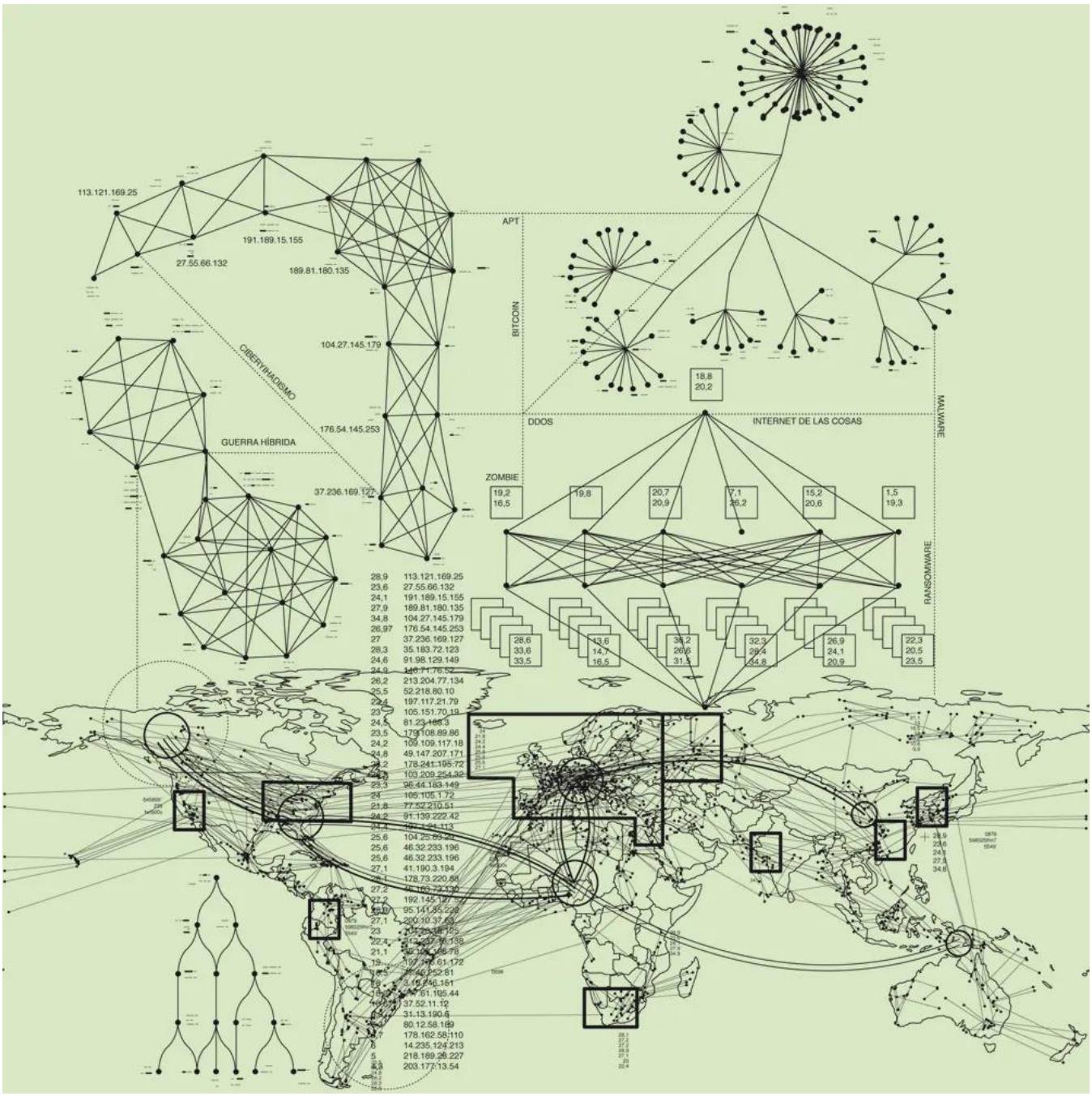
La ciberseguridad, determinante en el tablero internacional

La protección del ciberespacio se ha convertido en una de las principales prioridades de los gobiernos de todo el mundo, que lo consideran un asunto de seguridad nacional y un eje fundamental de la sociedad y de sus sistemas económicos. Mantener la infraestructura y los sistemas de información con unos niveles óptimos de seguridad, protegiendo la información y el patrimonio tecnológico de un país, formando al capital humano necesario y desarrollando estrategias y marcos legales posibilistas, representa una ventaja geopolítica incontestable en las relaciones internacionales actuales.

Tradicionalmente, la geopolítica se ha definido como la ciencia que analiza la influencia de los factores geográficos sobre las decisiones y los sucesos políticos, presentes y futuros, relacionados con la política internacional y las relaciones entre los distintos países. Todo ello teniendo en cuenta numerosos factores: ubicación, extensión, clima, recursos, fuerzas sociales y culturales, recursos económicos, etcétera.

La primera vez que se utilizó el término fue en 1900 por parte del geógrafo sueco Rudolf Kjellén, aunque fue desarrollada principalmente en la década de los años treinta por un grupo de geógrafos alemanes en la Universidad de Múnich. El principal de ellos, Karl Haushofer, mantenía que "el espacio supone poder" y aportó diversas teorías que daban argumentos para justificar la expansión territorial de la Alemania nazi: el denominado "espacio vital" o *Lebensraum*.

En aquel entonces, el espacio era un espacio físico y la expansión se centraba en la conquista de territorios. Sin embargo, los nuevos supuestos de la geopolítica se han ido sustituyendo. El carácter militar ha ido cediendo terreno al factor económico, al cultural o al de la información. Las fronteras actuales son electrónicas y el desarrollo de las Tecnologías de la Información y la Comunicación (TIC) ha posibilitado la aparición de un nuevo espacio, el ciberespacio, que se ha convertido en un factor decisivo a la hora de analizar las relaciones internacionales.



Mapa de ciberataques, estructuras de nodos de malware y ordenadores zombies. (Guerra híbrida, cibercrimen, APT). ILUSTRACIÓN: RAFA HÖHR

Espacio físico y virtual

Se entiende por ciberespacio al territorio digital o virtual donde están conectadas personas, objetos y procesos a través de una serie de dispositivos y redes de telecomunicación (internet). Según cifras de la UIT[1], a finales del año 2018, el número de usuarios conectados a la red sería de unos 3.900 millones —un 51,7 por ciento de la población mundial—. Por su parte, la compañía We Are Social muestra unas cifras muy similares: en octubre de 2018 se estimaban unos 4.176 millones de usuarios en todo el mundo —el 55 por ciento—.

La era de internet y la conectividad ha traído grandes avances y ventajas importantes que benefician, tanto a

los usuarios comunes, como a gobiernos y a empresas. No obstante, si bien es cierto que han permitido la aparición de nuevas oportunidades económicas y sociales de gran alcance, conllevan también una serie de riesgos. Las amenazas del ciberespacio, favorecidas por la rentabilidad económica o política, el bajo coste de las herramientas empleadas y la posibilidad de actuar de forma anónima, se dirigen transversalmente a los sectores público y privado, así como a los ciudadanos.

En este contexto, los ciberdelincuentes, los *hacktivistas* o los propios estados, son capaces de explotar las debilidades tecnológicas y no tecnológicas de un país para recabar información, desestabilizarlo, etcétera —guerra híbrida[2]—, sustraer activos de gran valor o amenazar servicios básicos para su normal funcionamiento, todo ello apoyado en acciones en el ciberespacio.

Así pues, garantizar e implementar seguridad en el ciberespacio, al tiempo que se respeta la privacidad y la libertad, se ha convertido en una de las prioridades estratégicas de los países más desarrollados, debido a su impacto directo en la seguridad nacional, en la competitividad de las empresas, y en la prosperidad de la sociedad en su conjunto.

> La industria de los ataques digitales constituye un nuevo modelo de negocio. La mayoría de sus servicios se ofrecen a través de la web profunda

Liderar el mundo

En España, la Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, gestionó en 2018 un total de 38.192 incidentes —un 43 por ciento más que en el ejercicio anterior—. Existe, por tanto, un número creciente de ciberamenazas que son perpetradas a través de muy diversas técnicas:

• **APT (Amenazas Persistentes Avanzadas).** Ataques selectivos de ciberespionaje o cibersabotaje llevado a cabo bajo el auspicio de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. Este ataque selectivo de ciberespionaje, dirigido por un Estado, emplea diversos tipos de *malware* para proceder al robo de propiedad intelectual, tratando de permanecer oculto el mayor tiempo posible.

• **Ransomware[3].** Es un código dañino para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado. Ha sido uno de los tipos de *malware* que más ha aumentado en los últimos tiempos junto a la minería oculta de criptomonedas. Por citar un ejemplo reciente, el pasado 3 de enero Luas, la web del tranvía de Dublín, Irlanda, fue *hackeada* por una persona que utilizó este método para inhabilitar la página y solicitar un rescate de 1 bitcoin —actualmente valorado en casi 3.800 dólares—. Los datos personales –nombre, número de teléfono móvil y dirección de correo electrónico– de al menos 3.226 usuarios fueron puestos en riesgo.

• **Internet de las Cosas[4].** Se refiere a redes de objetos físicos —artefactos, vehículos, edificios,

electrodomésticos, vestimenta, implantes, *software*, etcétera—; en definitiva, sensores que disponen de conectividad en red que les permite recolectar información de todo tipo. Una de las mayores ventajas es su conexión a internet, pero esa capacidad también es una de sus mayores debilidades, ya que esa conectividad puede amenazar la seguridad de todo el sistema al incrementar notablemente su superficie de exposición a ciberataques. Sus múltiples vulnerabilidades han sido explotadas a lo largo de 2018 y permiten que los dispositivos IoT (Internet de las Cosas, por sus siglas en inglés) se hayan utilizado como herramientas para llevar a cabo ciberataques (IoT en *botnets*), además de para espiar a sus usuarios o para manipular su entorno.

• **Bitcoin.** Es la criptomoneda digital por excelencia. Cuenta con numerosos riesgos, entre ellos el blanqueo de dinero y exención fiscal, así como la infección de dispositivos para minar criptomonedas ilegalmente. A finales de 2017 comenzaron a surgir webs con código incrustado para minar criptomonedas aprovechando la potencia del ordenador de sus visitantes. Esta técnica se ha extendido a multitud de webs, algunas lo advierten y otras lo ocultan y el visitante solo detecta que su ordenador está anormalmente acelerado y con la CPU (Unidad Central de Proceso, en sus siglas en inglés) muy ocupada. Incluso se han dado casos de webs que han sido atacadas y han inyectado este código de minado sin que sus propietarios lo supieran.

• **Huella digital.** Nuestros datos se han convertido en un activo muy valioso y, por tanto, debemos de ser conscientes de los peligros derivados de hacerlos públicos. Las redes sociales y los grandes proveedores de servicios en internet disponen de mucha información sobre sus usuarios que puede ser utilizada con un fin distinto al original.

• **Ataques a la cadena de suministro.** Se oculta *malware* (programa maligno o malicioso) en las propias infraestructuras de descargas de servicios, en teoría, de confianza, para lograr introducir virus antes de la propia instalación. El caso de CCleaner (*software* de limpieza) es uno de los ejemplos de este tipo de ataques. Los servidores de la empresa fueron comprometidos y la versión original del *software* fue cambiada por otra que contenía el *malware*, afectando a todos los usuarios que procedían a su descarga. Se estima que afectó a más de dos millones de usuarios entre agosto y septiembre de 2017.

• **Cibercrimen como servicio (CaaS).** La industria de los ataques digitales constituye un nuevo modelo de negocio. La mayoría de sus servicios se ofrecen a través de lo que se conoce como la *deep web*. Existe el fraude como servicio, *malware* como servicio, ataques de DDoS[5] como servicio, *ransomware*, o secuestro de información, como servicio. A veces se ofrece soporte técnico las 24 horas e incluso disponen de estrategias de marketing y plataformas de compraventa donde los cibercriminales pueden comprar más de 70.000 servidores *hackeados* en internet.

Influenciar, alterar, manipular la opinión pública de una nación es una nueva arma de guerra que destaca por su eficacia, su bajo coste y su compleja trazabilidad

• **Hacktivismo.** Es la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines socio-políticos. Es el traslado al mundo digital de los tradicionales grupos activistas. El tipo

de acciones que realizan se basan principalmente en desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales y sabotajes virtuales.

• **Ciberyihadismo.** Los grupos yihadistas y terroristas constituyen una amenaza, aunque todavía no parecen ser capaces de desarrollar ciberataques sofisticados. Sin embargo, no es menos cierto que el Dáesh, parece estar decidido a desarrollar esta vía de agresión, aún cuando hasta el momento los resultados más evidentes han sido las desfiguraciones y los ataques DDoS, todos ellos de naturaleza propagandística. Además de lo anterior, los grupos yihadistas también pretenden desarrollar ciberataques dirigidos al desenvolvimiento diario de los ciudadanos mediante tácticas violentas o en la perturbación social, aunque no se han producido manifestaciones en tal sentido.

• **Guerra híbrida.** Las guerras de opinión pública se han convertido en una estrategia generalizada y recurrente a nivel global. Durante los últimos años se ha podido constatar y demostrar el interés que determinados estados tienen por influir en el debate público de países extranjeros. Influenciar, alterar, incluso manipular la opinión pública de una nación considerada adversaria se está convirtiendo en una nueva arma de guerra que destaca por su eficacia, su relativo bajo coste y, sobre todo, por su compleja trazabilidad. Las amenazas híbridas se caracterizan por pasar inadvertidas y por emplear recursos, técnicas, acciones, y métodos legales, o ilegales; bajo la cobertura de identidades difícilmente rastreables y no ligadas a los verdaderos actores ofensivos. Dichos actores generan contenidos narrativos transmedia (*fake news*), que difunden a través de medios propios y redes sociales, pero empleando para ello perfiles y redes de *bot*[6] que, de forma automática, amplían la resonancia de sus mensajes9.

Prioridad nacional

Ante este panorama, garantizar e implementar la seguridad en el ciberespacio, al tiempo que se respeta la privacidad y la libertad de los ciudadanos, se ha convertido en una de las prioridades estratégicas de los países más desarrollados, debido a su impacto directo en la seguridad nacional, en la competitividad de las empresas, así como en la prosperidad de la sociedad en su conjunto.

La capacidad de recuperación de las personas y las organizaciones todavía sigue a la zaga de las crecientes amenazas. De hecho, las medidas adoptadas para mejorar su resiliencia digital son, todavía, limitadas. El crecimiento en el número de ciberincidentes señala que la resiliencia de los países occidentales sigue por detrás del crecimiento de las amenazas.

La adaptación a este escenario implica mejorar las capacidades de prevención, monitorización, vigilancia y respuesta en todas las instancias del Estado —ciudadanos, empresas y sector público—, con el fin de aumentar la disuasión para generar dudas sobre el coste/beneficio del ciberatacante —desgraciadamente, mientras que los autores de ataques solo teman al fracaso, carecerán de motivos para dejar de intentarlo—.

De igual modo, es necesario incrementar y mejorar las capacidades de inteligencia para la identificación de los atacantes, la determinación de sus objetivos y, sobre todo, la formación y concienciación de las personas para que los mecanismos de protección sean eficientes.

El Centro Criptológico Nacional intenta dar respuesta al gran desafío que supone preservar el ciberespacio español de todo tipo de riesgos y ataques y, por tanto, defender los intereses nacionales y garantizar a nuestro país su seguridad y progreso.

Frías, Z. y Pérez, J. (2018): “Organizaciones multistakeholder para la gobernanza global” en Revista de Economía Industrial. Disponible en: https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndus

trial/407/FRIAS%20Y%20P%C3%89REZ.pdf

Frías, Z.; Pérez, J. y Steck, C. (2018): "Gobernanza de Internet y derechos digitales" en De la Quadra-Salcedo, T. y Piñar, J.L. (Eds.) Sociedad Digital y Derecho. Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad. Disponible en: https://tienda.boe.es/detail.html?id=9788434024830

Kleinwächter, W. (2019): Internet Governance Outlook 2019: Innovative Multilateralism vs. Neo-Nationalistic Unilateralism. CircleID. Disponible en: http://www.circleid.com/posts/20190108_internet_governance_2019_innovative_multilateralism_vs_neo

Olmos, A. (2015): "Recursos críticos. Avances destacados en la gobernanza de Internet" en Serrano, S. (Ed.), La gobernanza de internet en España 2015. (pp. 48-58). Madrid, Fundetel. Disponible en: https://igfspain.files.wordpress.com/2017/04/gobernanza_internet_spain_2015_pdf.pdf

Internet Society (2016): Internet Governance–Why the Multiskeholder Approach Works. Disponible en: https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works