CIBERINTELIGENCIA, LA VÍA PARA LA CIBERSEGURIDAD

JOSÉ MARÍA BLANCO NAVARRO

DIRECTOR DE CIBERINTELIGENCIA ESTRATÉGICA EN PROSEGUR CIBERSEGURIDAD

RESUMEN

Internet y las Tecnologías de la Información y las Comunicaciones han contribuido decisivamente al desarrollo de nuestras sociedades. Organizaciones, empresas y ciudadanos cuentan con nuevas vías, eficientes, para comunicarse, relacionarse y prestar servicios. Pero a su vez, las nuevas tecnologías son explotadas por delincuentes, terroristas y grupos de crimen organizado, siendo Internet el objetivo de sus actividades, el medio o un facilitador de las mismas. En este marco, las empresas se ven obligadas a adoptar medidas para proteger sus valores: personal, infraestructura, patrimonio, datos e información, procesos de negocio y reputación.

Internet y las TIC se han convertido en un medio para la delincuencia tradicional, a la vez que un habilitador para nuevas actividades criminales. Las tecnologías de la información y comunicación permiten a las organizaciones criminales financiarse, adoctrinar y reclutar, gestionar su logística, blanquear capitales, planear ataques, cometer nuevos y viejos delitos de forma anónima, actuando como emprendedores delictivos en el marco de un modelo de negocio que se ha denominado “crimen como servicio”, sin necesidad de una fuerte infraestructura.

La nueva Estrategia de Seguridad Nacional (ESN) de 2017 es sensible a esta situación. En el capítulo 4, **considera como amenaza la vulnerabilidad del ciberespacio.** Las amenazas en el espacio digital son transversales, sirviendo el ciberespacio como facilitador y potenciador de gran parte del resto de amenazas (terrorismo, conflictos, crimen organizado, espionaje, inestabilidad económica, etc.).

A través de la identificación de las principales tendencias, se mostrará cómo la ciberinteligencia se convierte en la vía hacia la ciberseguridad, detallando su conceptualización, que carece de consenso, su proceso, y sus elementos y metodologías.

Palabras clave: Ciberseguridad, ciberinteligencia, tendencias, ciberespacio, amenazas, riesgos

ABSTRACT

The Internet and Information and Communication Technologies have made a decisive contribution to the development of our societies. Organizations, companies and citizens have new efficient ways to communicate, interact and provide services. But in turn, new technologies are exploited by criminals, terrorists and organized crime groups, with the Internet being the target of their activities, the medium, or a facilitator of them. In this framework, companies are forced to adopt measures to protect their values: personnel, infrastructure, assets, data and information, business processes and reputation.

The Internet and ICT have become a means of traditional crime, as well as an enabler for new criminal activities. Information and communication technologies allow criminal organizations to finance, indoctrinate and recruit, manage their logistics, launder money, plan attacks, commit new and old crimes anonymously, acting as criminal entrepreneurs within the framework of a business model that has been called “crime as a service”, without the need for a strong infrastructure.

The new National Security Strategy (ESN) of 2017 is sensitive to this situation. In chapter 4, it considers the vulnerability of cyberspace as a threat. Threats in the digital space are transversal, serving cyberspace as a facilitator and enhancer of many of the other threats (terrorism, conflicts, organized crime, espionage, economic instability, etc.).

Through the identification of the main trends, it will be shown how cyber-intelligence becomes the path towards cybersecurity, detailing its conceptualization, which lacks consensus, its process, and its elements and methodologies.

Keywords: Cybersecurity, Cyber-intelligence, trends, Cyberspace, threats, risks

1. TENDENCIAS EN CIBERSEGURIDAD

1.1. CONCIENCIACIÓN

El año 2017 resultó positivo en materia de concienciación, con la inestimable ayuda, a este fin, de Wannacry (12 de mayo) y su elevado impacto mediático. Incluso la reacción de Telefónica supuso un importante punto de inflexión en el tratamiento de estos riesgos. No fue el único caso, dado que meses después NotPetya (27 de junio) ponía de nuevo el foco internacional en los ciberataques. A ello se unen brechas de seguridad como la de Equifax, los denominados “Paradise Papers”, los casos Uber, Verizon, y una larga serie de incidentes (Online Trust Alliance, 2018).

Los ataques ejecutados en 2017 han servido para extraer importantes lecciones, que precisan ser incorporadas al acervo de ciberseguridad como “lecciones aprendidas”. El caso Equifax, en el que se expusieron los datos financieros de 143 millones de estadounidenses, muestra cómo las empresas que no protejan a sus clientes se exponen a acciones legales, a sanciones de reguladores y a un elevado impacto reputacional. Una segunda lección, derivada de dicho caso, es la necesidad de reevaluar qué se considera información sensible a proteger.

Wannacry y NotPetya fueron una llamada de atención, con varias enseñanzas: la función de los proveedores, en este caso Microsoft, para mejorar la ciberseguridad (en marzo había publicado actualizaciones que solventaban la vulnerabilidad que posteriormente fue explotada); la responsabilidad compartida entre empresas de tecnología y toda la cadena del sistema, incluyendo a proveedores, resto de *stakeholders*, clientes; y la necesidad de emprender una nueva Convención Digital de Génova, llamada que hizo Microsoft en febrero de 2017 para analizar la situación actual (Microsoft, 2017).

También de interés, a la hora del necesario aprendizaje, tuvieron los ataques de denegación de servicio (DDoS) del 21 de octubre, que afectaron a Amazon, Twitter, Netflix y GitHub, a través de la utilización de una red de bots de internet de las cosas, Mirai (USENIX, 2017).

A pesar de todo ello, el nivel de alerta del usuario (*"user awareness"*) continúa siendo muy bajo, un claro facilitador de la perpetuación de este tipo de ataques, más cuando se estima que en el 95% de los mismos la clave radica en el factor humano.

En el futuro se espera la llegada de nuevos "ciber-huracanes", utilizando el término empleado en el "MMC Cyber Handbook 2018". Cualquier organización debe asumir que va a ser atacada, siendo la única duda en qué momento se producirá dicho ataque.

1.2. REGULACIÓN

Organismos internacionales y Estados comienzan a ser conscientes de los riesgos del ciberespacio. La nueva Estrategia de Seguridad Nacional dedica varias reflexiones acerca de las denominadas amenazas híbridas, aquellas que combinan diferentes formas de ataque, tradicionales y no tradicionales, como los ciberataques o la manipulación de la información. Recoge, de esta manera, uno de los mayores riesgos a los que se están enfrentando las democracias en todo el mundo, procesos de desestabilización promovidos desde el exterior, por actores tanto estatales como no estatales, y que tratan de polarizar y fragmentar nuestras sociedades. Ataques que suponen una amenaza, que pudiera ser de carácter existencial, y que exigen una rápida reacción.

Sobre este tipo de acciones ya existían advertencias, como las de John Arquilla y David Ronfeldt a finales del siglo pasado en *"Networks and Netwars"* (2001) *o en "The Advent of Netwar"* (1996*).* Pero lo que es más llamativo, también lo anunciaron los coroneles chinos Qiaio Liang y Wang Xiang Sui, en su "*Guerra sin límites"* (1999*),* libro dirigido a explicar a sus compañeros de armas las características de la *guerra* moderna. En esa obra detallaban toda una estrategia tendente a derrotar al enemigo sin derramar su sangre, a través del ataque económico o el uso de la información. El objetivo que manifiestan es *"la destrucción estructural del enemigo".* Cualquier cosa puede ser un arma y cualquier individuo un soldado.

Los frentes regulatorios se centran en el conocimiento y registro de los ataques, en la protección de los datos personales y en la generación de estándares. En las XI Jornadas del CCN-CERT (2017), que bajo el lema "Ciberamenazas, el reto de compartir", reunió a cerca de 2.000 profesionales de la ciberseguridad en diciembre de 2017, se hizo un claro diagnóstico de la situación, mostrando una decidida voluntad en afrontar la situación y en devolver al ciudadano parte del poder que el uso de sus datos está generando a organizaciones, delictivas o no. En 2018 está prevista la creación de un Centro de Operaciones de Seguridad de la Administración General del Estado, que permita ofrecer una respuesta "más eficaz" ante las ciberamenazas.

Entre las prioridades en materia de ciberseguridad proteger la privacidad, facilitar el derecho al olvido en la Red, garantizar el honor y la intimidad, así como la defensa de la propiedad intelectual y la detección y defensa ante la desinformación, propaganda y la manipulación informativa.

Aunque en el tema de desinformación algunos sectores señalan que se puede tratar de justificar por esa vía un control de la libertad de expresión y de información, es evidente que se trata de cuestiones diferentes. La diversidad informativa, la existencia de medios con orientación política, y por tanto con sesgos informativos, no es un fenómeno nuevo. Y además es un fenómeno necesario, un pilar básico en un sistema

democrático. Pero en este caso el foco se pone básicamente en ataques desde el exterior, con la clara intención de desestabilizar el sistema democrático.

A todo ello se ha unido el debate sobre el odio en internet y redes sociales, con propuestas regulatorias para identificar a los usuarios (identidad digital). Otra tendencia en materia regulatoria puede ser la adopción de reglas para prevenir el pago de *ransomware*.

La entrada en vigor, en mayo de 2018, de la normativa de la Unión Europea de protección de datos personales, es, posiblemente, la gran revolución en materia regulatoria del año, generando dudas sobre las capacidades para su cumplimiento, gestión y supervisión. Su entrada en vigor va a exigir a las empresas esfuerzos y costes adicionales, en mayor medida en cuanto exista voluntad para actuar correctamente, concienciados sobre la importancia de la protección de los datos y no únicamente como la necesidad de satisfacer un requisito legal más. Las empresas se moverán entre el temor y la desorientación.

Entre sus contenidos destaca:

- La obligación de informar de violaciones de seguridad de datos a las autoridades nacionales, e incluso a los individuos, cuando el daño sea elevado, en un plazo de 72 horas. Su incumplimiento puede suponer multas de un 4% de los ingresos de la compañía (lo que puede poner en riesgo incluso su supervivencia). Marsh & McLennan Companies estima que las multas en el primer año podrían alcanzar los cinco billones de libras. El alto importe de las multas pudiera llegar a incentivar ataques a bases de datos empresariales con finalidad extorsiva.
- Se refuerzan los derechos de los individuos, en el uso de sus datos. Ninguna empresa podrá obtener datos personales sin notificar previamente a los individuos como serán almacenados, protegidos y compartidos con terceras partes. Su consentimiento debe ser libre, específico, informado e indudable, y marcándolo de forma afirmativa. También incluye el derecho al olvido, pudiendo solicitar en cualquier momento que sus datos sean borrados y no utilizados, o incluso su portabilidad.
- La figura del delegado de protección de datos adquiere una enorme relevancia.
- Su impacto sale del ámbito de la propia UE, al intentar involucrar a cualquier organización que obtenga o utilice datos personales de individuos sujetos a la jurisdicción de la UE.
- Las organizaciones están obligadas a realizar evaluaciones de impacto de datos, de carácter previo. No existiendo una cultura empresarial, salvo en ámbitos determinados, de evaluación de riesgos, puede suponer un verdadero quebradero de cabeza, especialmente para PYMES, a pesar del desarrollo de aplicaciones de la AEPD para facilitar el cumplimiento de este requisito, como “Facilita RGPD”.

Por otro lado, la Directiva de Seguridad de redes de Información (NIS- Network Information Security, 2016), que debería tener efecto en 2018, impone obligaciones a los Estados y operadores de infraestructuras: disponer de una estrategia de ciberseguridad, una autoridad competente nacional, existencia de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), e identificación por los Estados de los

Operadores de Servicios Esenciales (OSE) y los Proveedores de Servicios Digitales (PSD) establecidos en su territorio para cada sector. España aún no ha aprobado la trasposición interna que la UE fijó con fecha 9 de mayo como límite, aunque ya dispone de un borrador de Anteproyecto de Ley sobre la Seguridad de las Redes y Sistemas de Información. El Anteproyecto ha sido ya informado por el Consejo Nacional de Ciberseguridad, ha incorporado aportaciones del proceso de consulta previa y prosiguió su tramitación mediante la apertura del período de audiencia pública que se extendió hasta el 8 de enero de 2018.

Como efecto de la señalada concienciación, la Unión Europea ha desarrollado una intensa labor en los últimos meses de 2017, con medidas de gran calado, proponiendo reforzar la resiliencia, la disuasión y la respuesta de la UE a los ciberataques mediante:

- Establecimiento de una Agencia de Ciberseguridad de la Unión Europea más sólida, basada en la Agencia para la Seguridad de las Redes y la Información (ENISA), para ayudar a los Estados miembro a abordar los ciberataques (Parlamento Europeo, 2018).
- Creación de un esquema de certificación de ciberseguridad en toda la UE, que aumente la ciberseguridad de los productos y servicios en el mundo digital. La Comisión propone la creación de un marco europeo de certificación de ciberseguridad que se espera que ofrezca numerosos sistemas europeos de certificación de ciberseguridad individual, es decir, descripciones claras de los requisitos de seguridad que deben cumplir los productos, sistemas o servicios. Cumplir los nuevos requisitos facilitaría a las empresas el comercio transfronterizo y que los compradores comprendan las características de seguridad de los productos o servicios. Los ciudadanos y los usuarios finales de los productos, los proveedores de productos y los gobiernos nacionales serán los beneficiados del marco de certificación. La certificación desempeña un papel fundamental para aumentar la confianza y la seguridad en los productos y servicios que son cruciales para el mercado único digital. Sin un marco común para los esquemas de certificados de ciberseguridad válidos en toda la UE, existe un riesgo creciente de fragmentación y barreras en el mercado único. ENISA implementará este proceso de certificación. El uso del marco de certificación no es obligatorio a menos que esté prescrito en la futura legislación de la UE, sin embargo, habrá un incentivo para certificar la calidad y seguridad. Existen algunos esquemas de certificación en la UE, tales como el Commercial Product Assurance (CPA), desarrollado en el Reino Unido, la Certificaction Sécuritaire de Premier Niveau (CSPN), en Francia, o el Dutch Baseline Security Product Assessment (BSPA), en los Países Bajos.
- Un plan detallado de cómo responder de manera rápida, operativa y al unísono cuando ocurre un ciberataque a gran escala.
- Una red de centros de competencia en los Estados miembro y un Centro Europeo de Investigación y Competencia en Ciberseguridad, que ayudará a desarrollar y desplegar las herramientas y la tecnología necesarias para mantenerse al día con una amenaza en constante cambio y garantizar que nuestra defensa sea lo más fuerte posible.
- Una nueva Directiva sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo para proporcionar una respuesta más

eficaz del Derecho penal al delito cibernético. El fraude de pago no en efectivo puede tomar diferentes formas. Los delincuentes pueden desencadenar la ejecución de pagos utilizando la información del pagador obtenida a través de, por ejemplo, suplantación de identidad, robo u obtención de información en sitios web dedicados que venden credenciales de tarjetas de crédito robadas en la *Darknet*. Los pagos también pueden ejecutarse fraudulentamente mediante tarjetas falsificadas o robadas, utilizadas para pagar en tiendas o retirar efectivo en cajeros automáticos o mediante el pirateo de sistemas de información para procesar pagos, por ejemplo, alterando los puntos de venta para transacciones con tarjeta o aumentando ilegalmente los límites de la tarjeta de crédito que permita que los gastos excedentes no sean detectados. La normativa actual no refleja las realidades del momento y no será suficiente para abordar los nuevos desafíos y desarrollos tecnológicos tales como monedas virtuales y pagos a través del móvil.

- Un marco para una respuesta diplomática conjunta de la UE a actividades cibernéticas maliciosas y medidas para reforzar la cooperación internacional en ciberseguridad, incluida la profundización de la cooperación entre la UE y la OTAN.
- El objetivo de impulsar el desarrollo de habilidades de alto nivel para los profesionales civiles y militares a través de la provisión de soluciones para los esfuerzos nacionales y la creación de una plataforma educativa y de capacitación en defensa cibernética.

1.3. HIBRIDACIÓN ENTRE LO FÍSICO Y LO LÓGICO

Las amenazas en el espacio digital son transversales, el ciberespacio sirve de facilitador y potenciador de gran parte del resto de amenazas que se plantean en el campo físico, y su carácter es global. El ciberespacio es una dimensión desde la que se generan riesgos en cualquiera de los ámbitos que señala, por ejemplo, la Estrategia de Seguridad Nacional (2017): terrorismo, crimen organizado, estabilidad económica, espionaje, conflictos, etc.

En el ámbito empresarial, y especialmente en procesos de internacionalización, ha aumentado la concienciación sobre cómo el ciberespacio es un ámbito que genera riesgos a la seguridad física de infraestructuras, y del personal y directivos. Las empresas, en esos procesos de internacionalización, no pueden dejar de acudir a zonas de conflicto, pero de enorme interés empresarial. Pero esos procesos deben contar con unos requisitos básicos de seguridad, y un conocimiento sociocultural. Cualquier tipo de riesgo para los desplazados (atentado, agresión, secuestro, asaltos y robos, robo de datos) y para las propias empresas (por rechazo a la presencia de empresas internacionales, por las características del negocio y posible oposición de comunidades y minorías) cuenta en el ciberespacio con un riesgo adicional. En el caso de autoprotección de los trabajadores, la actividad en Internet y redes sociales exige una "higiene" básica.

El reciente caso del secuestro del experto en criptomonedas y alto cargo de la compañía de intercambio de criptomonedas EXMO, Pavel Lerner, es paradójico, tras ser liberado después de pagar un millón de dólares en bitcoins.

Durante muchos años el pensamiento colectivo ha venido separando los impactos de la acción en ciberespacio y en el espacio físico. Nunca ha sido así, pero cada vez lo será menos.

Por otra parte, a la hora de entender algunos ciberataques es preciso disponer de un fuerte bagaje en geopolítica, geoeconomía y geoestrategia. Conflictos, procesos electorales, inversiones internacionales, alianzas, licitaciones internacionales, son cuestiones que pueden ser coetáneas a determinados tipos de ataques.

1.4. TENDENCIAS EN EL SECTOR/MERCADO

En todos los ámbitos se señala que, como ha comenzado a suceder en 2017, la ciberseguridad preocupará más a la dirección de las empresas. Siendo cierto, los comentarios de muchos directores de seguridad indican que la situación actual aún está lejos de lo deseable, al continuar percibiendo la seguridad como un coste. Pero la seguridad, y la ciberseguridad, seguirán cotizando en Bolsa. Al igual que las empresas que no son responsables socialmente o se ven involucradas en casos de corrupción ven afectadas sus cuentas de forma drástica, lo mismo sucederá con las empresas que no se muestren seguras en la gestión de datos e información de sus clientes y proveedores.

Gartner predice que en 2018 se producirá un incremento del gasto en ciberseguridad de un 8%, alcanzando los 96 billones de dólares (eSP European Solution Providers, 2018). A este crecimiento contribuye el nuevo marco regulador, además de los impactos de los ataques conocidos en 2017. La predicción de esta empresa para 2020 apunta a un incremento de un 35%, con más del 60% de las empresas invirtiendo en herramientas para seguridad de los datos, prevención de fugas de información, encriptación y auditoría.

Continuará el proceso de outsourcing de tareas a proveedores MSSPS (Managed Security Service Provider) y SaaS (Software as a Service). Gartner estima un gasto de 18,5 billones en 2018 un 11% más que en 2017.

Otro sector afectado será el de los ciberseguros, actor clave en la gestión de las ciberamenazas.

También a nivel organizacional se endurecerá la guerra por el talento en ciberseguridad, ante la elevada demanda de profesionales y la necesidad de incorporar perfiles multidisciplinares. Según ISACA, en 2019 se precisarán dos millones de nuevos empleos en ciberseguridad.

2. CIBERAMENAZAS

Para afrontar este apartado es preciso realizar una clasificación de las mismas. La Estrategia Nacional de Ciberseguridad (2013), pendiente de próxima actualización, contenía una clasificación confusa, en la que mezclaba riesgos y actores. A efectos de este trabajo vamos a considerar la siguiente tipología: cyberwarfare (ámbito político/económico y espionaje), ciberdelincuencia y ciber crimen organizado, terrorismo, sabotajes y hacktivismo (y aunque no sea tratado en el presente artículo, aquellas situaciones no controlables de fallos de sistema y accidentes y catástrofes).

Todo ello sin perder de vista que las fuentes de amenaza serán los Estados, actores no estatales al servicio o no de Estados, grupos criminales, grupos terroristas, hackers, hacktivistas o los denominados *insiders*.

2.1. CYBERWARFARE

Existiendo multitud de definiciones optamos por la combinación del US Department of Defense y las enseñanzas de Sun Tzu, para considerar cyberwarfare "al arte y la ciencia de lucha sin luchar, de derrotar al enemigo sin derramar su sangre".

Desde el ciberespacio se desarrolla una clara guerra política y económica, siendo la tecnología parte de ese engranaje. Así lo entendió Francia, por ejemplo, cuando en el año 1997 decidió crear una Escuela de Guerra Económica. La denominada inteligencia económica es una cuestión de Estado, centrada en la defensa de los intereses estratégicos nacionales, y a desarrollar en continua relación de confianza con las empresas.

El concepto de posverdad, tan de moda, ha puesto en evidencia cómo el ciberespacio, apoyado en desarrollos tecnológicos, se utiliza al servicio de procesos de engaño, decepción o manipulación, invocando a las emociones por encima de los hechos con ánimo desestabilizador, con la intención de polarizar la sociedad, de favorecer posturas radicales o extremistas desde el exterior, e influir y afectar a los procesos electorales.

El hecho es que las denominadas "fake news" funcionan, básicamente debido al sesgo de confirmación. Los seres humanos hacen suyas inmediatamente piezas de información, aunque sea falsa, que reafirme sus creencias. Todo ello lleva a pensar en la continuidad y crecimiento de este tipo de desinformación, a pesar de toda una serie de acciones desencadenadas para su control (fact-checks, concienciamiento de medios de comunicación tradicionales, sistemas de evaluación de información, compromiso de operadores para su detección, utilización de algoritmos o iniciativas educativas).

En este ámbito político-económico podríamos incluir también el espionaje, una cuestión tradicional que, en el día a día, sigue mostrando elevada casuística.

2.2. CIBERDELINCUENCIA Y CIBER CRIMEN ORGANIZADO

En este apartado asumimos las consideraciones del jefe del Grupo de Delitos Telemáticos de la Guardia Civil, que habitualmente destaca la necesidad de diferenciar ciberdelincuencia de cibercrimen organizado. No le falta razón, puesto que en la seguridad tradicional siempre se ha tratado de diferenciar entre ambos ámbitos. Todo ello asumiendo que posiblemente la definición de Europol de crimen organizado no encaje perfectamente para definir este nuevo y adaptativo cibercrimen organizado.

A estos efectos, Cohen y Blanco (2016), diferenciaban cómo se configuraba el crimen organizado tradicionalmente y cómo está sucediendo en la actualidad, especialmente debido a la utilización de Internet y las TIC:

Figura 1. Configuración actual del crimen organizado. Blanco y Cohen, 2016

El año 2018 seguirá presentando malware (que actuará en función de criterios de oportunidad), casos de extorsiones digitales, robos de identidad, el denominado fraude al CEO (que según Trend Micro supone nueve billones al año), ransomware en versiones RaaS (ransomware as a service), troyanos financieros, phishing, smishing, etc.

El "Cybercrime as a Service", que adopta modelos de gestión empresarial, es actualmente uno de los mayores negocios del mundo, junto a los tráficos ilícitos (armas, drogas y personas). El modelo Crime as a Service, potenciará el recurso a sistemas de croudsourcing criminal. Un claro ejemplo está en los ataques bancarios para obtener credenciales de tarjetas bancarias, que posteriormente son impresas por organizaciones criminales en diferentes países, y a su vez vendidas a otros grupos que acuden a los cajeros para extraer fondos. O con otras formas de atacar cajeros automáticos, ofreciendo cibercriminales "malware-as-a-service" en foros de deepweb, con manuales, videos y aplicaciones para acceder a los mismos. Quien paga por ese servicio solo tiene que elegir un cajero y seguir las instrucciones. Este modelo de negocio hace accesible la introducción en el cibercrimen de individuos no profesionales en nuevas tecnologías.

Los troyanos financieros son una buena fuente de ingresos para los criminales. Una vez infectado el equipo, y a través de "keylogging", roban las contraseñas tecleadas para acceder a los servicios bancarios. Utilizan técnicas sofisticadas, como técnicas "Man-in-the-Browser" (MiB), como "web injections" o redirecciones para ocultar operaciones. La proliferación de la banca a través del móvil ha afectado a ese negocio ilegal, que buscará cómo llevar sus ataques a esas plataformas móviles.

El recurso de muchas organizaciones a aplicaciones "serverless" amplifica también la superficie de ataque. Una vulnerabilidad es el tránsito de datos a través de una red, además de los niveles de privilegios que se definan. Este tipo de aplicaciones precisan unos protocolos de seguridad específicos y asegurar que el tráfico esté protegido por VPNs o encriptación. Igualmente, hay una ausencia de cultura de seguridad en aplicaciones Cloud, con las necesarias y pendientes políticas, procesos y controles.

El robo de más de dos billones de registros personales en 2017 será un factor clave para su utilización a lo largo de 2018 con diferentes fines. Y el robo masivo de datos personales, siguiendo casos como el de Equifax o Uber seguirá siendo un objetivo. El hacking de datos sanitarios seguirá creciendo.

El fraude al CEO o "Business e-mail compromise" es otra de las grandes fuentes de ingresos criminales y la tendencia apunta a un crecimiento, quizás matizado por un mayor perfilamiento de los objetivos.

Una tendencia será la especialización, con objetivos más dirigidos, ataques más sofisticados y elección de objetivos de mayor valor. El ransomware evolucionará de la extorsión a individuos hacia el ciber sabotaje y la disrupción de organizaciones. Investigadores de McAfee consideran a WannaCry, NotPetya u ONI como pseudo-ransomware, porque, aunque tengan parte de las características de dicha tipología delictiva su verdadero objetivo no es obtener rescates, sino actuar como pantalla de humo para la disrupción de los negocios, la exfiltración de datos o el robo de credenciales. El ransomware ha crecido un 2.000% en los últimos dos años.

Otra tendencia será la proliferación de ataques a criptomonedas, tanto al sistema que las soporta, como a las transacciones, los monederos y las personas. Según el Departamento de Seguridad Interior de Estados Unidos, un tercio de los intercambios de Bitcoin fueron hackeados entre 2009 y 2015, mientras que ha aumentado el número de ataques a inversores individuales. Los hackers han atacado a los intercambios, monederos, ICOs, Organizaciones Autónomas Descentralizadas, compañías de minería, servidores VP y servicios hosting. A finales de año el ataque a la compañía de minería NiceHash causó pérdidas de 60 millones de dólares. Es uno más de múltiples casos como el de Bitfinex (hackeo de 120.000 bitcoins, valorados en ese momento en 75 millones de dólares) o el de Mt. Gox (robo de 800 millones de dólares en Bitcoin). La empresa Chainalysis estima en 225 millones de dólares los robos a inversores en criptomonedas en 2017.

Internet de las Cosas, con la ilimitada expansión de productos conectados a la red (wearables, televisiones, frigoríficos, dispositivos de salud, juguetes...) llevará a que se amplifiquen los ataques a través de su utilización, por ejemplo, para DDoS. Pero también, y teniendo en cuenta el elevado coste de algunos dispositivos IoT para su secuestro virtual y petición de rescate. Los dispositivos IoT pueden permitir un permanente acceso de los criminales a la red de la víctima, generando puertas traseras en el sistema.

Se ha mencionado anteriormente el caso Mirai, una botnet que escaneaba continuamente dispositivos IoT con "user names" y claves de fábrica por defecto. Por esta vía se lanzaron potentes ataques DDoS. Symantec ha analizado las importantes vulnerabilidades de muchos dispositivos IoT (que no usan SSL, que permiten accesos por puertas traseras o que no disponen de actualizaciones de firmware encriptadas).

Los investigadores de Fortinet predicen que los criminales sustituirán botnets con clusters inteligentes de dispositivos comprometidos (hivenets), para lograr vectores de ataques más efectivos. "Hivenets" con capacidad de autoaprendizaje.

Toda la cadena de suministro seguirá siendo comprometida: proveedores, contratistas, socios, VIPS e individuos clave por acceso a información o credenciales. Los

cibercriminales detectarán el eslabón más débil de la cadena para lanzar el ataque y comprometer a la cadena completa.

Radware, finalmente, predice ataques a APIs, a proxy CDN (ataques a contenido dinámico, ataques DDos SSL-based, ataques a servicios no CDN, ataques directos a IP, ataques a aplicaciones web). Igualmente advierte de la automatización de la ingeniería social, el conjunto de técnicas utilizadas para engañar a individuos a efectos de obtener información o acceso a sistemas.

2.3. TERRORISMO

En el marco de los conflictos híbridos actuales no cabe descartar un avance en la confluencia de terrorismo y ciberataques.

A la hora de tratar el ciberterrorismo tenemos que separar dos cuestiones. La primera, el uso de internet y tecnologías de la información y las comunicaciones para favorecer sus actividades. La segunda, la realización de ciberataques o atentados apoyados desde el ciberespacio.

Sin duda Internet ha resultado un gran facilitador para el terrorismo. Una potente vía de comunicación, de carácter viral, a bajo coste, que permite la ubicuidad, la acción desde cualquier lugar y en cualquier momento y que facilita la ocultación del origen.

Frente a otros fenómenos, como el crimen organizado, la visibilidad y presencia es una característica propia del terrorismo. Es un acto de comunicación. Sin ello se diluyen sus efectos. Los grupos terroristas utilizan las redes para informar, adoctrinar, difundir sus mensajes y "éxitos", reclamar la autoría de los atentados, propaganda, captar y reclutar, planificar objetivos y atentados, formar y publicar tutoriales, etc. Pero es en la radicalización donde encuentran sus mayores ventajas, evitando el contacto físico y favoreciendo procesos de radicalización asistida (puesto que Internet no deja de ser interacción) y, en casos muy particulares, de autorradicalización.

Esa actividad de comunicación de grupos yihadistas era absolutamente libre y abierta hace años. La presencia de fuerzas y cuerpos de seguridad en internet y redes, especialmente desde los atentados de 2015, ha desplazado su acción hacia otras vías de comunicación, como la Deep Web, IRC o aplicaciones de telefonía móvil (especialmente Telegram). Pero, debido a esa necesidad de comunicar, siguen recurriendo a redes, foros y blogs clásicos. Los mensajes en aplicaciones móviles no permiten distribuir grandes documentos o videos, y cualquier link que se quiera compartir precisa de una web para su alojamiento. En ocasiones Twitter o Facebook sirven para una primera aproximación a objetivos para reclutamiento, vínculo que posteriormente se profundiza a través de Telegram.

En cuanto al segundo aspecto, la posibilidad de ciberatentados, sigue considerándose un hecho de baja probabilidad, alto impacto, pero quizás acortándose los plazos para su producción. El nivel técnico del denominado cibercalifato es muy bajo. Hasta el momento no se ha producido un ciberatentado, aunque sí pequeñas acciones de bajo impacto (denegación de servicios y acciones de hacking de bajo nivel). No son buenos ni programando, ni en malware (repletos de *bugs)*, encriptación, ni en acciones de hacking. A pesar de ello, oficiales de inteligencia de Estados Unidos han advertido

sobre la posible maduración de un cibercalifato, situación que en los últimos meses parece más controlada tras la caída de los feudos de Mosul y Raqqa del Daesh.

Quizás las acciones más preocupantes han sido acciones de hacking en las que han expuesto identidad y datos de personal vinculado a aparatos de seguridad. En todo caso, el escenario en el ciberespacio no es alentador, dada la facilidad para recurrir a herramientas, con dichos fines, creadas por grupos de crimen organizado (lo que se denomina *Crime as a Service),* que son efectivas y no precisan un desarrollo técnico propio. Es cuestión de tiempo que o bien desarrollen sus capacidades o bien las adquieran en el propio ciberespacio.

2.4. SABOTAJES

Los posibles ataques a infraestructuras críticas no son una cuestión de ciencia ficción. Por aquí se pueden producir futuras sorpresas estratégicas. Lo que militares norteamericanos han denominado un “Cyber Pearl Harbour” es un escenario que se otea en el horizonte. Hackers tienen en sus objetivos centrales nucleares, plantas químicas, sistemas eléctricos, sistemas de transporte y aviación. La ausencia de reporte de incidentes, hasta el momento, hace difícil ser conscientes de una amenaza que ya se ha manifestado.

En julio de 2017 el español Rubén Santamarta descubrió un fallo en los sistemas de las centrales nucleares que permitiría a un atacante simular fugas radioactivas o evitar que se detectaran. Una investigación que expuso posteriormente en el Black Hat de dicho año.

2.5. HACKTIVISMO

El hacktivismo continuará siendo una forma de acción en 2018, con campañas contra el sistema o acciones de “justicia”. Frente al activismo, que en general es admitido en las sociedades democráticas como una vía de ejercicio de política desde fuera de la política, aunque en ocasiones algunas de sus acciones puedan estar al límite de la legalidad, en el hacktivismo se suele producir una actividad delictiva.

Al margen de los tradicionales ataques de denegación de servicio, en general de bajo impacto, el mayor riesgo se genera por el acceso a datos e información de las organizaciones y de sus miembros. El hacktivismo puede comprometer instalaciones físicas, seguridad personal de empleados, datos e informaciones sensibles y afectar a la marca.

En todo caso, la tendencia apunta a su mantenimiento, pero representando un nivel muy bajo de amenaza. Como ha señalado repetidamente el CCN-CERT, no existe una articulación de un tejido hacktivista operativo insurgente en España, ni siquiera alrededor del movimiento Anonymous.

2.6. GAME CHANGERS

Entendemos por *game changers* aquellas variables que, sabiendo de su elevado impacto, existen dudas sobre si este va a ser positivo o negativo. La tecnología, en

general, es considerada un gran *game changer*, puesto que genera nuevos riesgos, siendo a la vez la vía para poderlos enfrentar.

2.7. INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING

Elon Musk, el gurú de Tesla, afirmó recientemente que deberíamos tener más preocupación por la Inteligencia Artificial (IA) que por Corea del Norte. Nick Bostrom, que dirige el Instituto para el Futuro de la Humanidad y el Centro de Investigación de Estrategia de Inteligencia Artificial de la Universidad de Oxford, es otro de los líderes de opinión académica que ha mostrado su preocupación por la IA. La mayoría de los análisis prospectivos sobre 2018 señalan que durante este año se podría incrementar el uso de la IA por parte de los cibercriminales, frente a una situación anterior en la que la IA era una posible herramienta para luchar contra el cibercrimen, para detectar anomalías y establecer patrones. Se produciría, en ese caso, y pendiente aún de poder demostrar fehacientemente, una guerra de IA contra IA, de máquinas contra máquinas. Actividades automatizadas, como mostró el Reaper botnet en 2017, para localizar vulnerabilidades en código fuente y búsqueda de nuevos conceptos zero-day.

Imaginemos un malware que analiza la forma en que nos comunicamos con diferentes contactos, y que fuera capaz de simular ese estilo para enviar mensajes personalizados a tus propios contactos. El propio Vladimir Putin ha llegado a señalar que quien consiga el liderazgo en IA gobernará el mundo. Una declaración abierta, de claro carácter estratégico, a la que todo analista debe atender.

McAffee, señalando la importancia de Machine Learning para procesar grandes cantidades de datos, que pueden ayudar a detectar y corregir vulnerabilidades, conductas sospechosas o ataques zero-day, insiste en la importancia del intelecto estratégico humano, señalando que el factor de éxito será la inteligencia humana amplificada por la tecnología. Una reflexión importante en un entorno de “solucionismo tecnológico”, usando la terminología de Eugeny Morozov, en el que a cada problema se le busca una solución tecnológica o incluso se crean problemas que no existen a tal fin.

2.8. BLOCKCHAIN

Una prometedora revolución tecnológica, aplicable en multitud de sectores, que elimina intermediarios y logra seguridad en el acceso y uso de la información, pero que aún está en un estado de infancia en el desarrollo de aplicaciones. Esa situación hace que ahora mismo no esté en el foco de los cibercriminales, que se seguirán centrando en todo el ecosistema de las criptomonedas (inversores, intercambios, monederos, instalación de aplicaciones ocultas para minar aprovechando la CPU de sus equipos y la energía eléctrica de internautas).

Blockchain tiene utilidad para seguridad de las TIC. El almacenamiento de datos de una forma descentralizada y distribuida puede prevenir su hackeo. Pero la implementación de sistemas financieros basados en blockchain puede producir errores o vulnerabilidades aprovechadas por atacantes. En los dos últimos años se han detectado errores de este tipo en los denominados smart contracts, basados en Blockchain.

3. CIBERINTELIGENCIA PARA LA CIBERSEGURIDAD

3.1. CONCEPTO

Sin existir un amplio debate sobre la cuestión, ni siquiera un volumen significativo de publicaciones, sí existe consenso en la dificultad para definir este término. Así se expresó, en repetidas ocasiones, en la I Jornada de Inteligencia y Seguridad organizada por la Fundación Borredá el 30 de noviembre de 2017. El propio Javier Candau, jefe de Ciberseguridad del Centro Criptológico Nacional, así lo indicaba en el número 79 de Red Seguridad (2017), destacando cómo es un concepto recurrente, que se vincula a la oferta de servicios en ciberseguridad, pero sobre el cual no existe consenso y se utiliza de forma ambigua.

La ausencia de un concepto de general o, al menos, amplia aceptación tiene importantes consecuencias: impide determinar los elementos configuradores de la posible disciplina, los contenidos de la función a desarrollar, y el diseño de planes de formación (conocimientos y habilidades), así como el desarrollo de carrera profesional.

Atendiendo a su origen etimológico estamos ante un término formado por dos palabras: *ciber* (que se refiere al ciberespacio) e *inteligencia*. Esta sencilla aproximación aporta claramente una pista a seguir, la ciberinteligencia como la confluencia de dos posibles disciplinas.

La RSA (2012) define ciberinteligencia como *"el conocimiento sobre los ciber-adversarios y sus métodos, además del conocimiento sobre la posición de seguridad de una organización sobre sus adversarios en el ciberespacio y sus métodos"*. En base a este conocimiento las organizaciones desarrollan inteligencia accionable. Otra definición habitual, pero excesivamente limitada es la siguiente: "*el análisis de las capacidades, intenciones y actividades de un adversario en el ciberespacio"*. INSA (2015) lo define, de forma más acertada y completa, como *"los productos y los procesos del ciclo de inteligencia para analizar las capacidades, intenciones y actividades –no solo técnicas- de los potenciales adversarios y competidores en el ciberespacio"*. INSA considera a la ciber contrainteligencia como una subdisciplina. En cualquier caso, estas aproximaciones basadas únicamente en adversarios parecen limitativas, obviando que la acción de los mismos se desarrolla en un entorno, un contexto político, social, económico, legal, tecnológico que conviene analizar. Incluso la propia naturaleza del ciberespacio, las tendencias detectadas, las nuevas amenazas y oportunidades, que surgen a cada instante, son un conocimiento vital a manejar.

Carnegie Mellon Software Engineering (2013) define ciberinteligencia como *"la adquisición y análisis de información para identificar, seguir y predecir ciber-capacidades, intenciones y actividades que ofrezcan líneas de acción para apoyar la toma de decisiones"*. Este concepto está mucho más próximo a la conceptualización clásica de inteligencia.

La *"U.S. National Intelligence Strategy 2014"* (Office of the National Director of Intelligence, 2014) identifica la ciberinteligencia como una de las cuatro misiones de la Comunidad de Inteligencia. El Department of Homeland Security (2012), en un informe de 2012, *"DHS Task Force of Cyber Skills",* se acerca también al contenido de la función de ciberinteligencia: *"conocimiento de la superficie de ataque, sus objetos de*

mayor valor y objetivos, y cómo sus vulnerabilidades pueden ser explotadas; mantener un situational awareness sobre actores maliciosos; desarrollar técnicas y aplicaciones para contrarrestar, identificar y vigilar; en su versión más avanzada entender las motivaciones de los atacantes, su lenguaje, organización, comportamiento individual y grupal, con objeto de perfilar grupos, actores y campañas".

Javier Candau (CCN-CERT, 2017) muestra su coincidencia con la definición de ciberinteligencia propuesta por el profesor Manuel Torres Soriano: *"actividad analítica cuyo propósito es proporcionar información relevante para apoyar la toma de decisiones en cuestiones relativas al ciberespacio".*

Consideramos que, a la hora de adoptar una definición que aúne el mayor grado de consenso, es preciso atender tanto a la raíz del concepto, con sus dos componentes "ciber" e "inteligencia", como a la doctrina de inteligencia que muestra claramente el CCN-CERT, proponiendo el siguiente concepto: *"proceso (y producto final) de la obtención y análisis de datos e información en/sobre el ciberespacio, realizado por especialistas y orientado a la toma de decisiones, en tiempo, lugar y forma".*

3.2. ELEMENTOS INVOLUCRADOS EN LA DEFINICIÓN:

- Es un proceso característico de inteligencia.
- Sobre una materia, que es el ciberespacio. El ciberespacio es el centro de dedicación de la ciberinteligencia, tomando al mismo tanto como un medio del que obtener y analizar datos e información, como una fuente de riesgos y amenazas, como señala la Estrategia de Seguridad Nacional.
- Una interpretación amplia del concepto de ciberinteligencia incorporaría la denominada Inteligencia de Fuentes Abiertas (OSINT), en la medida en que se centra en la información en el ciberespacio, aunque sea con otros objetivos adicionales a la ciberseguridad (protección de eventos, directivos, marca y reputación, etc.). Básicamente, lo que denominamos como "vigilancia digital" es OSINT.
- Consideramos que la ciberinteligencia no se ciñe a analizar las capacidades de los adversarios, sino también a analizar el entorno en el que dichos competidores toman decisiones estratégicas. El análisis del entorno configura la (in) seguridad, y la ciber (in)seguridad, y al menos debe ser tratado de entender en la dimensión estratégica de la ciberinteligencia.
- Es realizado por especialistas, tanto en ciberseguridad como en análisis de inteligencia.
- Exige unos requisitos formales para poder ser considerado como inteligencia, y siendo válido para un momento y lugar.
- Es finalista, su objetivo es la acción, el apoyo a la toma de decisiones:
    1. Identificando riesgos y amenazas.
    2. Analizando las variables involucradas y los actores intervinientes.
    3. Determinando oportunidades (quizás la orientación actual de nuestras sociedades está muy basada en riesgos). Esto no se incluye en las definiciones clásicas.

4. La inteligencia debe responder a las clásicas 5W+H (who, what, why, when, where, how). En el ciberespacio, con personal técnico adecuado, se puede responder a qué sucede, cómo, cuándo y dónde. Más complejo es poder responder a quién y por qué (o para qué). Por ejemplo, no fue difícil analizar qué estaba pasando con Wannacry o con NotPetya, ni cómo se producía y propagaba. Pero sí es complejo decidir quién está detrás, por qué y para qué.
5. Debe considerar implicaciones posteriores: ¿qué será lo próximo?, ¿qué hacemos ahora?
6. A diferencia de lo señalado en la definición de Torres Soriano, la toma de decisiones no se limita únicamente al ciberespacio, sino que también abarca el mundo físico. Todo lo que sucede en el ciberespacio puede tener impactos en el día a día de personas y organizaciones. La hibridación entre mundo físico y mundo ciber tiende a ser absoluta.

Al igual que sucede con la Inteligencia, es imposible su consideración como una ciencia e incluso como una disciplina, aunque sí tiene elementos que configuran una profesión y una especie de arte (una forma de hacer y actuar). Como un área emergente está pendiente de desarrollar lo que se conoce como "tradecraft": conjunto de conocimientos y habilidades adquiridas a través de la experiencia en un oficio. Los elementos, de manera más concreta, y siguiendo a INSA (2015), serían:

- Un cuerpo común de conocimiento.
- Un marco de competencias.
- Un modelo dual de desarrollo, entre aspectos técnicos y analíticos.
- Unos planes de formación y desarrollo.
- Una carrera profesional.

3.3. TIPOLOGÍA

Realizando un estudio bibliográfico, algunas de las aportaciones de mayor interés han sido las realizadas por la Intelligence and National Security Alliance (INSA).

Ciberinteligencia Estratégica (INSA, 2014a)

Tal y como señala INSA, es posible que la Ciberinteligencia Estratégica tenga matices en su conceptualización en diferentes organizaciones en base a su tamaño, objetivo o misión.

Para INSA depende de seis criterios:

- La naturaleza e identidad del cliente.
- Las decisiones que debe tomar el cliente.
- El marco temporal en el que actuará.
- El alcance de la obtención de información.
- El carácter de los potenciales adversarios.

- El nivel de aptitudes técnicas para la función.

Características de la ciberinteligencia estratégica:

- Amplia en la obtención.
- Más allá del sector.
- Mira a medio y largo plazo.
- Es amplia en la consideración de posibles adversarios.
- Desarrolla un análisis del entorno.
- Es esencialmente una tarea no técnica.
- Es clave en el análisis de riesgos: amenazas, vulnerabilidades, impactos, políticas.

Un proceso de ciberinteligencia estratégica considera:

- Qué información se precisa por el decisor (Information Requirement).
- Qué información se precisa sobre el entorno que configura el ámbito espacial y temporal en el que las organizaciones se desenvuelven (político, social, económico, tecnológico, legal…)
- Qué información se precisa sobre amenazas y riesgos para nuestra organización o nuestros clientes.
- Qué información se precisa sobre potenciales adversarios.
- Qué posición tiene la organización en seguridad:
    1. Objetivos a proteger.
    2. Vulnerabilidades.
    3. Nivel de riesgo: bajo, medio o alto riesgo ciber.
    4. Qué valor tiene la información de la organización.
    5. Qué valor tienen los aspectos digitales en sus procesos.
    6. Qué requisitos legales tiene la información.

Ciberinteligencia operacional (INSA, 2014b)

Características:

- Orientada a los managers de IT, CIO, CISO.
- Utilizable para adopción de decisiones sobre riesgos.
- El énfasis se pone en los procesos y operaciones de la organización, incluyendo proveedores, aliados y socios, competidores, clientes y otras relaciones.
- Analiza a los adversarios, con mayor grado técnico que en el nivel estratégico.
- Combina tareas técnicas y no técnicas, orientadas a aquellos vectores que suponen mayor riesgo para la continuidad del negocio.

Ciberinteligencia táctica (INSA, 2014c)

Características:

- Según INSA es el nivel en el cual las "batallas se planifican y ejecutan".
- Se produce específicamente para los equipos de respuesta a incidentes.
- Su objetivo es la resiliencia: restaurar las operaciones y recoger evidencias para el análisis forense.
- El análisis sobre el atacante centra parte de los esfuerzos: modus operandi, motivaciones, capacidades, etc.
- Su carácter es técnico.

3.4. EL "PARA QUÉ" Y EL "CÓMO" DE LA CIBERINTELIGENCIA

De una forma simplificada, las organizaciones deben proteger a las personas, las instalaciones, los procesos de negocio, los bienes y valores, los datos e información, y la marca y reputación. La ciberinteligencia se configura como la vía para el logro de dichos objetivos.

Figura 2. Ciclo de Ciberinteligencia del National Institute of Standards and Technology (NIST)

En base a la definición señalada en apartado anterior, y considerando el ciclo del NIST, sería posible construir un ciclo o proceso más cercano al del análisis de inteligencia clásico.

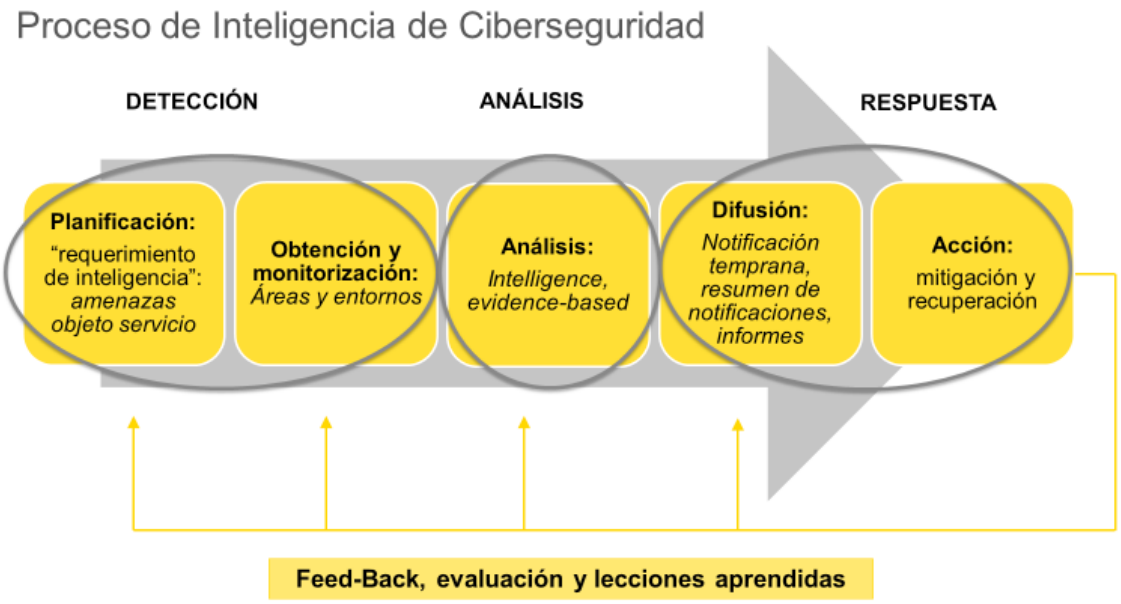

Figura 3. Proceso de Ciberinteligencia (Prosegur, 2017)

Las actividades del citado proceso son las siguientes:

1. **Definición, planificación y parametrización:** De acuerdo con el requerimiento de inteligencia (el "para qué" que genera la necesidad del análisis), se procede a determinar el alcance, plazos y recursos precisos. Posteriormente se lleva a cabo un plan para la parametrización de las fuentes y keywords sobre las herramientas de detección automatizada que se puedan utilizar, de manera que los sistemas queden preparados para la monitorización automática.

2. **Obtención y monitorización:** Una vez los sistemas de inteligencia han sido parametrizados y puestos en operación de acuerdo con la fase anterior, los mismos se encargarán de la recopilación automática de la información para la detección de potenciales eventos de ciberseguridad y su posterior análisis por parte de los operadores y analistas del servicio. En esta fase se realizan tareas como la propia obtención, filtrado, evaluación, clasificación e integración de la información.

3. **Análisis:** Estudio e interpretación de la información. A estos efectos se puede combinar el clásico método científico, con técnicas tanto cuantitativas como cualitativas, junto a las denominadas técnicas estructuradas de análisis de inteligencia, desarrolladas por los servicios de inteligencia. Estas aproximaciones, junto al análisis de riesgos, siguiendo la Norma ISO 31000, complementan marcos propios de la Ciberinteligencia, como el proceso NIST, The Kill Chain o el modelo de diamante. A ello se unen disciplinas que incrementan las capacidades del analista, ante las dificultades cuantitativas y cualitativas derivadas del elevado grado de infoxicación y de los crecientes procesos de manipulación, desinformación y engaño (posverdad): análisis semántico, Big Data, Machine Learning, algoritmos avanzados, ingeniería de sistemas de decisión, redes neuronales, etc.

4. **Acción. Resiliencia y respuesta:** Ante las posibles conclusiones y recomendaciones derivadas de las notificaciones e informes corresponderá al decisor la adopción de las medidas oportunas o necesarias.

5. **Retroalimentación y mejora continua:** Periódicamente se llevan a cabo ejercicios para compartir conocimientos, mejorar la calidad de los entregables, disminuir los tiempos de respuesta y abordar oportunidades de mejora. Igualmente abordan desviaciones y oportunidades de mejora en base a los resultados de los indicadores de medición de cada servicio, con el objetivo de mejorar de manera continuada y maximizar la eficiencia de las actividades, la calidad de los entregables y minimizar los tiempos de respuesta.

3.5. LA CIBERINTELIGENCIA COMO FACTOR DE COHESIÓN EN LA CIBERSEGURIDAD

La ciberinteligencia, adicionalmente, puede desempeñar un papel cohesionador de diferentes líneas de acción en ciberseguridad. Desde una visión estratégica, y sin ánimo de ser exhaustivo, algunas de las líneas de acción que pueden ser apoyadas por la ciberinteligencia serían:

Avanzar en concienciación.

Algunas recetas para mejorar la concienciación serían:

- El desarrollo de una labor didáctica. La complejidad del ciberespacio ha llevado a la utilización de un lenguaje muy técnico, difícil de seguir y entender. Por este motivo, hacia las empresas, es importante desarrollar una filosofía *"storytelling",* que traduzca el lenguaje técnico en implicaciones para las empresas, en posibles costes. A estos efectos la utilización de escenarios y simulaciones es un apoyo, posiblemente más eficaz que el recurso a la presentación de frías estadísticas.

- La utilización de casos de estudio y ejemplos para hacer comprender a las organizaciones cómo desde el ciberespacio se puede afectar a la seguridad de instalaciones e infraestructuras, la seguridad física de empleados y directivos, los procesos de negocio, los datos y la información, los valores y la marca y reputación.

Colaboración público-privada

Esta colaboración ya no es una opción, es la única vía. El fortalecimiento del marco normativo, por sí mismo, ya hará que exista un mayor grado de relación, aunque sea por vía de requerimiento de acciones de información y comunicación, o garantía de protección de datos.

Esta colaboración presenta multitud de vías para su desarrollo, como proyectos de investigación conjuntos, intercambios de información puntuales, coorganización de jornadas y talleres, grupos de expertos para debate, intercambio de buenas prácticas, etc.

Gobernanza en las organizaciones

Posiblemente el gran reto a abordar, donde es preciso desarrollar una verdadera cultura de ciberseguridad en las organizaciones. La ciberseguridad debe actuar de forma transversal y los responsables de estas áreas sentarse muy cerca del Consejo de Dirección.

Inteligencia en sentido amplio

La inteligencia, definida como el proceso de obtención y análisis de la información para apoyar la toma de decisiones, es una de las vías para poder gestionar los riesgos, atendiendo a diversos objetivos que se plantean en el campo de la ciberseguridad. Uno de ellos pudiera ser cómo reducir el periodo entre el que un sistema es comprometido y es detectada la intrusión. Según FireEye es de 469 días en Europa (siendo la media mundial de 146).

El análisis de lecciones aprendidas y el estudio de casos forman parte de las tareas a desarrollar desde la inteligencia. Procesos para los cuales existen metodologías que ayudan a enmarcar un proceso que no debe ser tan intuitivo, en caso de existir, como sucede en ocasiones.

La inteligencia también debe tener como misión su propio autodesarrollo a través del apoyo tecnológico preciso. La tecnología, por una parte, es fuente de amenazas, pero a su vez se configura como posible solución a muchos riesgos.

Por otra parte, como proceso de análisis, la inteligencia camina de la mano de la geopolítica, la geoeconomía o la geoestrategia. Un entendimiento del entorno, a través de la inteligencia estratégica, puede proveer del contexto necesario para entender algunos riesgos cibernéticos.

Finalmente, y de nuevo sin ánimo exhaustivo, la inteligencia es la base para desarrollar la necesaria *Cyber Awareness,* similar a lo que conocemos como consciencia situacional (*situational awareness),* el mantenimiento de un elevado nivel de alerta ante posibles señales débiles (eventos que pueden sugerir una tendencia o que, conectados con otros eventos, generen nuevos riesgos).

Análisis de riesgos

La base para gestionar cualquier tipo de riesgo es partir de un buen análisis y evaluación de riesgos. Una evaluación que debe ser continua. En 2017 Gartner proponía un modelo CARTA (Continuous Risk and Trust Assessment Approach, 2017), un proceso continuo de evaluación y reajuste. Pero no hace falta ser Gartner para llegar a esa conclusión. El análisis de riesgos se debe desarrollar en tiempo real. Las metodologías de análisis de riesgos deben evolucionar, para incorporar aproximaciones como el análisis de datos, las redes neuronales y otras técnicas de minería de datos, el juicio de los expertos, el análisis bayesiano, etc.

Gestión de crisis

Cualquier incidente ciber es capaz de producir una crisis. Las organizaciones deben prepararse para estas situaciones, específicamente a través de simulaciones. Que cuando el momento se produzca existan protocolos de acción y la comunicación a desarrollar. Mientras que las crisis pueden ser improvisadas, la gestión de crisis nunca debe improvisar.

Seguridad desde el diseño

Garantizar la seguridad desde el mismo momento en que se diseña un producto o servicio puede ser la mejor manera de prevenir.

Prospectiva

En entornos que denominamos VUCA (acrónimo de volatilidad, incertidumbre, complejidad y ambigüedad), la capacidad para interpretar qué está sucediendo es un valor para las organizaciones, que se debe complementar con las capacidades para identificar posibles escenarios futuros, con objeto de adoptar en el presente las decisiones estratégicas que eviten los más desfavorables y, si es posible, nos guíen a los más beneficiosos para nuestras organizaciones. La prospectiva no es una técnica de adivinación, sino que cuenta con técnicas específicas para su desarrollo.

Pensar en futuro es una obligación. Conocemos más cosas del futuro de las que solemos creer. Pensar en futuro induce elementos causales en su devenir.

Tradecraft, el oficio del analista de ciberinteligencia

Finalmente, y desde el punto de vista de la Ciberinteligencia, es preciso desarrollar lo que se conoce como *Tradecraft,* el oficio: qué conocimientos son precisos, qué aptitudes y qué actitudes, qué habilidades se exigen para poder entender las actuales ciberamenazas y poder luchar contra ellas. Todo ello a nivel estratégico, operativo y táctico. Implica adicionalmente el establecimiento de un plan de carrera, que considere la formación precisa y las condiciones para la promoción.

4. CONCLUSIONES

Frente a la falta de consenso sobre la definición y delimitación de la ciberinteligencia es posible apuntar que la misma puede contar con los mismos fundamentos que la doctrina de inteligencia clásica, nacida en el ámbito militar y de la seguridad física. Los elementos caracterizadores de la misma son coincidentes, una forma de pensar orientada a la acción, un proceso racional de obtención y análisis de información, una finalidad en el apoyo a la toma de decisiones, y unas características propias (tiempo, forma y lugar) que permiten diferenciar la inteligencia de la información o el conocimiento.

Los intereses a proteger de Estados, organizaciones o empresas coinciden en el ámbito físico y en el ciberespacio: las personas, las infraestructuras, la información y los datos, los procesos de negocio, los bienes y valores, y la marca y reputación. Los seis elementos pueden ser atacados tanto físicamente como a través del ciberespacio. Internet y las Tecnologías de la Información y las Comunicaciones son un facilitador o potenciador de lo que se denomina en la literatura anglosajona como *"cyber enabled crimes",* referido a aquellos delitos que pueden realizarse tanto con apoyo tecnológico como sin él.

La definición propuesta de ciberinteligencia como "*proceso (y producto final) de la obtención y análisis de datos e información en/sobre el ciberespacio, realizado por especialistas y orientado a la toma de decisiones, en tiempo, lugar y forma",* goza del contenido necesario para ser adoptado, tanto en el ámbito público como en el sector privado, facilitando la creación de un lenguaje común que, aún lejos de poder configurar una disciplina, ***sí defina a una actividad profesional.***

Al igual que la inteligencia ha contribuido clásicamente a la seguridad física, la ciberinteligencia lo hace hacia la ciberseguridad. La sociedad digital se enfrenta a retos hasta ahora desconocidos, riesgos probables de muy incierto impacto. Parte de los

planteamientos distópicos del futuro se centran bien en ciberataques, bien en formas híbridas o combinadas de acción. Los conflictos en el ciberespacio se acrecientan, sustituyendo viejas formas de enfrentamiento. Los ciberdelitos y, lo que es más serio, el cibercrimen organizado, disponen de los mejores recursos: tecnólogos, hackers, abogados, blanqueadores, expertos en sistema financiero. Incorporan a sus acciones desarrollos como la Inteligencia Artificial. Los terroristas, hasta el momento, han utilizado Internet en funciones de propaganda y comunicación, adoctrinamiento, captación y reclutamiento. Es decir, un uso de Internet y las TIC como medio, pero no como el fin de los ataques. Cuentan con la intención, y las capacidades para ello no son tan necesarias, en un modelo de negocio de "Crime as a Service". Las capacidades precisas pueden ser adquiridas o arrendadas a otros grupos criminales.

En este marco, la Ciberinteligencia se enfrenta a los siguientes retos:

- Su conceptualización, como base para la determinación del "oficio" de analista de ciberinteligencia.
- *Tradecraft* u oficio. Determinación de conocimientos y habilidades, junto al desarrollo de un plan de formación y una carrera profesional para los analistas de ciberinteligencia. El documento de ENISA (2015) es una de las propuestas más elaboradas en este sentido.
- El desarrollo de metodologías propias o adaptadas de otras disciplinas o profesiones.
- El apoyo de nuevas tecnologías, en ningún caso sustitutivas del ser humano.

BIBLIOGRAFÍA

Arquilla, J. y Ronfeldt D. (2001). Networks and Netwars. The Future of Terror, Crime, and Militancy. RAND Corporation. Extraído el 2 de julio de 2018 de: https://www.rand.org/pubs/monograph_reports/MR1382.html

Arquilla, J. y Ronfeldt D. (1996). The Advent Of Netwar 1996. RAND Corporation. Extraído el 2 de julio de 2018 de: https://www.rand.org/pubs/monograph_reports/MR789.html

Blanco, J. M. y Cohen, J. (2016). Macro-environmental factors driving organized crime. Using Open Data to Detect Organized Crime Threats. Springer.

Candau, J. (2017). Ciberinteligencia, complemento perfecto para la ciberseguridad. Red Seguridad 4º trimestre 2017. Extraído el 2 de julio de 2018 de: http://www.redseguridad.com/especialidades-tic/inteligencia/ciberinteligencia-complemento-perfecto-para-la-ciberseguridad

Carnegie Mellon University (2013). Cyber Intelligence Tradecraft Project: Summary of Key Findings. SEI Emerging Technology Center. Extraído el 2 de julio de 2018 de: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=40201

Centro Criptológico Nacional (2017). XI Jornadas CCN-CERT Ciberamenazas, el reto de compartir. Extraído el 2 de julio de 2018 de: https://www.ccn-cert.cni.es/xijornadas.html

Department of Homeland Security (2012). Cyber Skills Task Force Report. Washington, DC: Homeland Security Advisory Council.

Gartner (2017). CARTA (Continuous Risk and Trust Assessment Approach, 2017). Extraído el 2 de julio de 2018 de: https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age/

Gobierno de España (2017). Estrategia de Seguridad Nacional. Extraído el 2 de julio de 2018 de: http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/Documents/2017-1824_Estrategia_de_Seguridad_Nacional_ESN_doble_pag.pdf

Gobierno de España (2013). Estrategia de Ciberseguridad Nacional (2013). Extraído el 2 de julio de 2018 de: https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Intelligence and National Security Alliance INSA (2013) Operational Levels of Cyber Intelligence. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/operational-levels-of-cyber-intelligence/

Intelligence and National Security Alliance INSA (2014a) Strategic Cyber Intelligence. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/strategic-cyber-intelligence/

Intelligence and National Security Alliance INSA (2014b) Operational Cyber Intelligence. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/operational-cyber-intelligence/

Intelligence and National Security Alliance INSA (2014c). Tactical Cyber Intelligence. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/tactical-cyber-intelligence/

Intelligence and National Security Alliance INSA (2015). Cyber Intelligence: Preparing Today's Talents for Tomorrow's Threats. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/cyber-intelligence-preparing-todays-talents-for-tomorrows-threats/

eSP European Solution Providers (2018). 2018 Security Spending to Reach $96bn . Extraído el 2 de julio de 2018 de: http://www.it-sp.eu/index.php?option=com_content&view=article&id=3651:gartner-2018-security-spending-to-reach-96bn&catid=38:security&Itemid=74

Liang, Q. y Xiangsui, W. (1999). Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House.

Microsoft (2017). A Digital Geneva Convention to protect cyberspace. Extraído el 2 de julio de 2018 de: https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

MMC Cyber Handbook 2018. Extraído el 2 de julio de 2018 de: https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf

NIST (2018). Cybersecurity Framework. Extraído el 2 de julio de 2018 de: https://www.nist.gov/cyberframework

Office of the National Director of Intelligence (2014). The National Intelligence Strategy of the United States of America. Extraído el 2 de julio de 2018 de: https://www.dni.gov/files/documents/2014_NIS_Publication.pdf

Online Trust Alliance (2018). Cyber Incident & Breach Trends Report Review and analysis of 2017 cyber incidents, trends and key issues to address. Extraído el 2 de julio

de 2018 de: https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

Parlamento Europeo (2016). Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Extraído el 2 de julio de 2018 de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

Parlamento Europeo (2018). ENISA and a new cybersecurity act. Extraído el 2 de julio de 2018 de: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282017%29614643

RSA (2012). Getting Ahead of Advanced Threats. The Security Division of EMC. Extraído el 2 de julio de 2018 de: https://www.rsashare.com/leadership/articles/getting-ahead-of-advanced-threats.htm

USENIX (2017). Understanding the Mirai Botnet. Vancouver, BC, Canada. Extraído el 2 de julio de 2018 de: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

Fecha de recepción: 21/06/2018. Fecha de aceptación: 25/06/2018