ADOLFO ARREOLA GARCÍA

EL VALOR DE LA (CIBER) INTELIGENCIA EN LA ERA DIGITAL

ORCID
HTTPS://ORCID.ORG/0000-0002-2799-1882

UNIVERSIDAD ANAHUAC MÉXICO
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

En la Era Digital, el estudio de la inteligencia ha pasado de un enfoque centrado en la estrategia militar hacia un concepto integral que abarca múltiples sectores. Históricamente, la inteligencia ha sido un factor determinante en la seguridad y la política de los diversos actores del sistema internacional ya que actúa como multiplicador de poder. Entre los principios que rigen la recolección de inteligencia se encuentran la precisión, la fiabilidad y la oportunidad, aplicados a través de metodologías avanzadas que incluyen la inteligencia de señales, geoespacial y de fuentes abiertas. Estas prácticas son cruciales en áreas como la seguridad nacional, la defensa, el comercio y la diplomacia. Por ello, el objetivo de este trabajo es analizar el valor de la (ciber)inteligencia en un momento de la historia dependiente de medios digitales.

Para tal efecto, la teoría de la información de Claude Shannon, proporciona un marco para comprender cómo los datos procesados permiten la toma de decisiones más eficiente a fin de enfatizar el valor del conocimiento anticipado y enfatizar la importancia de la codificación y transmisión eficiente de información, una piedra angular de los aparatos de inteligencia. En breve, la revolución digital ha transformado la inteligencia, permitiendo el análisis masivo de datos mediante tecnologías como la inteligencia artificial y el big data; herramientas que han ampliado la capacidad de predecir comportamientos y optimizar decisiones estratégicas. De igual forma, han traído la ciberinteligencia para proteger el ciberespacio usando fuentes y herramientas tecnológicas.

Palabras clave: inteligencia, ciberinteligencia, Era Digital, análisis de datos, inteligencia artificial

"La revolución digital redefine la inteligencia como un pilar estratégico en un mundo interconectado."

La noción de inteligencia, en su acepción tradicional, ha sido un pilar fundamental en la estrategia militar y la toma de decisiones políticas desde tiempos remotos. Desde las redes de espías en la antigua China hasta el "Great Game" entre el Imperio Británico y Rusia en Asia Central (Fromkin, 1980), la recolección y análisis de información siempre ha influido en el poder y la seguridad de las naciones. De la misma forma, el uso de redes de espías en el antiguo Egipto o en Sunzi Bingfa ("El arte de la guerra" presentado por Sun Tzu y otros autores) en China destacan como ejemplos tempranos del valor de la recolección de información estratégica. En la era moderna, la inteligencia pasó a ser un componente fundamental para la seguridad nacional y la toma de decisiones globales, especialmente con la profesionalización de las agencias de inteligencia en el siglo XX. Lo cual de alguna forma

permite recordar que "la tecnología es el gran separador pero a la vez el gran igualador en el arte de la guerra" (Boot, 2006) y está ahora es ampliamente utilizada para la recolección de inteligencia.

De hecho, Sherman Kent, conocido como el "padre de la inteligencia moderna", definió la inteligencia en varios niveles, considerando tanto su dimensión teórica como práctica. En sus escritos, particularmente en Strategic Intelligence for American World Policy (1949), Kent plantea la inteligencia desde tres perspectivas: 1) inteligencia como conocimiento (información obtenida, analizada y procesada para reducir la incertidumbre en la toma de decisiones); 2) inteligencia como actividad organizacional (la inteligencia como un proceso, que abarca desde la recolección y análisis de datos hasta la producción de informes y su distribución); y, 3) Inteligencia como institución (la inteligencia como una comunidad o sistema institucional). Estas consideraciones sobre la definición de inteligencia son fundamentales para el desarrollo del campo de estudios de inteligencia; organizar los modernos sistemas de inteligencia y desarrollar un modelo de recolección de inteligencia.

Sin embargo, con la llegada de la era digital, el concepto de inteligencia ha evolucionado para adaptarse a un entorno en constante cambio y dominado por la información. Dicho concepto se ha ampliado para pasar de un enfoque puramente militar hacia la comprensión y gestión de enormes flujos de datos en ámbitos como la economía, la política y la ciberseguridad. Desde una perspectiva teórica, la Teoría de la Información de Claude Shannon proporciona una base conceptual para entender cómo los datos y su procesamiento afectan la comunicación, el control y la toma de decisiones. Esta teoría, que enfatiza la importancia de la codificación y transmisión eficiente de información, que se ha convertido en una piedra angular para el desarrollo de sistemas de inteligencia en la actualidad.

Indudablemente, Shannon definió la información y por ende la inteligencia como la reducción de la incertidumbre en un sistema, lo cual está directamente relacionado con los principios fundamentales de la inteligencia que incluyen precisión, verificabilidad, oportunidad y relevancia; y, la convierten en la capacidad de obtener, procesar y analizar información para influir en decisiones estratégicas. Esta perspectiva coloca a la información en el centro de la toma de decisiones, realzando su valor en un mundo interconectado y digitalizado.

Características y Principios de la Recolección de Inteligencia

Como fue mencionado, la recolección de inteligencia en la Era Digital se basa en principios clave como la precisión, la fiabilidad y la capacidad de anticipación; características que se logran mediante procesos rigurosos de análisis y la validación de fuentes. La precisión se refiere a la exactitud de los datos recolectados, la verificabilidad asegura que la información sea corroborada por fuentes fiables, la oportunidad se enfoca en la entrega de inteligencia en el momento correcto, y la relevancia implica que la información sea útil para el contexto

específico de la toma de decisiones. Además, la inteligencia debe ser adaptable a distintos contextos, desde la prevención de amenazas hasta el desarrollo de políticas económicas y tecnológicas.

De hecho debido a la gran cantidad datos que se generan día a día "se necesitan soluciones concretas, capaces de controlar y convertir en conocimiento útil las ingentes

cantidades de informacionque deben procesar las agencias de inteligencia de un país" (Flores, 2015, p.82).

Entre los métodos más empleados para la recolección de inteligencia se encuentran la inteligencia de señales (SIGINT), inteligencia geoespacial (GEOINT), inteligencia de fuentes humanas (HUMINT), e inteligencia de fuentes abiertas (OSINT), cada uno con su propio conjunto de técnicas para la adquisición y evaluación de datos. En la era digital, la integración de estas metodologías con tecnologías avanzadas permite que los analistas procesen datos masivos con mayor rapidez y eficiencia. De hecho, para Lee S. Strickland "las redes de información y la tecnología adecuada para su obtención, análisis y transformación en conocimiento y, como consecuencia, en comprensión de los hechos para tomar una decisión, forma parte de las principales herramientas de la guerra futura" (Strickland, 2001 citado en Bonilla, 2005). Lo cual es una tendencia a la alza en el mundo del presente y que requiere del desarrollo de ciencia y tecnología avanzada para obtener inteligencia útil para todos los sectores productivos, económicos, políticos y sociales.

Áreas Esenciales para la Aplicación de la Inteligencia

En el mundo contemporáneo, la inteligencia es vital en sectores como la seguridad nacional, la defensa, el comercio, la tecnología, y hasta en la diplomacia. En la llamada Era Digital, la inteligencia y sobre

DEFENSA

Operación de Inteligencia contra ISIS (2015):

En 2015, agencias de inteligencia estadounidenses y europeas utilizaron ciberinteligencia para desarticular las operaciones de reclutamiento y propaganda del Estado Islámico (ISIS) en redes sociales. Mediante la monitorización y análisis exhaustivo de plataformas como YouTube, Twitter y Telegram, se identificaron y desactivaron cuentas estratégicas utilizadas por los extremistas. Esta acción no solo dificultó la difusión de su mensaje, sino que también permitió desactivar células operativas, marcando un avance significativo en la lucha contra el terrorismo digital.

TECNOLOGÍA

Protección contra Vulnerabilidades en el Software (2021):

En 2021, Microsoft enfrentó una amenaza crítica relacionada con una vulnerabilidad en su sistema Exchange, explotada por grupos de hackers para acceder a correos corporativos. A través de la detección temprana respaldada por ciberinteligencia, la empresa desarrolló y desplegó con rapidez parches de seguridad que mitigaron los daños a nivel global. Esta respuesta eficiente no solo limitó el impacto de la amenaza, sino que también estableció un nuevo estándar en la gestión proactiva de riesgos cibernéticos.

todo la ciberinteligencia han resurgido como la mejor opción para la obtención de información que de otra forma estaría velada para nosotros. De forma clara, la inteligencia se ha vuelto esencial en una amplia gama de sectores a fin de obtener ventajas competitivas y comparativas. En la seguridad nacional, permite identificar amenazas emergentes y anticipar ataques, mientras que en la defensa militar, optimiza la estrategia y la logística. En el ámbito económico, la inteligencia competitiva permite a las empresas anticiparse a los movimientos de sus rivales, comprender el mercado y ajustar sus estrategias. Además, la inteligencia es vital en la formulación de políticas públicas y en la diplomacia, proporcionando información precisa para negociaciones y acuerdos internacionales.

Desde otra perspectiva, en el ámbito corporativo, la inteligencia competitiva permite a las organizaciones y empresas prever movimientos de sus potenciales rivales/competidores y ajustar estrategias en tiempo real. En la política, los gobiernos utilizan la inteligencia para la formulación de políticas exteriores y la protección de intereses nacionales con el fin último de lograr el bienestar de su sociedad. En todos estos casos, la inteligencia actúa como un multiplicador de poder, transformando información en decisiones estratégicas fundamentadas en un conocimiento detallado tanto de la problemática cómo de los actores, factores y medios. Para justificar lo que se menciona en los párrafos anteriores a continuación se incluyen algunos ejemplos de empleo exitoso de la ciberinteligencia para contener, mitigar y responder a eventos adversos de ciberseguridad.

Existen varios casos de éxito en la aplicación de la ciberinteligencia, ya no solo de la inteligencia, en diversos sectores como la seguridad nacional, defensa, comercio, tecnología y diplomacia. Aquí se presentan algunos ejemplos destacados:

Seguridad Nacional: En 2017, fue mitigado un intento de ciberataque dirigido a la red eléctrica de Ucrania gracias a la ciberinteligencia. La acción combinó análisis de tráfico de red y monitorización en tiempo real, sin descartar el apoyo de naciones amigas, detectando señales de ataques conocidos vinculados a grupos como Sandworm, lo que permitió la neutralización del ataque antes de que causara apagones masivos. Este caso subraya la importancia de la ciberinteligencia y la cooperación internacional para la protección de las infraestructuras críticas.

Defensa: Operación de Inteligencia contra ISIS (2015): En 2015, fuerzas de inteligencia estadounidenses y europeas emplearon ciberinteligencia para desarticular operaciones de reclutamiento y propaganda del Estado Islámico (ISIS) en redes sociales. A través de la monitorización y análisis de plataformas como Youtube, Twitter y Telegram, se lograron identificar y desactivar cuentas clave utilizadas por extremistas, dificultando la expansión de su mensaje y desactivando células operativas.

Comercio: Protección contra Fraudes en el Sector Financiero (2020). El sector bancario ha implementado ciberinteligencia avanzada para detectar y prevenir fraudes financieros. Un caso notable es el de JP Morgan, que en 2020 utilizó algoritmos de aprendizaje automático y análisis de grandes volúmenes de datos para identificar patrones sospechosos en transacciones. Esta iniciativa permitió una reducción significativa en los intentos de fraude, mejorando la confianza y seguridad de los usuarios; así cómo, evitar potenciales riesgos para las finanzas sanas de este gigante financiero.

Tecnología: Protección contra Vulnerabilidades en el Software (2021). Microsoft enfrentó en 2021 la amenaza de una vulnerabilidad crítica en su sistema Exchange, utilizada por grupos de hackers para acceder a correos corporativos. Gracias a la detección temprana mediante ciberinteligencia, Microsoft pudo desarrollar y desplegar rápidamente parches de seguridad, limitando los daños a nivel global y estableciendo un nuevo estándar en la respuesta a amenazas cibernéticas.

Diplomacia: Desmantelamiento de Campañas de Desinformación (2019). Durante las elecciones europeas de 2019, la Unión Europea utilizó ciberinteligencia para detectar y desmantelar campañas de desinformación dirigidas por actores estatales. A través de la monitorización de redes sociales y fuentes en la web oscura, se logró rastrear la fuente de desinformación y ejecutar contramedidas antes de que influyeran de forma significativa en el electorado.

Lo anterior pudo implementar algunas medidas diseñadas para evitar la manipulación de la opinión pública y la intervención extranjera en comicios electorales como resultado de las lecciones aprendidas de las elecciones estadounidenses de 2016 y de la incorporación de la inteligencia artificial en labores de defensa.

De conformidad con lo expuesto, los casos presentados demuestran cómo, bajos las condiciones actuales de hipercomexión, la ciberinteligencia es esencial para anticipar, detectar y neutralizar amenazas en un mundo cada vez más interconectado y digital. La pregunta es ¿cuanta inteligencia es suficiente? y sí ¿podremos contener a las amenazas emergentes del desarrollo tecnológico?

Impacto de las Tecnologías de Información y Computación en la función de Inteligencia

Con la explosión de datos en la era digital, las tecnologías de la información y la computación han revolucionado la recolección y análisis de inteligencia. La automatización, el big data y la inteligencia artificial (IA) permiten procesar grandes volúmenes de datos a velocidades sin precedentes, identificando patrones ocultos y proporcionando análisis predictivos más precisos. Las redes sociales, foros en línea y las plataformas digitales son ahora fuentes críticas de información, lo que ha generado nuevas disciplinas dentro de la inteligencia, como la inteligencia en redes sociales2 (SOCMINT) y la ciberinteligencia.

De hecho, las redes sociales son una fuente valiosa para la recolección de inteligencia, tanto en el ámbito gubernamental como comercial. A continuación, se describen tres técnicas comúnmente empleadas para obtener inteligencia a partir de estas plataformas.

Primero, el análisis de sentimiento implica la evaluación de las emociones y opiniones expresadas en publicaciones, comentarios y mensajes en redes sociales para clasificar las opiniones como positivas, negativas o neutrales, e identificar tendencias en la percepción pública sobre un tema específico. Su principal objetivo sería la

detección anticipada de la opinión pública.

Segundo, monitoreo de palabras clave y hashtags, una técnica que rastrea menciones de términos específicos o hashtags relevantes para un objetivo de inteligencia. Las herramientas de monitoreo permiten seguir las conversaciones en tiempo real, identificar temas populares y detectar la aparición de palabras clave relacionadas con amenazas, productos o eventos. Es un monitoreo que incluye en algunas ocasiones el uso de diccionarios personalizados.

Tercero, análisis de redes sociales, técnica que examina las relaciones e interacciones entre usuarios en las plataformas, identificando influenciadores clave, nodos de comunicación y comunidades. Todo lo cual permite la identificadores de "influencers" y el análisis de estructuras sociales, a veces sin el conocimiento de los usuarios.

Sí bien estas formas de recoleccion de la inteligencia en las redes sociales pueden ser muy útiles, deben aplicarse considerando tanto sus beneficios como las limitaciones para maximizar su efectividad y minimizar riesgos éticos. La obtención de la ciberinteligencia debe estar supeditada al respeto de los derechos humanos y digitales de los usuarios finales.

Ciberinteligencia y sus Fuentes

La ciberinteligencia, o ciberespionaje, se ha convertido en un campo central para los estados y organizaciones en el siglo XXI. Esta disciplina se enfoca en la protección de infraestructuras críticas, la identificación de amenazas en el ciberespacio y la prevención de ataques a sistemas digitales. Las fuentes de ciberinteligencia abarcan desde la monitorización de actividades en la web oscura, análisis de tráfico de red, hasta la detección de vulnerabilidades en software y hardware. Los ciberataques a menudo se dirigen a obtener secretos comerciales, estratégicos o gubernamentales, y la capacidad de anticipar y contrarrestar estas amenazas define el ciberpoder de una nación o corporación, así mismo, funciona como un aliciente para construir y/o fortalecer los planes, programas y sistemas de ciberresiliencia.

Ampliando un poco sobre cada una de las fuentes de ciberinteligencia se puede decir lo siguiente para cada una de ellas:

1. Monitorización de la Web Oscura: Se pueden encontrar foros de hackers, mercados de información robada, y otras operaciones ilícitas. La ciberinteligencia extrae información de estos entornos para identificar amenazas, prevenir fraudes, y rastrear operaciones criminales utilizando herramientas avanzadas de rastreo para prevenir ataques.

2. Análisis de Tráfico de Red: El análisis de tráfico implica monitorear paquetes de datos en busca de patrones anómalos o señales de posibles ataques cibernéticos. Se emplean herramientas como Sistemas de Detección de Intrusiones (IDS). El objetivo es detectar ataques en curso, como intentos de acceso no autorizado, exfiltración de datos o todo tipo de actividad maliciosa.

3. Detección de Vulnerabilidades en Software y Hardware: El proceso de detección implica escanear sistemas en busca de fallos de seguridad, tanto conocidos como emergentes. Esta fuente de ciberinteligencia se nutre de informes de errores, análisis de código y pruebas de penetración. El objetivo es identificar y mitigar posibles vulnerabilidades antes de que sean explotadas, fortaleciendo así la ciberseguridad de una organización.

A partir del texto anterior se puede afirmar que estas fuentes de ciberinteligencia no solo permiten la identificación y mitigación de amenazas actuales, sino que también proporcionan información clave para el desarrollo de estrategias preventivas en el ámbito digital.

Valor de la ciberinteligencia en la Era Digital

Partiendo de lo expuesto en el presente documento, el valor agregado de la inteligencia en la Era Digital reside en su capacidad para transformar datos masivos en conocimiento aplicable, anticiparse a las amenazas, y tomar decisiones estratégicas en un entorno complejo y en constante cambio. Lo anterior se logra a partir de actividades que incluyen, pero no se limitan a los siguientes temas:

1) Manejo de Grandes Volúmenes de Información (Big Data), para transformar grandes volúmenes de datos en conocimiento estratégico para tomar decisiones más informadas explotando así la riqueza que surge de lo que se conoce como "el oro digital";

2) Anticipación y Mitigación de Amenazas, explotando la capacidad de detectar patrones de comportamiento sospechosos y responder rápidamente es crucial para la continuidad del negocio y el fortalecimiento de la ciberresiliencia;

3) Toma de Decisiones Estratégicas Basadas en Datos, lo cual permite a gobiernos, empresas y organizaciones tomar decisiones más efectivas y ajustadas a la realidad cambiante reduciendo la incertidumbre y ampliando las posibilidades de éxito;

4) Innovación en Ciberseguridad y Defensa, clave para desarrollar estrategias proactivas de ciberseguridad y mejorar las capacidades de ciberdefensa;

5) Ventaja Competitiva en el Ámbito Empresarial, que permite a las empresas anticiparse a los movimientos del mercado, identificar oportunidades de negocio, y adaptar sus estrategias de forma dinámica; y

6) Mejoras en la práctica de la Diplomacia y la Política Global, siendo esenciales para evaluar las intenciones de otros actores, gestionar crisis y negociar acuerdos internacionales de manera más eficiente.

En resumen, es evidente el valor agregado que trae consigo la ciberinteligencia para los diversos actores internacionales, dada su capacidad para transformar datos masivos en conocimiento aplicable y estratégico, anticiparse a las amenazas a partir del reconocimiento de sus patrones o firmas, y tomar decisiones estratégicas en un entorno complejo y en constante cambio con base en un conocimiento sólido de las condiciones cambiantes de los escenarios de competencia y conflicto. Lo cual permite asegurar que el conocimiento anticipado se emplea como una herramienta de éxito.

Perspectivas Futuras de la Ciberinteligencia

Mirando hacia adelante, la ciberinteligencia continuará evolucionando hacia un enfoque más predictivo y autónomo,

impulsado por la IA y el machine learning. En un mundo donde los ciberconflictos son cada vez más frecuentes, se espera que las naciones desarrollen capacidades cibernéticas avanzadas que combinen inteligencia artificial con estrategias de ciberdefensa para proteger sus activos más valiosos.

Además, la integración de la ciberinteligencia con sistemas de defensa tradicionales abrirá nuevas fronteras en la seguridad global, estableciendo un equilibrio entre el uso ético de estas tecnologías y la necesidad de salvaguardar intereses nacionales.

Sin embargo, la complejidad y dificultad para ahora procesar la gran cantidad de datos representa uno de los principales desafíos para la generación de productos de inteligencia de alto valor y la protección de los mismos; algunos autores mencionan que una característica del nuevo ambiente de Inteligencia Estratégica "es la dificultad para la recolección de información y la complejidad de transformar ésta en análisis" dado que al estar hiperconectados "el mundo es plano" (Friedman, 2005).

En resumen, la inteligencia, potenciada por la tecnología digital así como la aparición de la IA y otras tecnologías emergentes, se posiciona como una herramienta estratégica indispensable para abordar los desafíos de un mundo cada vez más interconectado y tecnológicamente avanzado. Es de esperar, que en los próximos años se de una mayor automatización en la recolección de inteligencia y en la protección de los secretos de los diversos actores.

Conclusiones:

En la era digital, la inteligencia ha evolucionado de un enfoque centrado en la estrategia militar hacia un concepto integral que abarca múltiples sectores, impulsado por el desarrollo tecnológico y la interconexión global. Con ello, a permitido la aparición de la ciberinteligencia, que se posiciona como la herramienta por excelencia para obtener información estratégica del ciberespacio. Históricamente, la inteligencia ha sido un factor determinante en la seguridad y la política, pero hoy, su análisis se enriquece con la teoría de la información de Claude Shannon, que proporciona un marco para comprender como los datos procesados permiten la toma de decisiones más eficiente.

La recolección de (ciber)inteligencia se basa en principios como la precisión, la fiabilidad y la oportunidad, aplicados a través de metodologías avanzadas que incluyen la inteligencia de

señales, geoespacial y de fuentes abiertas. Estas prácticas son cruciales en áreas como la seguridad nacional, la defensa, el comercio y la diplomacia.

La revolución digital ha transformado la inteligencia, permitiendo el análisis masivo de datos mediante tecnologías como la inteligencia artificial y el big data. Estas herramientas han ampliado la capacidad de predecir comportamientos y optimizar decisiones estratégicas.

La ciberinteligencia, como una rama emergente, se centra en la protección del ciberespacio y utiliza diversas fuentes como la web oscura y el análisis de vulnerabilidades. Se puede afirmar que, el campo de la ciberinteligencia continuará evolucionando con el uso de la computación cuántica y la IA, consolidándose como un pilar esencial para la seguridad global en el presente y en el futuro. En resumen, la ciberinteligencia es un factor decisivo en el mundo contemporáneo, transformando información en poder y adaptándose a los desafíos y oportunidades que plantea un entorno cada vez más digitalizado.

Referencias:

Kent, Sherman. Strategic Intelligence for American World Policy. Princeton University

Press, 1949.

Boot, M. (2006). War made new: technology, warfare, and the course of history, 1500 to

today. Penguin.

Friedman, T. L. (2005). The world is flat: A brief history of the twenty-first century.

Macmillan.

Strickland, L. S. (2001). Information and the war against terrorism. Bulletin of the American

Society for information Science and Technology, 28(2), 12-12.

Bonilla, D. N. (2005). Medios tecnológicos e Inteligencia: bases para una interrelación

convergente. Arbor, 180(709), 289-313.

Fromkin, D. (1980). The great game in Asia. Foreign Affairs, 58, number 4, 936.


GUARDIA
NACIONAL