ieee.es
Instituto Español de Estudios Estratégicos

Documento
Marco

10/2021 7 de septiembre de 2021

Enrique Cubeiro Cabello

Unidades de ciberinteligencia y ciberguerra al servicio de Estados

Unidades de ciberinteligencia y ciberguerra al servicio de Estados

Resumen:

En los últimos años, el ciberespacio se ha convertido en un escenario de intensa confrontación a través de cual actores muy heterogéneos persiguen objetivos muy diversos. La mayoría de Estados cuentan desde hace años con unidades especializadas para operar en el ciberespacio, tratando de explotar las singularidades que hacen de él un ámbito de extraordinario interés, tanto desde el punto de vista militar como el de la inteligencia. En este artículo, se pretende dar una visión del por qué y para qué emplean los Estados este tipo de unidades, cómo actúan y de qué forma están constituidas.

Palabras clave:

Ciberguerra, ciberespionaje, ciberataque, guerra híbrida, Amenaza Persistente Avanzada.

Cyber-intelligence and cyber-warfare units in the service of states

Abstract:

Cyberspace has become a scene of intense confrontation through which heterogeneous actors pursue very different objectives. Many States have specialized units to operate in cyberspace, trying to exploit the singularities that make it a domain of extraordinary interest, both from the military and intelligence points of view. This article tries to give a vision of why and for what the States use this type of units, how they act and in what way they are constituted.

Keywords:

Cyberwar, cyberespionage, cyber-attack, Hybrid warfare, Advanced Persistent Threat.

Cómo citar este documento:

CUBEIRO CABELLO, Enrique. *Unidades de ciberinteligencia y ciberguerra al servicio de Estados*. Documento Marco IEEE 10/2021. http://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM10_2021_ENRCUB_Ciberinteligencia.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción

Prácticamente a diario los medios de comunicación informan de ciberataques severos en algún punto del globo. En España, tenemos algunos casos sonados muy recientes. Ataques que afectan a la banca, a empresas tecnológicas, a organismos gubernamentales, a partidos políticos, a ciudadanos… En algunos casos, esos ciberataques tienen alcance global, mientras que en otros han sido cuidadosamente diseñados y dirigidos a un objetivo concreto. Robo o secuestro de información, caída de servicios, daños a infraestructuras críticas… Las consecuencias de los ciberataques son muy diversas y casi siempre se traducen en interrupción de servicios, pérdidas económicas o daños a la reputación de la víctima, cuando no todo ello de forma simultánea.

Las últimas ediciones del *Global Risk Report*, que anualmente publica el World Economic Forum, sitúan a los ciberataques como el principal riesgo global de origen humano, posición que se explica fácilmente por la confluencia de una elevada probabilidad de ocurrencia con su alto impacto potencial.

Las motivaciones tras los ciberataques son muy heterogéneas. Obviamente, la gran mayoría persigue un fin económico (el ciberdelito es, desde hace ya unos cuantos años, la forma delictiva que más dinero mueve a nivel mundial), pero también hay otros que se realizan con fines activistas, o para obtener información sobre un adversario, o como acciones integradas en un plan militar. En estos dos últimos casos, nos encontraríamos ante lo que se ha dado en llamar ciberespionaje y ciberguerra.

El hecho de que el ciberespacio se haya convertido, casi de repente, en un escenario de confrontación en el que (o a través del que) pueden llevarse a cabo acciones contra un adversario y, al mismo tiempo, hay que defenderse contra la acción enemiga, ha llevado a que prácticamente todos los Estados se hayan dotado (o estén en el proceso de dotarse) de unidades especializadas para operar en él, tanto en el ámbito militar como en el de la inteligencia. En este artículo, modesto ya por su propia extensión, se pretende dar una visión del por qué y para qué emplean los Estados este tipo de unidades, cómo actúan y de qué forma están constituidas. Empecemos por el por qué.

Por qué

Hoy en día existe una permanente e intensísima actividad hostil en el ciberespacio (figura 1). Una parte importante de esa actividad, más en términos cualitativos que cuantitativos, está siendo desarrollada por lo que se denomina actores-Estado. Podemos hablar, incluso, de una guerra soterrada, que se mantiene en el tiempo, independientemente de que el «mundo real» se encuentre en estado de paz, crisis o conflicto.

Mientras escribo estas líneas, los medios de comunicación se hacen eco de las acusaciones del presidente Biden contra China por los ciberataques perpetrados contra Microsoft en marzo del presente año y de la apertura de una investigación sobre el presunto espionaje de Marruecos contra ciudadanos franceses a través del *software* Pegasus para telefonía móvil.

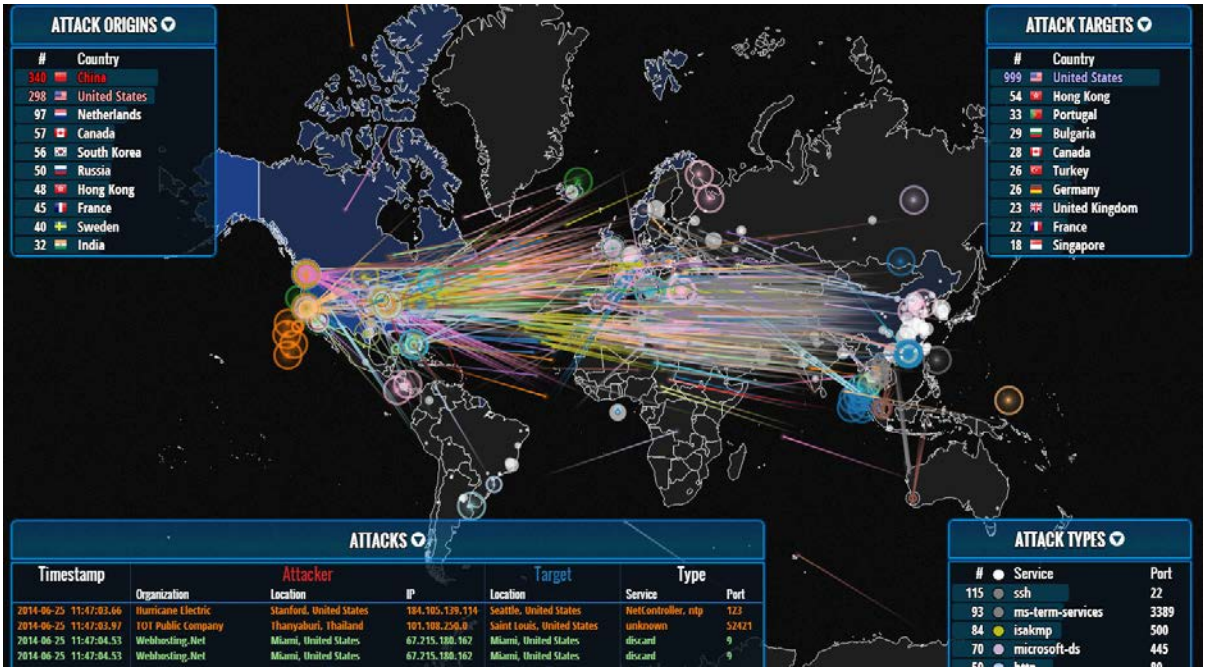

Figura 1. Un instante cualquiera en el ciberespacio. Fuente. Disponible en: www.map.ipviking.com

¿Por qué ocurre esto en el ciberespacio? O, más concretamente, ¿cuáles son las razones que explican el enorme interés que para los Estados suscita el ciberespacio y esa extraordinaria actividad hostil que no se produce en ningún otro ámbito? Tratemos de identificarlas.

En primer lugar, nos encontramos con la «ciberdependencia». Prácticamente todas las actividades de un Estado (y, por extensión, las de sus organismos, empresas y ciudadanos) se apoyan y dependen, en mayor o menor medida, del ciberespacio. Energía, comunicaciones, transporte, finanzas… y hasta el ocio o el deporte. Por tal motivo, el ciberespacio juega un papel esencial en las rivalidades entre Estados. Ello implica, a su vez, infinidad de objetivos alcanzables en o a través del ciberespacio.

Desde el punto de vista militar, esa dependencia del ciberespacio se traslada a todos los aspectos relacionados con el planeamiento, conducción y desarrollo de la actividad militar y, muy especialmente, de las operaciones. Y tiene muy serias consecuencias, en tanto cada vez resulta más evidente que, en un conflicto entre Estados, la superioridad en el ciberespacio de una de las partes puede desnivelar la contienda a su favor, incluso en el caso de que el adversario sea superior en el resto de ámbitos operacionales. Y la superioridad en un ámbito solo puede obtenerse a través del empleo de capacidades ofensivas. Otro de los motivos a los que más habitualmente se recurre para explicar la singular situación en el ciberespacio es el de su indefinición legal.

Si esta es la situación ideal (Figura 2):

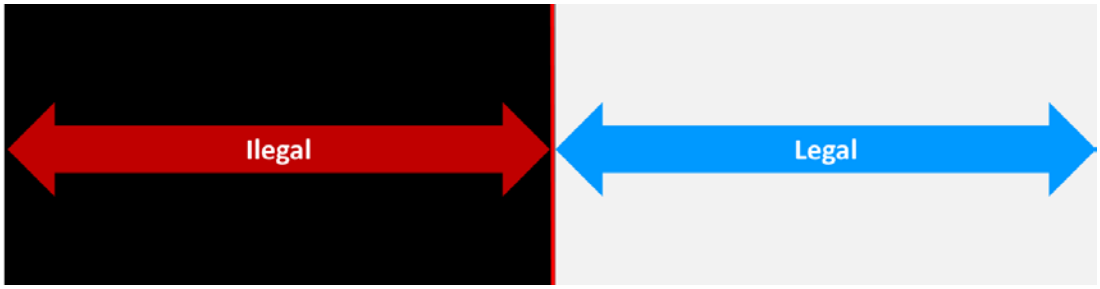

Figura 2. Marco legal ideal. Fuente. Elaboración propia.

Lo que nos encontramos en el ciberespacio es esto (Figura 3):

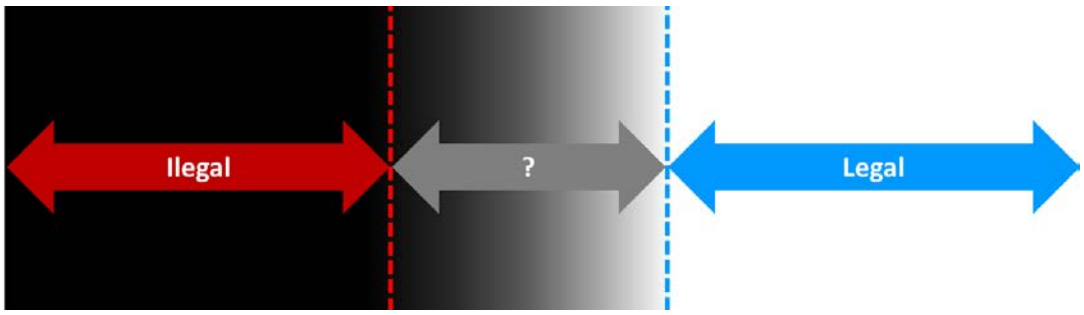

Figura 3. Marco legal en el ciberespacio. Fuente. Elaboración propia.

Hay demasiadas zonas grises[1]. Derivadas de legislaciones deficientes y no universales, o de diferentes interpretaciones de las normas existentes y de la forma en la que aplican en el ciberespacio. Zonas grises que para unos Estados suponen un límite y para otros ninguna diferencia con la zona blanca.

Porque ante las zonas grises hay dos posibles aproximaciones: a) Si no está claro que se pueda hacer, no lo hago, y b) Si no está claro que no se pueda hacer, lo hago.

Es evidente que hay gobiernos menos sometidos que otros a los contrapoderes del Estado y al escrutinio de la opinión pública. Por lo general, los estados totalitarios son más proclives a actuar conforme al patrón b), en tanto que las democracias se ven casi siempre obligadas a seguir el patrón a). Y esta diferente aproximación deriva en que las reglas no condicionan de la misma forma a unos y otros, originando lo que se ha dado en llamar *asymmetrical lawfare*.

Traslademos la situación descrita al plano militar. El derecho internacional de los conflictos armados limita enormemente las acciones que pueden llevarse a cabo contra los servicios esenciales e infraestructuras críticas del adversario. Muy difícilmente un objetivo de este tipo será capaz de cumplir los requisitos que exige la aplicación de los principios de distinción, necesidad militar o proporcionalidad, por citar los más claramente afectados.

Esto lleva a que, mientras para una democracia occidental puede resultar inaceptable un ataque contra una infraestructura crítica, incluso en caso de conflicto armado, sea muy probable que, como consecuencia de la enorme dificultad de demostrar la autoría de estas acciones, determinados Estados con pocos escrúpulos lleven años posicionando *malware* en sistemas de control de infraestructuras críticas de potenciales adversarios. Es decir, estarían llevando a cabo acciones precursoras en diversos objetivos, dudosamente legítimos hasta en el caso de estar encuadrados en un conflicto armado, en lo que podríamos denominar Fase 0, previa incluso al inicio de una crisis.

A todo lo anterior se suma la enorme imperfección del ciberespacio, plagado de vulnerabilidades físicas, lógicas y humanas que pueden ser explotadas: errores de diseño, fallos de programación, arquitecturas o interconexiones inadecuadas, emanaciones electromagnéticas, políticas imperfectas, carencia o incumplimiento de los

[1] SCHMITT, Michael N. *Grey Zones in the International Law of Cyberspace.* 42:2 Yale Journal of International Law Online 1 (2017). Publicado el 30 de mayo de 2018.

procedimientos, desconocimiento, falta de concienciación…

En términos de eficacia-coste y riesgo, los ciberataques y el ciberespionaje también presentan claras ventajas sobre otros métodos más tradicionales: son relativamente baratos, pudiendo provocar limitaciones funcionales en el objetivo similares a las de un sabotaje físico y sin arriesgar vidas humanas, pueden hacerse en remoto y con el mayor sigilo, imposibilitando la alerta previa para los sistemas de protección y defensa. También están sujetos a diferentes condicionantes espacio-tiempo: no exigen desplazamientos al área objetivo de fuerzas o agentes y la actividad maliciosa puede mantenerse dilatadamente en el tiempo sin excesivos riesgos para el atacante y en la mayor opacidad para el adversario.

Pero aún hay más. Cualquier acción en represalia contra un agresor requiere de una secuencia en la que, en primer lugar, hay que detectar la agresión para, a continuación, investigar la autoría y, con las pruebas acumuladas, tratar de proceder a la atribución del hecho, como condiciones previas a acciones legales o al ejercicio de la legítima defensa.

Y esto, que en cualquier ámbito del «mundo real» puede alcanzarse con mayor o menor dificultad, en el ciberespacio resulta casi imposible, por la dificultad que encierra ya cada una de las fases por separado. De mi experiencia acumulada tras casi siete años destinado en el Mando Conjunto de Ciberdefensa (ahora, del Ciberespacio), me atrevo afirmar que la atribución solamente puede darse, y no siempre, cuando se cumplen simultáneamente dos condiciones: que el defensor sea muy bueno y el atacante muy malo, referidas bondad y maldad a la capacitación técnica de las personas y los recursos de que disponen.

Tenemos infinidad de ejemplos de campañas de ciberespionaje que han estado activas durante seis, siete y hasta ocho años antes de ser detectadas. Si el atacante está cualificado y cuenta con ciertos recursos, puede resultar imposible para una gran mayoría de las víctimas incluso llegar a conocer que sus sistemas han sido penetrados.

Pero supongamos que existe esa detección y que se procede a investigar el incidente. Por lo general, lo que obtendrá el equipo investigador será, en el mejor de los casos, algunas piezas de *malware* de las que, tras un proceso que puede llegar a ser muy dilatado y complejo, puedan extraer cierta información, como direcciones IP de algún elemento de la infraestructura empleada por los atacantes o etiquetas en algún idioma dejadas por error por los programadores, insuficientes en la mayoría de los casos para

señalar a un determinado actor.

El ataque de WannaCry ocurrió en mayo del 2017. Ha sido el ciberataque más mediático y uno de los más investigados. Y hoy, más de 4 años después, con millares de víctimas repartidas en más de setenta países, aún no se tiene seguridad, más allá de toda duda razonable (que es lo que debería ser exigible para iniciar acciones legales o de legítima defensa), sobre quién fue su autor.

Y, por último, la atribución. El anonimato, la suplantación de identidad o la utilización de infraestructuras de terceros son relativamente fáciles de conseguir en el ciberespacio. Un atacante cualificado emplea sofisticadas técnicas de evasión para mantener el sigilo y ocultar las evidencias de sus acciones. Por tal motivo, carteles como el de la figura 4 o la atribución (¿política?) del ciberataque a Microsoft resultan excepcionales, pues lo habitual es que un altísimo porcentaje de acciones maliciosas en el ciberespacio queden impunes, al ser imposible reunir pruebas suficientes contra el agresor.

Figura 5. Cartel de busca y captura por el FBI de militares chinos acusados de ciberespionaje. Fuente. "China denounces US cyber-theft charges", BBC News. Disponible en: https://www.bbc.com/news/world-us-canada-27477601

Y esto empeora aún más las cosas. Esos Estados que al principio se asomaban sin recato a la zona gris han comprendido hace tiempo que pueden estar tranquilos actuando también en la zona negra, porque, aún en el caso de que fueran detectadas sus acciones, muy difícilmente alguien podría acumular pruebas suficientes para apuntarles con el dedo acusador.

Es principalmente por este motivo por el que el ciberespacio se convierte en el campo de actuación preferido de la amenaza híbrida, pues en él se llevan a cabo las principales actividades que soportan su forma de enfrentarse a un adversario, que son los ciberataques, la desinformación y la propaganda, que permiten al agresor erosionar de forma reiterada a su objetivo sin rebasar nunca el umbral que pueda desembocar en un conflicto armado o permita desencadenar acciones de represalia por parte del Estado víctima (Figura 6).

Figura 6. Principales campos de actividad de la amenaza híbrida. Fuente. Elaboración propia.

Todo ello se traduce, por una parte, en una elevada impunidad de las acciones ofensivas en y a través del ciberespacio, y, por otra, a que en este ámbito resulte muy poco eficaz la disuasión, al fallar una de sus principales dimensiones: la disuasión por represalia, lo que implica que a los defensores no les queda otra que apostarlo todo a la dimensión restante: la disuasión por negación; es decir, a dificultar al máximo el éxito del potencial adversario a través de la potenciación de la protección, la defensa y la resiliencia de los sistemas.

Por lo tanto, y resumiendo este apartado, la ciberguerra y el ciberespionaje presentan innumerables ventajas frente a sus contrapartes convencionales o tradicionales, especialmente en términos de eficacia-coste, riesgo, abanico de acciones posibles y espectro de objetivos alcanzables, a lo que se suma la ausencia en la práctica de

condicionantes éticos, políticos o legales (para determinados Estados) que deriva de la enorme dificultad de la atribución de las acciones.

Para qué

Veamos ahora qué es lo que buscan esos Estados a través de los ciberataques. En el informe *Ciberamenazas y Tendencias Edición 2020*, publicado por el Centro Criptológico Nacional (CCN), se analizan los principales objetivos y finalidades que persiguen los denominados actores Estado.

Como se puede ver en la figura 7, extraída del citado informe, sus objetivos lo abarcan todo: Sector público, infraestructuras críticas, empresas y hasta ciudadanos.

Y las motivaciones se centran, principalmente, en el espionaje y el sabotaje. Es decir, en la obtención de información del adversario y en el daño dirigido a infraestructuras o servicios.

Figura 7. Principales objetivos y formas de actuación de los actores-Estado en el ciberespacio. Fuente. *Informe Ciberamenazas y Tendencias Edición 2020*, CCN.

Empecemos por el ciberespionaje. Los Estados tienen necesidades de información de todo tipo: sobre los planes e intenciones de una potencia rival o competidora en alguna dimensión (militar, económica, tecnológica), sobre el estado de alianzas o pactos entre Estados, sobre capacidades o desarrollos científicos o tecnológicos, sobre armamento…

Para obtener esta información, los Estados (y organizaciones, empresas y personas) han recurrido a diversas técnicas a lo largo de la Historia, dando lugar a diferentes disciplinas de la inteligencia en función del método de obtención: HUMINT, SIGINT, COMINT, TECHINT, OSINT…

El hecho de que hoy en día la mayor parte de los datos y de la información se almacene, procese y maneje en formato digital y en o a través de sistemas de información y telecomunicaciones ha ido focalizando el esfuerzo de obtención de los Estados hacia el ciberespacio, en lo que se ha dado por llamar CYBINT, en detrimento de los otras disciplinas de obtención, por lo general más caras, con menor índice de éxito y con mayor riesgo de ser descubiertas o neutralizadas.

En la Figura 8 se muestra la que, a juicio de muchos analistas, es la mayor transferencia tecnológica de la historia, en forma de cientos de terabytes de información. Y, de ser ciertas las sospechas, sin consentimiento (ni conocimiento) por parte del proveedor. China habría pasado así del cazabombardero de tercera generación al de quinta, sin pasar por la cuarta, presumiblemente ahorrándose miles de millones de yuans en I+D.

Figura 8. Cazabombarderos de 5ª generación J31 (arriba) y F35 (abajo), fabricados por China y EE. UU., respectivamente. Fuente. Disponible en: https://es.daydaynews.cc/international/97834.html

En lo que respecta a los ciberataques, su utilización está enfocada, principalmente, a la degradación, paralización o destrucción de infraestructuras o servicios. Un actor amenaza encuadrado en el grupo del crimen organizado buscará algún tipo de beneficio económico (lo más habitual, mediante la exigencia de un rescate para revertir los efectos del ataque). Un actor *hackivista* buscará réditos a través de la repercusión en los medios que dé notoriedad a sus reivindicaciones. Tras un ciberataque llevado a cabo por un actor Estado puede haber otras muchas motivaciones, sin descartar las anteriores: posicionarse sigilosamente para actuar en el futuro, destruir infraestructuras de valor militar en caso de conflicto armado, provocar confusión, caos o desmoralización en la población del Estado adversario, infligir daños a la reputación o credibilidad de la víctima, debilitar la confianza en las instituciones, destruir elementos estratégicos que puedan suponer una amenaza potencial… hasta manipular resultados electorales para apoyar al candidato más afín a los intereses del Estado agresor.

Como se ha señalado anteriormente, es muy probable que numerosos Estados hayan ejecutado ya los pasos previos necesarios para posicionarse en infraestructuras críticas de potenciales adversarios para, llegado el momento oportuno, activar el *malware* para degradar o inutilizar esas infraestructuras y los servicios esenciales a ellas asociados.

Numerosos informes demuestran que, en su conflicto con Ucrania, Rusia ha empleado de forma profusa los ciberataques contra infraestructuras militares (por ejemplo, sistemas de telecomunicaciones y de mando y control), pero también contra infraestructuras críticas, como estaciones de la red eléctrica o aeropuertos.

El ejemplo más notable de destrucción de elementos estratégicos que puedan suponer una futura amenaza es Stuxnet, nombre dado tanto a la campaña como al *malware* empleado en el ataque contra la planta de Natanz en el año 2010, que se tradujo en la destrucción de cientos de centrifugadoras de enriquecimiento de uranio y en el consecuente retraso, estimado entre uno y dos años, infligido al programa nuclear iraní.

En lo referente a desinformación, no hay duda de que los rusos son los maestros, pero no los únicos que la practican. Muchos Estados, ante la evidencia de la rentabilidad y efectividad de estas campañas, se han dotado de capacidades para ello. En el año 2019, se estimaba en torno a 70 el número de Estados que llevaban a cabo actividades de influencia y desinformación en Internet. Veamos un par de ejemplos ilustrativos.

En el año 2018, se produjo la difusión de una falsa noticia según la cual un grupo de

soldados alemanes desplegados en Lituania habían violado a varias mujeres locales. Las tropas alemanas, desplegadas en el marco del apoyo de la OTAN a las repúblicas bálticas con fines disuasorios frente a Rusia, se encontraron con un tan injusto como inesperado rechazo de la misma población a la que su despliegue pretendía proteger. La noticia tuvo un impacto tremendo y obligó a la OTAN a un considerable esfuerzo de comunicación estratégica para desmentirla y neutralizar sus efectos negativos.

También existen evidencias contrastadas de que Rusia participó en la difusión de noticias falsas en apoyo a independentismo catalán. Su interés en esta crisis no era otro que erosionar a un Estado miembro de la OTAN agravando sus problemas internos, otra de las bases sobre las que se asienta la guerra híbrida.

Resumiendo, ¿para qué? Pues para obtener información de todo tipo que pueda suponer una ventaja (política, económica, militar, tecnológica…) para el Estado agresor, para sabotear infraestructuras o servicios, alterar resultados electorales, dañar la reputación de los adversarios, provocar caos y confusión, minar la moral de la población o exacerbar los conflictos internos de sus adversarios a través de la desinformación, la influencia y la propaganda. ¿Y cómo lo hacen?

Cómo

La siguiente figura muestra la secuencia de un ciberataque complejo. La que llevaría a cabo un actor-Estado, con fines de ciberespionaje o sabotaje.

En una primera etapa, reconocimiento, se trata de obtener la máxima información posible del objetivo: identidad de personas y cargos, direcciones de correo electrónico, relaciones, direcciones IP, sistemas operativos, aplicaciones *software*, protocolos, elementos de defensa perimetral… Tanto para esta como para el resto de fases hay técnicas y herramientas específicamente desarrolladas. Mucha de esta información puede obtenerse por medios pasivos, sin alertar a la víctima. También es muy frecuente que los atacantes se apoyen en técnicas de ingeniería social.

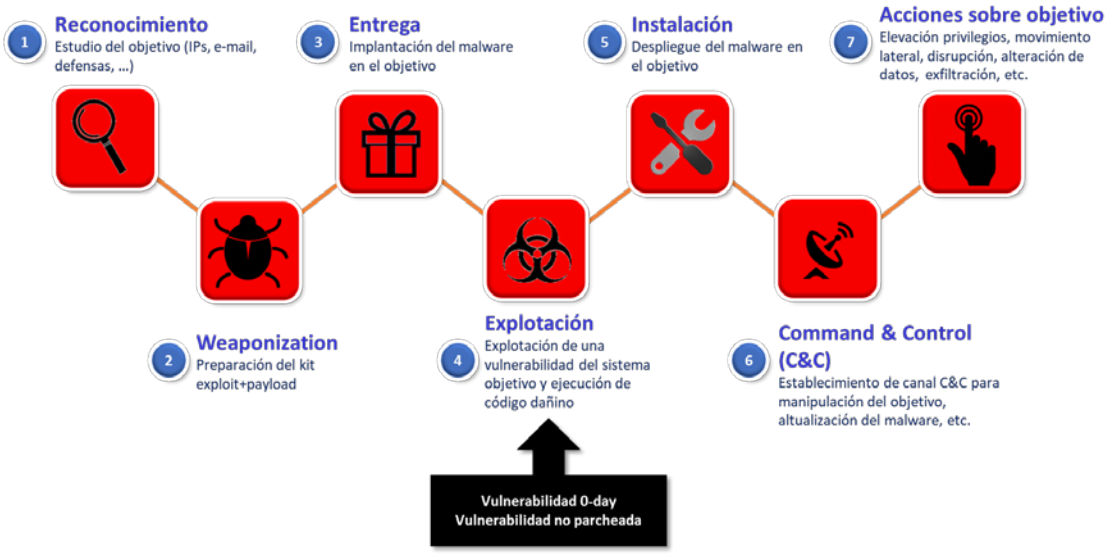

Figura 8. Fases de un ciberataque complejo (*killchain*).

Con la información obtenida en la fase anterior, los atacantes identifican las vulnerabilidades explotables y preparan una «ciberarma» a medida del objetivo. Básicamente, se trata de desarrollar el conjunto *exploit* + *payload*: piezas de *software* específicamente diseñadas para, sin ser detectados, explotar una vulnerabilidad identificada que permita sobrepasar el perímetro y ejecutar las acciones posteriores una vez dentro del sistema, respectivamente.

La entrega es una parte clave del ataque, siendo lo habitual que se apoye en técnicas de ingeniería social, correos de *phishing* o a través de la infección de algún dispositivo con acceso al sistema; por ejemplo, una memoria USB. Esta última técnica fue la empleada para infectar con el *malware* «agent.btz» los sistemas del departamento de Defensa de los EE. UU. en el año 2007, por el sencillo procedimiento de abandonar una memoria USB en el aparcamiento de una unidad perteneciente al US Central Command, memoria que fue conectada a la red de propósito general del DoD por la persona que la encontró. No obstante, la técnica más empleada, por su demostrada efectividad, es la que combina la ingeniería social, el *phishing* y el *spoofing*: correos electrónicos de alta credibilidad, dirigidos a miembros concretos de la organización víctima, en los que se suplanta la identidad del remitente, para todo lo cual se emplea la información obtenida en la fase de reconocimiento. También es frecuente que los atacantes empleen a personas de la propia organización objetivo, los denominados *insiders*, a los que captan por medio del soborno o el chantaje. Para asegurar que la entrega se produce, es posible

que se utilicen varios de estos métodos simultáneamente, aunque con ello también se incrementa el riesgo de ser detectados.

Una vez introducido el *malware* en el sistema objetivo, éste se ejecuta aprovechando alguna vulnerabilidad descubierta en la etapa de reconocimiento. Comienza entonces la instalación de elementos, como ocurre con cualquier *software*, si bien en este caso de forma absolutamente sigilosa, indetectable tanto para el usuario legítimo como para los elementos de protección del sistema. Elementos típicos de este *malware* son capturadores de pantalla o de teclado, activadores de micrófonos o cámaras web, recolectores de archivos en función de su extensión (.doc, .pdf, etc.), archivos que, posteriormente, otros elementos del software empaquetan, trocean, cifran y envían al exterior, enmascarados entre las conexiones legítimas del sistema.

Al mismo tiempo, se establecen las comunicaciones que permiten el control remoto, tanto del elemento infectado como del *malware* instalado, posibilitando a los atacantes su actualización y asegurando su persistencia.

Los siguientes pasos son la escalada de privilegios, mediante la cual los atacantes adquieren progresivamente los de administrador y de administrador de dominio, llegando a alcanzar en muchas ocasiones un control del sistema muy similar al de sus administradores legítimos. Mediante el desplazamiento lateral y la colonización sigilosa del sistema, se posibilitan las acciones posteriores en función de los intereses del atacante: robo de información, denegación de servicios, alteración de datos, etc.

Pero no toda la actividad de los actores Estado se desarrolla en esos parámetros de complejidad y sigilo. Hay diversos tipos de ataque que pueden producir efectos interesantes para un actor Estado y que requieren mucha menor cualificación técnica y recursos poco sofisticados.

Un tipo de ataque muy efectivo contra servicios expuestos a Internet es la denegación de servicio. Básicamente, se trata de inutilizar o degradar la funcionalidad de un activo por saturación. Hasta hace unos años, se utilizaban *botnets* para ello. Hoy en día, mediante técnicas de amplificación y reflexión y empleando masivamente dispositivos del Internet de las Cosas, han llegado a alcanzarse intensidades superiores a 2 Terabytes por segundo, contra las que las defensas perimetrales poco pueden hacer. La campaña contra Estonia en el año 2007, llevada a cabo por «ciberpatriotas» rusos, empleó de forma profusa este tipo de acciones para provocar el caos en la pequeña república báltica

y dejarla prácticamente *off-line* durante varias semanas.

Hay otra modalidad de ataque, el *defacement* o alteración del aspecto o contenido de un sitio Web, que se emplea profusamente para dañar la reputación del objetivo. Viene a ser algo así como un grafiti digital. Aunque está más asociada al *hackivismo* (activismo en la red), también está siendo empleada por actores Estado en el marco de campañas híbridas.

En cuanto a las campañas de desinformación, es mucho lo que se ha escrito sobre este tema en los últimos años. En realidad, es algo que los Estados llevan haciendo siglos, pero que, de la mano de las nuevas tecnologías y, sobre todo, de la expansión y evolución de Internet, ha experimentado un tremendo salto cualitativo y cuantitativo.

El informe *The Fake News Machine*[2], elaborado en el año 2017 por la empresa Trend Micro, publicaba los precios en el mercado de servicios de manipulación de la opinión pública, de los cuales extraigo algunos muy ilustrativos:

- Artículo falso de 800 palabras: 30€.
- Vídeo en página principal de YouTube durante 2 minutos: 550€.
- Comprar 2500 seguidores en Twitter para que retuiteen: 25€.
- Hundir a un periodista a través de artículos negativos con 50 000 *retuits* cada uno, durante cuatro semanas: 50 000€.
- Organizar una manifestación sobre un hecho que nunca ha ocurrido, con soporte en redes sociales y 40 000 *likes* en Facebook: 180 000€
- Influir en las elecciones en una campaña de 12 meses de duración con noticias falsas creadas en dos *websites* con contenido cruzado, contenido patrocinado en Facebook y un ejército de *bots* que lleven ese mensaje falso a los no-conversos: 360 000€.

Existen fuertes sospechas, cuando no evidencias, de que este tipo de actividades han tenido mucho que ver con los inesperados resultados en algunos procesos electorales en los últimos años, tales como las elecciones a la presidencia de los EE. UU. o el referéndum sobre el Brexit, ambos acontecidos en el año 2016.

En un artículo publicado en la prestigiosa revista *MIT Review Technology*, los

[2] Disponible en: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf?_ga=2.117063430.1073547711.1497355570-1028938869.1495462143

investigadores John Kelly and Camille François[3] exponían los resultados de su investigación sobre el impacto de las redes sociales en las elecciones que llevaron al candidato Donald Trump a ocupar la Casa Blanca. En el modelo 3D de la parte izquierda de la Figura 9, cada burbuja representa una cuenta de Twitter. Su tamaño expresa el número de seguidores y tienen asignados colores en función de la temática. Aparentemente, la distribución es bastante homogénea. Sin embargo, si se analiza desde el punto de vista de la campaña electoral (parte derecha de la Figura 9), la cosa cambia. La parte horizontal se corresponde con el apoyo al candidato Donald Trump, siendo el extremo izquierdo el de las cuentas de Twitter de sus partidarios acérrimos y el derecho el de sus opositores más radicales. En el eje vertical se representa la actividad de las cuentas. Como puede verse, la máxima actividad corresponde a las posiciones más extremas, siendo casi nula la de la parte intermedia.

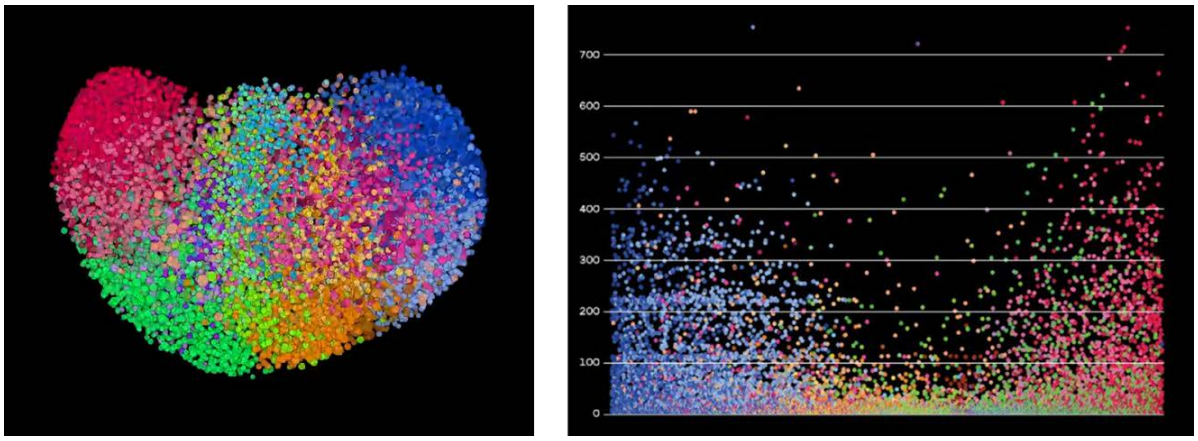

Figura 9. Análisis de la actividad de Twitter durante la campaña para las elecciones a la presidencia de los EE. UU. del año 2016. Fuente. Disponible en: https://www.technologyreview.com/s/611807/this-is-what-filter-bubbles-actually-look-like/

Esta situación evidencia tanto una enorme polarización como una tremenda radicalización, que se fue agudizando a medida que avanzaba la campaña. El informe atribuye parte de ese efecto a las campañas de manipulación de la opinión pública llevadas a cabo por agencias extranjeras y explica cómo los ejércitos de *trolls* atribuidos a Rusia exacerbaron esa polarización: en lugar de actuar sobre la corriente general, se dedicaron a actuar sobre infinidad de grupúsculos de ideología contraria, introduciéndose en ellos mediante cuentas de perfiles falsos, pero dotados de gran credibilidad. Los

[3] Disponible en: https://www.technologyreview.com/s/611807/this-is-what-filter-bubbles-actually-look-like/

operadores que gestionaban estas cuentas se ganaban la confianza de la comunidad e iban provocando divisiones y moldeando la opinión de sus componentes, introduciendo nuevos puntos de vista, empleando de forma profusa la difamación y las falsas narrativas, siempre con un lenguaje adaptado cada comunidad, alimentando sus particulares obsesiones y exacerbando sus fobias, en persecución de su objetivo final de encumbrar y ensalzar a un candidato y destruir la reputación del otro.

Las nuevas tecnologías se están incorporando rápidamente a estas actividades de desinformación, automatizando los procesos y, al mismo tiempo, tratando de hacerlas más creíbles y convincentes. Así, se tiene ya constancia de que se está empleando la inteligencia artificial en apoyo a los ciberataques y técnicas avanzadas de simulación, como *deep fake*, para la manipulación de fotografías o vídeos empleados en campañas de desinformación.

Resumiendo este apartado, la panoplia de acciones que se pueden ejecutar contra un adversario en y a través del ciberespacio es muy variada: ciberataques complejos, tanto para el ciberespionaje como para el sabotaje de infraestructuras críticas; denegación de servicios expuestos en Internet; alteración de páginas web, o campañas de manipulación en redes sociales, incorporando progresivamente nuevas tecnologías para incrementar su eficacia.

Quién

¿Y quiénes hacen todo esto?

La imagen que se ha construido en el imaginario universal a partir de series de televisión y *best sellers* sobre las personas tras este tipo de acciones nos lleva a evocar a individuos aislados, por lo general muy jóvenes, enfundados en sudaderas con capucha, que teclean código a velocidad de vértigo y que consiguen resultados inmediatos, saltándose en unos segundos todas las barreras que protegen el sistema objetivo. Nada más lejos de la realidad.

En la Figura 10 está representado el «ecosistema» de las ciberamenazas. La parte más baja y numerosa corresponde a los *script kidies* y *wanabees*, actores con baja cualificación y escasos medios, por lo general muy jóvenes, capaces solamente de explotar de forma limitada vulnerabilidades muy conocidas.

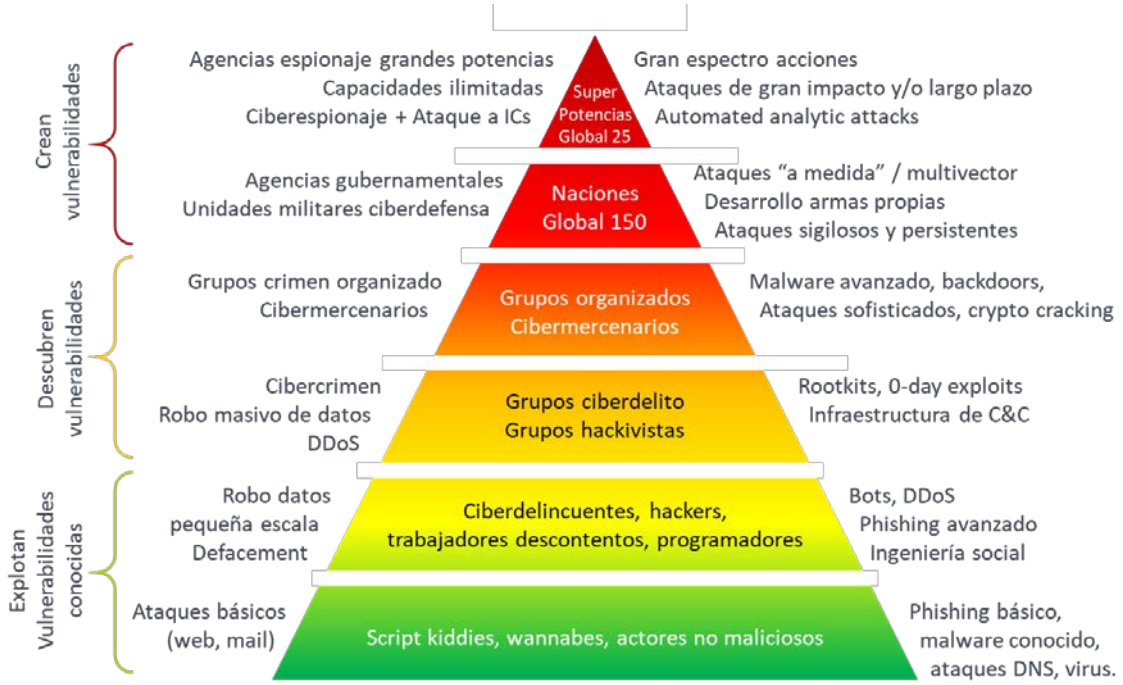

Figura 10. Ecosistema de las ciberamenazas. Fuente. Elaboración propia a partir de varias fuentes.

A medida que se asciende en la pirámide, los actores van creciendo en cualificación, medios y organización, lo que amplía su espectro de actividad. Gran parte de la zona intermedia tiene como motivación el beneficio económico.

En este heterogéneo ecosistema, las unidades de ciberespionaje y ciberguerra que trabajan al servicio de los Estados ocupan un lugar muy destacado, correspondiendo la cúspide a las superpotencias, entre las que se incrustan algunos Estados de menor peso (Irán, Israel, Corea del Norte) que han apostado fuerte por dotarse de estas capacidades.

Estas unidades se conforman como grupos multidisciplinares y con importantes recursos, vinculados a las grandes agencias gubernamentales de inteligencia o a organizaciones militares. Desde hace años, a este tipo de equipos se les denomina Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés). Estos grupos analizan cuidadosamente sus objetivos y llevan a cabo ataques extraordinariamente sigilosos y muy dirigidos. Dado que su fin habitual suele ser el espionaje, su actividad exige permanecer en la red objetivo el máximo tiempo posible sin ser detectados, para lo cual emplean técnicas de evasión avanzadas.

La mayoría de las unidades adscritas a organizaciones militares y a agencias de inteligencia estatales están constituidas por personas que, por su propia pertenencia a tales organizaciones, no son otra cosa que funcionarios al servicio del Estado en

cuestión.

Esta naturaleza funcionarial de los integrantes de estos equipos, desde los desarrolladores de *software* a los analistas que trabajan sobre la información obtenida, proporciona algunos hilos de los que tirar a los investigadores de ciberataques complejos. Así, por ejemplo, los horarios de compilación de las piezas de *malware* empleadas en una campaña permiten establecer con cierto grado de precisión el huso horario de la ubicación desde la que se trabaja. La campaña de ciberespionaje Red October, una de las más importantes de las descubiertas en los últimos años, se atribuyó a Rusia porque los horarios de compilación de la mayoría de las piezas de *malware* analizadas correspondían al período de 8 de la mañana a 5 de la tarde en el huso horario GMT+3, que es el de Moscú, donde se encuentran ubicadas las principales ciberunidades rusas, tanto en el plano militar como en el de la inteligencia.

La organización interna de un actor Estado tipo APT viene muy determinada por las fases de la *killchain*. Se tiende a pensar que los *hackers*, término generalmente aplicado a los expertos en penetrar sistemas, poseen una amplia gama de conocimientos que les permite trabajar la secuencia completa de un ciberataque. Esto es muy poco habitual, máxime si el ataque es muy complejo o el objetivo está bien defendido y es importante el sigilo. El altísimo grado de especialización requerido por cada actividad lleva a que se utilicen equipos de expertos para cada una de las etapas, que han de trabajar muy coordinados entre sí.

Para la fase de reconocimiento, el equipo ha de contar, como mínimo, con analistas de inteligencia, ingenieros sociales y *pentesters*. Con la información obtenida a lo largo del proceso, cuya duración puede estimarse entre semanas y meses, los desarrolladores de *software* tendrán que trabajar codo con codo con los expertos en vulnerabilidades con el fin de identificar la forma más efectiva de penetrar el objetivo y adecuar el código a las acciones que pretendan llevarse a cabo sobre la red objetivo. El *software* desarrollado debe incorporar fuertes medidas para dificultar tanto el análisis forense como la ingeniería inversa, por lo que es muy habitual que el código esté ofuscado y encriptado, lo que implica la necesidad adicional de expertos en estos campos.

La información obtenida en la fase de reconocimiento permitirá también decidir la forma de entrega más adecuada, en la que participarán ingenieros sociales, especialistas en técnicas de *phishing* o agentes de campo, según el caso.

Una vez que el *malware* se ha introducido en la red, expertos en sistemas han de llevar a cabo el control remoto, la escalada de privilegios y la expansión sigilosa. En cuestión de horas o pocos días, comenzarán a obtenerse los primeros resultados.

En el caso del ciberespionaje, se traducirá en la llegada masiva de documentos, que deberán ser convenientemente analizados por personal experto en las materias en cuestión. Dado que, en este caso, por lo general, los atacantes persiguen resultados a largo plazo, el objetivo es permanecer en la red el máximo tiempo sin ser descubiertos, por lo que será fundamental para ellos asegurar la persistencia y habrán de estar muy atentos a posibles acciones de los administradores del sistema víctima que puedan ser indicio de que han sido descubiertos. En este caso, activarán de inmediato las técnicas de evasión que les permitan abandonar el sistema sin dejar trazas que puedan ser empleadas por los investigadores para una posible atribución.

Si el objetivo es una infraestructura, lo único que cambia es la parte correspondiente al procesado de información, que en este caso no es necesaria. Si lo que se pretende es únicamente estar posicionado para llevar el ataque en el momento que se den unas condiciones concretas (por ejemplo, estallido de un conflicto armado) los atacantes tan solo deberán estar atentos a posibles actualizaciones o modificaciones de la red penetrada que puedan provocar la desactivación del *malware* insertado.

Hablamos, pues, de equipos constituidos por entre 10 a 30 personas por campaña. Como es obvio, en el caso de que estos grupos trabajen en régimen de 24/7 o se desarrollen varias campañas de forma simultánea, los recursos habrán de multiplicarse convenientemente.

Por otra parte, al estar integrados estos grupos, por lo general, en organizaciones militares o agencias de inteligencia estatales, tampoco resulta necesario que todos los recursos implicados en una campaña tengan carácter orgánico. Así, si se considera que en determinadas acciones precursoras deban intervenir agentes de campo o equipos de operaciones especiales, estos pueden ser proporcionados por otros departamentos de la agencia o por otras unidades militares. Y lo mismo ocurre, por ejemplo, con el análisis y procesamiento de toda la información obtenida, que será por lo general llevada a cabo por otros departamentos con personal experto en esas lides y que son los que tendrán que explotar en beneficio de la organización (y del Estado) la ingente información que se puede llegar a obtener en una campaña de ciberespionaje prolongado.

Debe existir, además, una vía de realimentación que permita a estos dirigir al equipo atacante a las áreas de mayor interés. Así, por ejemplo, un atacante que se introduzca en una red de una organización adversaria de defensa seguramente concentrará sus esfuerzos en la obtención de información relativa a operaciones, planificación, programas de armamento o relaciones internacionales, obviando las áreas departamentales que no sean de su interés.

También hay que tener en cuenta que estos grupos no actúan de forma autónoma, sino que requieren de una dirección superior que establezca los objetivos a alcanzar, plazos, recursos utilizables, etc. En el ámbito militar, lo lógico es que estén integrados en la estructura de inteligencia y de *targeting* conjunto y que su actividad esté planificada y sincronizada con las actividades en otros ámbitos operacionales.

Del mismo modo, en el caso de acciones encuadradas en una campaña híbrida, la actividad de los grupos APT deberá estar coordinada y sincronizada con la que se desarrolle en otros campos: desinformación, activismo, apoyo puntual a grupos disidentes del Estado víctima, acciones diplomáticas, maniobras militares de demostración de fuerza, etc.

Para toda esta actividad, tanto en el caso de ciberespionaje como en el de ataque a infraestructuras, los atacantes deberán contar con una infraestructura debidamente anonimizada y volátil, pues deberá ser renovada cada poco tiempo y, llegado el caso, desvanecerse. Ello implica la necesidad de cierto recurso económico, preferiblemente en criptomoneda, que permita la adquisición de máquinas y servidores, sin dejar trazas en el proceso.

Se sospecha que muchos actores Estado obtienen financiación a través de actividades propias del crimen organizado (por ejemplo, mediante campañas de *ransomware*). También se ha observado en los últimos años la aparición de grupos APT que no responden al «modelo funcionarial» y que ofrecen sus capacidades en la modalidad denominada *Crime as a Service* (*CaaS*). Se trata de grupos independientes, organizados de forma similar a la descrita, que de forma eventual actuarían contratados por agencias estatales para llevar a cabo una campaña concreta.

A continuación, se presentan, a modo de cata, algunas de las principales APT que operan actualmente en el mundo. Todas ellas reciben diversas denominaciones, que les han sido atribuidas por diferentes empresas dedicadas a la inteligencia de ciberamenazas.

Empecemos por APT1, una de las más activas, si no la que más, y que múltiples agencias vinculan desde hace años con la Unidad 61398 del Ejército chino. Se le atribuyen ataques a más de un millar de organizaciones y empresas de más de cien países, en su mayoría enfocados al espionaje industrial. En el informe elaborado por la empresa Mandiant en el año 2013 se llegaba a especificar la localización física desde la que operaban, y su encuadramiento orgánico dentro del Ejército Popular de Liberación.

El Lazarus Group, que se cree que opera desde Corea del Norte, es uno de los grupos que más notoriedad han alcanzado en los últimos años. Saltaron a la fama en el año 2014 tras el ataque contra la empresa Sony.

Durante sus primeros años, se especializaron en ataques contra el sector financiero y la banca. Es posible que comenzaran siendo un grupo de crimen organizado que buscaba únicamente el beneficio económico, si bien en los últimos años sus objetivos parecen coincidir cada vez más con los del gobierno de Corea del Norte.

Muchos analistas les atribuyen la autoría del famoso virus WannaCry que causó el caos en todo el mundo en el año 2017, con fines que aún no están muy claros, y, como resultado de diversos procesos, algunos de sus miembros están en busca y captura por el FBI.

Fancy Bear, también conocido como APT 28 y Sofacy, es uno de los grupos rusos más activos y conocidos. Se cree que opera principalmente desde Moscú y su actividad se enfoca, sobre todo, al ciberespionaje. Muchos analistas lo consideran integrado o vinculado al Servicio de Inteligencia ruso (GRU).

Entre sus objetivos se encuentran agencias gubernamentales, empresas de los sectores aeroespacial, defensa, energía y administraciones públicas de un gran número de países, fundamentalmente estados miembros de la OTAN o transcaucásicos.

Hay también informes que vinculan la actividad de Fancy Bear con la de APT 29, otro de los más conocidos grupos rusos. Según estos informes, ambos grupos coordinarían su actividad en función de sus capacidades técnicas.

Equation Group es, sin ninguna duda, el grupo APT más sofisticado y poderoso del mundo. Se le vincula a la superpoderosa Agencia de Seguridad Nacional de los Estados Unidos, la NSA.

Está especializada en ciberespionaje, si bien se le atribuyen algunas acciones contra

infraestructuras críticas. Supuestamente, son los creadores de algunos de los *malwares* más sofisticados que se han conocido, como Stuxnet y Flame.

Se cree que las ciberarmas puestas a subasta en 2016 por el grupo autodenominado Shadow Brokers fueron robadas a la NSA.

Las campañas atribuidas a Equation Group son muy pocas en comparación con las que se vinculan a las APT rusas, iraníes o norcoreanas y no digamos ya si se compara con la frenética actividad desplegada por las APT chinas. El analista Antonio Villalón, director de seguridad de la empresa valenciana S2 Grupo, considera que tal circunstancia se explica por dos motivos: el primero, por la calidad de las campañas llevadas a cabo por los EE.UU. que da lugar a que gran parte de ellas no sean detectadas; la segunda, porque el cuasimonopolio mundial ejercido por las sus empresas (Microsoft, Apple, Google, Oracle, Cisco…) en lo referente a sistemas operativos, *software* de base, elementos de comunicaciones y servicios en red hace que EE. UU. no requiera desarrollar *malware* puesto que ya tiene acceso a los *drivers*[4].

Y, para terminar, Rocket Kitten. Un grupo iraní con aún escaso recorrido, pero al que se le atribuyen algunas acciones interesantes en el terreno del ciberespionaje, principalmente contra los EE. UU., Israel y estados vecinos, así como una importante actividad interior focalizada en organizaciones y ciudadanos notables contrarios al gobierno. Resumiendo el quién: grupos multidisciplinares, dotados de importantes recursos, asociados a las grandes agencias de inteligencia o a unidades militares, si bien en los últimos años se han detectado algunos grupos organizados independientes que ofrecen sus servicios a esas organizaciones.

Epílogo

El lector puede haber interpretado (erróneamente) la oposición del autor hacia este tipo de unidades. En absoluto. El contar con unidades de ciberinteligencia y ciberguerra (entendiendo como tales aquellas capaces de llevar a cabo acciones ofensivas en o a través del ciberespacio en el contexto de una operación militar) no debe verse diferente de contar con unidades de inteligencia HUMINT o unidades navales con armamento ofensivo, por ejemplo. El hecho de que determinados Estados estén haciendo un uso

[4] VILLALÓN HUERTA, Antonio. *Amenazas Persistentes Avanzadas*. Nau Llibres. Valencia. 2016.

indebido de este tipo de unidades, explotando las zonas grises o incluso actuando completamente fuera de la ley, no implica que debamos demonizarlas y hasta renunciar a ellas. Sería algo así como si renunciáramos a poseer fragatas por el hecho de que determinados Estados las estuvieran utilizando para la piratería.

Es más, para un Estado, el contar con unidades especializadas para operar en el ciberespacio rival resulta hoy en día absolutamente necesario. Es la única forma de lograr cierta capacidad de disuasión y de optar, en caso de conflicto armado, a alcanzar al menos la paridad si el adversario también cuenta con capacidades ofensivas. Como se ha señalado anteriormente, la superioridad en el ciberespacio de una de las partes puede desnivelar la contienda a su favor, incluso en el caso de que el adversario sea superior en el resto de ámbitos operacionales.

Pero, por supuesto, la utilización de estas capacidades ha de hacerse siempre bajo los parámetros de la legalidad vigente y con las mismas garantías, controles y limitaciones que aplican para el resto de capacidades militares y de inteligencia del Estado, sea cual sea su ámbito de actuación.

*Enrique Cubeiro Cabello**
Capitán de Navío (reserva)

Bibliografía

BENDIEK, Annegret; METZGER, Tobias. *Deterrence theory in the cyber-century.* 2015.

Centro Criptológico Nacional (CCN). *Informe Ciberamenazas y Tendencias Edición 2019.*

Centro Criptológico Nacional (CCN). *Informe Ciberamenazas y Tendencias Edición 2020.*

CHERTOFF, Michael & CILLUFFO, Frank J. *Choosing to lead. American Foreign Policy for a Disordered World. Chapter 20: A strategy of cyber deterrence.* 2015.

FireEye. *Anatomy of Russia's 2016 Influence Operations: Hacks, Leaks, and the Manipulation of Political Opinion.* 2017.

FireEye. *APT28: A window into Russia's Cyber Espionage Operations?* 2014.

Kaspersky Lab. *Equation Group: The Crown Creator of Cyber-Espionage.* 2015.

Kaspersky Lab. *Operation "Red October".* 2013.

Kaspersky Lab. *Russian-speaking APTs Turla and Sofacy share malware delivery scheme and overlap some targets in Asia.* 2018.

KELLY, John y FRANÇOIS, Camille. *This is what filter bubbles actually look like.* MIT Review Technology. 2018. Disponible en: https://www.technologyreview.com/s/611807/this-is-what-filter-bubbles-actually-look-like/

LAN, Tang; XIN, Zhang; RADUEGE JR., Harry D.; GRIGORIEV, Dmitry I., DUGGAL, Pavan y SCHJØLBERG, Stein. *Global Cyber Deterrence. Views from China, the U.S., Russia, India, and Norway*. 2016.

LEE HSIANG WEI, Maj. *The Challenges of Cyber Deterrence.* 2015.

LIBICKI, Martin C. *Cyberdeterrence and cyberwar.* 2009.

Mandiant. *APT1. Exposing one of China´s Cyber Espionage Units.* 2013.

NATO Strategic Communications Centre of Excellence. *Russia's Strategy in Cyberspace.* 2021.

RICARDO TORRES SORIANO, Manuel. *Los dilemas estratégicos de la ciberguerra.* 2014.

SCHMITT, Michael N. *Grey Zones in the International Law of Cyberspace.* 42:2 Yale Journal of International Law Online 1 (2017). Publicado el 30 de mayo de 2018. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180687#

SIERS, Rhea. *The Myth of Cyber Deterrence.* 2016.

SORIANO AGUILAR, Joan. *Omniun contra omnes. Análisis político-militar de la guerra en el ciberespacio*. Nau Llibres. Valencia. 2021.

Trend Micro. *The Fake News Machine.* 2017.

TROMP, Joshua. *Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-attacks.* 2010.

VILLALÓN HUERTA, Antonio. *Amenazas Persistentes Avanzadas*. Nau Llibres. Valencia. 2016.

Wikipedia. Diversos artículos.

World Economic Forum. *Global Risk Report 2018.*

World Economic Forum. *Global Risk Report 2019.*

World Economic Forum. *Global Risk Report 2020.*