LAS NUEVAS FORMAS DE MERCENARISMO EN LA ERA DE LA CIBERGUERRA

Análisis sobre la expansión de los servicios de ciberseguridad y ciberinteligencia y su impacto en los derechos humanos y la gobernanza global.

Autores: Carlos Díaz Bodoque y Felipe Daza Sierra

Fecha: 12/02/2020

LAS NUEVAS FORMAS DE MERCENARISMO EN LA ERA DE LA CIBERGUERRA

Análisis sobre la expansión de los servicios de ciberseguridad y ciberinteligencia y su impacto en los derechos humanos y la gobernanza global.

Autores: Carlos Díaz Bodoque y Felipe Daza Sierra

El presente documento es una contribución del Observatorio Shock Monitor y el Observatorio Derechos Humanos y Empresas en el Mediterráneo (ODHE) al "Informe sobre provisión de productos y servicios militares y de seguridad en el ciberespacio por los 'mercenarios cibernéticos'" que producirá el Grupo de Trabajo de Naciones Unidas sobre el uso de mercenarios (GT) para la Asamblea General de la ONU que se celebrará en octubre de 2021.

Para la elaboración de esta contribución, Shock Monitor y ODHE han realizado una revisión de literatura, analizado bases de datos propias y casos de vulneraciones de derechos humanos identificados a nivel internacional en general, y Oriente Próximo y Norte de África en particular**.** A partir de estos datos se han identificado aspectos claves y tendencias para facilitar la labor del GT.

En este marco, el objetivo específico de este informe es exponer la expansión de la industria de las Empresas Militares y de Seguridad Privada (EMSP) en el ámbito de la ciberseguridad y la ciberinteligencia, identificando actores, funciones, servicios y motivaciones. En este proceso se identificarán otros actores no estatales, retos y aspectos controvertidos de la privatización de este sector. Asimismo, se prestará una especial atención a los impactos en los derechos humanos sobre la sociedad civil y las amenazas sobre las infraestructuras críticas, necesarias para el funcionamiento de los servicios esenciales de nuestras sociedades.

De la inteligencia tradicional al cibermercenarismo

Las formas del poder estatal se han transformado en consonancia con la era digital y los conflictos contemporáneos. Desde el 9/11, Estados Unidos de América ha priorizado tareas de inteligencia en el marco de la lucha contra el terrorismo internacional. Un proceso que ha ido acompañado de un aumento de la externalización de estos servicios a EMSP. Tim Shorrock, autor de Spies for Hire: The Secret World of Intelligence Outsourcing, afirma que en 2007 el 70% del presupuesto de inteligencia de EEUU se externalizó a contratistas de seguridad[1]. Un año más tarde, una investigación de The Washington Post averiguó que 1931 corporaciones privadas estaban colaborando en los ámbitos de seguridad nacional, anti-terrorismo e inteligencia desde 10.000 localizaciones del país norteamericano.

La contratación de tecnologías de (ciber) vigilancia y hardware de vanguardia por parte de las agencias gubernamentales de inteligencia no es un fenómeno nuevo. Lo que es inusual es la contratación de know-how y personal especializado para tareas de formación y aplicación real de funciones de inteligencia y seguridad nacional.

Una tendencia observada en la industria de las EMSP, es la adaptación de sus servicios de inteligencia y *risk assessment* al mundo cibernético, convirtiéndose de facto en lo que algunos autores han definido como nuevas formas de cibermercenarismo[2] con servicios en el ámbito de la ciberseguridad y ciberespionaje.

[1] Shorrock, T. (2007) "The corporate takeover of U.S. Intelligence". *Salon.* Online: www.salon.com/2007/06/01/intel_contractors/
[2] Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.

En 2017 el observatorio Shock Monitor publicó, conjuntamente con el grupo de investigación Centre Delàs, el informe "La Transformación del Complejo Militar-Industrial" donde se analizaron 22 empresas del sector armamentístico y EMSP[3]. Algunas conclusiones apuntaban que:

- Más del 90% de las empresas analizadas han creado o ampliado líneas de negocio de seguridad y de inteligencia en su vertiente tecnológica. Estas nuevas áreas de negocio ofrecen servicios y productos de tecnología avanzada: radares, sensores, cámaras (visión nocturna, de infrarrojos, ópticas), satélites, drones para funciones de vigilancia y reconocimiento, dispositivos de identificación biométrica, de rastreo y monitoreo, inteligencia, gestión (recogida, almacenamiento y análisis) de Big data, ciberseguridad, mando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento (C4ISR).
- El ámbito de la ciberseguridad, relacionado con la gestión de los sistemas Big Data, es uno de los campos de mayor crecimiento en el sector militar de seguridad y presenta perspectivas optimistas de expansión.
- La industria armamentística está ampliando su volumen y ámbito de actuación pasando a tener departamentos de Ciberseguridad y ciberespionaje, lo que puede representar una "intrusión" de las funciones más actuales que ofrecen las EMSP.

Algunas empresas armamentísticas realizan, por tanto, servicios que podrían estar categorizados en el ámbito de las EMSP. La norteamericana BAE Systems dispone de un departamento específico de *Applied Intelligence* donde a través de soluciones de ciberseguridad neutralizan "amenazas". Según un apartado de su web corporativa, los ciber activistas son catalogados como sospechosos y se convierten en una de las mayores ciberamenazas[4].

Otra empresa armamentística como Raytheon, obtuvo en 2015 uno de los mayores contratos de ciberseguridad que se hayan firmado jamás. El Departamento estadounidense de Homeland Security le otorgó un contrato por valor de 1.000 millones de dólares para defender a numerosas instituciones gubernamentales de ataques cibernéticos[5]. Según Forbes, la compañía estadounidense se ha convertido en uno de los principales proveedores de ciberseguridad del Pentágono, tanto para acciones ofensivas como defensivas[6].

Al mismo tiempo, las EMSP han desarrollado sus propios departamentos de ciberseguridad. Booz Allen Hamilton, una de los principales contratistas de inteligencia norteamericana, ofrece servicios de ciberseguridad con soluciones tecnológicas para realizar ataques en el dominio cibernético. Desde 2016, la EMSP rusa RSB Group se ha especializado en inteligencia y ciberseguridad, y ese mismo año la británica G4S creaba un Cyber Consulting and Security Operation Centre. Según el observatorio de multinacionales SOMO, la empresa británica no desarrolla la mayor parte de tecnologías de control y vigilancia sino que adquiere proveedores y expertos como Software House (subsidiaria de Tyco Security Products), Honeywell, Axis Communications o Hikvision[7]. Algunos ejemplos concretos serian el contrato de G4S y Avigilon, subsidiaria de Motorola Inc, en 2016 para proveer de soluciones de ciberseguridad de última generación que serían usadas en el estadio de los Miami Dolphin de la Liga

[3] Las empresas analizadas fueron: Airbus, BAE Systems, Boeing, CACI, Constellis, DynCorp, Finmeccanica, Fluor, G4S, General Dynamics, Harris Corporation, Huntington Ingalls, Indra, KBR, L3 Communications, Lockheed Martin, Northrop Grumman, Safran, Serco, Raytheon, Thales y United Technologies.
[4] BAE Systems. Página Web Corporativa. Online: www.baesystems.com/en/cybersecurity/feature/the-activist
[5] Davenport, C. (2015) Raytheon wins 1 billion cybersecurity contract. *The Washington Post.* Online: www.washingtonpost.com/news/the-switch/wp/2015/09/29/raytheon-wins-1-billion-cybersecurity-contract-to-battle-attacks-on-u-s-agencies/
[6]Thompson, L. (2020) Raytheon is posturing to be the Pentagon's Top Cybersecurity supplier. *Forbes.* Online: www.forbes.com/sites/lorenthompson/2020/05/08/raytheon-technologies-is-posturing-to-be-the-pentagons-top-cyber-supplier-both-offensive-and-defensive/
[7] Olivier De Leth, D., Cowan, Riezebrink, V., Hietland, M. (2020). G4S Company Scan. Amsterdam. SOMO. Disponible en: https://www.somo.nl/g4s-company-scan/

Nacional de Fútbol Americano o más recientemente, en 2019, cuando G4S firmó un acuerdo de colaboración con Anyvision para proveer de Inteligencia Artifical a sus clientes de Estados Unidos[8]

Otras empresas como la francesa Amarante International, la danesa Risk Intelligence, especializada en seguridad marítima, o la británica Control Risks han desarrollado sofisticadas herramientas de Big Data para elaborar informes de seguridad internacional identificando amenazas específicas para sus clientes.

Los servicios de ciberespionaje de las EMSP han implicado también la contratación masiva de hackers o *hacking teams* convirtiendo a estas corporaciones en auténticas "Private Cybersecurity Firms[9] o en "hack back companies"[10].

El Observatorio Shock Monitor registra en su base de datos 216 EMSP, de un total de 770, que disponen de servicios de inteligencia para gobiernos, empresas transnacionales y particulares. Esos servicios han ido evolucionando con el uso de las nuevas tecnologías para dar respuesta a las necesidades de sus clientes, incluyendo las amenazas del ciberespacio. Los contratistas de seguridad privada realizan análisis de riesgos, incluyendo evaluaciones de ciberresiliencia de infraestructuras tecnológicas y físicas; provén y mantiene sistemas tecnológicos software y hardware; recogen datos vinculados con la seguridad nacional a través de la intercepción de llamadas, hackeo de móviles, etc; analizan y sistematizan datos vinculados con la seguridad nacional; producen informes de evaluación de riesgos para altos mandos militares; manejan drones para actividades reconocimiento en contexto de protestas o en conflictos armados más allá de sus fronteras; realizan operaciones encubiertas que requieren actividades ilegales como infiltración en movimientos sociales o interrogatorios de sospechosos, entre otros.

El incremento de la demanda gubernamental de estos servicios ha ido acompañada de la contratación de servicios cada vez más sensibles y asertivos, utilizando las EMSP o *hacking teams* como actores proxies para evitar el escrutinio público e influir en los asuntos domésticos de otros Estados. La Agencia Militar de Inteligencia (GRU) rusa utilizó los servicios de la Internet Research Agency, también conocida como Troll Factory, del oligarca Yevgeny V. Prigozhin para interferir en las elecciones presidenciales estadounidenses de 2016 a través del hackeo de datos del Partido Demócrata y la desinformación en las redes sociales para favorecer la campaña presidencial de Donald Trump.

Las actividades de hackeo de información realizadas por la Troll Factory no son un caso aislado. A menor escala, numerosas EMSP ofrecen servicios de carácter ofensivo como Active cyberdefense (ACD)- o *hacking back* para recuperar información robada, interrumpir o dañar redes de potenciales infraestructuras enemiga. Asimismo, este personal realiza funciones de forma remota, como tareas de reconocimiento con el manejo de drones a miles de km de distancia, acciones ofensivas en internet o el apoyo a gobiernos autoritarios en acciones represivas contra su población. Es decir, los contratistas de seguridad pueden estar en la primera línea de los conflictos contemporáneos sin dejar el salón de su casa. Ambas situaciones suponen un reto para la regulación de las actividades de ciberseguridad de las EMSP en términos de jurisdicción aplicable y participación en guerra cibernética[11].

[8]Cuenta de Facebook de Anyvision. www.facebook.com/AnyvisionBT/photos/excited-to-announce-our-partnership-with-g4s-looking-forward-to-working-together/403406813793629/

[9] McMurdo, J. "Cybersecurity Firms – Cyber mercenaries?". McMurdo, Jesse, Cybersecurity Firms — Cyber Mercenaries? (December 12, 2014). Disponible en SSRN: https://ssrn.com/abstract=2556412 or http://dx.doi.org/10.2139/ssrn.2556412
Online at: papers.ssrn.com/sol3/papers.cfm?abstract_id=2556412

[10]McFate, S. (2018). "Mercenaries and War: Understanding Private Armies Today". Online: ndupress.ndu.edu/Media/News/Article/2031922/mercenaries-and-war-understanding-private-armies-today/

[11] Hoffman, W y Nyikos, S. (2018) "Governing Private Sector Self-Help in Cyberspace: Analogies from the physical world". *Carnegie Endowment*. Online:carnegieendowment.org/2018/12/06/governing-private-sector-self-help-in-cyberspace-analogies-from-physical-world-pub-77832

Actores, funciones y motivaciones de los hackers en las operaciones de ciberseguridad y ciberespionaje

Similar a la fragmentación de actores que encontramos en los conflictos contemporáneos, en el mundo cibernético se observa múltiples actores estatales y no estatales. Por una parte, identificamos empresas armamentísticas y EMSP que ofrecen servicios de ciberespionaje y ciberinteligencia desarrollados por personal propio a través de departamentos de ciberseguridad. Asimismo, se producen la contratación de proveedores de hackers y/o *hacking teams* para el desarrollo de operaciones específicas. Por otra parte, hay otras empresas tecnológicas que se dedican exclusivamente a desarrollar la herramienta (software) para luego venderla directamente a las administraciones públicas, empresas o EMSP. En algunos casos identificamos *hacking teams* que ofrecen ambos servicios; desarrollo y ejecución de servicios de inteligencia y ciberespionaje[12].

Una buena forma para comprender los diferentes roles en el ámbito de la ciberseguridad es analizar un ciberataque a través de ransomwares o malwares[13] para acciones de ciberespionaje y cibercrimen. En ese ecosistema operan diferentes actores o grupos de especialistas independientes, que normalmente no tiene vínculos entre sí más allá de las relaciones comerciales específicas. Incluso durante el desarrollo de una campaña de ciberataques, los actores involucrados suelen cambiar para modificar la estrategia y/o utilizar otras familias de botnets y/o ransomware. Por esta razón, la identificación y por tanto, la rendición de cuentas de los actores responsables de un ciberataques se complica. Es poco probable que el responsable de la brecha inicial fuera el que accedió a la información de la víctima, que a su vez no es el que escribió el código real del ransomware[14].

El siguiente cuadro mapea los diferentes grupos de especialistas que participan en un ecosistema de desarrollo y ejecución de un ransomware:

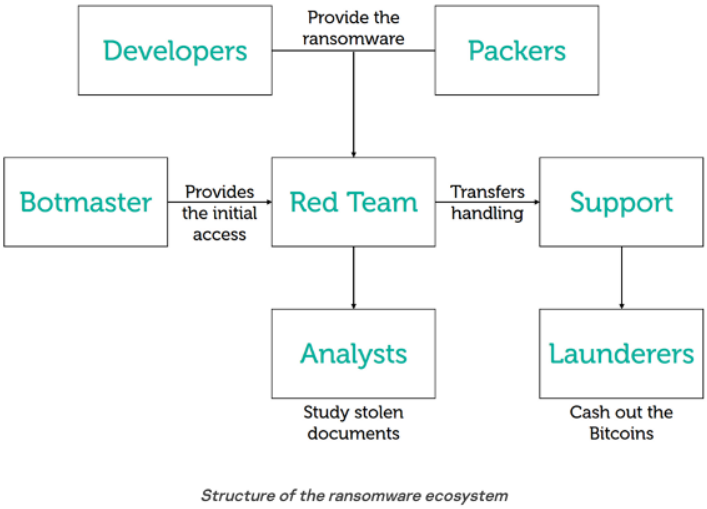

Imagen: ecosistema ransomware. Fuente: Securelist

Las motivaciones de los hackers pueden ser varias aunque probablemente la más importante es el lucro económico a través de contractos oficinales con agencias gubernamentales, EMSP u otros grupos

[12]Von Finckensiten, V. (2019). *Cybersecurity in the Middle East and North Africa*. *Konrad Adenauer Stiftung*. Online: www.kas.de/documents/284382/284431/Policy+Paper+on+Cybersecurity+in+the+Middle+East+and+North+Africa.pdf/50199440-b10e-3dea-52ca-c0e3714ebc75?version=1.0&t=1564581818218

[13] Malware: abreviatura de *software malicioso,* es un término general para virus, gusanos, troyanos y otros programas informáticos dañinos que los hackers utilizan para causar destrucción y obtener acceso a información sensible
Ransomware: es una forma de *malware* que encripta los archivos del usuario víctima.
Spyware: Es un tipo de malware que se instala en un dispositivo informático sin el conocimiento del usuario final. Invade el dispositivo, roba información sensible y datos de uso de Internet, y lo transmite a anunciantes, empresas de datos o usuarios externos

[14] Del Cher, P., Aime, F. y Kwiatkowski, I. (2020) "Lazarus on the hunt for the big game". *Securelist.* Online: securelist.com/lazarus-on-the-hunt-for-big-game/97757/

informales. La Walden University de Columbia (EEUU) además identifican las siguientes motivaciones[15]:

- Robo: de tarjetas de crédito o suplantación de identidades para acceder a cuentas bancarias como las actividades del Infinity Black Hacker.
- Espionaje: de actores o infraestructuras específicas para obtener información privilegiada. Estas actividades pueden desarrollarse con contratos con gobiernos u actores no estatales.
- Spamming: con el objetivo de vender productos de terceros, los spammers intentan controlar los navegadores web e inyectan anuncios no deseados al mismo tiempo que también pueden robar contraseñas para acceder a emails y redes sociales.
- Control: de sistemas de información y redes con fines de espionaje o sabotaje.
- Disrupción: en los sistemas, páginas web o cuentas de redes sociales de empresas o gobiernos para alterar su funcionamiento como acto de protesta, así como identificar y publicar información que exponga casos de corrupción.
- Testeos de vulnerabilidad: hackers son contratados por gobiernos y empresas para que ataquen sus sistemas a modo de test de vulnerabilidad con el objetivo de identificar los puntos débiles y desarrollar sistemas más efectivos de protección.
- Disfrute: algunos hackers se están motivados en hackear sistemas para divertirse y poner a prueba sus capacidades.

Retos de la privatización de la (ciber) inteligencia

El sector de la inteligencia fue diseñado para evitar el escrutinio público favoreciendo acciones fuera del marco legal y la impunidad de los actores implicados. La externalización de servicios de inteligencia a EMSP refuerza esta lógica reduciendo los mecanismos de supervisión y rendición de cuentas. Armin Krishnan define: "intelligence outsourcing is often to enhance the secrecy of intelligence operations and to deliberately undermine democratic accountability and oversight"[16].

La investigación periodística de *The Intercept* reveló las fraudulentas actividades de inteligencia de la EMSP Tiger Swan para recabar datos a través de su infiltración en el movimiento indígena y ecologista Standing Rock contra el proyecto extractivista de la empresa Energy Transfer en North Dakota (EEUU). Los informes producidos por Tiger Swan fueron utilizados por las agentes de la policía local, el FBI y los Fusion Center del Departament de Homeland Security[17] creados después del 9/11 para la lucha contra el terrorismo internacional. La complementariedad entre las agencias gubernamentales y la seguridad privada es un fenómeno extendido en muchos Estados, sin embargo la cooperación en el ámbito de la inteligencia implica el acceso de los contratistas de seguridad privada a información sensible vinculada con la seguridad nacional y a bases de datos de agencias de orden públicos con información personal de la ciudadanía.

Además, la participación de EMSP y contratistas de seguridad privada en los procesos de análisis de datos les coloca en una posición privilegiada para influir en la percepción de las amenazas a las que se enfrentan sus clientes gubernamentales, determinando la formulación de políticas públicas o planes de seguridad[18]. Uno de los casos que mejor ejemplifica esta capacidad, fue el informe de la empresa norteamerica SAIC sobre las armas de destrucción masiva en Iraq. Su informe confirmaba la presencia de este tipo de armamento y detallaba que los iraquíes estaban "listos para la guerra".

[15] Walden University. "What motivates hackers?". Online: www.waldenu.edu/online-doctoral-programs/doctor-of-information-technology/resource/what-motivates-hackers

[16] Krishnan, A. (2011). "The Future of U.S. Intelligence Outsourcing". *The Brown Journal of World Affairs, 18*(1), 195-211. Retrieved January 19, 2021, from http://www.jstor.org/stable/24590792

[17] Los Fusion Centers están diseñados para promover el intercambio de información a nivel federal entre agencias como la Oficina Federal de Investigación, el Departamento de Seguridad Nacional de Estados Unidos, el Departamento de Justicia de Estados Unidos y las autoridades estatales y locales.

[18] Pingeot, L. (2012). *A Dangerous Partnership: Private Military and Security Companies and the UN*. Rosa Luxemburg Foundation. Online: www.rosalux.de/fileadmin/rls_uploads/pdfs/sonst_publikationen/studie_dangerous_partnership.pdf

En este sentido, los fines de lucro económico, y el enfoque militar y técnico de seguridad de las EMSP moldean los resultados de sus investigaciones y sus propuestas para neutralizar las amenazas identificadas. Este enfoque acaba influyendo en la percepción de inseguridad de sus clientes, ignorando las dinámicas sociales y políticas de los contextos de análisis, las respuestas no-militares, diplomáticas o mediación[19].
Una de las causas que explicaría esta priorización, es el tradicional partenariado público-privado en el ámbito de la seguridad. Simbiosis que se ha cristalizado en escándalos de conflictos de intereses y puerta giratorias de altos mandos de agencias gubernamentales de inteligencia y EMSP, así como un alineamiento político e ideológico determinando una visión del mundo e interpretación de la seguridad internacional a favor de los intereses geoestratégicos de los gobiernos occidentales.

Por último, la privatización de la inteligencia ha supuesto que los expertos de agencias de inteligencia gubernamentales trabajen para el mejor postor; ya sea empresas, otros gobiernos u élites económicas. En 2019, un exagente de la National Security Agency destapó el proyecto Raven, una unidad de inteligencia desarrollada por los Emiratos Árabes Unidos formada por cibermercenarios incluyendo ex miembros de unidades de inteligencia norteamericana. Los analistas de Raven además contaban con un sistema muy sofisticado, de origen desconocido, para hackear móviles iPhone, conocido como Karma. El proyecto Raven se dedicó durante años al monitoreo de disidentes y voces críticas con el gobierno de Abu Dhabi como el periodista británico Rori Donaghy, el activista emirato Ahmed Mansoor o Tawakkol Karman, líder yemení de las protestas de la "Primavera Árabe"[20].

Impacto del ciberespionaje sobre los actores de la sociedad civil: casos de estudios en el mundo árabe.

El artículo académico "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society" publicado en el Journal of Information Technology and Politics, analiza 700 informes de ciberseguridad de corporaciones privadas entre 2009 y 2019, concluyendo que la gran mayoría de los análisis ignoraban las amenazas a la sociedad civil creando una imagen distorsionada de la situación y los objetivos de los ciberataques e influyendo en gobiernos y instituciones académicas[21].

Los movimientos sociales, sindicalistas, activistas, periodistas y líderes indígenas han sido un objetivo tradicional de los gobiernos, empresas transnacionales y agencias privadas de inteligencia. Son numerosos los casos de empresas transnacionales que han contratado los servicios de EMSP para espiar activistas; Kroll fue contratada por Texaco Chevron en Ecuador, Academi se convirtió en el departamento de inteligencia de Monsanto o Stratfor trabajó para Coca-Cola[22]. Los servicios de inteligencia de las EMSP han sido fundamentales para identificar líderes sociales y armar campañas de desprestigio contra los mismos, unas prácticas trágicamente extendidas en América Latina por orden de empresas petroleras y mineras, y en complicidad con las autoridades locales.

Con la evolución de los servicios de ciberseguridad y la emergencia de especialistas en hackeo, las vulneración de los derechos civiles y políticos se está agudizando. Un reciente ejemplo de la complejidad de actores que participan en los ciberataques contra activistas lo ejemplifica el caso de Dark Basin, un *hacking team* vinculado con la empresa india BellTroX InfoTech Services de acuerdo a una investigación de Citizen Lab. Dark Basin realizó tareas de ciberespionaje contra activistas,

[19] Daza, F. (2017) . "Delimitation and Presence of PMSCs: Impact on Human Rights". In: Torroja H. (eds) *Public International Law and Human Rights Violations by Private Military and Security Companies*. Springer, Cham. https://doi.org/10.1007/978-3-319-66098-1_3
[20] Schectman, J y Bing, C. (2019). "UAE used cyber super weapon to spy on iPhones of Foes". *Reuters investigates.* www.reuters.com/investigates/special-report/usa-spying-karma/
[21] Lennart Maschmeyer, Ronald J. Deibert & Jon R. Lindsay (2020): "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society, Journal of Information Technology & Politics", DOI: 10.1080/19331681.2020.1776658
[22] Ahmed, N. (2013). "The war on democracy. How corporations and spy agencies use 'security' to defend profiteering and crush activism". *The Guardian*. Online: www.theguardian.com/environment/earth-insight/2013/nov/28/war-on-democracy-corporations-spy-profit-activism

periodistas y otras organizaciones vinculadas con una campaña contra la petrolera Exxon[23]. Observamos, por tanto, como la empresa norteamericana Exxon contrata los servicios de la india BellTroX InfoTech que a su vez crea o contrata un *hacking team* para las operaciones de ciberespionaje.

En 2019, través de una demanda federal impuesta por Microsoft contra el *hacking team* Charming Kitten (también conocido como APT35, Phosphorous and Ajax Security Team), se descubrió que una amplia campaña de *phishing* para robar credenciales de periodistas, activistas y profesores del Golfo Pérsico, Oriente Próximo, Europa había estado en funcionamiento desde 2013. La última campaña de ciberataques de Charming Kitten fue lanzada durante las navidades de 2020 con un sistema sofisticado que combinaba emails y mensajes SMS[24]. Empresas de ciberseguridad como Serfa, Claire Sky and Atlanta afirman que detrás de estos ataques se encuentra Irán, que parece haber contratado los servicios de Charming Kitten para espiar a voces disidentes a su gobierno[25].

Desde 2013, el *hacking team* Syrian Electronic Army (SEA), vinculado con el régimen sirio de Al-Assad, ha hackeado cuentas de correo y redes sociales de voces disidentes y de figuras de la oposición siria, tales como: Salim Idris, exjefe del Estado Mayor del Consejo Militar Supremo del Free Syrian Army; Louay Sakka y Mazen Asbahi directivos del Syrian Support Group, un grupo de incidencia norteamericano que daba apoyo a las fuerzas rebeldes en Siria; Oubab Khalil, responsable del Syrian Opposition Coalition's en Washington, DC; y Oubai Shahbandar, exanalista del Pentagono y asesor de la Syrian Opposition Coalition; así como Microsoft, the Associated Press, CNN, etc[26].

El activismo también ha sufrido el ciberespionaje a través del software ofrecido por *hacking teams* a gobiernos como es el caso de la empresa italiana Hacking Team, que desarrolló spyware para los gobiernos de Líbano, Túnez, Marruecos, Egipto, Oman, Bahrain, Iraq, Arabia Saudí, Sudan y los Emiratos Árabes para ser utilizados sobre las voces disidentes[27]. Otro caso ampliamente estudiado por Citizen Lab y otros expertos fue el spyware Pegasus de la empresa israelí NSO group utilizada por el gobierno español para espiar a los representantes políticos pro-independentista, así como activistas de Marruecos, Egipto, Ruanda y México, entre otros[28].

A pesar de que estas empresas se centraban en el desarrollo de software de vigilancia y ciberespionaje, probablemente también ofrecían servicios de hackeo y espionaje directo con sus profesionales. La empresa de ciberseguridad estadounidense Fireye afirma que algunos *hacking teams* combinan funciones de desarrollo de software y servicios de hackeo[29].

En resumen, en la región árabe observamos como los gobiernos están desarrollando auténticos ciberejércitos para atacar objetivos estratégico en el exterior, defenderse de amenazas internas y neutralizar a voces disidentes en el interior de sus territorios. Con la justificación de la lucha contra el cibercrimen y el terrorismo, gobiernos del Norte de África y Oriente Próximo están imponiendo estrictas leyes nacionales para los espacios digitales, afectando de forma directa los derechos civiles y políticos en general, y la libertad de expresión en particular, sin reducir los cibercrimenes.

---

[23] Holden E. (2020). **"**Hack-for-hire group targeted climate activists behind #ExxonKnew campaign". *The Guardian.* Online: www.theguardian.com/technology/2020/jun/11/exxon-hack-for-hire-climate-activists-campaign

[24] Cimpanu, C. (2021). "Iranian cyberspies behind major Christmas SMS spear-phshing campaign". *ZDnet.* Online: www.zdnet.com/article/iranian-cyberspies-behind-major-christmas-sms-spear-phishing-campaign/

[25] Asokan, A. (2020). "Fraudsters Pose as Journalist in Phishing Campaign: Report". *Data Breach Today.* Online: www.databreachtoday.com/fraudsters-pose-as-journalist-in-phishing-campaign-report-a-13694

[26] Franceschi-Bicchierai,L. (2015). "The Syrian electronic army's most dangerous hack". *VICE by Motherboard.* Online: www.vice.com/en/article/nze5nk/the-syrian-electronic-armys-most-dangerous-hack

[27] Business and Human Rights Resource Centre. (2015). "Leaks confirm the use of Hacking Team to spy on activist in the Middle East and North Africa". Online: www.business-humanrights.org/en/latest-news/leaks-confirm-the-use-of-hacking-team-tools-to-spy-on-activists-in-the-middle-east-north-africa/

[28] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Citizen Lab Research Report No. 113, University of Toronto, September 2018. Online: citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[29] Para más información ver: www.vicetv.com/en_us/video/hacking-the-infrastructure/5786ba04272f9b1b43240f43

En Túnez, Jordania, Cisjordania y la Franja de Gaza, y Turquía, las autoridades públicas están aplicando estrategias represivas para contrarrestar el ciberterrorismo, la desinformación y el discurso del odio, aumentando la presión sobre los medios de comunicación, reprimiendo a los periodistas o aprobando nuevas leyes que criminalizan y persiguen el activismo en línea, promoviendo la censura y vulnerando el derecho a la libertad de expresión. Esto crea un "efecto pánico" entre los jóvenes; dos tercios de los jóvenes palestinos tienen miedo de expresar su opinión política en línea y las mujeres se enfrentan a altos niveles de ciberacoso y violencia de género en las redes sociales[30]. La reducción del espacio está limitando el espacio off- y online para el activismo político. En 2021, 1200 jóvenes activistas de entre 15 y 25 años fueron encarcelados durante los acontecimientos en torno al último aniversario de las Primaveras Árabes. En 2019, en Irak, los jóvenes activistas que protestaban contra la corrupción, el desempleo y los malos servicios públicos, se enfrentaron a la violencia y a la persecución. Además, el gobierno iraquí ha impuesto el cierre de Internet, alegando que el objetivo es acabar con la incitación al odio.

Ciberataques contra infraestructuras críticas: la era de la ciberguerra

Las infraestructuras críticas son claves para el desarrollo de servicios esenciales en las sociedades. Uno de los primeros ataques de ciberataques más importante, se produjo en 2015 contra el sistema eléctrico de Ucrania, afectando a un cuarto de millón de personas en pleno invierno y durante 6h. Dos años más tarde, el virus Petya atacó a la multinacional de mercancías Maersk provocando un disrupción masiva en la cadena de suministro global con un coste de 300 millones de dólares y el bloque del sistema automatizado del puerto de Rotterdam durante una semana[31]. Los puertos norteamericanos de San Diego, Long Beach y el Puerto de Barcelona también sufrieron los ataques de los WannaCry y Petya durante el mismo período.

El incremento de los ciberataques contra infraestructuras críticas ha ido aumentando de forma exponencial en los últimos años. Por ejemplo, en España en 2013 se detectaron tan solo 17 ataques contra infraestructura críticas; mientras que 2019 esa cifra aumentó a 8086[32]. En el actual contexto de la pandemia, este fenómeno se ha intensificado aun más. Los Emiratos Árabes Unidos han sufrido un aumento de 250% ciberataques en el 2020 afectando infraestructuras públicas y sistemas IT del gobierno, principalmente a través de armas ransomware[33].

Los ataques contra las infraestructuras críticas se están desarrollando con una nueva generación de malwares que atacan los sistemas de control y automatización industrial. Expertos en ciberseguridad como la empresa rusa Kaspersky afirman que detrás de los malware Kahuna Mata, spyware Dtrack o el ransomware Wannacry se encuentra el grupo norcoerano Lazarus Group[34]. Según Kaspersky, Lazarus Group fue también responsable de los ataques contra 3000 servidores de agencias militares de Corea del Sur en 2016, el National Health System británico, una cadena de supermercados surcoreana, la empresa Sony Pictures y el Banco de Bangladesh, así como los ciberataques contra la planta nuclear Kudankulam en India, plantas de petróleo en Oriente Próximo, etc. Sin embargo, Lazarus group ha priorizado especialmente los ataques contra el sistema financiero internacional con ciberataques contra el Bangladesh Bank robando más de 81 millones de dólares o la red internacional de ATMs en 2017.

[30] Para más información: www.unwomen.org/en/news/in-focus/in-focus-gender-equality-in-covid-19-response?gclid=CjwKCAiA65iBBhB-EiwAW253W4jzm5Fe0b1Q1YXFU-oofSontA8sxwlwJmUtfNrGm2gmsMqF4AsLxxoCkZUQAvD_BwE

[31] Gronholt-Pedersen, J. (2017). "Maersk says Global IT breakdown caused by cyber attack". *Reuters*. Online: https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO

[32] Departamento de Seguridad Nacional (2020). *Informe Anual de Seguridad Nacional 2019*. Ministerio Presidencia del Gobierno de España. (pp.127-135) Online: https://www.dsn.gob.es/sites/dsn/files/MASTER%20IASN2019%20WEB_0.pdf

[33] Murphy, D. (2020). "Middle East facing 'cyber pandemic' as Covid exposes security vulnerabilities, cyber chief says". *CNBC*. Online: www.cnbc.com/2020/12/06/middle-east-facing-cyber-pandemic-amid-covid-19-uae-official-says.html

[34] Del Cher, P., Aime, F. y Kwiatkowski, I. (2020) "Lazarus on the hunt for the big game". *Securelist*. Online: securelist.com/lazarus-on-the-hunt-for-big-game/97757/

Según fuentes oficiales, el gobierno norcoreano está contratando a *hacking teams* como Lazarus Group, Hidden Cobra o BlueNoroff para cometer ataques contra compañías financieras, plataformas de intercambio de criptomonedas y bancos con el propósito de obtener recursos económicos para realizar sus actividades ilícitas antes las sanciones económicas que sufre el país según afirman fuentes del gobierno estadounidenses y Naciones Unidas[35]. Según la empresa de ciberseguridad Fireye, los hackers norcoreanos están ofreciendo sus servicios y desarrollando softwares para terceras partes interesadas con el beneplácito del gobierno de Corea del Norte[36].

En 2020, Estados Unidos anunció uno de los peores ciberataques contra el país. El Sunburst hack afectó a múltiples agencias federales incluyendo el departamento de Energía y Homeland Security, Defensa y Comercio. La operación fue realizada a través de un software desarrollado por la empresa tecnología Solar Winds de Texas (EEUU) con el objetivo de controlar los sistemas y provocar una disrupción en su funcionamiento, sin embargo, el ataque se limitó al robo de información. La empresa Microsoft también identificó que los ataques habían afectado a sistemas y usuarios en Canadá, México, Bélgica, España, Reino Unido, Israel y los Emiratos Árabes.

El exsecretario de Estado, Mike Pompeo acusó a Rusia de estar detrás de estos ciberataques[37]. No obstante, The Washington Post informó que probablemente el *hacking team* ruso Cozy Bear (también conocido como APT29), con vínculos con las agencias gubernamentales rusas, estaba detrás del ataque[38].

Nos encontramos en un contexto de ciberguerra entre grandes potencias y bloques, donde cada parte interesada prioriza determinados objetivos estratégicos. Rusia utiliza cibermercenarios para atacar infraestructuras críticas, obtener información confidencial de sus oponentes y desastabilizar los sistemas políticos a través de la desinformación y el discurso del odio. Mientras que China, prioriza el robo de propiedad intelectual comercial e información confidencial como el ataque contra la Office of Personnel Management (OPM) de la Administración Estadounidense que comprometió información de al menos 20 millones de trabajadores federales. Irán y Corea del Norte, tienen menor capacidad de impacto, pero sus ciberataques son altamente maliciosos. A modo de ejemplo, el virus de origen iraní Shamoon atacó la empresa petrolera saudí ARAMCO destruyendo cerca de 30.000 ordenadores o el ataque que sufrió la empresa de gas y petróleo italiana Saipem, inutilizando el 10% de su flota de ordenadores[39]. Mientras que los *hacking teams* sponsorizados por Corea del Norte desvelaron miles de datos confidenciales de Sony Picture[40]. Asimismo, en 2015 el periodico pro-saudi al-Hayat fue hackeado por el *hacking team* Yemen Cyber Army. Posteriormente, este grupo estuvo detrás de la publicación en Wikileaks de centenares de documentos del Ministerio de Asuntos Exteriores saudí. La empresa de ciberseguridad Clearsky afirmó que Irán estaba detrás de los ciberataques a través del Yemen Cyber Army[41].

Conclusiones y tendencias futuras

[35] *Ataque contra Cosmos Bank – UN Security council report: "*"The panel notes a trend in the Democratic People's Republic of Korea's evasion of financial sanctions of using cyber attacks to illegally force the transfer of funds from financial institutions and cryptocurrency exchanges" Online:economictimes.indiatimes.com/industry/banking/finance/banking/un-security-council-panel-finds-cosmos-bank-cyber-attack-motivated-by-n-korea/articleshow/68589549.cms

[36] Vencat, A. Y Ferguson, S. (2020). "US offers 5million dollars reward for North Korea Hacker information". *Data Breach Security*. Online: *www.databreachtoday.com/us-offers-5-million-reward-for-n-korea-hacker-information-a-14134*

[37] BBC News (2020). "US Cyber-attack: Russia "clearly" behind SolarWinds operation, says Pompeo". Online:www.bbc.com/news/world-us-canada-55374945

[38] BBC News (2020). "US Cyber-attack: US energy deparment confirms it was hit by Sunburst hack". Online:www.bbc.com/news/world-us-canada-55358332

[39] Cimpanu, C. (2019). "The world's most famous and dangerous APT". ZDnet. Online: www.zdnet.com/pictures/the-worlds-most-famous-and-dangerous-apt-state-developed-malware/4/

[40] Para más información ver: www.heritage.org/cybersecurity/heritage-explains/the-growing-threat-cyberattacks

[41] Frenkel, S. (2015). "Meet the mysterious new hacker army freaking out the Middle East". *Buzzfeed News*. Online: www.buzzfeednews.com/article/sheerafrenkel/who-is-the-yemen-cyber-army

La demanda de servicios de ciberseguridad y ciberinteligencia por parte de las agencias gubernamentales está en expansión desde el inicio de la Guerra contra el Terror. Esto ha convertido el ciberespacio en un campo de batalla caracterizado por una fragmentación de actores estatales y no estatales. Las EMPS y algunas empresas del sector armamentístico ofrecen sofisticados sistemas en este ámbito. Para ello desarrollan departamentos de ciberseguridad o contratan directamente proveedores externos como *hacking teams*.

La multiplicidad de actores también se cristaliza en los diferentes especialistas que acaban participando en los ciberataques. En el desarrollo y el lanzamiento de randomware, malware u otros tipos de virus se desarrollan múltiples roles: desde desarrolladores hasta analistas. Todos ellos son necesarios para el objetivo final, pero podrían no desconocer el objetivo final de la actividad como sucedió con los desarrolladores del *network management software* de SolarWinds en el caso de Sanburst.

Esta situación complejiza el escrutinio público y la rendición de cuentas. A todo ello hay que añadir que se difumina la tradicional categorización entre Estado de origen, contratante y territorial de las actividades de las EMSP especialmente por lo que se refiere al territorio de operaciones y actividades de las EMSP. Los cibermercenarios podrían estar realizando operaciones ofensivas desde sus ordenadores a miles de kilómetros de los servidores atacados.

En el marco de esta ciberguerra global, los gobiernos utilizan nuevas formas de cibermercenarismo, ya sea a través de EMSP o *hacking teams*, como actores proxy para atacar objetivos estratégicos de sus oponentes a nivel internacional. Esos objetivos varían de acuerdo a los intereses estatales pero la mayoría se centran en los sistemas operacionales de infraestructuras críticas incluyendo el sistema financiero internacional. En este sentido, los ciberataques contra el sistema financiero (bancos, ATMs, plataforma de criptomonedas, etc) que han afectado a los Bangladesh Bank, Cosmos Bank de la India, Rank Bank (EAU), BMI (Omán), etc, sirven para financiar actividades ilícitas.

De acuerdo con gobiernos occidentales y empresas de ciberseguridad, detrás de los cada vez más sofisticados ciberataques de *hacking teams* se encuentra los gobiernos de Rusia, China, Irán y Corea del Norte. La nueva administración estadounidense, priorizará la lucha contra la ciberseguridad lo que hacer prever una escalada de tensión en el marco de la ciberguerra[42].

En la práctica, la gran mayoría de las agencias gubernamentales y empresas occidentales a nivel de ciberinteligencia y ciberseguridad ha recurrido a la contratación de EMSP y empresas tecnológicas para frenar ciberataques o atacar objetivos estratégicos (operaciones ACD). En este proceso se identifican varias tendencias: 1) casos de puertas giratorias entre directivos y analistas de agencias de inteligencia gubernamental y EMSP; 2) contratación de analistas de agencias gubernamentales de EEUU por parte de otros gobiernos, en particular EAU; 3) la persecución de activistas que luchan contra los gobiernos.

Las EMSP de ciberinteligencia occidentales también contratan a proveedores para el desarrollo y/o adquisición software como el caso de G4S que ha establecido relaciones comerciales con empresas tecnológicas como Avigilion de la empresa norteamericana Motorola o la israelí Anyvision, ambas implicadas en graves vulneraciones de derechos humanos en el contexto de la ocupación de Palestina, incluyendo actividades económicas en los asentamientos ilegales de Israel en Cisjordania[43]. Destacar, que no parece una práctica habitual que las EMSP desarrollen sus propios softwares para las tareas de inteligencia y ciberespionaje.

[42] BBC News (2020). "US Cyber-attack: US energy deparment confirms it was hit by Sunburst hack". Online:www.bbc.com/news/world-us-canada-55358332

[43] Oficina del Alto Comisionado de las Naciones Unidas por los Derechos Humanos. *Report on business activities related to settlements in the Occupied Palestinian Territory*. Online: www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25542

La ciberguerra es un fenómeno clave para entender las dinámicas políticas en el Oriente Próximo y Norte de África. En esta región se observan principalmente ataques contra infraestructuras que pertenecen al sistema financiero y voces disidentes en el interior de los Estados. Los marcos normativos domésticos en estos países lejos de acabar con el cibercrimen, restringen la libertad de expresión y el espacio de la sociedad civil en el ciberespacio.

En esta región, el Estado de Israel es líder en ciberseguridad[44] y sus empresas mantienen un estrecho vínculo con las Israel Defence Forces (IDF) por lo que están involucradas de forma directa en la ocupación militar de los Territorios Ocupados Palestinos. Las EMSP que contratan servicios de empresas de ciberseguridad israelíes no están aplicando sistema de debida diligencia efectivos para la prevención de vulneraciones de derechos humanos y el Derecho Internacional Humanitario.

Los casos analizados en la región árabe demuestran que la experiencia transformadora que nació durante las Primaveras Árabes en 2011, se está convirtiendo en una experiencia violenta y traumática. Los informes de ciberseguridad gubernamentales y corporativos no hacen referencia a las amenazas cibernéticas de la sociedad civil, más bien al contrario. EMSP y empresas armamentísticas consideran al activismo una potencial amenaza disruptiva para el funcionamiento de los sistemas de información y comunicación. Además, las normas nacionales en el ámbito digital inicialmente planteadas y/o justificadas por motivos de luchas contra el terrorismo y ciberdelincuencia, están limitando los derechos civiles y políticos, promoviendo la autocensura y reduciendo la libertad de acción de la sociedad civil.

Ello refuerza el paradigma público-privada en el sector de seguridad y contribuye a la persistencia de soluciones militares y técnicas de seguridad contra los retos que se enfrentan las sociedades, marginalizando las respuestas noviolentas, civiles y de transformación de las causas estructurales de los conflictos.

******

ACERCA DE

ODHE Observatori de Drets Humans i Empreses a la Mediterrània

El ODHE nace con el objetivo de contribuir a sensibilizar a la ciudadanía catalana, española y europea sobre la violación de los derechos humanos en países de la región mediterránea donde hay conflicto. Uno de los principales objetivos del ODHE es influir en los responsables de la toma de decisiones con el fin de regular el sector empresarial para respetar y cumplir con los Derechos Humanos.

www.odhe.cat/es/el-observatorio/ **@ObservatoriDHE**

[44] Daza, F (2020). *Los Muros Invisibles de la Ocupación. La trazabilidad de los productos de Magal Security Systems en las cadenas de suministros de la (ciber)Seguridad en Israel y Palestina.* Barcelona. ODHE. Disponible en: http://www.odhe.cat/es/los-muros-invisibles-de-la-ocupacion-la-trazabilidad-de-los-productos-de-magal-security-systems-en-las-cadenas-de-suministro-de-la-ciber-seguridad-en-israel-y-palestina/

SHOCK MONITOR

Shock Monitor se crea para documentar y estudiar la evolución de la guerra privada y su impacto mundial en los derechos humanos. A través de la documentación, sistematización y análisis de incidentes que involucran a EMSP y a contratistas privados, estudia no sólo el desarrollo de la industria, sino también los incidentes y casos legales conexos, la rendición de cuentas de los perpetradores y la reparación a las víctimas.

http://shockmonitor.org/ **@ShockMonitor**