LOS RETOS DE LA CIBERINTELIGENCIA

EVA MARTÍN IBÁÑEZ

DOCTORA EN CIENCIAS DE LA INFORMACIÓN Y ANALISTA DE INTELIGENCIA

RESUMEN

Para cualquier organización, pública o privada, la inteligencia es clave para alcanzar y mantener la superioridad en el ciberespacio. El objetivo de la ciberinteligencia es obtener, analizar y elaborar información para proporcionar una evaluación de amenazas completa, precisa, oportuna y relevante, que ayude a los decisores a actuar basándose en ese análisis. En un entorno tan dinámico como el ciberespacio hace falta una visión integral para comprender las ciberamenazas. El enfoque reactivo debe dar paso al proactivo, que implica esbozar un panorama más completo sobre qué sucede y por qué.

Palabras clave: inteligencia, ciberinteligencia, ciberespacio, ciberdefensa, ciberseguridad, análisis de inteligencia.

ABSTRACT

To any public or private organization, intelligence is the key to reach and maintain superiority in cyberspace. The aim of cyberintelligence is to collect, analyze and produce information to provide a complete, accurate, timely and relevant threat assessment that helps decision-makers to take action based on that analysis. In such a dynamic environment as cyberspace, an integral vision is required to understand cyber threats. Reactive focus has to be replaced by a proactive one, which involves outlining a more detailed outlook on what happened and why.

Keywords: intelligence, cyberintelligence, cyberspace, cyberdefense, cybersecurity, intelligence analysis.

1. INTRODUCCIÓN

El debate sobre la ciberdefensa tiende a fijarse en un solo aspecto de las posibles operaciones en el ciberespacio: las respuestas defensivas y las acciones dentro de la red. Algo similar sucede con la ciberinteligencia, que suele limitarse a apoyar misiones defensivas generalmente restringidas a la propia red. A ese nivel, las acciones son típicamente reactivas y suelen producirse cuando el adversario ya está dentro. Lo habitual es centrarse en lo visible dentro de una red, en lugar de mirar fuera de ella, y completar ese conocimiento con información adicional. Por el contrario, el enfoque proactivo se ocupa de verificar continuamente la información, buscando nuevos datos e intentado entender lo desconocido. En el enfoque proactivo las fronteras entre lo táctico, lo operativo y los estratégico se difuminan.

2. CONCEPTOS PRELIMINARES

Una definición clásica describe la inteligencia como información procesable. En primer lugar, es información que ha sido previamente analizada, no simples datos. En segundo, debe ser procesable, en el sentido de susceptible de ser utilizada para tomar una decisión o una acción. En caso contrario, no sirve de nada. En un entorno tan cambiante como el ciberespacio, el valor de la inteligencia puede desvanecerse en días o incluso en horas; caduca enseguida (Farmham y Leune, 2013: 2).

Ciberinteligencia, según el SEI Emerging Technology Center de la Universidad Carnegie Mellon, es la adquisición y el análisis de la información para identificar, rastrear y predecir cibercapacidades, intenciones y actividades que ofrecen cursos de acción para mejorar la toma de decisiones (Ludwig et al., 2013, 2).

Por su parte, para la compañía RSA, ciberinteligencia, en sentido amplio, es el conocimiento sobre los ciberadversarios y sus métodos, combinado con el conocimiento sobre la postura sobre la seguridad de una organización frente a esos adversarios y sus métodos, a partir de los cuales se genera consciencia situacional y/o inteligencia procesable (INSA, 2014 marzo: 3).

3. LA INTELIGENCIA EN LA ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

¿Qué dice la Estrategia de Ciberseguridad Nacional de España sobre la inteligencia? En el objetivo I, Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia, indica que “además de mejorar las capacidades de los sistemas militares de Defensa y de inteligencia es necesario reforzar la seguridad de los Sistemas de Información y Comunicación estratégicos, adaptándolos a los nuevos riesgos y amenazas del ciberespacio” (Gobierno de España, 2013: 23).

La línea de acción 1 (Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas) establece dos medidas relacionadas con la inteligencia, la primera y la última:

Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas que permitan la identificación de procedimientos y orígenes de ataque, y la elaboración de la inteligencia necesaria para una defensa y protección más eficaz de las redes nacionales (...)

Potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional (Gobierno de España, 2013: 31-32).

En la línea de acción 4 (Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia) la segunda medida señala la conveniencia de:

Ampliar y mejorar las capacidades de los organismos con competencias en la investigación y persecución del ciberterrorismo y la ciberdelincuencia así como asegurar la coordinación de estas capacidades con las actividades en el campo de la ciberseguridad, a través del intercambio de información e inteligencia por los canales de comunicación adecuados (Gobierno de España, 2013: 35).

Por otro lado, la Estrategia de Ciberseguridad Nacional española no solo contempla la inteligencia como una necesidad, sino que también valora la inteligencia de Estados extranjeros como una amenaza: “existen evidencias de que determinados

países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la Seguridad Nacional" (Gobierno de España, 2013: 10). España no es el único país con una visión similar; es el caso de Canadá, Reino Unido o Australia, por ejemplo. La estrategia canadiense apunta que las ciberamenazas más sofisticadas provienen de servicios de inteligencia y militares de Estados extranjeros (Government of Canada, 2010: 5). Por su parte, la de Reino Unido también lo recoge entre las amenazas: distintos grupos -delincuentes, terroristas, servicios de inteligencia extranjeros y fuerzas militares extranjeras- están actuando contra intereses de Reino Unido en el ciberespacio (Cabinet Office, 2011: 16). Igualmente, la ciberestrategia australiana destaca que hay un número creciente de actores estatales y no estatales que están comprometiendo, robando, modificando o destruyendo información y, por tanto, causando potencialmente alteraciones críticas en los sistemas australianos. La distinción entre actores tradicionales -hackers, terroristas, redes de crimen organizado, espías industriales y servicios de inteligencia extranjeros- se está desdibujando (Australian Government, 2009: 3).

La obtención de inteligencia es una práctica aceptada entre los Estados para llevar a cabo las relaciones exteriores. A lo largo de la historia, los actores estatales han recopilado información sobre las intenciones, capacidades y las políticas, tanto de Estados amigos como rivales. Y, en la era actual, la inteligencia desempeña un papel cada vez más importante. La información es la nueva posición de ventaja estratégica (Crane, 2002: 312).

4. POSICIÓN DE VENTAJA EN EL CIBERESPACIO MEDIANTE LA INTELIGENCIA

Históricamente, la humanidad ha librado batallas, ha comerciado y ha establecido un régimen de política internacional en un entorno tridimensional de tierra, mar y aire. Sin embargo, el ser humano ha creado otra dimensión que moldeará su evolución a lo largo de este nuevo milenio. Esa cuarta dimensión es el ciberespacio, en el que la comunidad de la inteligencia y la jurídica, entre otras, deben desarrollar la habilidad de operar. Al fin y al cabo, la cuarta dimensión del ciberespacio es el campo de batalla del futuro (Crane, 2002: 312).

El ciberespacio es un dominio global dentro del entorno de la información, formado por Internet, redes de comunicaciones, sistemas informáticos, procesadores embebidos y usuarios. Las fuerzas armadas cada vez dependen más de sistemas informáticos en red. El ciberespacio es una fuente de fortalezas y debilidades para la guerra moderna (Eom, Kim, Kim y Chung, 2012: 295).

A nivel operativo, el ciberespacio presenta los mismos retos que un campo de batalla tridimensional. Los conceptos de velocidad, masa, maniobra, sorpresa, conquista de la posición de ventaja, mando y control, y apoyo de avance, entre otros, resultan aplicables. El comandante debe ser capaz de operar en el ciberespacio con la misma familiaridad y precisión que en tierra, mar o aire, integrando fluidamente esos cuatro entornos para conseguir un dominio integral. La superioridad en la información está relacionada con la nueva posición de ventaja. Quien logre el dominio de la información puede conformar la batalla de modo que no solo resulte más letal para el adversario, sino que además facilite la supervivencia de las fuerzas aliadas (Crane, 2002: 315).

La superioridad en el ciberespacio es la ventaja operativa en, a través de y desde el ciberespacio para llevar a cabo operaciones militares en cualquier momento y lugar

sin interrupciones. Depende de la idea de evitar que los rivales bloqueen las fuerzas propias e impidan la consecución del objetivo final. Las operaciones en el ciberespacio incluyen operaciones en redes informáticas y acciones para gestionar y defender los sistemas globales de información. La ciberguerra se puede librar entre naciones, pero también puede acontecer entre actores no estatales. Sucede cuando las operaciones en el ciberespacio extienden su poder más allá de las fronteras defensivas de la rejilla de información global para detectar, disuadir, denegar y vencer a los enemigos. La ciberguerra usa la ciberexplotación, el ciberataque y la ciberdefensa en el ciberespacio (Eom et al., 2012: 296).

En la doctrina militar, el punto clave se refiere a aquellas áreas que, si son conquistadas, proporcionan una ventaja al atacante o al defensor. Si se aplica al terreno geográfico, ese concepto resulta claro; puede aludir a una colina que domina un valle que un enemigo quiere controlar o a un puente sobre un río que debe atravesarse antes de emprender un ataque. El dominio del punto clave decide el resultado de la batalla. Sin embargo, el punto clave dentro del ciberespacio presenta algunas diferencias respecto al mundo físico, porque el ciberterreno existe en cinco planos: el geográfico, el físico, el lógico, el de las ciberpersonas y el supervisor (Raymond et al., 2014: 291), tal y como muestra el cuadro siguiente.

Ciberterreno y planos del ciberespacio				
Planos del ciberespacio	**Puntos clave del ciberterreno**	**Ejemplos según los niveles de guerra**		
		Táctico	**Operativo**	**Estratégico**
Plano **supervisor**	Canal de mando y control	Canales inalámbricos usados para comunicaciones con el mando y control	Sistemas de seguridad localizados en el centro de seguridad y operaciones de red	Sistemas de lanzamiento nuclear
Plano de **ciberpersonas**	Cuentas de usuario; certificados	Cuentas del administrador local del sistema	Credenciales de red para el mando del centro de seguridad y operaciones de red	Cuentas de correo electrónico y contraseñas de un candidato presidencial u otros figura clave
Plano **lógico**	Software; direcciones lógicas	Sistema operativo de los ordenadores de sobremesa en la organización objetivo	Servidor acreditado de nombres de dominio (DNS) de un sitio web	El software de una red de comunicaciones móviles regional
Plano **físico**	Hardware; direcciones físicas	Una llave USB; un teléfono móvil; un conmutador Ethernet	Cables de comunicación regionales; radares de defensa antiaérea; red de alerta temprana	Centro de datos de una agencia gubernamental o de una compañía industrial
Plano **geográfico**	Ciudad, país; lugar físico	Localización física de los dispositivos de red que proporcionan servicio	Central eléctrica que suministra energía a la ciudad	Desarrollar capacidades ofensivas en el ciberespacio para la nación
Fuente: Elaboración propia a partir de Raymond et al., 2014: 296				

1. El plano supervisor proporciona la vigilancia y la autoridad para iniciar, parar, modificar o redirigir una ciberoperación. Comprende los elementos del

ciberespacio que desempeñan una función supervisora o proporcionan un conducto para el mando y control.

2. El plano de las ciberpersonas está relacionado con las identidades dentro del ciberdominio. Un mismo individuo físico puede mantener varias identidades. Aquí el ciberterreno se extiende a cuentas de usuario y credenciales que dan acceso a recursos de información.

3. El plano lógico está formado por el sistema operativo, las aplicaciones de software y la configuración de un dispositivo, y los enlaces lógicos entre dispositivos de una red. El ciberterreno incluye una amplia variedad de sistema de software, servicios y protocolos con los que funcionan las redes.

4. El plano físico es el mapa de la capa física del modelo de interconexión de los sistemas abiertos, incluyendo los componentes de un sistema informático y el hardware conectado. El ciberterreno son los routers, los conmutadores y otros dispositivos conectados físicamente a la red.

5. El plano geográfico describe el área física donde reside el sistema de información o alguna de sus partes. Es el plano más estático de los cinco. Aunque la localización lógica de una red dentro del ciberespacio sea importante, también es relevante su posición geográfica. Cualquier fallo de localización puede resultar costoso, sobre todo en ciberoperaciones realizadas por actores estatales. Sobrevolar el espacio aéreo de un tercer país para bombardear otro puede causar incidentes internacionales, igual que reenviar paquetes de ataque a través de un tercero neutral. Los riesgos son particularmente importantes en las ciberoperaciones donde la ruta que los datos siguen a través de Internet raramente se puede controlar o incluso predecir con precisión (Raymond et al., 2014: 291-292).

El ciberespacio se puede examinar usando métodos militares tradicionales de análisis del terreno como OCOKA (Observation and Fields of Fire, Cover and Concealment, Obstacles, Key Terrain, and Avenues of Approach). Este acrónimo inglés equivale a observación y campos de fuego; cobertura y ocultación (camuflaje); obstáculos (naturales o artificiales); puntos clave (zonas importantes del campo de batalla); y vías de acceso (rutas de aproximación). Ahora bien, en el caso del ciberespacio, ese análisis presenta algunas particularidades (Raymond et al., 2014: 292):

1. Observación y campos de fuego. Observar implica la habilidad de ver las fuerzas enemigas. Un campo de fuego combina la observación con la capacidad de combatir los objetivos enemigos dentro del alcance máximo del arma disponible. La idea de observar el terreo sigue teniendo sentido en el ciberespacio. El reconocimiento puede extraer información útil a partir de rangos de direcciones IP y nombres de dominio (DNS). Escaneando puertos, es posible saber qué servicios están activos en las redes. Otras herramientas pueden desvelar las versiones del sistema operativo y del resto del software. Como en el mundo físico, la observación del ciberterreno está basada en el punto de observación panorámico. Por ejemplo, escanear una red desde fuera de un cortafuegos ofrece resultados totalmente distintos que hacerlo desde dentro. La actividad de un intruso dentro de un *honeypot* (equipo trampa) suministra información valiosa sobre sus verdaderos recursos de red.

2. Cobertura y ocultación. En términos cinéticos, la ocultación protege a un individuo de la observación, mientras que la cobertura protege de la observación y del fuego enemigo. A veces el camuflaje sirve para proporcionar ocultación. En el ciberespacio, al igual que en el mundo físico, existe una tercera categoría en la que se puede avistar un objetivo pero no es posible enfrentarse a él porque está fuera del alcance de las armas que tiene el adversario. Un defensor de una red puede recurrir a cortafuegos para evitar que el tráfico alcance servidores de almacenamiento específicos a la vez que protege esos sistemas de la observación. Un atacante precisa ocultarse para evitar ser detectado. Códigos polimórficos y otras técnicas de ofuscación que reducen la detección del malware basada en firmas suelen usar códigos maliciosos que se camuflan para sortear el bloqueo de los sistemas anti-intrusiones.

3. Obstáculos. En el ciberespacio, los obstáculos son aquellas tecnologías y políticas que limitan la libertad de movimientos dentro de una red. Por ejemplo, listas de control de acceso, cortafuegos y otros medios para restringir la circulación de paquetes por la red. En el ciberterreno, la distinción entre obstáculos y cobertura no siempre está clara. Un dispositivo instalado para limitar la libertad de movimiento del enemigo también puede proporcionar cobertura frente a una intrusión. En el campo de batalla cinético, los obstáculos pueden ser naturales o artificiales. Una distinción similar se produce en el ciberespacio, donde algunos obstáculos son deliberados (como un cortafuegos) y otros involuntarios, como el enmascaramiento de puntos de acceso dentro de una red doméstica inalámbrica resultado de la asignación de una única dirección IP a múltiples dispositivos por parte de un proveedor de acceso a Internet.

4. Puntos clave. El ciberterreno clave abarca todos los aspectos relacionados con sistemas, dispositivos, protocolos, datos, software, procesos, ciberpersonas y otras entidades de red, cuyo control ofrece una marcada ventaja para un atacante o un defensor.

5. Vías de acceso. Las rutas de aproximación en el ciberespacio están compuestas de varios caminos que pueden recorrerse para alcanzar un objetivo. Las vías físicas que conectan los sistemas como los conmutadores, los routers, la fibra o los cables Ethernet a menudo son menos relevantes que las conexiones lógicas que facilitan y limitan esos dispositivos, porque los flujos de Internet pueden cambiar a lo largo del tiempo. Una vía de acceso a una red puede ser una conexión HTTP a un servidor web. También pueden incluir ataques de *phising* (Raymond et al., 2014: 292-294).

La ciberinteligencia es un prerrequisito para mantener la superioridad en el ciberespacio. Incluye la cibervigilancia y el ciberreconocimiento, el ciberorden de batalla, el orden preposicional de cibertareas, la evaluación de ciberdaños y las ciberoperaciones psicológicas. En primer lugar, necesita un sistema de vigilancia para monitorizar ciberataques de forma efectiva. En segundo, debe configurarse el ciberorden de batalla, con información detallada sobre nuestros sistemas y los sistemas rivales. En tercero, el orden preposicional de cibertareas abarca las vulnerabilidades de los sistemas objetivo, las herramientas de pirateo, los servidores zombis y de mando y control, y la planificación temporal del ataque. En cuarto lugar, hace falta desarrollar un método de evaluación de ciberdaños, que estime los perjuicios resultantes de la aplicación de fuerza militar letal

y no letal en el mundo físico. Finalmente, las operaciones ciberpsicológicas deben comprender la propaganda y otras técnicas de comunicación persuasiva para influir en las opiniones, sentimientos y actitudes de todos los países y los grupos relacionados para alcanzar los intereses nacionales en el ciberespacio (Eom at al., 2012: 298).

El reto para la comunidad de la inteligencia es determinar hasta dónde puede llegar a la hora de preparar la batalla o la defensa en el ciberespacio. Existen preocupaciones operativas y políticas durante la transición, desde las operaciones tridimensionales a la cuarta dimensión del ciberespacio. Para entender el contexto, el analista de inteligencia debe conocer, entre otros datos, los sistemas de información del adversario; la composición política, económica, social y cultural; los procesos de toma de decisiones; las fortalezas y debilidades geográficas; y los perfiles biográficos y psicológicos. El concepto de medios mínimamente intrusivos es aplicable a los límites de la obtención de inteligencia [incluso en el ciberespacio], igual que el principio de proporcionalidad recogido en el derecho internacional humanitario (Crane, 2002: 315-316).

5. LA PRÁCTICA ACTUAL DE LA CIBERINTELIGENCIA

Recientemente el SEI (Software Engineering Institute) de la Universidad Carnegie Mellon ha publicado un estudio sobre el estado de la práctica de la ciberinteligencia. Los participantes son 26 organizaciones, entre las que figuran seis agencias gubernamentales, empresas de diversos sectores y universidades. En las conclusiones, el informe destaca que existe una gran variedad de enfoques para abordar la ciberinteligencia en los ámbitos gubernamental, empresarial y universitario. No hay ningún estándar para desarrollar programas, recopilar datos, ni entrenar a los analistas de ciberinteligencia. Cualquier organización (gobierno, empresa o universidad) puede conseguir un rendimiento excelente en ciberinteligencia si logra un equilibrio entre la necesidad de proteger el perímetro de la red y la necesidad de mirar más allá para buscar conocimientos estratégicos (Ludwick et al., 2013: 17).

Un problema endémico detectado por el SEI es que los analistas funcionales no saben comunicarse de forma efectiva con personas no técnicas. Eso además demuestra la reticencia de las organizaciones a compartir información dentro de sus propias entidades, con el resto de la industria y con otros sectores económicos. El estudio del SEI ha identificado once retos a los que se enfrenta la ciberinteligencia:

1. Aplicar un enfoque estratégico a los análisis de ciberinteligencia. A pesar de la abundancia de datos disponibles, muchas organizaciones tiene dificultades para ir más allá del análisis funcional de datos de red de bajo nivel para incorporar un análisis estratégico de las amenazas y los indicadores de amenazas.

2. No se comparte información. Solamente las organizaciones más avanzadas comparten datos activamente, en lugar limitarse a consumirlos, por vías formales e informales.

3. Entender las amenazas a la cadena de proveedores de software. El origen desconocido del software complica la capacidad para delimitar el entorno ciber.

4. Determinar dónde ubicar la ciberinteligencia dentro de la organización. El área donde esté encuadrada la función de ciberinteligencia puede afectar a su enfoque, su rendimiento y su efectividad.

5. Acaparamiento de datos. Las organizaciones saben que necesitan datos para realizar análisis de ciberinteligencia funcionales y estratégicos, pero la falta de planificación y el uso ineficaz de la tecnología tienen como resultado que se recopilen y almacenen más datos de los que se pueden realmente procesar.

6. Falta de estándares para la inteligencia de fuentes abiertas. La prevalencia de contenidos no integrados y no estandarizados en los proveedores de inteligencia de fuentes abiertas y en los servicios bajo suscripción complica el trabajo de los analistas a la hora de establecer correlaciones y contribuye a que pierdan oportunidades.

7. Adoptar un repertorio común de términos sobre el oficio de la ciberinteligencia. La falta de un léxico común es un impedimento para la credibilidad de los datos sobre las ciberamenazas, que lastra el análisis, la atribución y la acción.

8. Filtrar las ciberamenazas críticas de la maraña de datos. Las organizaciones tienen dificultades para centrarse en el análisis de amenazas críticas, porque no pueden filtrar adecuadamente los datos que, una vez analizados, terminan clasificados como amenazas leves o moderadas.

9. Inexistencia de un estándar para la formación y el entrenamiento en ciberinteligencia. El personal dedicado a la ciberinteligencia está formado por una mezcla heterogénea de expertos técnicos y analistas de inteligencia no técnicos; ninguno de ellos conoce bien los matices y la complejidad de los otros.

10. Adaptar las metodologías de la inteligencia tradicional al ciberespacio. Como la tecnología cambia tan rápido, el proceso de elaborar análisis de ciberinteligencia debe ser lo bastante dinámico para capturar rápidamente las herramientas, las capacidades y la sofisticación de los adversarios en constante evolución.

11. Comunicar lo ciber a los líderes de la organización. Los decisores que no proceden del entorno cibernético generalmente carecen de formación técnica y los analistas funcionales no suelen tener experiencia de escribir para público no técnico (Ludwick et al., 2013: 5-16).

Por su parte, el Instituto Ponemon acaba de publicar los resultados de una investigación sobre las actividades de ciberseguridad en diversas organizaciones radicadas en Estados Unidos. Respecto a los problemas de la ciberinteligencia, para el 84% de los encuestados el principal es la dificultad de diseminar de forma temprana la inteligencia sobre amenazas que sea relevante para los decisores. En segundo lugar está la elevada tasa de falsos positivos (81%), seguida de que a menudo la inteligencia está demasiado anticuada para permitir tomar decisiones (67%) y de que frecuentemente la inteligencia es incorrecta o incompleta (66%). Otros problemas mencionados son que las actividades y los procesos de ciberinteligencia son difíciles de gestionar (64%), que no son fácilmente integrables con diversas tecnologías de seguridad (59%) y que son demasiado complejos (56%) (Ponemon, 2015: 6).

6. FUSIÓN DE DATOS TÉCNICOS CON OTRAS FUENTES DE INTELIGENCIA TRADICIONALES

La ciberinteligencia no debe limitarse a comprender las actividades y operaciones de red. Incluye la obtención y el análisis de información para elaborar un producto

oportuno, relevante y con contexto que ayude a los decisores. Las fuentes de información pueden extenderse a una amplia variedad de datos sobre redes, ciberactividades en curso por todo el mundo y hechos geopolíticos destacados. Lo esencial es que contribuya a reducir la incertidumbre para el decisor. Cuando la información es analizada y situada en un contexto, se convierte en inteligencia. El origen de los datos no importa, ni tampoco el nivel de clasificación de la información. En definitiva, hacen falta múltiples fuentes de información (abiertas, cerradas o de otras comunidades de inteligencia, públicas o privadas). Es necesaria una visión holística para entender las amenazas del entorno (INSA, 2013: 1).

Conviene fusionar los datos técnicos con otras fuentes de inteligencia tradicionales para mejorar la imagen situacional, ya sea un ámbito militar o civil. No basta con analizar qué ha pasado, sino también identificar cómo se ha hecho, quién lo ha hecho y por qué. La ciberinteligencia se diferencia de las operaciones de inteligencia convencionales en que debe abarcar no solo la intención del adversario, sino además su capacidad. Entre las fuentes de inteligencia tradicionales que pueden resultar útiles figuran las humanas (HUMINT), las abiertas (OSINT), las de imágenes (IMINT), las de señales (SIGINT, y las de geolocalización (GeoINT) (Kornmaier y Jaouën, 2014: 139, 147, 148).

El primer paso es el entrenamiento transversal del personal relacionado con ciberinteligencia en las organizaciones, para que sea capaz de entender y transferir los requerimientos y las limitaciones de los otros dominios de trabajo. A continuación, el proceso debe definir quién comparte qué, con quién, bajo qué circunstancias y cómo se maneja la información, se clasifica, se procesa y se almacena. Esta regulación es necesaria por dos motivos. En primer lugar, no existe un estándar para compartir información, ni inteligencia entre agencias gubernamentales y/o empresas privadas. En segundo, la confianza es clave para fomentar el intercambio de información (Kornmaier y Jaouën, 2014: 152).

El análisis y la fusión de los acontecimientos técnicos y geopolíticos están basados en la experiencia, los antecedentes y la opinión experta de cada analista. Por lo tanto, conviene que los analistas tengan acceso a información clara para evitar que lleguen a conclusiones erróneas sobre la consciencia situacional. En el entorno ciber, es de gran importancia la inteligencia, la vigilancia y el reconocimiento (ISR) a lo largo de múltiples disciplinas de inteligencia. Las operaciones y los métodos no han cambiado; solamente deben adaptarse al ciberespacio (Kornmaier y Jaouën, 2014: 139, 152-153).

7. EL PAPEL DE LA CIBERINTELIGENCIA

Una ciberinteligencia efectiva debe empezar por ser predictiva, por proporcionar alertas estratégicas respecto a ciberamenazas, por mitigar los riesgos asociados a las amenazas, por mejorar la habilidad para evaluar los efectos de una ciberintrusión y por racionalizar la ciberseguridad, convirtiéndola en un proceso más eficiente y eficaz basado en decisiones bien informadas (INSA, 2011: 3).

El papel de la inteligencia es obtener, analizar y elaborar información para proporcionar una evaluación de amenazas completa, precisa, oportuna y relevante que ayude a los decisores a actuar basándose en ese análisis. Normalmente resulta más efectiva si se disemina con el nivel de clasificación más bajo posible entre el máximo

número de usuarios relevantes que afrontan esas amenazas. En un entorno en constante cambio y evolución, la inteligencia debe mantenerse al día sobre las innovaciones tecnológicas. En caso contrario, sería demasiado lenta o incluso se equivocaría a la hora de valorar la dinámica de las amenazas. Por eso es importante que las actividades de ciberinteligencia persigan una misión estratégica, ya sean organizaciones públicas o privadas, civiles o militares (INSA, 2011: 13-14).

7.1. NIVELES DONDE APLICAR CIBERINTELIGENCIA

Las ciberoperaciones requieren un enfoque proactivo, en el sentido de defensa dinámica y planificada, basada en la inteligencia, que sea aplicable a las amenazas actuales. Implica involucrar todas las capacidades de la organización. Ser más proactivo supone entender las redes de forma precisa (en tiempo real y tan pronto como sea posible) y esbozar un panorama más completo sobre lo que sucede y por qué. Las fronteras entre lo táctico, lo operativo y lo estratégico se diluyen. Por eso es imprescindible sincronizar los elementos procedentes de cada nivel para coordinar las operaciones y la toma de decisiones (INSA, 2013: 2-3).

Es posible distinguir tres niveles (estratégico, operativo y táctico) en cualquier ciberactividad. A menudo esos tres niveles se superponen, pero tenerlos en mente contribuye a facilitar las tareas de los decisores y los planificadores de actividades en el ciberespacio (INSA, 2013: 7).

1. El nivel estratégico de lo ciber. El nivel estratégico de una ciberactividad es determinar los objetivos y la dirección por parte de la entidad del más alto nivel que representa a un grupo o a una organización y que puede utilizar los recursos del grupo o de la organización para lograr esos objetivos. Eso puede incluir la decisión de usar cibercapacidades para adquirir información o tecnología; la decisión de atacar un objetivo sensible o estratégicamente importante; y la acción de asignar recursos para desarrollar acciones de explotación o ataque.

   Aquí el papel de la inteligencia es concentrarse en todo aquello que revele cambios y nuevos riesgos con respecto a los objetivos estratégicos de la organización. Algunos ejemplos son la decisión de un competidor potencial de introducirse en un mercado; los indicios de que un gobierno extranjero o un competidor ha adquirido previamente propiedad intelectual vía ciberexplotación; o las señales sobre una relación de influencia atípica respecto a una parte de nuestra cadena de proveedores.

2. El nivel operativo de lo ciber. En el nivel operativo, los actores maliciosos planean sus campañas basándose en lo que han obtenido a través de su propia inteligencia y en los requerimientos derivados de sus metas estratégicas. Los actores construyen las capacidades necesaria para realizar operaciones tácticas. Un grupo hacktivista podría planificar actividades tanto en el ciberespacio como en el mundo físico.

   La inteligencia a nivel operativo puede conllevar el análisis de tendencias sobre las evolución de las capacidades técnicas del adversario; indicadores de que un adversario ha elegido un ruta de aproximación hacia una organización; revelaciones sobre procedimientos, técnicas y tácticas del adversario;

vulnerabilidades técnicas, sociales, legales, financieras u otras del adversario; o información para defenderse de la influencia de un adversario según se mueve por la cadena de ejecución.

3. El nivel táctico de lo ciber. El nivel táctil del ciberdominio es donde se producen las acciones dentro de la red. Es donde los actores maliciosos y los defensores de la red maniobran unos contra otros. Donde las redes de ordenadores zombis se dirigen a un objetivo específico y sueltan su carga. Donde un adversario encuentra una vulnerabilidad y se infiltra en una red. Donde un actor que usa una técnica de ataque avanzado persistente (APT) se desplaza lateralmente dentro de la red objetivo, encuentra la información deseada, la copia y exfiltra los datos. Hoy en día este nivel es el centro de atención de la ciberdefensa. El problema es que este nivel táctico implica que el adversario ya está dentro de la red o en la puerta. Eso probablemente no habría sucedido si se hubieran dedicado suficientes recursos a los dos niveles anteriores.

   La inteligencia también puede realizar aportaciones en este nivel táctico a la hora de estimar la probabilidad y acotar el marco temporal mediante un análisis geopolítico. Por ejemplo, ante la amenaza de un ataque de denegación de servicio distribuido (DDoS) sería posible coordinar la defensa por adelantado y redirigir el tráfico entrante procedente de puntos de alta demanda. Ese tipo de coordinación previa y de alerta avanzada pueden marcar la diferencia entre seguir funcionando o la caída de servicios web críticos (INSA, 2013: 7-10).

7.2. RELACIONES ENTRE LOS TRES NIVELES DE CIBER-INTELIGENCIA: TÁCTICA, OPERATIVA Y ESTRATÉGICA

Generalmente el énfasis suele ponerse en los aspectos tácticos de la ciberinteligencia, obviando los niveles estratégico y operativo a la hora de comprender las metas, los objetivos y las interrelaciones asociados a los ataques. Ese enfoque táctico dificulta la capacidad de la ciberinteligencia para comunicar los ciberriesgos de forma que los decisores puedan entenderlos e interpretarlos completamente (INSA, 2014 octubre: 1).

La meta final de la ciberinteligencia estratégica es disminuir los riesgos para la misión crítica y los activos de una organización. Su función es realizar una evaluación estratégica de las amenazas y las vulnerabilidades, especificando los impactos potenciales en caso de incidentes. Aumenta el conocimiento sobre la superficie de ataque y permite a la organización relacionar la superficie de ataque con potenciales actores que tienen la intención y la capacidad de explotar sus vulnerabilidades. Ese análisis facilitar la toma de decisiones informadas para defender de modo proactivo la misión y las operaciones de la organización (INSA, 2014 marzo: 11).

La inteligencia operativa conecta los niveles estratégico y táctico. Sirve a los gestores de la organización para desarrollar estrategias de defensa frente a ataques potenciales y campañas de adversarios más amplias. Contribuye a proteger a la organización facilitando análisis predictivos frente a amenazas específicas. Reduce el riesgo mediante cuatro pasos esenciales: definir el entorno operativo; describir el impacto sobre el entorno operativo; evaluar al adversario; y determinar el curso de acción del adversario. En resumen, conecta la probabilidad y el impacto de un ciberataque con

sus implicaciones a nivel estratégico, proporcionando un marco coherente de análisis y priorizando las amenazas potenciales y las vulnerabilidades según el contexto donde se mueve la organización (INSA, 2014 octubre: 1, 11).

7.3. ANÁLISIS DE LA CADENA DE EJECUCIÓN EN CIBERDEFENSA

Toda operación en el ciberespacio comienza con un ser humano. Son seres humanos quienes planifican las actividades en el ciberespacio. Los encargados de la ciberdefensa están empezando a reconocer una trayectoria o cadena de ejecución asociada a las actividades maliciosas en las redes. Esa cadena es una secuencia de actividades que cualquier vector de amenaza debe recorrer para causar un efecto. Si ese proceso se interrumpe o se quiebra en cualquier punto, el atacante no podrá lograr su objetivo. Conocer la cadena de ejecución de un adversario basándose en su actividad pasada en la red es muy útil. Pero lo realmente contundente es combinarlo con una estimación de las acciones potenciales [o cursos de acción] que el adversario puede tomar, basadas en inteligencia que informe sobre sus capacidades, sus motivaciones, y sobre qué datos puede perseguir ese actor (INSA, 2013: 4).

El modelo de la cadena de ejecución se puede utiliza para describir las fases de las intrusiones, especialmente en supuestos de ataques persistentes avanzados (APT). La evolución de ese tipo de ciberamenazas requiere el empleo de un modelo de inteligencia donde los defensores no sólo mitiguen la vulnerabilidad, sino también el componente de riesgo de la amenaza. Esa cadena de ejecución se convierte en un instrumento apto para la toma de decisiones cuando los defensores despliegan sus capacidades en función de los procesos específicos que un adversario sigue para aproximarse a un objetivo (Hutchins et al., 2011: 3, 5).

INSA (Intelligence and National Security Aliance) ha ampliado el modelo de la cadena de ejecución de Hutchins, extendiendo el campo de acciones que pueden tomar los defensores a medidas proactivas. El resumen de esa ampliación figura en el siguiente cuadro.

Matriz ampliada de cursos de acción en la cadena de ejecución						
FASE	Detectar	Denegar	Interrumpir	Degradar	Engañar	Destruir
Motivación	Inteligencia de fuentes abiertas	Relaciones públicas; fama de demandar		Relaciones públicas		
Objetivos	Análisis web; inteligencia de fuentes abiertas			OPSEC (*)	Relaciones públicas	
Vía de aproximación	Análisis web / red		Defensa dinámica	Defensa dinámica; OPSEC (*)	Directa hacia defensas fuertes	
Capacidad	Inteligencia de fuentes abiertas		Programa de amenazas infiltrado	Defensa dinámica	Directa hacia defensas fuertes	
Accesos	Inteligencia de fuentes abiertas; análisis web / red	Programa de amenazas infiltrado		Defensa dinámica; OPSEC (*)		

Acciones	Programa de amenaza infiltrado; alertas de la cadena de suministro; CND (*) guiada por inteligencia	Acceso basado en roles		Calidad de servicio	*Honeypot*	
Valoraciones	Análisis web / red; social media	Relaciones públicas			Relaciones públicas; *honeypot*	
Repetición	Análisis web / red; inteligencia de fuentes abiertas	Defensa dinámica			Relaciones públicas; *honeypot*	
* CND (Computer Network Defense) / * OPSEC (Operations Security)						
Fuente: Elaboración propia a partir de INSA, 2013: 6						

8. TENDENCIAS DE INTELIGENCIA PARA 2025

La Oficina del director de Inteligencia Nacional (DNI) de Estados Unidos ha elaborado un informe que recoge las tendencias de la inteligencia para el año 2025. En él se analizan cuatro escenarios probables y se proponen seis conceptos para definir qué capacidades necesita desarrollar la comunidad de inteligencia para afrontar las misiones futuras. Se cierra con cuatro conclusiones, dos de las cuáles merece la pena destacar (Office of the Director of National Intelligence USA, 2009: 19-20).

La primera es que la comunidad de inteligencia tendrá que mantener relaciones muy fluidas con sus socios, sus fuentes y sus objetivos para poder afrontar el dinamismo de un entorno de seguridad más competitivo. Además deberá correr más riesgos, incluso a pesar de los desafíos de seguridad y de la contrainteligencia ajena cada más compleja. La creciente dependencia de expertos externos requerirá una contrainteligencia efectiva para asegurar la integridad de la información y la protección de los sistemas. Aparte, la comunidad de la inteligencia tendrá que reclutar, entrenar, formar, orientar y retener una cantidad suficiente de profesionales en cada organización que sean capaces de mantener un diálogo riguroso con expertos externos.

La otra conclusión resalta que la comunidad de inteligencia necesitará cambiar el papel del agente de inteligencia para lidiar con un entorno externo dinámico y adaptarse a las necesidades de los nuevos consumidores de inteligencia. Requerirá analistas de inteligencia entrenados en múltiples campos, desde la tecnología hasta la metodología, pasando por el análisis de diversas fuentes, que sean capaces de desempeñar múltiples roles simultáneamente. El personal de inteligencia todavía va a necesitar entrenamiento especializado, incluyendo el aprendizaje de idiomas, pero además deberá comprender el contexto en profundidad. La comunidad de la inteligencia asimismo va a necesitar preparar carreras profesionales donde la distinción entre análisis y obtención de datos será irrelevante, especialmente en el ámbito del ciberespacio. Harán falta equipos que cubran una amplia variedad de habilidades para tratar con problemas complejos, por lo que persistirá un cierto grado de especialización individual.

9. CONCLUSIONES

La inteligencia es clave para alcanzar y mantener la superioridad en el ciberespacio. Sin embargo, la comunidad de la inteligencia se enfrenta a retos muy diversos, como hasta dónde puede llegar para operar en el ciberespacio. En las organizaciones se acaparan datos que luego no se pueden procesar. A la vez, existen fuertes obstáculos a la hora de compartir información e inteligencia dentro y fuera de la misma entidad. A esto hay que sumar la carencia de un léxico común y la ausencia de estándares para la formación del personal.

La ciberinteligencia no solo es aplicable a nivel táctico o de red, sino también a nivel operativo y estratégico. Hace falta un enfoque proactivo, en lugar de meramente reactivo. La inteligencia puede contribuir con valiosas aportaciones para descubrir la cadena de ejecución de los ciberataques. Un entorno tan dinámico como el ciberespacio requiere una visión integral para entender las amenazas y el contexto en que se desarrollan.

Actualmente, el principal problema de la comunidad de ciberinteligencia es la brecha de comunicación entre técnicos y no técnicos. Esa falta de entendimiento conlleva ineficiencias y pérdidas de tiempo, porque cada uno tiende a moverse en la zona que le resulta más cómoda. Una parte no sabe explicar lo que puede ofrecer y la otra tampoco sabe cómo pedir lo que necesita. Si lo ciber es transversal, será necesario tomar medidas para evitar que barreras mentales lastren la labor de la inteligencia.

BIBLIOGRAFÍA

Australian Government. (2009). *Cyber Security Strategy*. Commonwealth of Australia.

Cabinet Office. (2011). *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. Crown, United Kingdom.

Crane, David M. (2002). Fourth Dimensional Intelligence: Thoughts on Espionage, Law, and Cyberspace. *International Law Studies, 76*, 311-321.

Eom, Jung-Ho, Kim, Nam-Uk, Kim, Sung-Hwan y Chung, Tai-Myoung. (2012). Cyber Military Strategy for Cyberspace Superiority in Cyber warfare. En *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, IEEE (295-299).

Farnham, Greg y Leune, Kees. (2013). Tools and Standards for Cyber Threat Intelligence Projects. SANS Institute. Extraído el 5 de octubre de 2015 de https://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375

Gobierno de España. (2013). *Estrategia de Ciberseguridad Nacional*. Presidencia del Gobierno, Departamento de Seguridad Nacional.

Government of Canada. (2010). *Canada's Cyber Security Strategy: For a stronger and more prosperous Canada*. Her Majesty the Queen in Right of Canada.

Hutchins, Eric M., Clopperty, Michael J. y Amin, Rohan M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011. Extraído el 5 de octubre de 2015 de http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

INSA. (2011). *Cyber Intelligence: Setting the landscape for an emerging discipline*. Arlington: Intelligence and National Security Alliance (INSA).

INSA. (2013). *Operational Levels of Cyber Intelligence*. Arlington: Intelligence and National Security Alliance (INSA).

INSA. (2014, marzo). *Strategic Cyber Intelligence*. Arlington: Intelligence and National Security Alliance (INSA).

INSA. (2014, octubre). *Operational Cyber Intelligence*. Arlington: Intelligence and National Security Alliance (INSA).

Kornmaier, Andreas y Jaouën, Fabrice. (2014). Beyond technical data - a more comprehensive Situational Awareness fed by available Intlelligence Information. En P.Brangetto, P., Maybaum, M. y Stinissen, J. (Eds.), *2014 6th International Conference on Cyber Conflict* (pp. 139-154). Tallinn, Estonia: NATO CCD COE Publications.

Ludwick, Melissa, McAllister, Jay, Mellinger, Andrew O., Ambrose Sereno, Kathryn. (2013). Cyber Intelligence Tradecraft Project: Summary of Key Findings. Software Engineering Institute (SEI), Carnegie Mellon University. Extraído el 5 de octubre de 2015 de http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=40201

Office of the Director of National Intelligence USA. (2009). *Quadrennial Intelligence Community Review (QICR) Final Report*. Extraído el 9 de diciembre de 2014 de http://www.documentcloud.org/documents/1283939-qicr-final-report-2009.html

Ponemon Institute LLC. (2015, febrero). *Intelligence Driven Cyber Defense*. Extraído el 7 de octubre de 2015 de http://cyber.lockheedmartin.com/intelligence-driven-cyber-defense-survey-results

Raymond, David, Conti, Gregory, Cross, Tom y Nowatkowski, Michael. (2014). Key Terrain in Cyberspace: Seeking the High Ground; En Brangetto, P., Maybaum, M. Stinissen, J. (Eds.), *6th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 287-300.

Fecha de recepción: 30/12/2015. Fecha de aceptación: 20/06/2016