LA REVOLUCIÓN DIGITAL Y EL CIBERESPACIO. ESTADOS UNIDOS, UN HEGEMÓN SIN LIDERAZGO.

Enrique Utrilla Quintanar
Universidad Complutense de Madrid
UNISCI
20 febrero 2019

1. Introducción

La revolución digital ha significado un proceso de aceleración hasta el punto de que resulte difícil imaginar cómo se había vivido hasta ese instante sin los adelantos que trae aparejados consigo, ha cambiado por completo el paradigma de convivencia social, político y económico global.

Con el pistoletazo de salida a esta revolución y la aparición de una red masiva dedicada al intercambio de información e investigación como fue *ARPANET*, embrión del posterior Internet, emergió tempranamente el espacio de cultivo para múltiples amenazas cibernéticas latentes. En un comienzo tales amenazas se tornaban experimentales y tan solo buscaban demostrar su capacidad de ataque sin poner en peligro a ningún actor o agente internacional, sin embargo con el paso de las décadas y la irrupción del siglo XXI las amenazas se han sofisticado y abandonado su latencia a la vez que algunas de ellas han mutado en movimientos ciudadanos coordinados en forma de *hacktivismo* y son capaces de aprovechar la ventaja asimétrica que representa el ciberespacio para poner en jaque tanto a grandes corporaciones como a Gobiernos, entre los que ejerce un papel esencial Estados Unidos, en tanto que *hegemón* internacional. En la actualidad, los viejos ataques de denegación de servicio en red o los procesos experimentales de los primeros virus informáticos han dejado paso a amenazas de características oceánicas capaces de comprometer infraestructuras de seguridad de Estados, como sucedió en el pasado en Estonia en 2007 o en Georgia en 2008; servicios administrativos gubernamentales, como ocurrió con el ataque coordinado a la *Office of Personnel Management* estadounidense o de sustraer la información privada de millones de cuentas de usuarios mediante los ataques de *ransomware Cryptolocker y WannaCry* , protagonistas del último lustro y última evolución de la criptovirología moderna.

Tal es la magnitud de las consecuencias que muchas de sus amenazas representan que el ciberespacio ya ha sido catalogado como el quinto dominio de la guerra junto a la tierra, el mar, el aire y el espacio.[1] Se trata de un nuevo "*campo de batalla*" en pleno siglo XXI, totalmente asimétrico, debido fundamentalmente a su eficacia y rentabilidad operativa si se compara con cualquiera de los otros dominios de la guerra. De esta manera, en el ciberespacio se aloja un nuevo espacio de guerra marcado por el ciberataque y el ciberconflicto. Los servicios de inteligencia atacan tanto a enemigos como a aliados y a elementos neutrales con tal de obtener acceso a información privilegiada, que utilizan como moneda de cambio en el ciberespacio. Los militares buscan interrumpir las operaciones del enemigo y por ello atacan sistemas de sensores, logísticos, de comunicaciones y de control en el ciberespacio. Los delincuentes, por su parte, buscarán ingresos ilegales para financiar sus actividades de ataque frente a Gobiernos extranjeros o domésticos.[2]

Una de las características a tener en cuenta en el ciberespacio es que no sólo los actores que intervienen en él sino también el mapa de objetivos y la información clave, cambian en cuestión de

[1] Dossier: "War in the fifth domain", *The Economist*, Volume 396, number 8689, July 3, 2010, p. 22.
[2] Instituto Español de Estudios Estratégicos (*IEEEs*): "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", Ministerio de Defensa, *Cuadernos de Estrategia*, Número 149, (colaboración con el Instituto Universitario General Gutiérrez Mellado), Diciembre, 2010, p. 55, en http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

segundos. Esta finitud extrema del ciberespacio garantiza la dificultad a la hora de prever tanto ataques como tendencias en un entorno tan complejo y cambiante.

Incluso Estados Unidos ha demostrado ser un actor internacional incapaz de controlar los vaivenes producidos en este entorno digital. Una clara y reciente muestra de ello salió a la luz en junio de 2016, cuando el FBI alertó a las autoridades de que el sistema electoral de los Estados de Arizona e Illinois se había visto comprometido por ciberataques rusos. El ataque cibernético perpetrado contra el Partido Demócrata dilapidó por completo sus posibilidades de alcanzar la presidencia, al airear secretos de Estado vinculados a la candidata Hillary Clinton durante las primarias.

A pesar de la respuesta acometida desde el seno de la Administración Obama con el cierre de dos agencias de inteligencia rusas en suelo americano, y la expulsión de varios diplomáticos rusos, se refutan varios hechos. El primero es que el *hegemón* internacional, capaz de liderar la respuesta armada global ante cualquier conflicto, resulta virtualmente inoperante y del todo vulnerable en el entorno del ciberespacio. El segundo, la presidencia de Donald Trump no es sino el comienzo de la demostración de cómo el juego de la política de injerencia en el ciberespacio es capaz de configurar poderes globales en el espacio físico. Y por último, tal éxito ruso en las elecciones presidenciales estadounidenses pone de manifiesto una severa duda acerca de su reiteración en el futuro en posteriores elecciones o participaciones democráticas, pervirtiendo tal espíritu y en aras de continuar la partida virtual de ajedrez, dinamitando poderes políticos o favoreciendo intereses geoestratégicos mediante la explotación del ciberespacio.

2. La revolución digital

El proceso de revolución digital ha de entenderse como una etapa más dentro del contexto iniciado en Gran Bretaña en la segunda mitad del siglo XVIII o lo que es lo mismo, como parte integrante de la revolución industrial.[3] Es precisamente este fenómeno de industrialización el que marca un punto de inflexión en la historia cambiando el paradigma de convivencia. Según Eric J. Hobsbawm, llamar revolución industrial a este proceso resulta algo lógico, aunque durante tiempo existiera una tendencia entre algunos historiadores a negar su existencia y a sustituir el término por el de "evolución acelerada". Del mismo modo, señala que, aunque cabe tener en cuenta que la revolución industrial no fue un episodio con principio y fin, preguntar cuándo se completó es absurdo, pues su esencia era que, en adelante, nuevos cambios revolucionarios constituyeran su norma.[4] De este modo la revolución industrial no es sino un proceso retroalimentador que carece de caducidad y que permanece en constante evolución.

La revolución digital, también llamada tercera revolución industrial, marca el comienzo de la era de la información y constituye el salto definitivo de la tecnología analógica y mecánica a la digital, proceso que comienza a finales de la década de los cincuenta del pasado siglo XX y que abarca hasta nuestros días. En esta tercera revolución industrial el punto de vista cambia y ya no es tanto el del progreso tecnológico sino el de la conexión de este con el factor humano. Es en esa intersección de caminos donde tienen lugar las transformaciones que están cambiando la cotidianeidad de las sociedades y creando un mundo radicalmente distinto al conocido. Dentro de esta denominada

[3] En palabras del profesor británico David S. Landes: "*El término Revolución Industrial suele referirse al complejo de innovaciones tecnológicas que, al sustituir la habilidad humana por la maquinaria y la fuerza humana y animal por energía mecánica, provoca el paso desde la producción artesana a la fabril, dando así lugar al nacimiento de la economía moderna*".
Véase Landes, S. David (1979): *Progreso tecnológico y revolución industrial*, Madrid, Ed. Tecnos, p. 15.

[4] Hobsbawm, J. Eric (2009): *La era de la Revolución, 1789-1848*, Biblioteca E. J. Hobsbawm de Historia Contemporánea, Buenos Aires, Ed. Crítica, p. 36.

revolución digital encontramos diferentes etapas que los expertos catalogan como necesarias a la hora de comprender el progreso de la misma. Estas son:

- Primera revolución digital. [1960-1980]
- Segunda revolución digital. [1980-1990]
- Tercera revolución digital. [1990-2000]
- Cuarta revolución digital. [2000-Actualidad]

3. De ARPANET hacia el marco regulatorio como factor de lucha incipiente

El pistoletazo de salida de la primera revolución digital (1960-1980) sucedió a finales de 1969, momento en que tuvo lugar una conferencia sobre informática en la ciudad de Gatlinburg, Tennessee, allí se presentó por primera vez la idea de *ARPANET*, una red creada por la *Advanced Research Projects Agency* y empleada para investigación en el Departamento de Defensa. El propósito de *ARPANET* era proporcionar una herramienta que facilitara la investigación por medio de tecnologías de comunicaciones mediante conmutación de paquetes y en apoyo de la investigación en las diversas ciencias de la universidad, siempre patrocinada por el Gobierno.[5]

No obstante, la llegada de una red masiva dedicada al intercambio de información y la investigación se convirtió tempranamente en el espacio de cultivo para múltiples amenazas cibernéticas. Así pues, desde su origen el progreso tecnológico fue concebido de la mano del avance pero del mismo modo de la amenaza, que encontraba en este nuevo entorno una nueva posibilidad de propagación.

Fue durante la segunda revolución digital (1980-1990), y cuando el aspecto normativo adquiere toda la relevancia, el momento en que se articularon los primeros mecanismos de defensa frente a tales amenazas. Así, a lo largo de 1985, tanto el Congreso como el Senado de Estados Unidos celebraron audiencias sobre potenciales delitos informáticos y que culminaron en la *Computer Fraud and Abuse Act*, promulgada por el Congreso en 1986, que evolucionó el estatuto anterior y se incorporó como Ley de naturaleza de ciberseguridad en la *Comprehensive Crime Control Act*. Además de aclarar algunas de las disposiciones de la sección original 1030, la *Computer Fraud and Abuse Act* también criminalizó actos adicionales relacionados con la informática. En este sentido, el Congreso agregó una disposición para penalizar el robo de propiedad a través de una computadora,[6] al igual que también añadió una disposición para penalizar a aquellos que intencionalmente alterasen, dañasen o destruyesen datos que perteneciesen a terceros.

Si bien la *Computer Fraud and Abuse Act* es principalmente una Ley en materia penal destinada a reducir las instancias de piratería maliciosa, con el paso del tiempo y del conjunto de enmiendas aplicadas, se ha producido una expansión en la aplicación de la misma ya que, en la

---

[5] Dennett, Stephen & Feinler, J. Elizabeth & Perillo, Francine (1985): *ARPANET information brochure*, Menlo Park, NIC 50003, Defense Communications Agency, Published by the DDN Network Information Center, SRI International, p. 7, en: http://www.dtic.mil/dtic/tr/fulltext/u2/a164353.pdf

[6] Las únicas computadoras, en teoría, cubiertas por la *Computer Fraud and Abuse Act* se catalogan como "*computadoras protegidas*" y se definen como:

- exclusivamente aquellas destinadas al uso de una institución financiera o del Gobierno de los Estados Unidos, o cualquier computadora, cuando la conducta que constituye la infracción afecte el uso de la computadora por o para la institución financiera o el Gobierno;
- aquella computadora que se usa o afecta al comercio o comunicación interestatal o extranjera, incluida una computadora ubicada fuera de los Estados Unidos que se usa de una manera que afecta al comercio interestatal o extranjero o la comunicación de los Estados Unidos.

Doyle, Charles: *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, Congressional Research Service, CRS Report, October 15, 2014, p. 7, en https://fas.org/sgp/crs/misc/97-1025.pdf

práctica, cualquier computadora ordinaria ha caído bajo la jurisdicción de la Ley, incluidos los teléfonos móviles, debido a la naturaleza interestatal de la mayoría de las comunicaciones en Internet. Hoy, toda evolución tecnológica se enmarca en la conceptualización de "computadoras protegidas".

Por otra parte, en el recorrido de la década en la que nos encontramos, también tuvo especial protagonismo la *Electronic Communications Privacy Act,* promulgada en octubre de 1986. La *Electronic Communications Privacy Act*, protege las comunicaciones por cable, orales y electrónicas mientras se realizan dichas comunicaciones, están en tránsito y cuando están almacenadas en computadoras. Del mismo modo, la Ley se aplica al correo electrónico, las conversaciones telefónicas y los datos almacenados electrónicamente y establece excepciones para llevar a cabo actividades de vigilancia electrónica.

Además, en su Título II, conocido como la *Stored Communications Act*, se protege la privacidad del contenido de los archivos almacenados por los proveedores de servicios y de los registros que los proveedores mantienen sobre el suscriptor. Datos como el nombre del suscriptor, los registros de facturación o direcciones IP. Los usuarios generalmente confían la seguridad de la información, cuando esta se lleva a cabo en línea, a un tercero, un proveedor. No obstante, se plantea aquí un debate sobre el grado de privacidad de la información almacenada en línea. Cuando se aplica a información almacenada en línea, las protecciones de la Cuarta Enmienda son potencialmente mucho más débiles. Fundamentalmente esto se debe a que la Cuarta Enmienda define el derecho a la seguridad en términos espaciales que no se aplican directamente a la expectativa razonable de privacidad en un contexto en línea. La sociedad no ha alcanzado aún un consenso claro sobre las expectativas de privacidad en términos de información grabada o transmitida, más si cabe en un contexto de evolución tecnológica permanente.

En muchos casos, la aplicación de la Cuarta Enmienda ha sostenido que, al confiar implícitamente en un proveedor cuando la información se transmite en línea, al hacerlo, los usuarios renuncian a cualquier expectativa de privacidad. En este sentido la conocida como "*Third-Party Doctrine*" sostiene que "*revelar a sabiendas información a un tercero implica la renuncia directa a la protección de la Cuarta Enmienda en esa información*".[7]

4. El *ransonware* y la era del ciberataque geoestratégico

Durante la tercera revolución digital (1990-2000), a medida que se desarrolla la última década del siglo XX, el grado de sofisticación de las amenazas aumenta dotándose de nuevas funcionalidades lo que obliga a implementar nuevos protocolos de seguridad. En este sentido, la mayoría de los protocolos responden a criterios criptográficos. No obstante, desde la perspectiva de la ciberseguridad también surgen nuevas técnicas que alteran el paradigma propio de la criptografía de tal modo que lo que antes se presentaba como barrera fundamental de cara a los ciberdelincuentes, ahora se muestra como una nueva ventaja en las prácticas ilícitas acaecidas en el ciberespacio con su readaptación a lo que en esta última década se conoce como la criptovirología.

Es por este planteamiento por lo que años después a la implementación en el ciberespacio de estos criptovirus se les ha conocido como el antecedente más inmediato del *ransomware* moderno. En este sentido, ya inmersos en pleno siglo XXI, con el comienzo de la cuarta revolución digital (2000-Actualidad) emergen amenazas relativamente recientes como *Cryptolocker* o *WannaCry*.

[7] Consiste en una teoría legal que sostiene que las personas que voluntariamente brinden información a terceros, como entidades bancarias, compañías telefónicas, proveedores de servicios de Internet, etc., carecen de la protección de la Cuarta Enmienda y esa ausencia en la protección de la privacidad le permite al Gobierno de Estados Unidos obtener información de terceros sin orden judicial y sin vulnerar la Cuarta Enmienda contra el registro y la incautación sin causa probable.
Véase Kerr, S. Orin: "The case for the third-party doctrine", *Michigan Law Review*, Vol. 107, nº 561, February 2009.

Hasta la fecha, según señala el *European Cybercrime Centre, WannaCry* consiguió extenderse a más de 300.000 sistemas informáticos repartidos en más de 150 países.[8] Los países más afectados fueron Rusia y China, aunque se registraron de igual modo impactos significativos en otros territorios, especialmente en el *National Health Service* del Reino Unido.

El éxito en la propagación de *WannaCry* cabe atribuirlo al empleo de un *exploit* concreto que facilitó el contagio entre dispositivos rápidamente. Este *exploit* es el conocido como *EternalBlue*, desarrollado por la *National Security Agency* y robado por el grupo de *hackers, Shadow Brokers,* para obtener *Bitcoins* a cambio de una futura venta del mismo a un tercero. En relación al origen de la amenaza, la *National Security Agency* ha vinculado al Gobierno de Corea del Norte con la creación de *WannaCry*, según funcionarios de inteligencia de Estados Unidos.[9] La evaluación, que se emitió internamente, se basaba en un análisis de tácticas, técnicas y objetivos que apuntaban a la Agencia de espionaje de Corea del Norte, la *Reconnaissance General Bureau* (*RGB*).

No obstante, más allá de la amenaza desde el cariz tecnológico, la actual cuarta revolución Digital en que nos encontramos ha sido ya campo de representación de ciberataques como eje de respuesta a intereses geoestratégicos. Así, para Stephen Herzog, la situación que se desarrolló en Estonia en la primavera de 2007 ilustra la creciente capacidad de diferentes grupos transnacionales para utilizar herramientas digitales y desafiar así a las políticas y la soberanía de los Estados en todo el mundo.[10]

Los ciberataques acaecidos en Estonia en la primavera de 2007 se produjeron dentro del clima general de tensión y la escalada de desconfianza entre la etnia estonia y la minoría rusa del país. Tuvieron lugar entre el 27 de abril y el 18 de mayo. Durante este periodo aunque los ataques fueron muy variados se pueden distinguir dos fases en su aplicación y desarrollo. La primera fase se apoyaba en el componente emocional identitario y en la motivación nacionalista para unirse a los ciberataques, aunque se trataba de una etapa experimental dado el poco carácter organizativo del movimiento.[11] Durante la segunda fase, los ataques se volvieron más complejos tanto en el aspecto técnico como en el organizativo. Un uso elevado de *Botnets* y una coordinación precisa sirvieron para que los sitios web empleados en la primera fase como plataforma de lanzamiento siguieran en funcionamiento en esta segunda, pero con mejoras añadidas, como listas de objetivos y calendarios en los que se indicaban hora y lugar de los ataques.[12]

Para Herzog, este tipo de movilización digital transnacional para explotar las vulnerabilidades de un Estado con fines políticos ejemplifica la amenaza emergente del terrorismo cibernético.[13] Según James Lewis, este terrorismo no es sino el uso de herramientas de red informática para cerrar infraestructuras nacionales críticas (como la energía, el transporte y el Gobierno) o para coaccionar o intimidar a un Gobierno o la población civil.[14]

---

[8] European Cybercrime Centre (*EUROPOL*): *Internet organised crime threat assessment*, EC3 European Cybercrime Centre, 2017, p. 19, en https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

[9] Nakashima, Ellen: "The NSA has linked the WannaCry computer worm to North Korea", *The Washington Post*, June 14, 2017, en https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.ebdeed303ba3

[10] Herzog, Stephen: "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", en *Journal of Strategic Security*, Vol. 4, nº 2, (Summer 2011), pp: 49-60.

[11] Instituto Español de Estudios Estratégicos: "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", op. cit., p: 178, en http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

[12] *Ibíd*., p. 180.

[13] Herzog, Stephen: "Revisiting the Estonian Cyber Attacks", *op. cit*., p. 52.

[14] Lewis, A. James: *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic & International Studies, Washington, December 2002, p. 1, en

Entre los objetivos de los ataques cabe diferenciar: objetivos políticos, económicos y de comunicaciones. Los objetivos políticos más importantes fueron los sitios webs, redes y servicios del Gobierno, primer ministro, Presidente de la república, Parlamento, oficina de estudios estatales, ministerios, policía y partido político del Gobierno. Los objetivos económicos estuvieron enfocados principalmente a los servicios de *e-banking* de los principales bancos nacionales, *Hansapank* y *SEB Eeesti Uhispank*. Los objetivos de comunicaciones se orientaron a los proveedores de servicios de Internet más importantes: *Elion*, *Elisa* y *Starman*. Los administradores de servicios de nombres de dominio: *DNS Nacional*, *EEnet* y los medios electrónicos de comunicación, los más influyentes: *Postimees*, *Delfi*, *EPL* y *Baltic News*. En definitiva, Estonia reunía una serie de requisitos que la hacían altamente atractiva para sufrir un ciberataque masivo por parte de su vecino, la Federación Rusa, principal sospechoso de instigar y organizar los ataques.

Mientras que el caso de Estonia en 2007 mostró que un Estado por completo puede sufrir y padecer las alteraciones en materia de infraestructura de seguridad digital por un conjunto de ciberataques, el caso posterior de Georgia en 2008 fue un ejemplo de cibercampaña que apuntaba a un conflicto armado.

A medida que se intensificaba el conflicto armado iniciado a raíz de la Guerra de Osetia del Sur entre Georgia, por un lado, y Osetia del Sur, Abjasia y Rusia por el otro; con un ataque que emprendieron las Fuerzas Armadas de Georgia contra Fuerzas Separatistas el 7 de agosto de 2008, a su vez se incrementaban los ciberataques fundamentalmente orientados a debilitar la capacidad de información y de comunicación entre el Gobierno y los ciudadanos, gracias a técnicas de ciberpropaganda para tratar de influenciar en la opinión pública hacia la postura defendida por Rusia, Osetia del Sur y Abjasia. Se observa así, no solo la capacidad de mimetización en función del tipo de conflicto y propósito que persiguen los ciberdelincuentes, sino del mismo modo, la cualidad de acompasar operaciones armadas con ciberoperaciones, que en este caso, sirvieron para debilitar la respuesta militar y política de Georgia, pero también para desmoralizar al bando rival al bloquear las comunicaciones entre Gobierno y pueblo georgiano.

Desde el punto de vista estadounidense, el siglo XXI tampoco ha traído de la mano gratas noticias para las administraciones de gobierno en lo que al ciberespacio se refiere. En este sentido, cabe destacar el anuncio que hizo *Google* el 12 de enero de 2010, en el que se reconocía como víctima de una guerra cibernética originada en China desde mediados de 2009.[15] Según el anuncio, el objetivo de la operación, conocida en clave como operación Aurora, era acceder a las cuentas de correo electrónico de *Gmail* de los activistas chinos de derechos humanos.

Literalmente, pocos minutos después del anuncio de *Google*, *Adobe*, otro importante proveedor de *software*, anunció que sus sistemas corporativos también habían sido pirateados. Resultó que tanto *Google* como *Adobe* eran objetivos del mismo adversario, que realizó la misma operación contra 32 compañías más. Entre estas empresas se incluyeron: *Dow Chemichal*, *Northrop Grumman*, *Juniper Networks*, *Rackspace*, *Symantec, Morgan Stanley* y *Yahoo*, entre otras. Parece que el propósito de la operación fue el de filtrar no solo la información sobre los activistas chinos de

---

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

[15] Ya desde 2003, el Gobierno de Estados Unidos comenzó a ser consciente de una serie de ataques coordinados a las redes de computadoras del Pentágono, en lo que se denominó como la operación *Titan Rain*. Los *hackers* obtuvieron acceso a muchas redes informáticas de contratistas de defensa del Gobierno estadounidense, incluidas las de *Lockheed Martin*, *Sandia National Laboratories*, *Redstone Arsenal* y la *NASA*. En función de informes publicados, se cree que la serie de ataques fueron acciones coordinadas del Ejército Popular de Liberación chino, y no de piratas informáticos chinos independientes.

Véase Jahankhani, Hamid & Hessami, Ali & Hsu, Feng (2009): *Global Security, Safety, and Sustainability*, London, UK, 5th International Conference, ICGS3 2009, Series: Communications in Computer and Information Science (Book 45), Ed. Springer, p. 141.

derechos humanos sino también comprometer la propiedad intelectual, es decir, el código fuente del *software* desarrollado comercialmente por estas corporaciones.

Por otro lado, el 4 de junio de 2015, la *Office of Personnel Management* (*OPM*) de Estados Unidos reveló que se había producido una intrusión cibernética pudiendo llegar a exponer a agentes delictivos del ciberespacio, los registros federales de hasta 4 millones de actuales y antiguos empleados del Gobierno. La investigación inmediata posterior reveló que los datos robados podían haber acabado afectando a 21,5 millones de empleados federales.[16]

La investigación indicó que la primera violación de los sistemas de seguridad de la *OPM* se produjo tras el acceso de los piratas informáticos a información personal, incluidos los números de seguridad social de empleados, asignaciones de trabajo, calificaciones de rendimiento e información sobre capacitación, residencia y perfil educativo, historial de empleo, información sobre familiares cercanos y conocidos personales, historiales de salud, criminal y financiero y otros detalles. Algunos registros también incluyeron el robo de nombres de usuario y contraseñas que algunos de estos empleados crearon al completar diferentes formularios de la Administración. En este sentido, cerca de 1,1 millones de registros robados incluyeron huellas digitales así como información relativa a cónyuges o cohabitantes de estos solicitantes, lo que se estima en un total de 1,8 millones de no solicitantes también involucrados en el ataque.

En una conferencia de Inteligencia celebrada el 24 de junio de 2015, el almirante Michael Rogers, Director de la *National Security Agency* y jefe del *U.S. Cyber Command*, se negó a discutir quién podría ser el responsable o encontrarse detrás de los ataques, sin embargo, en la misma conferencia y tan solo un día después, el *Director of National Intelligence*, James Clapper, identificó a China como el principal sospechoso en los ataques.

Aún no está claro cómo se podrían emplear los datos extraídos de los sistemas de seguridad cibernética de la *OPM*, si en cierto modo realmente resultaran en la actualidad en manos del Gobierno chino. Diferentes expertos sobre infraestructuras de seguridad digital de tanto dentro como fuera del Gobierno estadounidense sospechan que China podría estar intentando construir una base de datos gigantesca de empleados federales, lo que podría ayudar a identificar a los funcionarios de Estados Unidos así como sus diferentes ocupaciones o roles en las Administraciones de Gobierno.[17]

Otras fuentes relacionadas con la comunidad de seguridad nacional han comparado el daño potencial a la *OPM* y su vinculación con los intereses de Estados Unidos a los causados por las filtraciones de información clasificada concerniente a la *National Security Agency* por Edward Snowden, no obstante, existen daños en el seno de la seguridad nacional que van más allá del simple robo de información clasificada o publicación de la misma. En esta dirección, el Senador republicano por Nebraska Benjamin Sasse, en la revista *Wired*, dejó caer incluso una posibilidad mucho más grave al insinuar que China podía ahora "*tener la base de datos de reclutamiento de espías más grande de la historia*".[18]

---

[16] Montford, John & McCool, Joseph & Kelleher, Herb (2016): *Board Games: Straight Talk for New Directors and Good Governance*, Ed. Praeger, p. 129.

[17] Liptak, Kevin & Schleifer, Theodore & Sciutto, Jim: "China might be building vast database of federal worker info, experts say", *CNN Politics*, June 6, 2015, en https://edition.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/index.html

[18] "*Nuestros enemigos tienen una ruta hacia nuestras vulnerabilidades. Al unir la información de una amplia variedad de bases de datos, incluso las no clasificadas, nuestros adversarios pueden construir una imagen que dañe nuestra seguridad nacional. Los analistas de inteligencia llaman a esto "mosaic theory". Este mosaico de nuestro personal de inteligencia los expone a serias amenazas. […] Algunos en las comunidades de defensa e inteligencia piensan que los ataques a la OPM constituyen un acto de guerra, sin embargo, las reglas de combate en la guerra cibernética aún se*

Asimismo, han surgido diferentes informes que indican que la *OPM* había intentado en el pasado incluir entre sus registros los de la base de datos *Scattered Castles*, la herramienta fundamental de registro del personal que conforma la Comunidad de Inteligencia de Estados Unidos. Aunque la Comunidad de Inteligencia negase tal vinculación y por tanto, haberse visto afectada por el ataque cibernético chino, realmente, si la principal base de datos y registro de la Comunidad de Inteligencia estuviera vinculada con la *OPM*, sería un factor determinante que ayudaría a los *hackers* a la hora de obtener acceso a información sobre el personal de las Agencias de inteligencia e identificar a los oficiales clandestinos y encubiertos distribuidos por el mundo. De la misma manera, podría revelar el proceso y los criterios para obtener autorizaciones y acceso especial a las Agencias de inteligencia, permitiendo a agentes extranjeros infiltrarse más fácilmente en el Gobierno de Estados Unidos.

5. Conclusiones

Podemos tomarlo de ejemplo. Tras el ataque, Estonia tomó una serie de medidas técnicas encaminadas a fortalecer la capacidad de prevención y respuesta ante incidentes informáticos, entre ellas destacaron el fortalecimiento de la infraestructura vertebral de Internet con la integración de todos los servicios electrónicos del Gobierno en un solo sistema centralizado llamado *X-Road* y una mayor inversión en el desarrollo de herramientas capaces de detectar ataques cibernéticos. En cierto sentido, al tratarse de un ataque a un Estado miembro de la *OTAN*, el Gobierno estonio contempló en un principio la posibilidad de requerir una consulta formal a los Estados miembros, en función del Artículo 4º del Tratado de Washington para después vislumbrar una posible aplicación del Artículo 5º, que prevé un respaldo de la comunidad ante un acto de agresión a un Estado miembro. Sin embargo, la tipicidad del Artículo 5º y el hecho de que un tipo de ataque como el que acontece en el ciberespacio no resulte abarcado en la terminología profundamente militar que se observa en la redacción del texto, impidió que el Gobierno estonio pudiera acogerse al mismo. Esto es un factor que claramente limita la respuesta organizada e internacional ante futuros casos de ciberataque, más cuando se tiene en cuenta que la cooperación internacional entre Estados así como el intercambio de información, resultan esenciales para combatir una amenaza asimétrica producida en el ciberespacio.

El ejemplo estonio, pero del mismo modo, la magnitud de la gravedad y las consecuencias de las amenazas que representa el ciberespacio vienen a demostrar que cuando hablamos de ciberseguridad como mecanismo de control de infraestructuras vitales de un Estado, aún queda mucho trabajo por hacer, incluso en el plano normativo. En este sentido, Estados Unidos, que parecía llevar la delantera y al igual que en el mundo físico, el liderazgo en este entorno dinámico y permanentemente cambiante que es el ciberespacio, se ha visto obligado a plegarse a la ciberdelincuencia organizada y a los ciberataques, ya respondan a un mero criterio de robo masivo de información, a la sustracción de cantidades ingentes de dinero para sufragar actividades delictivas de todo tipo o al interés geoestratégico en la configuración de poderes mediante la alteración de procesos electorales.

---

están escribiendo. No obstante, debemos enviar un mensaje claro: este tipo de intrusiones no serán toleradas. Debemos asegurarnos de que nuestros atacantes sufran todas las consecuencias de sus acciones".
Véase Sasse, Benjamin: "Senator Sasse: the OPM hack may have given China a spy recruiting database", *Wired,* July 9, 2015, en https://www.wired.com/2015/07/senator-sasse-washington-still-isnt-taking-opm-breach-seriously/