Revista Mexicana de Ciencias Penales

ISSN 0187-0416

Año 3 • Número 10 • enero-abril de 2020 • $100.00

Ciberdelitos

- Tecnología, derecho y conflictos
  Bibiana Beatriz Luz Clara
- Convertir una debilidad en fortaleza. Primeras experiencias acumuladas
  Damián Paret Francia
- Los Estados, las criptomonedas y la ciberseguridad
  Humberto Martín Ruani
- Las operaciones con recursos de procedencia ilícita y las *fintech*: responsabilidad penal de las personas morales
  Alberto Enrique Nava Garcés

INACIPE
INSTITUTO NACIONAL DE CIENCIAS PENALES

CONCIENTIZACIÓN, MÉXICO Y LA CIBERGUERRA

Carlos Ramírez Castañeda*

* Creador de contenido de la especialidad de Derecho Informático UNADM en temas de ciberseguridad; catedrático de diplomados, cursos y clases dentro de varias universidades de México.

PALABRAS CLAVE *KEYWORDS*

Ciberguerra	*Cyberwar*
Riesgos digitales	*Digital risks*
Cyberseguridad	*Cybersecurity*

Resumen. La carencia de concientización sobre riesgos digitales ha traído consigo una serie de peligros mayores que, hoy en día, dan paso a ser utilizados como armas digitales al alcance de cualquier persona con el conocimiento técnico suficiente. La necesidad de tener un control sobre poblaciones y gobiernos nos ha llevado a un punto de evolución en el cual la guerra ahora se convierte en una ciberguerra; la utilización de *malware*, los ataques a infraestructuras críticas, los vacíos legales y la carencia de una cultura digital apegada a los peligros más allá de un ciberdelito pueden resultar en consecuencias devastadoras. Cuando migramos de un ataque digital a uno con repercusiones tangibles en el mundo físico es donde debemos tener un punto de partida sobre las prospectivas y escenarios que requieren atención más allá de los asuntos políticos del país.

Abstract. The lack of awareness of digital risks has brought a number of major dangers, which today give way to being used as digital weapons available to anyone with sufficient technical knowledge. The need to have control over the populations and governments, has taken us to a point of evolution in which the war now becomes a cyber war; the use of malware, attacks on critical infrastructure, legal gaps and the lack of a digital culture attached to the dangers beyond cybercrime, can result in devastating consequences. When we migrate from a digital attack to one with tangible repercussions in the physical world, its where we must have a starting point on the perspectives and challenges that require attention beyond the political affairs of the country.

SUMARIO:

I. INTRODUCCIÓN

Vivimos en una sociedad dependiente de la tecnología, la cual evoluciona día a día; hemos trasladado nuestra identidad física a un espacio intangible, al espacio digital. Diariamente, alimentamos nuestros perfiles con contenidos multimedia, información a veces sensible, creyendo que está resguardada en un sitio seguro; sin embargo, cuando existe un factor disruptivo a toda la cadena de la ciberseguridad y migramos a un escenario de control y amenazas digitales mayores, no solamente contra el usuario o sistemas, sino contra una población en general o un país completo, estamos ante un escenario de ciberguerra, en el cual nadie está a salvo de las amenazas digitales que se potencian a diario.

Nos encontramos en un escenario donde los riesgos son latentes, donde el nuevo campo de guerra se ha convertido en el ciberespacio. México —ante el panorama previamente mencionado— queda en el limbo y propenso a mayores ciberataques: la ciberguerra es inminente. En este sentido, es importante conocer un poco más acerca de los puntos de afectación que podrían poner en shock a México; sin políticas públicas es necesario conocer el panorama técnico para dar una correcta atención legal.

II. CIBERGUERRA: CONTEXTO GENERAL

La industria de la guerra —a lo largo de la historia— ha sido un medio económico para potencializar naciones. El hecho de estar a la vanguardia en la industria armamentista con los avances, en cuanto a tecnología de punta para los conflictos bélicos, es una necesidad para el resguardo de varios países en el mundo. Con la llegada del internet y la revolución de las TIC, la guerra ha tomado un camino distinto, ya no se trata de causar bajas enemigas para dominar el territorio, se trata de tomar el control de los activos digitales del país antagónico para tener un control certero más allá de la parte militar: ejercer un control social, político e incluso mediático.

El control del ahora conocido como "quinto dominio" es un entorno clave para la seguridad nacional y la ciberdefensa de las naciones. La ciberguerra es una realidad inminente de la que sin ser actores directos somos participes día con día,

pues como usuarios de internet no escapamos de los riesgos ante los que nos podemos ver inmersos en este nuevo conflicto.

La llegada de nuevas herramientas digitales ha potencializado los alcances y rangos de impacto de muchas de las ciberamenazas que en años anteriores habían estado bajo control, como el *ransomware*, cuyo incidente mayor dejó un precedente en el mundo físico en aquellos meses de abril y mayo en el 2017. La masificación de WannaCry[1] dejó en claro que los daños producidos de manera digital tienen repercusiones en el mundo material, pues la pérdida de muchas vidas humanas y la carencia de planes reactivos en algunas infraestructuras críticas, como lo fueron hospitales, es una muestra del poderío de una amenaza digital. Claro está que ante un mal manejo de este tipo de códigos fuente, como el del *ransomware*, un atacante potencial, con el conocimiento debido, podría modificar a su antojo e incluso hacerlo más nocivo. El contraste lo vemos hoy en día ante una implementación para frenar a gobiernos antagónicos con ataques dirigidos a sus sistemas de gestión y, particularmente, a las infraestructuras críticas que hacen girar la vida diaria de un país.

El control de un medio de comunicación, como un canal unilateral de consulta de información como lo es para muchas personas internet, simboliza un gran punto de fractura social para el dominio de una población. No hace falta amedrentar con armas de manera física, el valerse de ciberarmas para el control mediático es un punto para considerar en las filas de la ciberguerra y toda la armamentización digital necesaria para llevarlo a cabo.

El mejor ejemplo de este tipo de control lo podemos constatar en la forma en como los grupos terroristas reclutan nuevos adeptos. Para no ir tan lejos tenemos el caso del narco y la forma en como busca tener control y presencia en redes sociales, dejando en claro una imagen de poderío, riquezas y lujos, por los cuales es una buena causa sumarse a las filas del cártel. Cuanto mayor sea la actividad en las redes sociales, mayor será el nivel de capacidad de supervivencia de una organización criminal.

Si las organizaciones criminales en México presentan una alta actividad en las redes sociales, entonces deberían demostrar un mayor nivel de resistencia a los reveses organizacionales. La organización debería tomar menos tiempo para reanudar actividades ilegales, demostrando un nivel más alto de adaptabilidad e impacto mínimo en sus operaciones

[1] Avast, WannaCry, recuperado de https://www.avast.com/es-es/c-wannacry

cuando se elimina el liderazgo (García, 2018).

La ciberguerra toma un giro vertiginoso al dejar en claro el poderío de una organización criminal que puede atentar contra el Estado o, en su caso, operar a instancias del mismo, todo mediante la conectividad y respuesta de los usuarios por medio de las tic; una opinión puede verse tergiversada en un canal de comunicación creando consigo un punto nuevo para los usuarios que logren familiarizarse con esto. El peligro de la desinformación no solamente consiste en sumar personas a las organizaciones criminales del mundo, sino manipular la opinión de las masas.

La llegada de las noticias falsas o *fake news* trae consigo a la ciberguerra un punto más simple de apoyo; las trincheras del periodismo entre países hacen que la verificación de información se convierta en un reto.

Las transformaciones en la producción y distribución de la información que han introducido las nuevas tecnologías, en especial las redes sociales, han provocado una gran eclosión de fuentes informativas y que el flujo comunicativo sea constante, lo cual ha originado que los medios de comunicación dejen de ser la fuente primaria de las noticias y que se pierda parte del valor añadido que el periodista imprime a sus informaciones: la verificación y contextualización de estas (Alonso, 2019).

El Estado puede modificar las tendencias de muchas redes sociales con la ayuda de *bots*, esto es una realidad que hasta el día de hoy no ha tenido algún tipo de atención, salvo la incorporación de algoritmos por parte de las grandes casas que manejan las compañías de redes sociales. La implementación legal rígida para la atención de noticias falsas y afectaciones de usuarios tipo algoritmo es una necesidad, no hace falta esperar la integración de inteligencia artificial para el combate técnico de riesgos mediáticos, se necesita el parámetro legal para una respuesta cuerda a los futuros ciberincidentes que se desarrollarán a través de las plataformas de redes sociales con el fin de manipulación; la ciberguerra libra otro aspecto, como lo dijimos.

Después de tener un contexto superficial de la ciberguerra y el tipo de control social, entremos en detalles de las ciberamenazas que pueden ser usadas para cometer actos que sobrepasan un ciberdelito común, pues el riesgo y las afectaciones son mayores.

Para tener un control certero de toda actividad, particularmente de periodistas y funcionarios gubernamentales, el ciberespionaje privatizado contratado por instancias gubernamentales, usualmente de seguridad y/o procuración de

justicia, ofertan servicios para tener el control de un móvil, usualmente teléfonos inteligentes de uso común con RAT's (Remote Administration Tools), que permiten tener acceso a los contactos, mensajes, llamadas, escuchar en vivo, activar cámaras frontales y traseras, así como estar a la escucha de toda actividad y ruta trazada de la persona.

Casos sonados de empresas como NSO, DarkMatter, BlackCube, en 2019, pusieron en shock a varios funcionarios con casos de ciberespionaje en sus dispositivos. En este sentido, la privacidad pasa a ser un mito cuando en una ciberguerra interna el Estado planea tener control de toda actividad digital de las personas a su servicio.

Para el caso de gobierno a gobierno, el ciberespionaje utiliza técnicas de *phishing* e ingeniería social mejoradas y potencializadas, por las cuales se busca obtener información sensible, planes de guerra, defensa, etc. Aquí no se busca comprometer un solo dispositivo mediante *malware*, sino un conjunto de sistemas o varios usuarios que podrían tener acceso a este tipo de información altamente confidencial. La necesidad de políticas públicas de manera interna para cada una de las agencias de seguridad —y seguridad nacional— requieren una inminente contemplación del *malware* para ciberespionaje, así como el robustecimiento de medidas de control y accesos de los usuarios para reducir el impacto nocivo que un ataque dirigido podría traer.

El ciberespionaje ha tenido una evolución enorme al poder llevar a cabo ataques dirigidos a protocolos DNS, identificados por algunos CERT, el caso es una alerta temprana del INCIBE (2019).

Desde el Centro Nacional de Ciberseguridad e Integración de las Comunicaciones (NCCIC), parte de la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA), se alerta sobre una campaña global de espionaje en la infraestructura de DNS. La información obtenida —gracias a esta campaña— podría permitir a los atacantes redirigir el tráfico hacia una infraestructura controlada por ellos y, de este modo, obtener certificados de las webs de las organizaciones pudiendo realizar ataques de *man-in-the-middle*. El NCCIC recomienda renovar las contraseñas de los registros DNS de las organizaciones, implementar un sistema multifactor de autenticación en las cuentas de dominio de los registradores, realizar auditorías de los registros DNS públicos, así como buscar certificados de cifrado relacionados con los dominios y revocar los certificados solicitados fraudulentamente (INCIBE, 2019).

El peligro puede ser mayor cuando hablamos de una pequeña línea que divide al ciberespionaje con el sabotaje digital. Para el caso, hablaremos de las infraestructuras críticas.

Las infraestructuras críticas son todas aquellas estructuras que, a pesar de un desastre natural o provocado, deben estar en funcionamiento 24/7, pues sus servicios son necesarios para que un país funcione con normalidad. Para el caso de México tenemos contemplación en la Estrategia Nacional de Seguridad (ENCS) de 2017, cuyo eje transversal contempla el establecimiento de políticas y acciones que se llevarán a cabo en el marco de la Ley de Seguridad Nacional, y demás instrumentos aplicables en materia de seguridad nacional y en colaboración con las instancias de seguridad nacional (Gobierno de México, 2017). Sin embargo, al hablar de políticas, pareciera que en cada cambio sexenal queda un proyecto en la ambigüedad, sin continuidad y sin adaptación a las necesidades actuales de una sociedad inmersa en el ciberespacio y la tecnología. Hasta el día de hoy, desafortunadamente, no existen pronunciamientos oficiales de actuación y continuidad de una ENCS, dejando a las infraestructuras críticas mexicanas en un punto abierto para ciberataques.

En la ciberguerra, si un acto interno de sabotaje se lleva a cabo sobre, el funcionamiento (retomando el ejemplo de WannaCry) de una IC que trabaje mediante sistemas digitales interconectados y de ello dependan vidas humanas, el resultado sería catastrófico, las consecuencias serían tangibles, a pesar de que el ataque fue de manera digital.

Dejar fuera de funcionamiento una IC mediante un ataque DDoS es una de las maneras más simples por las cuales la intermitencia de un servicio masivo puede verse afectada en cuestión de segundos. Está de sobra mencionar al *cybercrime as service* que a cargo de países antagonistas se podría producir un DDoS de incluso días. Las vulnerabilidades expuestas ante la parte técnica de atención son necesarias, junto con planes internos preventivos y reactivos ante ciberincidentes provocados.

Las IC necesitan formar parte de políticas públicas pues, al tener un acercamiento en pro de la concientización de los ciudadanos con un acervo mínimo de conocimiento digital, estos mismos harían algo para formar parte del ecosistema de cuidado a tan prioritarias unidades de servicios primordiales. Un caso a ejemplificar de carencias de cultura digital fue en Gatwick, dónde un *drone* ocasionó un problema en

el aeropuerto, poniendo en riesgo la vida de muchos usuarios.

Para prevenir incidentes de algo que podría resultar ser un objeto de esparcimiento y recreación, se hizo un pronunciamiento público por parte de las autoridades de Gatwick; el uso de drones está creciendo a un ritmo rápido en el Reino Unido y nuestros cielos son algunos de los más activos en cualquier parte del mundo. Los drones ahora están prohibidos dentro de los 5 km de Gatwick y todos los aeropuertos de Reino Unido. Es ilegal volarlos dentro de esta zona. Cualquier persona que vuele un avión no tripulado debe mantenerse alejado de aviones, aeropuertos y aeródromos. Hay una zona de restricción de vuelo de 5 km alrededor de Gatwick y es ilegal volar cualquier dron no autorizado dentro de esta área. Los drones no deben volar por encima de los 400 pies (aprox. 120 m) en ningún momento. Es un acto criminal romper la zona de exclusión aérea, y el operador podría poner vidas en peligro e ir a prisión por hasta cinco años (Gatwik, 2018). Lo mostrado es parte de políticas públicas para concientizar a la población y prevenir incidentes en sus IC, apegado a la legalidad de un nuevo peligro se adaptó para ser sancionado. El uso de drones en centrales aéreas, marítimas, de agua y electricidad podría causar pérdidas de vidas humanas; es por ello que, retomando el punto clave de concientización, la población usuaria debe estar al tanto de la importancia de las infraestructuras críticas y los daños que podrían provocar.

Ante un escenario incierto de construcciones mexicanas de nuevos puertos aéreos o mejoras a los existentes, la razón de tener contemplación de riesgos simples, que podrían provocar resultados fatales y complejos, hace que la regulación de drones comience desde las tiendas comerciales, pues los lineamientos existentes de la Secretaría de Comunicaciones y Trasportes (SCT, 2017) no son suficientes. Para el arte de la ciberguerra los drones modificados pueden ser los vehículos para cometer atentados terroristas, con un explosivo cargado y con posibilidad de ser detonado a distancia, se convierten en el medio perfecto para causar la pérdida de vidas humanas en todo sentido bélico. No hace falta voltear a Sudamérica con los hechos de atentados perpetrados con drones, sino pensar en prospectiva de los sitios y plazas públicas de México los cuales requieren atención para una correcta regulación sobre los mismos drones y, en el caso más pertinente, incorporar tecnología de *jamming* con cuerpos preparados para la inutilización del artefacto volador que podría convertirse en arma.

El peor de los escenarios para tener un avance y control sobre un Estado completo recaería en el daño de todas las infraestructuras críticas mediante ciberamenazas; pensemos en una central nuclear, el peligro que representa para las cercanías de una población, si esto es atacado por algún tipo de *malware* troyano para tomar el control, el o los artífices del ataque causarían un estallido, liberación de materiales tóxicos que, en consecuencia, provocarían decesos y heridos. La ciberguerra no necesita tanques o armas de grueso calibre, pues una infraestructura crítica puede jugar el papel de una bomba nuclear controlada a distancia sin exponer al atacante.

Las prospectivas planteadas son una realidad. Ya hay evidencia y ejemplos globales para poder ocuparnos, si bien es cierto que el cibercrimen es el negocio ilícito rentable de la actualidad, la industria de la ciberguerra moverá millones en los próximos años, el desarrollo de *malware* intrusivo, los daños a infraestructuras críticas, las denegaciones de servicios más prolongadas y en volúmenes mayores son un peligro latente, si lo sumamos a un impulso con la inteligencia artificial y redes venideras, como los estándares del 5G, tendremos sin duda ataques nunca antes vistos y de mayor impacto junto con la peligrosidad que representan no solamente para el control de un sistema o país, sino a la vida del usuario mismo.

III. CONCLUSIONES

Las carencias de políticas públicas en materia de ciberseguridad y el silencio a la actualización de una Estrategia Nacional de Ciberseguridad, ya cimentada y con buena participación de todos los niveles que la desarrollaron, es un punto vulnerable que requiere atención para estas nuevas amenazas digitales enunciadas a lo largo de este documento.

Los pronunciamientos por parte de la autoridad pertinente son necesarios para poder colaborar y seguir trabajando cada uno desde su propia trinchera, pues son temas que no pueden ser minorizados o dejados a la deriva, ya que la población usuaria de TIC crece día a día.

A nivel de seguridad nacional se entiende la confidencialidad de las autoridades para mantener información a resguardo; sin embargo, el ciberespacio es un medio propicio para que esta se vea filtrada. Lo ideal en un escenario de concientización de parte de la autoridad correspondiente es sumar esfuerzos con los usuarios de manera generalizada y abierta para su correcta participación como eslabones de esta cadena.

Si comenzamos a mejorar la cadena de ciberseguridad con conocimiento para el usuario y creamos sensibilización en los temas prioritarios, o de mayor importancia para la seguridad nacional, el trabajo se verá reducido al hacer que colaboren en el ecosistema digital, por lo que prepararnos para un escenario de ciberguerra es ya una necesidad en esta sociedad hiperconectada 24/7. Los escenarios digitales están iniciando, ¿nos preocupamos o nos ocupamos?

IV. FUENTES DE CONSULTA

Alonso González, M. (2019). "Fake News: desinformación en la era de la sociedad de la información". *Ámbitos. Revista Internacional de Comunicación*. (45). Disponible en https://revistascientificas.us.es/index.php/Ambitos/article/view/8399/8424

Garcia, N. M. (2018). *The Dark Side of Social Media: The Case of the Mexican Drug War.* Miami: Universidad de Miami.

Gatwick (2018). "Drone Safety". Disponible en https://www.gatwickairport.com/business-community/aircraft-noise-airspace/airspace/drone-safety/

Gobierno de México (2017). *Estrategia Nacional de Ciberseguridad*. Disponible en https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

INCIBE (2019). Campaña de espionaje en la infraestructura DNS. Disponible en https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/campana-espionaje-infraestructura-dns

Lonsdalem D. J. (2004). *The Nature of War in the Information Age*. London: Routledge.

Secretaría de Comunicaciones y Trasportes (SCT) (2017). Circular CO AV-23/10 R4. Disponible en http://www.sct.gob.mx/fileadmin/DireccionesGrales/DGAC-archivo/modulo3/co-av-23-10-r4.pdf

Schreier, F. (2015). *On Cyberwarfare*. Geneva Centre for the Democratic Control of Armed Forces.

ISSN 0187-0416