratan a los musulmanes, como sería el caso de China. Por otra parte, instaron a sus seguidores a planificar nuevas acciones violentas en las naciones occidentales, teniendo en cuenta que las fuerzas policiales y de seguridad de esos países estaban afectadas a los operativos vinculados con la crisis sanitaria (Bartolomé, 2020b).

Esos hechos coinciden plenamente con las lecturas elaboradas desde las Naciones Unidas y la Organización de Estados Americanos (OEA). En un reporte elaborado a mediados de año, la Oficina de Contraterrorismo del organismo internacional recordó que las organizaciones terroristas pueden explotar la disrupción y las dificultades económicas causadas por el Covid-19 para difundir odio y divisiones, y para radicalizar y reclutar nuevos combatientes. Además, la pandemia subrayó la peligrosidad que tendrían formas de terrorismo sobre las cuales se teorizó, aunque aún no se llevaron a la práctica, como ciberataques contra infraestructuras críticas. Frente a este escenario, se insistió en la importancia de la cooperación internacional, especialmente en materia legal y de intercambio de información, para prevenir y responder a estas amenazas (UNOCT, 2020). La OEA, a su turno, entendió que la pandemia de Covid-19 es un potencial catalizador para la desinformación y difusión de noticias falsas, que pueden ser utilizadas por grupos terroristas para sus beneficios (OEA, 2020).

En lo que hace al cibercrimen, de acuerdo a un sondeo de opinión ya referido en pasajes anteriores de este trabajo, para un 96 % de los encuestados esta amenaza se agravó en el escenario pandémico, configurando mayores riesgos para usuario y empresas (Harán, 2020). Los impactos se observaron tanto en sus conformaciones tradicionales, como en el novedoso formato de delitos ciberdependientes. En el primer caso, en la *Dark Web* se detectó la comercialización ilegal de vacunas y medicamentos presuntamente eficaces contra el Covid-19. También se vendieron máscaras y kits de prueba falsos, e incluso muestras de fluidos corporales contaminantes, que se cobraron, pero nunca entregaron (Europol, 2020b; Interpol, 2020). En la segunda opción, durante el primer trimestre aumentó de manera casi exponencial la apertura de dominios web vinculados con la pandemia, refiriendo o conteniendo las palabras "corona" o "covid", cuyo número saltó de casi cero a comienzos de año, hasta casi ochocientos diarios, a principios del mes de marzo (Insikt, 2020). Desde esos sitios se impulsaron ventas de bienes y servicios clandestinos, incluidos los medicamentos antes mencionados. A través de *phishing*, también se atrajo a incautos que dejaron datos personales, útiles para llevar a cabo fraudes y otros delitos (Europol, 2020b).

Sin embargo, en su evaluación sobre las repercusiones del Covid-19 en la ciberdelincuencia, Interpol observó un cambio sustancial en los objetivos de los ataques: antes eran mayoritariamente personas particulares y pequeñas empresas, y luego los blancos tendieron a ser grandes multinacionales, administraciones estatales e infraestructuras esenciales. Esto se debió al hecho de que las organizaciones y las empresas desplegaron rápidamente redes y sistemas a distancia para que el personal pudiera trabajar desde sus hogares. Con eso, los delincuentes tomaron ventaja del aumento de las vulnerabilidades en materia de seguridad para robar datos, obtener beneficios y ocasionar disrupciones.

Los ciberdelincuentes se han centrado cada vez más en los empleados para conseguir un acceso remoto a las redes corporativas. Empresas medianas han sido víctimas de campañas de *ransomware*, perpetrada principalmente por medio del *malware* Lockbit, un software malicioso diseñado para bloquear el acceso de los usuarios a los sistemas informáticos a cambio de un pago de rescate. Ese *malware* busca automáticamente objetivos valiosos, propaga la infección y cifra todos los sistemas informáticos accesibles en una red. Los delincuentes también intensificaron el uso de los medios sociales para la exploración sexual de menores a través de Internet, capitalizando la mayor cantidad de tiempo que se encuentran on-line así como su conducta, que escapa al control de adultos (Interpol, 2020).

Según fuentes especializadas, durante el primer semestre de 2020 los ataques con *phising* y *malware* pasaron de menos de 5 000 a más de 200 000 por semana. En ese lapso, la cantidad de ciberataques a nivel global creció un 34 % respecto al período inmediato anterior (Check Point, 2020). Las estadísticas de Interpol hasta el mes de mayo, basadas en la información proporcionada por los países miembros sobre ciberataques con malware, específicamente ransomware, y phishing, indican que el Covid-19 se relacionó con el 36 % y 59% del total mundial de esas agresiones, respectivamente (Interpol, 2020).

El hemisferio americano acompañó las tendencias verificadas a nivel global. En el caso de América Latina y el Caribe se verificó un fuerte aumento de casos de phishing y de campañas de estafas en relación con la Covid-19, que aprovechan la crisis del coronavirus y el consiguiente confinamiento. Así, los ataques con phishing que tenían software malicioso adjunto tuvieron en la región un aumento interanual del 17 % en enero, 52 % en febrero y 131 % en marzo. En términos absolutos, los ciberataques con malware en América Latina y el Caribe habrían sido unos tres millones, aproximadamente, durante el primer trimestre del año[1].

En tiempos de Covid-19, no puede dejar de mencionarse la intensificación del ataque de grupos cibercriminales a infraestructuras críticas de características muy específicas: hospitales y centros de salud. Hasta la eclosión de la pandemia, este tipo de instalaciones no habían estado entre las preferencias de las organizaciones criminales, a juzgar por evaluaciones independientes[2]; sin embargo, esta situación se revirtió, según consignaron agencias como Interpol (2020) y Europol (2020). Este tipo de acciones parece haber sido particularmente intenso en las naciones europeas, donde incluso se cobró una víctima fatal: en ocasión de un ataque a un hospital en la ciudad alemana de Dusseldorf, falleció un paciente mientras era trasladado de urgencia a otro lugar de internación. Empero, el punto álgido de estas acciones se registró en Estados Unidos durante el mes de octubre, con el ataque a más de 300 centros de salud de la red Universal Health Services, empleando el virus denominado Ryuk, un ransomware de alta peligrosidad y ya conocido en el mundo informático (Meskauskas, 2019).

Finalmente, la sinergia entre la eclosión del Covid-19 a escala global y las prácticas de ciber-espionaje por parte de grupos APT fue motivo de especial atención por parte de organismos estatales de los países susceptibles de ser blanco de esas prácticas. En el caso de Estados Unidos, la Oficina Federal de Investigaciones (FBI) y la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) informaron que entidades de esa nacionalidad que realizan investigaciones relacionadas con el virus se habían visto comprometidas en ciberataques ejecutados por actores afiliados a China. La alerta señaló que los sectores de salud, farmacéutico y de investigación que trabajan en la respuesta al Covid-19 deben ser conscientes que son los principales objetivos de esta actividad y tomar las medidas necesarias para proteger sus sistemas. El similar de CISA del Reino Unido emitió una advertencia de alerta similar, referida a agentes maliciosos que atacan a las organizaciones de respuesta al Covid-19 utilizando una táctica de pulverización de contraseñas (CERT-CISA, 2020).

Es necesario tener presente que, en línea con lo que se anticipó en otro pasaje del presente trabajo, no son únicamente de filiación china los grupos que realizaron ciber-espionaje vinculado al Covid-19. Así, se descubrieron actividades de ese tipo de un grupo vinculado a Irán, sobre el laboratorio Gilead Sciences, que desarrolló el fármaco Remdesivir, empleado en tratamientos contra ese virus; los intentos de penetración apuntaban al robo de información sensible sobre el antiviral (Klebnikov, 2020; Stubbs & Bing, 2020). Conductas similares desarrolló sobre laboratorios de Estados Unidos, Gran Bretaña y Canadá un grupo conocido como Cozy Bear (entre otros nombres), ligado a Rusia (NCSC et.al, 2020)[3]. En tanto, todavía no se ha identificado la nacionalidad (si hubiera una, de manera definida) de los grupos responsables de los últimos actos de ciber-espionaje ejecutados en el año: uno sobre organizaciones involucradas en la "cadena de frío" necesaria para la distribución de la vacuna, que integran el grupo Gavi[4]; otro sobre la Agencia Europea de Medicamentos, que evaluaba la habilitación de las vacunas elaboradas por diferentes laboratorios.

[1] Estas cifras surgen del monitoreo realizado por la compañía de ciberseguridad Fortinet y constan en su análisis de Inteligencia de Amenazas para América Latina. Disponible en https://www.fortinet-threatinsiderlat.com/es/Q1-2020/landing

[2] Según se desprende del análisis de la compañía de seguridad informática Accenture. Disponible en https://www.accenture.com/_acnmedia/PDF-99/Accenture-Cost-Cyber-Crime-Infographic.pdf#zoom=50

[3] De acuerdo a informes periodísticos y de compañías de ciberseguridad, Cozy Bear también habría participado del hackeo al Comité Nacional Demócrata de Estados Unidos, en 2016.

[4] Gavi es una alianza de organismos internacionales, instituciones de la Sociedad civil y socios privados para la distribución de vacunas en todo el planeta, incluyendo regiones de extrema pobreza. Entre sus miembros se incluye la Organización Mundial de la Salud (OMS), Unicef, el Banco Mundial y la Fundación Bill & Melinda Gates.

Sobre el primero de estos dos casos, el del grupo Gavi, expertos en seguridad informática de la compañía IBM han sugerido que, por la sofisticación del ataque y la especificidad de los blancos, el origen de la agresión sería estatal (Corera, 2020).

Un indicio de la gravedad que pueden tener estos incidentes surge del informe de la Comisión Solarium (United States of America, 2020), sobre las lecciones aprendidas de ciberseguridad durante la pandemia. El reporte confirmó que el Covid-19 desafió la resiliencia de los Estados Unidos a escala nacional e ilustró los desafíos de construir y mantener esa aptitud en un mundo moderno y conectado. Las lecciones aprendidas ofrecieron muchos paralelismos esclarecedores con un ciberataque significativo, así como una guía sobre cómo prepararse para un evento de ese tipo.

III. Nueva "normalidad" de la ciberseguridad

A pesar de la incidencia de la pandemia en los campos del cibercrimen, el ciberterrorismo y el ciber-espionaje, no es posible atribuir directamente al Covid-19 todo el aumento de los problemas relacionados con el amplio campo de la ciberseguridad en el año 2020. Tampoco se puede decir que el impacto de la pandemia haya tenido como resultado un comportamiento promedio anormal en los índices relacionados.

Al analizar los gráficos de las Figuras 1 y 2, extraídos del informe F5 Phising and Fraud 2020 (F5, 2020), se pueden notar algunas pruebas interesantes.

Inicialmente, se observa que hubo un aumento significativo de incidentes reportados por phising en relación a 2019, pero no tan expresivo cuando se compara con el año 2018. Comparando la tasa mensual de tales incidentes en el año 2020 con el promedio correspondiente a los años del lustro 2015-2019, hay un aumento significativo en los meses de marzo, mayo, junio y julio y un enfriamiento en el mes de septiembre. Asimismo, la tasa de nuevos certificados que contienen el término "covid" o "corona", indicativo del uso de dominios para cometer fraude, tuvo valores significativos en el trimestre enero-marzo y en julio, con una reducción considerable en los demás meses del año. Los robos de datos de tarjetas de crédito aumentaron de manera diferente de abril a junio, con una reducción en julio. El número de violaciones de datos en 2020 fue incluso menor que en 2019.

Trascendiendo las lecturas sectoriales que han sido consideradas en el presente trabajo, todavía no se dispone de suficientes datos para evaluar el impacto real del Covid-19 en los índices globales de ciberseguridad, a mediano plazo. No puede determinarse aún si las novedades registradas en el período aquí considerado se mantendrán en el tiempo, tornándose en permanentes, o si serán indicativas de situaciones coyunturales. El mundo seguirá viviendo la pandemia en 2021 y, aunque ya existe más información sobre el virus, están surgiendo nuevos temas con fuerte impacto en la población, relacionados con la capacidad de las vacunas existentes; el acceso a la vacuna; la fabricación de nuevos medicamentos y las previsibles variaciones del virus. Todas estas cuestiones serán propicias para la ejecución de nuevos tipos de delitos basados en la desinformación de la población. Sumado a esto, el estrés acumulado a lo largo de este tiempo se traducirá

Figura 1. *Datos estadísticos sobre incidentes de seguridad en 2020 (F5,2020)*

Figura 2. *Datos estadísticos de violaciones de datos en 2020 (F5,2020)*

en un factor de "acomodamiento cibernético" que abrirá posibilidades para la comisión de delitos. Nadie puede estar atento durante tanto tiempo en un entorno de tanta incertidumbre.

Hacia adelante, otro aspecto importante a considerar será el aumento de la capacidad de reacción ante los ciberincidentes, así como el aumento de la conciencia de los riesgos y amenazas en este dominio. Como se dijo anteriormente, el Covid-19 ha cambiado los hábitos en múltiples campos de la actividad humana, en todo el mundo. Si antes el teletrabajo era un beneficio para pocos, hoy forma parte de la rutina de una parte importante de la población. Este hecho, combinado con la preocupación de las grandes empresas por mantener adecuados niveles de ciberseguridad en el entorno de trabajo virtual, resulta en un aumento del nivel de conciencia. Las empresas incrementaron sus procesos y sistemas de protección. Aunque sin datos concretos para concluir el impacto positivo de esto, es razonable entender que contribuyó a mejorar el nivel de ciberseguridad. Pero del otro lado, los criminales, terroristas y grupos APT han estado utilizando toda su creatividad y capacidad para innovar en nuevas formas para explotar las vulnerabilidades en el entorno virtual. Al final de la crisis pandémica es posible que las sociedades emerjan más fuertes, pero con una "ciberdeuda" con la población.

Conclusiones

El dominio cibernético o ciberespacio se ha constituido en un ámbito particularmente relevante de los estudios contemporáneos de seguridad, como resultado del avance registrado durante los últimos decenios en materia de Tecnologías de la Información y las Comunicaciones (TICs). En ese plano, ocupan lugares prioritarios la cibercriminalidad, el ciberterrorismo y el ciber-espionaje. La cibercriminalidad puede estar vinculada a formatos delictivos tradicionales, o presentarse como un novedoso crimen ciberdependiente con intensivo empleo de técnicas de phishing, software malicioso y ataques de denegación distribuida de servicio. El ciberterrorismo, en general, focaliza en actividades de reclutamiento y propaganda, valiéndose de diferentes técnicas. El ciber-espionaje, en tanto, abarca una amplia gama de blancos y técnicas, exhibiendo una heterogeneidad que en buena medida se asocia con sus difusos contornos, sobre todo en relación a su independencia de actores estatales.

Las tres ciberamenazas mencionadas han revelado una importante permeabilidad a la irrupción súbita del Covid-19. El ciberterrorismo redobló sus esfuerzos de propaganda y reclutamiento, destacándose en este sentido organizaciones salafistas-yihadistas que justificaron a la pandemia desde el prisma de sus propios idearios, sin descartar por eso llamamientos a la acción directa contra blancos blandos, en Occidente. Grupos de ciber-espionaje se enfocaron en la vulneración de los dispositivos de seguridad de organizaciones públicas y privadas de la salud, involucradas en el desarrollo de respuestas a la pandemia.

La cibercriminalidad, finalmente, aumentó sus negocios ilícitos en la *Dark Web*, multiplicó sus acciones de engaño con la creación de dominios web apócrifos, intensificó las campañas de phishing para robar datos, e incluso atacó infraestructura crítica sanitaria. Tomando en cuenta, entonces, el efecto generado por el Covid-19 en las tres ciberamenazas analizadas, se confirma que operó a modo de "potenciador de riesgo" o "conductor de inseguridad". Sin embargo, teniendo en cuenta la perspectiva del presente trabajo, lo destacable no es tanto la vinculación entre salud y seguridad, que es innegable y ha sido explorada en el marco de diferentes perspectivas (por caso, desde la Seguridad Humana a nivel global, o la Seguridad Multidimensional en el hemisferio americano), como la extrema adaptabilidad de las ciberamenazas a las alteraciones de su entorno. Esa capacidad de adaptación plantea un importante desafío a los Estados, cuyas acciones en materia de ciberseguridad se encuentran sujetas a avances legislativos, organizacionales y doctrinarios que ocurren en períodos más dilatados. Igualmente, dilatados son los lapsos requeridos para complementar esos avances con los recursos materiales, humanos y financieros necesarios para su efectiva aplicación. Al momento de concluirse el presente trabajo, aparentemente el mundo se encuentra en la mitad de esta gran pandemia. Todavía queda un largo camino por recorrer antes de que se pueda adoptar la llamada "nueva normalidad". Por otro lado, trascendiendo la coyuntura sanitaria, aunque sus efectos en el ciberespacio se observan fácilmente, sigue siendo difícil evaluar sus impactos a mediano plazo. Además, en general, la pandemia está impulsando el desarrollo y maduración de toda la población en términos de conciencia cibernética, así como la evolución de los procesos y estructuras de ciberseguridad de las empresas. Como es habitual en las carreras del gato y el ratón, los cibercriminales, ciberterroristas y ciber-espías innovan cada día en la forma de ejecutar sus acciones ilegales. Sólo unos años después del final de este período pandémico, los beneficios y daños cibernéticos resultantes se definirán de manera precisa y concreta.

Referencias

Baezner, M. (2018). *Hotspot Analysis: Synthesis 2017. Cyber-Conflicts in Perspective*. Center for Security Studies

Bartolomé, M. (2020a). Las Ciberamenazas y su impacto en el campo de la Seguridad Internacional. *Revista de la Escuela Superior de Guerra, 602*, 151-163

Bartolomé, M. (2020b). Ciberseguridad: claves para entender su vigencia, dinámica y heterogeneidad en el mundo. *Infobae,* 26 de septiembre. https://www.infobae.com/def/defensa-y-seguridad/2020/09/26/ciberseguridad-claves-para-entender-su-vigencia-dinamica-y-heterogeneidad-en-el-mundo/

Benner, (2020). U.S. Charges Chinese Military Officers in 2017 Equifax Hacking. *The New York Times,* February 10. https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html

Burnett, P. (2015). El vital papel de la Protección de la Infraestructura de Información Crítica (CIIP) en la Seguridad Cibernética. En *Organización de Estados Americanos y Trend Micro* (editores) Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas (pp.13-14). Washington: Organización de Estados Americanos

Burton, J. (2015). NATO´s Cyber Defence. Strategic Challenges and Institutional Adaption. *Defense Studies*, 1-22

Buscaglia, E. (2015). *Lavado de dinero y corrupción.* Ciudad de México: Debate

Centro Criptológico Nacional (2020). *Ciberamenazas y tendencia*s. Edición 2020. Centro Criptológico Nacional

CERT-CISA (2020). Alert AA20-275A. *Potential for China Response to Heightened US – China Tensions*. October 01. https://us-cert.cisa.gov/ncas/alerts/aa20-275a

Check Point (2020). *Cyber Attack Trends: 2020 Mid-Year Report.* Tel Aviv & San Carlos (CA): Check Point Software Technologies

Corera, Gordon (2020). *Coronavirus: Hackers targeted Covid vaccine supply 'cold chain'*. BBC, 3 December. https://www.bbc.com/news/technology-55165552

Council of Economic Advisers (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy.* The Executive Office of the President of the United States

ESET (2020). Tendencias en Ciberseguridad para el 2021. *Welivesecurity by ESET*. https://www.welivesecurity.com/wp-content/uploads/2020/12/Cybersecurity_Trends_2021_ES.pdf

European Union Agency for Law Enforcement Cooperation (2019). *Internet Organized Crime Threat Assessment (IOCTA)*. European Union Agency for Law Enforcement Cooperation

European Union Agency for Law Enforcement Cooperation (2020a). *Internet Organized Crime Threat Assessment (IOCTA)*. European Union Agency for Law Enforcement Cooperation

European Union Agency for Law Enforcement Cooperation (2020b). *How COVID-19-related crime infected Europe during 2020.* European Union Agency for Law Enforcement Cooperation, November

F5 (2020). 2020 Phising and Fraud Report. *F5 Labs,* November 11. https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report

Harán, Juán (2020). 29 datos que deja el 2020 que hablan del estado actual de la ciberseguridad. *Welivesecurity by ESET*, 22 de diciembre. https://www.welivesecurity.com/la-es/2020/12/22/datos-2020-sobre-estado-actual-ciberseguridad/

Hathaway, M. & Klimburg, A. (2012). Preliminary Considerations on National Cyber Security. En Klimburg, A. (editor) *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE

Insikt Group (2020). Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide. *Recorded Future* FR-2020-0312. https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf

Interpol (2020). *Ciberdelincuencia: efectos de la COVID-19*. Interpol, Agosto

Kaspersky (2020). *What Is an Advanced Persistent Threat (APT)?* https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Klebnicov, S. (2020). Gilead Sciences targeted by Hackers lnked to Iran: Report. *Forbes,* May 8. https://www.forbes.com/sites/sergeiklebnikov/2020/05/08/gilead-sciences-targeted-by-iranian-linked-hackers-report/?sh=5f23e2c613db

Kumar, Aditi y Rosenbach, Eric (2019). La verdad sobre la web oscura. *Finanzas y Desarrollo*, septiembre, 22-25

Meskauskas, Tomás (2019). Cibersecuestro RYUK. *Accenture*, 6 de mayo. https://www.pcrisk.es/guias-de-desinfeccion/8879-ryuk-ransomware#:~:text=En%20contraste%20con%20otros%20virus,muchos%20equipos%20a%20la%20vez

Mitchell, I., Locke, M., Wilson, M., Fuller, A. (2012). *Big Data. The Definitive Guide to the Revolution in Business Analytic*s. Fujitsu Services

National Cyber Security Centre, Communications Security Establishment, National Security Agency and Cybersecurity and Infrastructure Security Agency (2020). *Advisory: APT29 targets COVID-19 vaccine development.* Version 1.0. 16 July. https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF

Organización de Estados Americanos (2020) *AG/RES.* 2950 (L-O/20)

Promoción de la Seguridad Hemisférica: un Enfoque Multidimensional (aprobada en la cuarta Sesión Plenaria), 21 de octubre, punto 151. http://scm.oas.org/Ag/documentos/Documentos/AG08262S03.docx

Paganini, P. (2019). Iran-linked group Cobalt Dickens hit over 60 universities worldwide. *Security Affairs.* https://securityaffairs.co/wordpress/91157/apt/cobalt-dickens-targets-universities.html

Portero Rodríguez, F. (2013). *Disfunciones de la globalización.* En Instituto Español de Estudios Estratégicos (editor) Los Potenciadores de Riesgo (pp.28-46). Ministerio de Defensa

Quintana, Y. (2016). *Ciberguerra.* Ediciones de la Catarata

Stang, G. (2013). Global Commons. *Between Cooperation and Competition. European Union Institute for Security Studies*, Issue Brief 17, April

Stubbs, Jack and Christopher Bing (2020). Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead – sources. *Reuters,* May 8. Disponible en https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV

The Hague Centre for Strategic Studies (2015). Assessing Cyber Security. A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks. *The Hague*: The Hague Centre for Strategic Studies

Unión Internacional de Telecomunicaciones (2014). *Comprensión del Ciberdelito: Fenómenos, dificultades y respuesta jurídica.* Unión Internacional de Telecomunicaciones.

United States of America (2020). *Cyberspace Solarium Commission Official Report.* March.

United Nations Office of Counter-Terrorism (2020). Virtual Counter-Terrorism Week. *Visibility Report*. July.

United States Government Accountability Office (2018). *Data Protection. Actions taken by Equifax and Federal Agencies in Response to the 2017 Breach.* United States Government Accountability Office

Williams, P. (2013). Lawlessness and Disorder: An Emerging Paradigm for the 21st Century. En Miklaucic, M., Brewer, J. y Barnabo, G. (editors) *Convergence. Illicit Networks and National Security in Age of Globalization* (pp.15-36). National Defense University Press