Año 27 No. 97
Enero-Marzo, 2022

RVG

Año 27 No. 97
Enero-Marzo, 2022

Revista Venezolana de Gerencia

UNIVERSIDAD DEL ZULIA (LUZ)
Facultad de Ciencias Económicas y Sociales
Centro de Estudios de la Empresa

ISSN 1315-9984

COMO CITAR Lominchar Jiménez, J., y Zunzarren Denis, H. (2022). La transversalidad estratégica de la ciber inteligencia. *Revista Venezolana de Gerencia*, *27*(97), 258-273. https://doi.org/10.52080/rvgluz.27.97.18

Universidad del Zulia (LUZ)
Revista Venezolana de Gerencia (RVG)
Año 27 No. 97 2022, 258-273
ISSN 1315-9984 / e-ISSN 2477-9423

La transversalidad estratégica de la ciber inteligencia

Lominchar Jiménez, José*
Zunzarren Denis, Hugo**

Resumen

El análisis de un ciberataque sencillo mostrará cómo los fundamentos de la Seguridad Nacional de cada país han cambiado, cómo las nuevas ciberamenazas son híbridas, cómo los actores y grupos maliciosos han evolucionado y conciben los conflictos desde la eficaz perspectiva de la guerra asimétrica y, finalmente, por qué las empresas no son capaces de reaccionar al desconocer que están inmersas en este tipo de conflicto; desglosando y definiendo estos nuevos tipos de conflicto en los que están inmersos las empresas. Mediante el paralelismo entre las Técnicas, Tácticas y Procedimientos (TTP´s) que se utilizan. El origen de la citada incapacidad se encuentra en la hiperconectividad de los sistemas; el mapa de riesgos no contempla dichas interrelaciones, provocando miopía estratégica. Desde el entendimiento del nuevo ecosistema del ciberespacio y modificando los sistemas de evaluación de riesgos, añadiendo la transversalidad de la metodología de ciberinteligencia, se podrá evaluar con mayor certeza el riesgo de ser objeto de ataques; y poner las salvaguardas lejos de las murallas mediante ciber influencia, desactivando los ataques incluso antes de que se conciban. Entender el riesgo del sistema de cada empresa a proteger, a través de la obtención y análisis de información fiable, actualizada y cotejada es fundamental.

Palabras clave: gestión de riesgos; ciber-inteligencia; guerras asimétricas

Recibido: 20.6.2021 **Aceptado**: 23.9.2021

* Doctor en Derecho UCJC. Doctor Honoris causa por la CUEJ. Profesor e Investigador de la Facultad de Ciencias Jurídicas y Sociales UDIMA. Profesor e Investigador Facultad de Comunicación y Empresa UNIR, Email: jose.lominchar@udima.es, ORCID: https://orcid.org/0000-0002-4025-8589

** Profesor de la Escuela de Inteligencia Económica de la Universidad Autónoma de Madrid Máster por la Escuela de Guerra Económica de París (EGE), Antiguo Oficial de Inteligencia Naval, Marine Nationale, France. Email: Hugo.zunzarren@inv.uam.es

The strategic transversality of cyber intelligence

Abstract

The analysis of a simple cyberattack will show us how the fundamentals of National Security of each country have changed, how the new cyberthreats are hybrids, how malicious actors and groups have evolved and conceive conflicts from the effective perspective of asymmetric warfare and, finally, why companies are not capable of reacting when not knowing that they are immersed in this type of conflict; breaking down and defining these new types of conflict in which companies are immersed. By means of the parallelism between the Techniques, Tactics and Procedures (TTPs) that are used, it will be shown that the origin of the aforementioned disability lies in the hyperconnectivity of the systems and that the risk map does not contemplate these interrelations, causing strategic myopia. From the understanding of the new cyberspace ecosystem and modifying the risk assessment systems, adding the transversality of the cyber intelligence methodology, the risk of being the object of attacks can be evaluated with greater certainty; and putting safeguards away from walls through cyber influence, disabling attacks before they are even conceived. Understanding the risk of the system of each company to protect, through the obtaining and analysis of reliable, updated and collated information is essential.

Keywords: Risk management; Cyber-intelligence; Asymmetric wars

1. Introducción

La Teoría de los “seis grados de separación” es una afirmación establecida por la húngara Frigyes Karinthy en 1929, que analiza la posibilidad de que cualquier persona en el mundo pueda estar conectada con cualquier otra, a través de una cadena de relaciones individuales que comprende como máximo otros seis eslabones. Esta teoría fue retomada en 1967 por Stanley Milgram a través de su estudio “Small-World Problem”.

Hoy, con el desarrollo de las redes sociales, el grado medio de separación se mide precisamente en 4,74 número a poner en perspectiva, puesto que se trata de amigos virtuales, pero para este artículo es irrelevante puesto que lo que interesa es el vínculo existente. En estos tiempos es una práctica común verificar digitalmente la calidad de un servicio antes de usarlo, pedir un producto sin contacto real con un vendedor e incluso consultar libros en su forma virtual. Las empresas, por su parte, también están cada vez más presentes en el sector digital, utilizando cloud computing, paquetes de software, procesos de negocio, accesos SAAS, entre otros (González, 2015).

Por lo tanto, se está asistiendo a una aceleración hacia "necesito velocidad: todo integrado, todo conectado"; y esto conlleva un cambio repentino en la forma en que se intercambia información. Tanto las herramientas digitales, destinadas a particulares, como las máquinas profesionales estarán interconectadas, enviando y recibiendo gran cantidad de datos en tiempo real. Estos cambios están provocando cambios profundos en la forma en que se intercambia, comunica y se envían datos en poco tiempo al otro lado del planeta. Los profundos trastornos no radican tanto en la invención de nuevas herramientas digitales, como en el uso y aprovechamiento diario que se hace de estas herramientas.

En este contexto, la digitalización de la economía aporta grandes beneficios gracias a la inmediatez del intercambio de información y la automatización es ya un factor clave de éxito. Sin embargo, la revolución digital también va acompañada de una exposición permanente, a un riesgo de un tipo relativamente nuevo: el riesgo cibernético.

Según la Agence nationale de la sécurité des systèmes d'information (ANSSI), fuente francesa de referencia mundial, se define al riesgo cibernético como: "un ataque a los sistemas informáticos llevado a cabo con intenciones maliciosas, dirigiéndose a diversos dispositivos informáticos: ordenadores o servidores, aislados o en red, conectados o no a Internet, equipos periféricos como impresoras, o incluso dispositivos de comunicación como teléfonos móviles, "smartphones" o tabletas.

Hay cuatro tipos de riesgos cibernéticos con diversas consecuencias, que afectan directa o indirectamente a personas, administraciones y empresas: ciberdelito, daño a la imagen, espionaje, sabotaje. El riesgo digital que cada día pesa más sobre las organizaciones puede llegar a poner en peligro su supervivencia y la de sus stakeholders".

Siempre de acuerdo con ANSSI y Management des risques et des Assurances de l´Entreprise (AMRAE), la hiperconectividad debe considerarse como un riesgo a ser abordado al más alto nivel de la organización y ya no solo como un riesgo cuya evitación es responsabilidad de los expertos técnicos. Sin embargo, las amenazas cibernéticas están creciendo exponencialmente.

Los atacantes aprenden a evadir los sistemas basados en firmas, y los delincuentes utilizan la inteligencia artificial para evadir la detección manteniéndose al tanto de las reglas de detección más comunes. Los equipos de ciberseguridad se sienten abrumados por el tamaño y la complejidad de este creciente desafío, ya que los medios técnicos que necesitan para contrarrestar los ataques con éxito son cada vez más caros y difíciles de encontrar (Deloitte Touche Tohmatsu Limited, 2019).

La multiconectividad de los dispositivos actuales y profesionales va de la mano con la exposición a riesgos y las pérdidas potenciales vinculadas a la informática. Los accidentes o ataques serán invaluables. Según Vélez (2019) consultora en Ciberinteligencia, el riesgo cibernético puede incluso transformarse en riesgo sistémico por la naturaleza multiplicativa de la multiconectividad en el mundo y de las herramientas inteligentes que se comunican automáticamente.

¿Y qué decir de las empresas? Toda organización debe afrontar riesgos. De hecho, según la ANSSI (2019) "el riesgo cibernético exige una necesidad de protección añadida por el valor

fundamental del riesgo para los actores sociales y económicos, llegando hasta a poner contra las cuerdas el propio funcionamiento del sistema, los medios financieros, la reputación y privacidad, e incluso la supervivencia de las empresas o personas. La fortaleza de una empresa, no es solo la adaptación de su producción a la evolución del mercado, sino que también radica en adaptación al nuevo y futuro contexto de intercambio de datos, impactando éste en la propia producción. Es hora de que las empresas hagan un balance del peligro que se cierne sobre el curso de sus negocios".

Si las personas están hiperconectadas, las empresas lo están también, formado el conjunto un sistema interrelacionado como nunca. Es esta conectividad la que provoca nuevos tipos de vulnerabilidad; y son estos nuevos tipos de vulnerabilidad los que dan lugar a nuevos tipos de actores maliciosos, con Modus Operandi diferentes a los hasta ahora vistos: aprovechan la información disponible, la capacidad acrecentada de comunicación vía redes sociales para hacer propaganda y acciones de desestabilización y así, no ya aprovechar vulnerabilidades existentes, sino crear ex nihilo el eje de ataque esperado.

Estas nuevas formas de ataque son muy similares a las que los militares ya llevan intentando modelizar desde la guerra de Vietnam: son las acciones híbridas enmarcadas en conflictos asimétricos. Esta vez la amenaza se cierne contra el propio sistema, pudiendo llegar a tener impacto sobre la propia sostenibilidad de este.

Por tanto, la nueva seguridad requiere un enfoque integrado, que tenga en cuenta tanto los aspectos regionales como globales, la dinámica tecnológica y militar, pero también la dinámica mediática y humana, o incluso la nueva dimensión que adquiere el terrorismo o la estabilización posconflicto. En enero de 2020, Guillaume Poupard, actual director de la Agencia Nacional para la Seguridad de los Sistemas de Información pronosticó que: "los conflictos del mañana serán digitales, todos los estados principales serán digitales. tanto en ataque como en defensa, (…), y comprenderán acciones emprendidas en el ciberespacio que produzcan efectos contra un sistema adverso, para alterar la disponibilidad o confidencialidad de los datos (ANSSI, 2019). Esta doctrina ha venido a fortalecer la postura de la guerra informática defensiva (LID) que tiene como objetivo "anticipar, detectar y reaccionar ante los riesgos" (ANSSI, 2019).

Para llevar a buen puerto esta nueva doctrina global, es necesario un nuevo enfoque, oponiendo a los Modus Operandi híbridos y asimétricos actuales a una nueva forma evaluación de los riesgos comprendiendo las interrelaciones empresariales, técnicas y estructurales del sistema.

La disciplina capaz de modelizar y entender las implicaciones de este nuevo mapa de riesgos es la disciplina de Ciberinteligencia, por su querencia natural a evaluar los invisibles y a descubrir, mediante el análisis de información, las implicaciones directas e indirectas de cada escenario de impacto, posible, probable o catastrófico.

Mediante la exposición de un ataque cibernético tipo, destacando las Técnicas, Tácticas y Procedimientos maliciosos más comunes y analizando los fundamentos de los mismos desde las definiciones de Guerra Asimétrica y acciones híbridas, se podrá exponer por qué la Ciberinteligencia mejora el alcance de la gestión de riesgos cibernéticos,

paliando las incoherencias actuales en la visión segmentada y miope que las empresas aplican en sus sistemas de ciberseguridad, planes de mitigación y respuesta ante incidentes (Bello, 2021).

2. Realidad que supera a la ficción

"Sábado, 8h AM, el ordenador que lleva recibiendo paquetes desde la IP[1] maliciosa 19V.16X.7Y.14Z abre una Shell[2] y se pone a compilar[3]. Escasas horas después, dicha Shell se cierra; se abre un cuadro de diálogo pidiendo reiniciar para instalar una actualización de seguridad. El ordenador es el que gestiona el sistema CCTV (Circuito Cerrado de Televisión) y está a cargo del personal de seguridad que trabaja los fines de semana. A este ordenador llegan las señales de las cámaras IP y de otros sistemas IOT[4], que han sido infectados al estar configurados por defecto.

El script[5] malicioso no es gran cosa, solo busca un terminal con acceso a internet; al encontrar uno, se conecta a la IP maliciosa antes citada y comienza a descargar paquetes, trozos de código, hasta completar la descarga, que no son más que todos los componentes del virus, aún sin ensamblar. El antivirus no detecta nada ya que los paquetes no están en la Base de Datos de "Indicadores de Compromiso (IOC´s[6])" del antivirus, puesto que se han se han programado ad hoc para la empresa y se han codificado en hexadecimal, los sistemas no tienen catalogada la IP como maliciosa, y tampoco hay un sniffer de red, una herramienta -literalmente significa "olfateador"- que se emplea para observar los mensajes que intercambian dos nodos conectados a través de una red y que captura las tramas, o paquetes, a nivel de enlace que se envían/reciben a través de los interfaces de red del sistema implementado para analizarlos, que detecte el comportamiento anómalo. La Shell monta el virus y lo instala, el sistema de reinicio confirma la instalación: game over.

Unos meses después, tras dejar más de 100 días al virus hacer aquello

1 Una dirección IP es una representación numérica del punto de Internet donde está conectado un dispositivo. Se usa para identificar dónde hay algo y, en cierto modo, qué es. https://www.avast.com/es-es/c-what-is-an-ip-address

2 Es un intérprete de órdenes o intérprete de comandos es el programa informático que provee una interfaz de usuario para acceder a los servicios del sistema operativo directamente y ejecutar órdenes. El shell es la capa más externa del sistema operativo. Los shells incorporan un lenguaje de programación para controlar procesos y archivos, además de iniciar y controlar otros programas. https://www.ibm.com/docs/es/aix/7.2?topic=administration-operating-system-shells

3 Convertir un programa en lenguaje máquina a partir de otro programa de computadora escrito en otro lenguaje. https://dle.rae.es/compilar

4 La definición de IoT es la agrupación e interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet, la red de redes), dónde todos ellos podrían ser visibles e interaccionar. https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

5 O archivo de órdenes o archivo de procesamiento por lotes es un programa usualmente simple, que generalmente se almacena en un archivo de texto plano. El uso habitual de los scripts es realizar diversas tareas como combinar componentes, interactuar con el sistema operativo o con el usuario. Por este uso es frecuente que los shells sean a la vez intérpretes de este tipo de programas. https://es-academic.com/dic.nsf/eswiki/552399

6 Los Indicadores de Compromiso o «Indicators of Compromise» (IOCs) hacen referencia a una tecnología estandarizada que consiste en definir las características técnicas de una amenaza por medio de las evidencias existentes en un equipo comprometido, es decir, se identifican diferentes acciones como ficheros creados, entradas de registro modificadas, procesos o servicios nuevos, etc. de manera que puedan servir para identificar otros ordenadores afectados por la misma amenaza o prevenirlos de la misma. https://www.incibe-cert.es/blog/indicadores-de-compromiso

para lo que fue diseñado, escalando permisos poco a poco (es lo que se denomina "ataque dirigido"), usando los protocolos internos para propagarse (impresoras, bridges, documentos), ocurren dos cosas: ciertos discos duros quedan cifrados, y cierta información crítica sale de la organización hacia un C&C[7] (un servidor central para distribuir de forma lo más insidiosa posible malware a las máquinas infectadas o a infectar, ejecutar comandos para el programa malicioso y tomar el control de un dispositivo) gobernado por un grupo hacktivista vinculado a una APT. La APT, o Amenaza Avanzada Persistente[8], está vinculada a una nación cuyos intereses económicos coluden con los intereses de la nación a la que pertenece la empresa. Y es que la empresa atacada es una PYME Biotech que está trabajando en una vacuna revolucionaria.

Como se requiere en estos casos, un Ciber grupo desconocido, pero a priori ligado con un antiguo grupo de ciber malhechores ya extinto, hay que dejar miguitas de pan plausibles para dificultar la investigación, reclama la autoría del ataque y pide un rescate por la información cifrada. En bitcoins, por supuesto, dejando las wallets[9] para que reciban el pago o si no los datos irán destruyéndose. De la exfiltración de información, nadie sabe nada. Curiosamente, un mes después, la nación a la que pertenece la APT antes citada pone a la venta una vacuna muy parecida a la que desarrollaba la PYME atacada.

Evidentemente, el ransomware[10] en un señuelo; el objetivo del ataque era la fórmula. Pero no acaba ahí: este hecho no pasa desapercibido y ciertos medios, ayudados por informaciones recibidas por fuentes anónimas no trazables, se hacen eco del asunto. Comienza el

7 Del inglés "command and control", se refiere a paneles de mando y control (también referenciados como C2), por el cual atacantes cibernéticos controlan determinados equipos zombie infectados con muestras de la misma familia de software dañino. El panel de comando y control actúa como punto de referencia, control y gestión de los equipos infectados. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

8 La definición ampliamente aceptada de amenaza persistente avanzada es que se trata de un ataque selectivo de ciberespionaje o cibersabotaje llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados son una amenaza persistente avanzada. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=47.html

9 Una cartera o monedero Bitcoin es un archivo con una lista de claves criptográficas que sirven para crear direcciones, cada una de las cuales está enlazada a un determinado saldo en bitcoins, y también para confirmar transacciones con criptomonedas. La cartera o monedero Bitcoin es un tipo especial de archivo cifrado wallet.dat, cuya contraseña conoce sólo el usuario del monedero. Las claves se pueden guardar en una tarjeta de memoria o simplemente, anotarse en un papel. Además, existen diversos servicios que ofrecen monederos para almacenar bitcoins en línea. https://alpari.com/es/beginner/glossary/bitcoin-wallet/

10 El Ransomware es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados, El virus lanza una ventana emergente en la que nos pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual (bitcoins por ejemplo). Uno de los Ransomware más famosos es el Virus de la Policía, que tras bloquear el ordenador infectado lanza un mensaje simulando ser la Policía Nacional y advirtiendo que desde ese equipo se ha detectado actividad ilegal relacionada con la pederastia o la pornografía. Para volver a acceder a toda la información, el malware le pide a la víctima el pago de un rescate en concepto de multa. https://www.pandasecurity.com/es/mediacenter/malware/que-es-un-ransomware/

ataque de desestabilización porque ya puestos, la APT no solo quiere que su país pueda vender la vacuna milagrosa, sino que pretende que su país sea el único en comercializarla. Para ello, tiene en mente conseguir que la Agencia Europea de Medicamentos (EMA) bloquee la comercialización, mediante la generación de dudas razonables sobre la trazabilidad y fiabilidad de los ensayos, o en cuanto a alguno de los principios activos que lleva la fórmula (no el principal, claro, ¡puesto que el que lleva la suya es el mismo!), o cualquiera de las razones posibles para retrasar o anular un lanzamiento de un medicamento.

Claro, los medios están encantados, y están siendo ayudados por una inusual viralidad y difusión no esperada. El alcance de sus informaciones nunca había sido visto antes, ciertos rumores, fake news y videos con testimonios de personas desconocidas que participaban en los ensayos, afloran, y abundan en lo que dichos medios denuncian. El caso se amplifica, y se convierte en crisis política. No solo interna, sino a nivel europeo, donde unos y otros gobernantes dejan lo que están haciendo para tratar este asunto. Mientras tanto, en otro continente, alguien se frota las manos…"

Esta ficción puede parecer novelada, pero la realidad sobrepasa este guion ampliamente. Tanto es así que la Estrategia Española de Seguridad Nacional (ESN, 2017[11]) destaca que "de manera notable, el desarrollo tecnológico está asociado a una mayor exposición a nuevas amenazas, especialmente las asociadas al ciberespacio. La hiperconectividad actual agudiza algunas de las vulnerabilidades del sistema de seguridad y exige una mejor protección de las redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano" porque, también según la Estrategia de Ciberseguridad de 2019[12] (sobre la cual se volverá más adelante), "Las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual. La tecnología e infraestructuras que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio uno de los principales riesgos para el desarrollo como nación. Por ello, la seguridad en el ciberespacio es un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su Seguridad Nacional y una competencia del Estado para crear una sociedad digital en la que la confianza es un elemento fundamental" (ANSSI, 2019).

Abundando en lo anterior, dicha Estrategia Nacional de Ciberseguridad determina que: "La nueva ciberseguridad se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social. Además de las acciones para causar efectos en los sistemas digitales, se debe tener en cuenta la concepción

11 Según la ESN 2017, las amenazas en el espacio digital adquieren una dimensión global que va más allá de la tecnología. El ciberespacio es un escenario con características propias marcadas por su componente tecnológico, fácil accesibilidad, anonimidad, alta conexión y dinamismo.

12 https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

del ciberespacio como un vector de comunicación estratégica, que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las acciones de carácter híbrido. Su potencial aplicación en situaciones muy diversas, donde se incluyen los procesos electorales, genera un elevado grado de complejidad" (ESN, 2017).

Se trata de una evolución, necesaria y adaptada a los avances actuales, de la Estrategia de Ciberseguridad Nacional de 2013[13], debido a los cambios significativos del entorno de la ciberseguridad en los últimos años. La Estrategia de 2019[14] está adaptada al nuevo paradigma geo-eco-socioeconómico y cultural, avanza un concepto amplio y ante todo transversal de ciberseguridad nacional (pero con capilaridad hasta las empresas) en relación con un nuevo análisis de riesgos en cuanto a los intereses a proteger, identificando las amenazas globales, determinando la relación con los objetivos a alcanzar en correlación con las capacidades de dichas amenazas, y adelantando las líneas de acción a seguir.

Debido a la capacidad de apalancamiento en el uso de la hiperconectividad y a la amplificación nunca vista en la comunicación debida a Internet, estados, organizaciones, grupos y colectivos o incluso individuos lambda pueden alcanzar una capacidad de influir, y por tanto de tener poder, solamente mesurable desde las técnicas de inteligencia más punteras.

La conectividad digital lleva a que, a nivel social, hoy realmente una mariposa que bata las alas en Pekín pueda provocar un tsunami en Londres[15]. Esto da a cualquier evento de seguridad una importancia estratégica que se sigue negligiendo. Como se ha visto en el ejemplo: actores estatales, privados o movidos por ideales, con método o sin método de guerra cognitiva, de la información o incluso Psyops[16], aprovechan las capacidades que ofrece Internet para la desinformación, propaganda, adoctrinamiento, avasallamiento o coerción. Según el prisma desde el que se mire la situación, es lógico estar interesado en la obtención y desarrollo de

13 https://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20ciberseguridad%20nacional.pdf

14 Por la Orden PCI/487/2019, de 26 de abril, Boletín Oficial del Estado (BOE) del 30 de abril de 2019, se publicó la Estrategia Nacional de Ciberseguridad 20191, aprobada por el Consejo de Seguridad Nacional. La publicación de esta estrategia de ciberseguridad cumple con uno de los retos identificados en el Informe Anual Seguridad Nacional2 del 2018 (IASN 2018), tal y como se contempla en la Estrategia de Seguridad Nacional 2017 (ESN 2017).

15 «El aleteo de las alas de una mariposa se puede sentir al otro lado del mundo». Este proverbio chino es el origen, junto a las investigaciones del matemático y meteorólogo Edward Lorenz, de una de las más cinematográficas teorías físicas: el efecto mariposa. Según este concepto vinculado a la Teoría del Caos, el aleteo de un insecto en Hong Kong puede desatar una tempestad en Nueva York. […] En un sistema no determinista, pequeños cambios pueden conducir a consecuencias totalmente divergentes. Una pequeña perturbación inicial, mediante un proceso de amplificación, puede generar un efecto considerable a medio y corto plazo. https://www.nationalgeographic.es/ciencia/2017/11/el-efecto-mariposa

16 Las PSYOPS, según la definición de la OTAN, son «actividades planificadas que utilizan métodos de comunicación y otros medios dirigidos a una audiencia aprobada con el fin de influir en las percepciones, actitudes y comportamientos, incidiendo así a la consecución de objetivos políticos y militares». Las PSYOPS en sí son tan antiguas como la guerra misma, aunque fueron teorizadas solamente en 1945 por Ellis M. Zacharias. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO81_2019JOAPRA_Psyops.pdf

métodos, tácticas, manuales operativos y capacidades militares para llevar la guerra al ciberespacio, incluyendo en muchos casos capacidades ofensivas; conocer la espada permite tener un mejor escudo.

No en vano, y según el "Informe Anual de Seguridad Nacional": "El ciberespacio ha jugado un papel cada vez más notable en los conflictos durante este periodo. Aumenta el interés de actores, tanto estatales como no-estatales, por los medios de comunicación en internet y las redes sociales, que adquieren consideración tanto de "campo de batalla", como de "arma de persuasión masiva" o incluso de elemento de desestabilización de la sociedad en momentos relevantes, como en los periodos electorales" (IASN, 2018).

Visto todo lo anterior, cuando ocurre un incidente cibernético, puede escalar rápidamente a una crisis económica, lo que lleva a una exposición significativa a los medios, pérdidas financieras, interrupción del negocio y deterioro de la lealtad del cliente y la confianza de los inversores; esto llevado a la enésima potencia, puede hacer caer gobiernos. Pero no solo, con el método y medios adecuados, y por las interrelaciones económicas ya listadas por las propias redes de comunicación, un análisis de la superficie de ataque que ponga de manifiesto los mejores disparos posibles a los puntos más débiles -es decir, entender cómo caerá el castillo de naipes si se actúa un poco en un punto de una forma, un poco en otro de otra forma- nos indicará qué estrategia híbrida será necesaria para que incluso un agresor asimétrico sea capaz de aprovecharlo. En el mundo hiper relacionado en el que vivimos, la lógica de análisis de conflicto debe entenderse ya como una relación habitual del débil frente al fuerte en donde, sorprendentemente, el débil ataca primero.

Ante este ecosistema, tener un plan de respuesta a incidentes, de continuidad de negocio, de resiliencia, o como quiera denominarse no es suficiente; debe formar parte de un todo mucho mayor en donde se comprendan las interrelaciones para hacer un correcto mapa de riesgo. Dicho mapa de riesgo implica la humildad de conocer el valor propio, de hacer el trabajo de evaluar la exposición real respecto de la de otros (una cadena es tan fuerte como su eslabón más débil) y de entender en qué puesto se está en el orden de ataque de los adversarios. Como se verá más adelante, la disciplina de la Ciberinteligencia es una solución interesante, por su capacidad de evaluación de escenarios y ponderación, acorde a la realidad del terreno, de las amenazas y actores sobre el mapa de conflicto respecto de las vulnerabilidades existentes.

La situación actual, de una gran competición en todos los ámbitos, impacta en el orden internacional y en los acuerdos que daban estabilidad al sistema. Los terrenos conflictivos son muchos y difusos; van desde los puramente militares, pasando por los ciberataques, llegando hasta una profunda guerra de las ideas en donde los terrenos antes citados no son sino los diversos teatros de operaciones interrelacionados en la guerra que trata de imponer un sistema de ideas frente a otros.

En este punto, destacan el crecimiento de los denominados conflictos y acciones híbridas planteadas desde el concepto de conflicto asimétrico.

2.1. Características generales de las acciones híbridas

No existe una definición universalmente aceptada, considerándose que el término es demasiado abstracto y que una guerra híbrida es en realidad una guerra irregular. La guerra híbrida es una guerra con los siguientes aspectos:

- Un adversario híbrido no siempre es un estado.
- Es un oponente híbrido que utiliza una combinación de métodos convencionales y no convencionales.
- Los métodos y tácticas empleados combinan armas convencionales y armas no convencionales (municiones que pueden incluir dispositivos nucleares, biológicos, químicos y explosivos improvisados, así como ciberarmas.), tácticas irregulares, acciones terroristas, violencia indiscriminada y actividades delictivas de financiación o de debilitamiento del oponente.
- Un adversario híbrido también realiza acciones encubiertas (como acciones terroristas y ciberterroristas de falsa bandera) para evitar ser detectado. Estos métodos se utilizan simultáneamente durante el conflicto con una estrategia unificada pero usando todo el arsenal posible.
- Uso de herramientas de comunicación masiva para propaganda. El desarrollo de redes de comunicación masiva ofrece poderosas herramientas de propaganda y captación, así como posibilidades de ciberataques y para realizar campañas de desinformación.
- Los límites morales, legales y éticos no son los mismos para cada beligerante.

Haciendo la suma de todo lo anterior, la noción de amenazas híbridas se refiere a las diversas actividades coercitivas que comprometen la seguridad, mezclando métodos convencionales y no convencionales, que pueden ser diplomáticos, militares, económicos o técnicos, siendo el ámbito cibernético un teatro de operaciones más, aunque transversal, como veremos. Estas actividades son utilizadas de manera coordinada, metodológica, con doctrina y herramientas adecuadas, por actores estatales y no estatales, para lograr objetivos específicos sin traspasar el umbral de una guerra declarada oficialmente.

En general, estas amenazas se dirigen a vulnerabilidades importantes que el atacante habrá listado en los análisis de interdependencias listadas en un documento llamado “análisis de la superficie de ataque”, y tienen como objetivo multiplicar los ejes de ataque aunque en realidad se trate de uno solo. Los ciberataques, la interferencia electoral y las campañas de desinformación son ejemplos. Las redes sociales se pueden utilizar para orientar las discusiones sobre políticas o para radicalizar, polarizar, reclutar y liderar actores intermediarios.

Estas amenazas híbridas de rápido desarrollo plantean un desafío considerable para la seguridad de los bloques políticos porque tienen por objetivo, y tienen la capacidad de, afectar a varios Estados al mismo tiempo y así desestabilizar los bloques de poder en su conjunto.

Como el análisis de interdependencias busca hacer aflorar los vínculos más débiles para que se puedan efectuar los mejores disparos,

son las infraestructuras críticas los objetivos de nivel uno, evidentemente. Pero para hacer caer un muro fortificado, solo es necesario encontrar una grieta.

3. Características generales de las guerra asimétricas

El mariscal Tito, héroe de la resistencia yugoslava contra los alemanes durante la Segunda Guerra Mundial, solía decir a sus hombres: "Nunca luches contra el adversario en su terreno. Agáchate, escóndete y golpéalo entonces, cuando no esté en una posición capaz de dominarte...". Su fuerza fue vencer a los nazis negándose a tener enfrentamientos directos, pero aprovechándose del desequilibrio que existía entre sus tropas y el ocupante.

Los conflictos asimétricos oponen a adversarios con diferentes lógicas de guerra, lo cual las hace extremadamente difíciles de gestionar. Una guerra asimétrica es un conflicto entre combatientes cuyas fuerzas no son equiparables y en donde el desequilibrio militar, sociológico, cultural y político entre los dos campos es total: un ejército regular fuerte contra un movimiento guerrillero aparentemente débil; una nación contra un movimiento terrorista, un sistema fuerte contra un grupo reducido pero ágil y técnicamente fuerte, etc. En una guerra asimétrica, lo que entra en conflicto, son las ideas, las normas y percepciones.

Para Moreau-Defarges (2016) este es "un conflicto asimétrico, todos los medios son buenos para lograr la victoria, las reglas se rompen". La Globalización es la causa principal de las actuales guerras asimétricas puesto que han creado frustraciones a escala planetaria cuando, en otro nivel, facilita el comercio de armas, materiales peligrosos y el flujo de capital".

La guerra asimétrica enfrenta a dos fuerzas desiguales entre sí, no solo en los medios que despliegan, sino también en la forma en que se utilizan. Los posibles de los estados con ejércitos y fuerzas policiales con misiones claramente definidas, doctrinas, códigos de conducta suscritos e impuestos (p.e. Convención de Ginebra) es reemplazada por percepciones sobre el bien y el mal muy difusas en el lado contrario. Desde individuos hasta grupos, clanes, familias, tribus o colectivos, se contempla entre los posibles las nuevas áreas de enfrentamiento como la infosfera[17] y el ciberespacio que complementan los lugares tradicionales de oposición (aire, tierra, mar) siendo el ciberespacio, otro teatro de operaciones considerado transversal. Las formas asimétricas de guerra, utilizadas de forma independiente o en combinación son: no violencia; violencia política; terrorismo y guerra de la información.

Finalmente, dentro de la doctrina de acción en guerras asimétricas se cita los siguiente: "Sin inteligencia, sin

17 Portail de l´IE: Como la palabra "biosfera", la palabra "infosfera" es un neologismo compuesto por las palabras "información" y "esfera". Designa tanto un entorno global, compuesto por información, como todo tipo de datos que pasan o se almacenan allí. El ciberespacio es un ejemplo de una esfera de información, pero la infosfera no se limita solo a los entornos en línea.

información, las fuerzas difícilmente pueden distinguir entre los enemigos asimétricos y la población en cuyo seno operan, dando lugar a procedimientos tales como los de realizar detenciones indiscriminadas y prolongadas. Lograr una inteligencia de calidad se convierte en un aspecto clave en este tipo de conflictos. Los requerimientos de inteligencia e información serán diferentes a los de operaciones convencionales: En un conflicto asimétrico asumen una gran importancia las evaluaciones de factores tales como la personalidad de los individuos involucrados, las razones de la lucha y sus objetivos últimos, las costumbres locales y otros aspectos sociopolíticos. Importancia de la Inteligencia. Se deben potenciar todas las fuentes de información, tanto civiles como militares, siendo conveniente montar acciones de alcance variable y con finalidad primordialmente informativa. Adquieren una importancia vital los elementos infiltrados y las tecnologías aplicadas a la vigilancia por lo que será indispensable la colaboración con las agencias estatales encargadas de obtener información." (Díaz-Caneja, s/f).

4. Gestión de riesgos como problema

Según el Instituto Nacional de Ciberseguridad (INCIBE) "En la actualidad nuestras organizaciones tienen una gran dependencia de sus sistemas de información. Proteger estos sistemas implica que destinemos una serie de recursos para implantar las medidas de seguridad adecuadas. La mejor manera de destinar estos recursos de un modo adecuado es identificar los principales riesgos a los que están expuestos nuestros sistemas de información. ¿Cómo? A través de un análisis de riesgos, (INCIBE, 2014)"

El riesgo es una proyección, más o menos matemática, de lo que puede ocurrir: es el producto del impacto (estimado) por la probabilidad (estimada) de que la amenaza se materialice, una vez detectada y perfilada dicha amenaza. Identificados y estimados los riesgos, el proceso pasa por implementar medidas de seguridad adecuadas tanto a las capacidades de las amenazas (podría darse la casuística de la existencia de vulnerabilidades que ninguna amenaza pueda aprovechar en un instante $T_{0)}$ como a los posibles de la empresa u organización. Las medidas de seguridad a implantar deben ser tales que cubran todas las capacidades de ataque de los actores sin exceder esa capacidad de ataque detectada, ya que nuestro sistema de seguridad no gestionaría el riesgo correctamente (la gestión del riesgo es, en suma, una especulación sobre la materialización de un riesgo, en donde organización apuesta a que no se materializa).

El enfoque habitual en la gestión del riesgo podría no ser el adecuado cuando hablamos de sistemas interrelacionados: amenazas que se solapan, actores externos que colaboran, elevada interdependencia de infraestructuras, varias dimensiones superpuestas de exposición (tierra, mar, aire, espacio junto al ciberespacio), a través de medios híbridos en lo que, a todas luces y por la naturaleza de los atacantes, puede categorizarse de conflicto asimétrico (MAGERIT, 2012).

En la compleja tarea del análisis de riesgos que estudia y estima por parejas activo-amenaza no se contempla, por ejemplo que:

- Las amenazas pueden solaparse y probablemente lo hagan.

- Los agentes externos pueden tener intereses comunes contra nosotros y probablemente se alíen temporalmente o aprovechen un ataque en curso, cada uno aportando sus puntos fuertes.
- Las empresas están fuertemente relacionadas, pero su gestión (y, por tanto, su análisis de riesgos) es independiente.
- Los actores maliciosos efectúan su propia inteligencia y descubren las interrelaciones entre los sistemas, atacando a empresas relacionadas para llegar a su auténtico objetivo principal. Si bien, estos actores saben cómo hacer un mapa de riesgos, las empresas rara vez saben o lo hacen.
- Limitar el ámbito de la ciberinteligencia al análisis técnico del software y las infraestructuras y equipamientos que sustentan el ciberespacio, origina un problema de falta de concreción, relevancia y gestión del riesgo real en toda su magnitud.
- El ciberespacio no es el 5º campo de batalla tras tierra, mar, aire y espacio; es transversal a todos ellos y aumentará sus riesgos de forma exponencial.
- La ausencia de un componente estratégico en el análisis impide la comprensión de los ciber incidentes dentro de un contexto amplio, en el cual operan variables de carácter político, económico, social y cultural.

En el 2021, este enfoque está obsoleto. En nuestra realidad ya no hay amenazas segmentadas, cuantificadas y aisladas actuando en un solo ámbito. Los actores maliciosos ya no son independientes: se asocian por unidad de negocio o por pool de expertise (el ejemplo claro es el grupo hacktivista Anonymous, en donde existen "especialistas", de diferentes grupúsculos hacktivistas, para diferentes fases de reconocimiento de objetivos plausibles a atacar). La complejidad del escenario geo-eco-político actual nos impele a abordar esta nueva forma de conflicto económico, expresado en el ciberespacio, con otras metodologías y herramientas, las de una disciplina que trabaja siempre desde la incertidumbre, la valoración de información y de fuentes, la evaluación escenarios futuros, el descubrimiento de hipótesis no aparentes y la sistemática analítica: la Inteligencia.

En esta disciplina se usan, por ejemplo, metodologías de análisis morfológico, procedimientos sistemáticos para identificar todas las combinaciones posibles entre varios conjuntos de variables combinando la metodología de Comprobación de Supuestos Clave con la Generación de Escenarios Múltiples con el fin de eliminar los puntos ciegos, siempre basándonos en información fresca, cotejada y validada.

Desde la perspectiva de la Inteligencia debemos identificar las amenazas, los actores, sus capacidades y motivaciones, el modus operandi y estimar su impacto en el funcionamiento de las empresas en su contexto complejo. La aplicación de estas metodologías identificará las variables que rigen el sistema, evaluará las capacidades de los actores y sus veleidades, haciendo, por fin, correcta la evaluación del riesgo. Entendido, éste, desde la interrelación e hiper conexión.

La Ciberinteligencia, debe ser aclarado, no pretende controlar el ciberespacio sino obtener información sobre él para, una vez analizada, integrarla con información proveniente de otras fuentes y favorecer una mejor

comprensión de las capacidades, intenciones, acciones potenciales, vulnerabilidades e impacto en el entorno operativo del adversario, cruzando cada dato uno a uno y todos entre sí (LISA Institute 2019 y 2020).

La clave es pasar de un modelo de ciberseguridad de carácter preventivo y defensivo completamente reactivo a uno más proactivo y que incorpore elementos de mayor capacidad evaluativa, debido al contexto actual de competencia geopolítica, en donde todo vale menos que se pueda atribuir un ataque de forma correcta al atacante correcto. El modelo, por tanto, debería comportar "ver lejos" mediante inteligencia, colocar captores de información en los lugares en donde se pergeñan las acciones maliciosas; y hacer contra influencia en esos mismos sitios para desactivar los ataques incluso antes de que se concreten.

5. Reflexiones finales

Las empresas están fuertemente relacionadas, comparten recursos, medios, colaboradores, distribuidores, proveedores, cadenas de suministro, redes y sistemas, etc. Cabe preguntarse: ¿Si cae el suministro eléctrico son igual de potentes mis salvaguardas?; ¿Si mi marca se ve afectada por una fake new, puedo seguir financiándome en mercados alternativos, por ejemplo?; ¿Si mi proveedor principal cae, tengo plan B?; ¿Si un ataque informático me obliga a teletrabajar, mi información seguirá teniendo el mismo nivel de protección?; ¿Qué pasa si a + b+ c + d? ¿Hasta dónde aguanto los embates del temporal?; ¿Cuántas incidencias más puedo añadir antes de caer?

Lo necesario en estos casos es hacer el mapa de interrelaciones de primer, segundo y hasta tercer nivel, evaluar las variables del sistema en general y del sistema propio en particular, y hacer el análisis de los impactos cruzados para entender las interdependencias directas e indirectas. Solo así se conoce cada punto débil de la cadena y cómo podría ser atacado desde la perspectiva "¿qué podrían hacer mis enemigos/contrincantes/adversarios/competidores contra mí si tuvieran veleidades maliciosas y todos los recursos necesarios? ¿Cuá sería el peor ataque posible y cómo se lograría?". Es la única forma de evitar la miopía de la auto confirmación y el concepto de satrapía bastionada que entiende que cada organización navega sola.

Existe una disciplina, la inteligencia económica, y más concretamente y para este caso, la Ciberinteligencia, que es capaz de ver las cosas desde otro modo. Y el modo en que lo ve es el diametralmente opuesto al que se aplica por norma: entender el riesgo del sistema en el que está cada empresa a proteger, a través de la obtención y análisis de información fiable, actualizada y cotejada.

La metodología de análisis de inteligencia, proviene del mundo militar, y por citar algunos métodos como Quadrant Crunching (QC), (desarrollado para ayudar a los analistas de contraterrorismo a identificar todas, y cada una, de las posibles formas de ataques terrorista), ayuda a los analistas a evitar sorpresas estratégicas al examinar múltiples combinaciones posibles de variables clave seleccionadas, sin dejar ninguna fuera. Esto permite catalogar cada escenario entre las categorías de posible, probable, deseable y catastrófico. De esta forma, advierte del peor escenario posible, permitiendo evitarlo. También ayuda a los analistas a identificar y desafiar sistemáticamente

los supuestos, explorar las implicaciones de suposiciones contrarias y descubrir "incógnitas desconocidas", evitando todo sesgo en la evaluación de la información.

Sin embargo, hay una cantidad de relaciones de riesgo no evaluadas, las empresas no se lanzan a este tipo de ejercicio y especulan con que ningún ataque híbrido de beligerante asimétrico pueda colapsar el sistema desde pequeñas pero quirúrgicas acciones maliciosas. O puede ser que desconozcan el proceloso mar en el que navegan. Hay que decirlo, los grupos maliciosos son atacantes experimentados, pacientes, rigurosos y bien financiados: ejecutarán el ataque al punto más débil para obtener lo que buscan, y esto puede ser incluso hacer caer el sistema.

Desde el entendimiento del nuevo ecosistema del ciberespacio y modificando los sistemas de evaluación de riesgos añadiendo la transversalidad de la metodología de Ciberinteligencia, se podrá evaluar con mayor certeza el riesgo de ser objeto de ataques; y poner las salvaguardas lejos de las murallas mediante ciber influencia, desactivando los ataques incluso antes de que se conciban.

Referencias bibliográficas

Agence nationale de la sécurité des systèmes d'information-ANSS (2019). Maîtrise du risque numérique : l'atout confiance. https://www.ssi.gouv.fr/uploads/2019/11/anssi_amrae-guide-maitrise_risque_numerique-atout_confiance.pdf

Bello, E. (2021). Ciberseguridad: Tipos de ataques y en qué consisten. IEBSCHOOL. https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Deloitte Touche Tohmatsu Limited (2019). *Inteligencia cibernética ¿Cómo puede la IA ayudar a manejar el riesgo cibernético?* https://www2.deloitte.com/content/dam/Deloitte/cr/Documents/risk/doc/2019-Inteligencia-Cibernetica.pdf

Díaz-Caneja, J. (s/f). *Manual de Ciberinteligencia*. Universidad Francisco de. Fco de Vitoria.

González Hernández, M. (2015). *Las Redes Sociales y su Incidencia en la Forma en que los Jóvenes se Comunican y Utilizan la Lengua: Perspectiva de los Docentes de Lenguaje y Comunicación*. [Tesis para optar al Título de Magíster en Educación, Mención Currículo y Comunidad Educativa]. https://repositorio.uchile.cl/bitstream/handle/2250/136443/Tesis_Melisa_Gonz%C3%A1lez_Hern%C3%A1ndez.pdf

Illinois Association of School Nurses-IASN (2018). *Informe Anual de Seguridad Nacional*. https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

Instituto Nacional de Ciberseguridad-INCIBE (2014). *Informe Anual de Actividad de INCIBE 2014*. https://www.incibe.es/extfrontinteco/img/File/actividad_2014.pdf

Instituto Nacional de Ciberseguridad-INCIBE (2014). Sigue el camino del análisis de riesgos. [Mensaje de Blog]. https://www.incibe.es/en/node/2676

LISA Institute (2019). *Ciberinteligencia: ventajas de su uso a nivel táctico y estratégico*. https://www.lisainstitute.com/blogs/blog/ciberinteligencia-ventajas-uso-tactico-estrategico

LISA Institute (2020). ¿Qué es y para qué sirve la Ciberinteligencia?.

https://www.lisainstitute.com/blogs/blog/ciberinteligencia-que-es-y-para-que-sirve

MAGERIT – versión 3.0 (2012) Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Edita: © Ministerio de Hacienda y Administraciones Públicas. Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones Colección: administración electrónica NIPO: 630-12-171-8. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Moreau-Defarges, P. (2016). *Que sais-je?* Edit. Puf Code

Seguridad Nacional (2017). *Estrategia de Seguridad Nacional 2017*. https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

Vélez, P. (2019). Una de las principales transformaciones de la revolución 4.0 es la digitalización. La alta dependencia a las tecnologías hace indispensable contar una adecuada gestión. LR La República. https://www.larepublica.co/internet-economy/la-importancia-del-riesgo-cibernetico-2928179