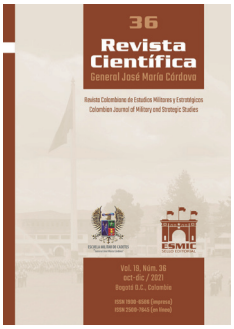

Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia

ISSN 1900-6586 (impreso), 2500-7645 (en línea)
Web oficial: https://www.revistacientificaesmic.com

El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio

Claudio Payá-Santos
https://orcid.org/0000-0002-1908-9960
claudio.paya@ui1.es
Universidad Isabel I de Castilla, Burgos, España

José María Luque Juárez
https://orcid.org/0000-0002-3707-7621
jluque@iniseg.es
Instituto Internacional de Estudios en Seguridad Global (Iniseg), Madrid, España

Citación: Payá-Santos, C., & Luque Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. *Revista Científica General José María Córdova*, *19*(36), 1121-1136. https://dx.doi.org/10.21830/19006586.855

Publicado en línea: 1.º de octubre de 2021

Para enviar un artículo:
https://www.revistacientificaesmic.com/index.php/esmic/about/submissions

ESMIC
SELLO EDITORIAL

Miles Doctus

Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia

Volumen 19, número 36, octubre-diciembre 2021, pp. 1121-1136
https://dx.doi.org/10.21830/19006586.855

El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio

The criminal intelligence system facing new cyberspace threats and opportunities

Claudio Payá-Santos
Universidad Isabel I de Castilla, Burgos, España

José María Luque Juárez
Instituto Internacional de Estudios en Seguridad Global (Iniseg), Madrid, España

Resumen. Este trabajo analiza las distintas fases y ciclos de la inteligencia criminal para discernir de qué manera el ciberespacio supone un impacto en ellas, así como establecer si el ciclo clásico de la inteligencia es válido para el trabajo de inteligencia en este dominio. A partir de ello, se evidencia cómo las fases de inteligencia clásica guardan una estrecha relación en su concepto con características transversales que pueden ejecutarse para obtener inteligencia en el ciberespacio, pero cuyos procedimientos provienen de otras épocas en que el ciberespacio no existía como concepto. Se plantean, entonces, las necesidades ante las nuevas amenazas y las inéditas oportunidades que brinda el desarrollo tecnológico del dominio ciberespacial.

Palabras clave: cibernética; ciclo de la inteligencia; inteligencia; inteligencia criminal; seguridad

Abstract. This work analyzes how cyberspace impacts the different phases and cycles of criminal intelligence. It also seeks to establish whether the classic intelligence cycle is valid for intelligence work in this domain. From this, it evidences how the concepts of classic intelligence phases are closely related with transversal characteristics that can be executed to obtain intelligence in cyberspace; however, their procedures are from other times before the existence of the concept of cyberspace. To conclude, it discusses the needs in the face of the new threats and the unprecedented opportunities offered by the technological development of the cyberspace domain.

Keywords: criminal intelligence; cybernetics; intelligence cycle; intelligence; security

Sección: Dosier • Artículo de investigación científica y tecnológica
Recibido: 24 de mayo de 2021 • Aceptado: 4 de septiembre de 2021

Contacto: Claudio Payá-Santos ✉ claudio.paya@ui1.es

Introducción

Desde tiempos remotos, los gobernantes han querido tomar las decisiones más acertadas para gestionar la vida en sociedad. Para ello, contar con la mayor información posible permite disponer de elementos en los cuales sustentar la compleja tarea de gobernar. Con esta finalidad, los procesos de recopilación de información en tiempos pasados tenían distintos orígenes o los datos eran recopilados de manera inconexa y sin una finalidad específica (Calleja & Delgado, 2017). Esto derivaba en una incomprensión de los datos y, por consiguiente, en un mal planteamiento de las respuestas que se buscaban. En este escenario surgió la necesidad de armonizar la información recabada en distintos ámbitos para poder ofrecer un producto final coherente para la toma de decisiones; se puede argumentar que es allí cuando nace la *inteligencia* como concepto.

Este concepto ha llevado a lo que la doctrina de seguridad conoce como el "ciclo de la inteligencia", cuyo objetivo es seguir un procedimiento sistemático y estandarizado para producir conocimiento útil como base para la toma de decisiones, reduciendo así la incertidumbre generada ante las posibles medidas a adoptar. Este instrumento para obtener inteligencia fue perfeccionándose al dotarse de especialidades según la fuente de datos a explotar; de esta forma, aparecieron denominaciones basadas en el origen de los datos, según provinieran de personas (HumInt), de imágenes (ImInt), de señales (SigInt) o de fuentes abiertas (OsInt). Por ello, se puede afirmar que el concepto de origen o fuente de la información es fundamental en el ámbito de la inteligencia, pues ello condiciona la metodología y los procedimientos adecuados de explotación con el fin de obtener resultados útiles y analizar con garantías la información recopilada.

En este sentido, la inteligencia es una herramienta que permite simular posibles escenarios a través de la interpretación de datos y situaciones, con lo cual ayuda a definir los objetivos estatales y las políticas y planes que contribuyen a alcanzarlos. Esto es, entonces, lo que se llama *inteligencia estratégica*.

Un mundo en constante cambio, debido al proceso de globalización, suscita la aparición de nuevas amenazas en el escenario de seguridad (Delgado-Morán et al., 2019; 2020a). Estas nuevas amenazas tienen características que retan la estabilidad, lo que implica nuevos desafíos en el sector de la seguridad de los Estados. Por ello, se debe llevar a cabo un rediseño en materia conceptual con el objetivo de estar en capacidad de hacer frente a las nuevas amenazas, lo cual significa un rediseño estratégico que involucre los servicios de inteligencia. Así, dadas las características de una sociedad globalizada, resulta conveniente el desarrollo de un sistema de inteligencia que asuma los retos causados por la incertidumbre, que a su vez permita el desarrollo de políticas adecuadas para responder a los nuevos desafíos a la seguridad (Delgado-Morán et al., 2019; 2020b). El fenómeno de las nuevas amenazas a la seguridad obliga a adoptar un modelo de seguridad inteligente, lo cual requiere incentivar la cultura de la evidencia basada en el conocimiento por medio de diagnósticos de campo, que permita diferenciar los problemas internos y externos.

Esto conduce a que cada uno de los Gobiernos adapte sus diferentes respuestas de manera efectiva para las distintas áreas y amenazas, lo que conlleva la existencia de distintos tipos de ciclos de inteligencia.

Dada la necesidad de un rediseño de las bases conceptuales de las estrategias que se formulan desde el sector defensa de los Estados, se requieren asimismo modificaciones en los servicios de inteligencia que permitan a los Estados obtener mayor conocimiento del contexto para formular estrategias adecuadas y reducir aún más el grado de incertidumbre. Anteriormente, la inteligencia estratégica en cualquiera de los diferentes ciclos de la inteligencia se basaba en escenarios determinados y acorde a las necesidades de seguridad del momento. Las nuevas amenazas desbordan este planteamiento, fundamentado en la recolección del dato físico y tangible mediante seguimientos y vigilancias, explotación de confidentes, denuncias, medios de comunicación, etc. Con el avance de las TIC, la obtención de datos mediante el ciclo de la inteligencia resulta ser una metodología obsoleta o inadecuada a la hora de enfrentarse al denominado ciberespacio o "quinto dominio" (Joyanes, 2011).

El ciberespacio presenta particularidades propias, como la virtud o dificultad, según se quiera enfocar, que comporta la velocidad de su desarrollo y que se puede considerar que impacta de lleno en las tradicionales formas de obtención de inteligencia, dado que la fuente básica o principal de todas las especialidades del "ciclo de la inteligencia" podrían ser cubiertas en el ciberespacio. Por ejemplo, hoy en día se puede establecer contacto con una persona sin necesidad de presencia física mediante medios y métodos basados en el ciberespacio, con lo que se estaría atribuyendo una funcionalidad tradicional HumInt a un modelo basado en el quinto dominio. Asimismo, la inteligencia de imágenes (ImInt) también es susceptible de ser elaborada a partir de fotografías aéreas que existen en numerosas páginas o aplicaciones web. Siguiendo con esta extrapolación de posibilidades de obtener información, la inteligencia de señales (SigInt) también se puede desarrollar sobre la propia información abierta que existe en la red, lo que abarcaría la funcionalidad asignada a la elaboración de inteligencia OsInt. Por lo tanto, se vislumbra un mayor protagonismo del concepto de *ciberinteligencia*, entendida como "la adquisición y análisis de información para identificar, rastrear y predecir cibercapacidades, intenciones y actividades que ofrezcan vías de actuación para mejorar la toma de decisiones" (Townsend et al., 2013).

Pero centrar la inteligencia únicamente en el potencial de la ciberinteligencia sería infravalorar el potencial de la inteligencia clásica, por lo cual, a las tradicionales formas de obtención de inteligencia mencionadas que forman parte del ciclo de la inteligencia, hay que añadir ese quinto dominio denominado "CybInt". De este nuevo marco se podrían extraer los distintos datos para, en un proceso sinérgico, sumar esta capacidad como un apoyo para el proceso de toma de decisiones basadas en el ciclo clasico de la inteligencia, pero potenciadas con las herramientas del quinto dominio, con lo cual se puede lograr un alcance mucho más amplio, cualquiera que sea el ámbito de obtención del dato.

Metodología

Para la elaboración del presente trabajo, se ha hecho una investigación de tipo exploratorio para brindar una visión general de la inteligencia, con el fin de establecer una metodología aplicada a la búsqueda de mayor certidumbre sobre las nuevas amenazas a la seguridad. Esta investigación se basó en distintos estudios exploratorios en el ámbito de la seguridad y la prospectiva de inteligencia, con el objeto de obtener mayor conocimiento sobre el impacto del ciclo de la inteligencia como concepto aplicado a la inteligencia criminal. Esta exploración se centra en cómo el análisis de inteligencia puede aprovechar las funciones de la ciberinteligencia para mejorar sus resultados, y busca favorecer la creación de nuevos procedimientos adaptando el ciclo clásico de la inteligencia, para garantizar la elaboración de inteligencia criminal en los contextos tecnológicos actuales. Ante este escenario se pretende mostrar una visión general de los distintos ciclos de la inteligencia y analizar si estos, de forma particular, junto con las capacidades basadas en el ciberespacio, pueden facilitar la tarea de afrontar los nuevos retos de la seguridad desde una nueva metodología de la inteligencia criminal, así como reducir incertidumbres en la toma de decisiones al servicio de los Gobiernos (Payá-Santos & Delgado-Morán, 2016).

El ecosistema de los ciclos clásicos de inteligencia

En los estudios sobre inteligencia, la doctrina ha asumido los postulados planteados por Sherman Kent (1949) como la base para desarrollar las tesis sobre los distintos ciclos de la inteligencia conocidos, donde cada organización ha acomodado en función de sus intereses las distintas fases de la metodología propuesta por Kent. Estos ciclos pueden contener al menos cuatro fases, como las definidas por el Centro Nacional de Inteligencia español (CNI): dirección, obtención, elaboración y difusión. Por su parte, para verificar la elasticidad de la propuesta de Kent, la Agencia Central de Inteligencia americana (CIA), homóloga del CNI, dispone de cinco fases en su ciclo: planificación y dirección; obtención; procesamiento; análisis y producción, y difusión.

Coetáneo con el modelo de la CIA, el ciclo del Departamento de Defensa de EE. UU. (DOD) dispone de un modelo basado en el de la CIA, pero con siete fases, donde la diferencia radica en añadir al ciclo de la CIA la retroalimentación en cada fase y la evaluación en conjunto de todo el proceso. Esta versión resulta muy interesante para el interés de esta investigación; cabe añadir que, posiblemente, cada ciclo de inteligencia ya contenga implícitamente estas dos particularidades de manera interna sin necesidad de diferenciarse en nuevas fases.

La particularidad de estos tres ciclos (CNI, CIA y DOD) es su disposición circular, donde cada fase cuenta con su "tempo" y establecimiento de acciones para que cada una, una vez satisfecha, pueda ser reportada a la siguiente fase de forma lineal. En este trabajo se analiza un modelo habitual para las fuerzas y cuerpos de seguridad españoles (FFCCSE) que se asemeja al modelo publicado por el Centro Criptológico Nacional

Español (CCN), que cuenta con cinco fases más una fase de evaluación, pero que tiene la particularidad de que su disposición no es circular como las basadas en el modelo de Kent, dado que las fases del CCN se adaptan a las necesidades de cada organismo, de modo que pueden existir dentro de cada fase otras subfases orientadas a una tarea específica, por lo que el número de fases final puede multiplicarse según las necesidades. Dependiendo del organismo que extraiga la inteligencia, se utilizan diferentes modelos existentes.

En la mayoría de las FFCCSE, al igual que en otros países del entorno, se han utilizado sistemas 4x4, 5x5, o 6x6, que enfatizan dos aspectos: la evaluación de la fuente y la consistencia de la información que esta proporciona la fuente. Para categorizar, la evaluación de la fuente se establece como A, B, C, D y así sucesivamente, según el sistema sea 4x4, 5x5, 6x6, para confrontarlo con la consistencia de la fuente, a la que se asignan valores numéricos 1, 2, 3, 4 y así sucesivamente, según el modelo de la organización. En algunas FFCCSE se utiliza el conocido sistema 4x4, que evalúa de forma independiente tanto la fuente de donde procede el dato como la consistencia de la información. Así, se puede encontrar desde información de cuya fiabilidad no se tenga ningún tipo de duda porque ha sido proporcionada por un agente de policía o un organismo oficial, hasta información cuya fiabilidad no se puede determinar porque no se conoce la fuente de la que procede. La codificación, por lo tanto, utiliza estas dos variables de las cuales pueden surgir varias combinaciones en el proceso de evaluación (A1, B3, X4, etc.).

A continuación se presentan *grosso modo* las cinco fases matrices del ciclo de inteligencia usual en las FFCCSE. Si bien este ciclo no se publicita de forma específica mediante un pictograma o elemento visual, se pueden deducir sus fases mediante el pictograma publicado por el CCN (2015), pues se basan, por lo general, en el mismo diseño.

Fase 1. Dirección/planificación

La inteligencia se asemeja a las disciplinas de las ciencias sociales, ya que ambas persiguen un propósito y requieren determinar qué se va a hacer, cómo se va a llevar a cabo, cómo se organizarán las fuentes a consultar o cómo se recopilarán los datos que las fuentes suministren, etc.

Fase 2. Recolección

En esta fase, la inteligencia está recogiendo datos. Conforme al ejemplo citado de las ciencias sociales, esta fase corresponde a la recopilación de datos mediante diversos métodos (por ejemplo, cuestionarios, entrevistas, etc.). En el ámbito de la inteligencia, se trata de determinar qué y cuántos datos específicos son aceptados, en qué formatos se necesitan, con el fin de evitar la adquisición de información redundante o de nulo valor.

Fase 3. Transformación/tratamiento

En esta fase se comienzan a evaluar los datos obtenidos. Una vez comprobada su fiabilidad, corroboradas varias fuentes y contrastados diversos elementos, se procede a su

trasformación en una forma de dato que posibilite su análisis y que, además, sea comprensible, pueda ser tratado y almacenado para su recuperación en cualquier momento posterior para un nuevo análisis.

Fase 4. Análisis/producción

El objetivo de esta fase es emitir productos finales de inteligencia útiles para la toma de decisiones, una vez interpretada y evaluada la información adquirida. En esta fase se pueden ver los resultados de la fase 1, en la que se definió el objeto y alcance de la información a recabar. Así mismo, es el momento de desechar la información que resulte vaga o inconexa. Esta fase ayuda a comprender o favorecer la elección de las diferentes líneas de acción que puedan desarrollarse sobre el escenario analizado para determinar cuál es la idónea o para alterar su desarrollo.

Fase 5. Difusión

En esta fase se materializa el proceso y se dispone la información para ser difundida a su destinatario, de forma que pueda tener un mayor porcentaje de certezas y tomar las decisiones necesarias bajo los parámetros, directrices u órdenes establecidas por la dirección de cada organización. En esta fase desembocan todas las anteriores para constituirse en una herramienta útil a disposición del agente o el usuario.

El ciclo de inteligencia empleado por las FFCCSE no es lineal o circular tal y como están dieñados los ciclos convencionales; se trata más bien de un modelo dinámico, que se retroalimenta constantemente de una fase a otra, donde cada fase no se desarrolla linealmente tras la anterior. Incluso su programación puede producirse en sentido inverso, sobre todo cuando se aprecien lagunas o carencias en algún tramo del ciclo y sea necesario retrotraer el estado del dato a la fase donde se obtuvo o analizó, para apreciar nuevamente su valoración.

Cada una de estas fases tiene componentes trasversales, lo cual identifica el CCN como la sexta fase, denominada "evaluación". Se denomina así, dado que en ella se evalúan cada una de las fases y sus procesos asociados, con el objeto de reconducir los procedimientos si se observa alguna desviación metodológica que impida alcanzar el objetivo planteado por la dirección en la fase inicial.

Tipos de inteligencia

La inteligencia puede ser clasificada según diferentes criterios: por su naturaleza, por los objetivos que persiga o por el nivel de decisión que la sustenta. Estos, a su vez, pueden subclasificarse en otras categorías ligadas a la inteligencia que podrían analizarse desde el ciclo clásico. En este trabajo se definen dos tipos de inteligencia según su nivel de actuación, con el objeto de que sirvan de sustrato a la hora de analizar, en el próximo epígrafe, la denominada inteligencia criminal. Seguidamente se muestran, según el criterio de clasificación mencionado, dos de los tipos de inteligencia más utilizados: la inteligencia estratégica y la inteligencia operativa.

Inteligencia estratégica

Esta disciplina de la inteligencia se alinea con las políticas públicas establecidas por las instituciones, razón por la cual tiene en cuenta en su desarrollo la propia organización y entorno en el que se encuentra. Está orientada a elaborar diagnósticos sobre situaciones que afecten la seguridad pública, y puede dirigir acciones para intervenir en los escenarios actuales, con la intención de corregir la problemática detectada. Por ello, las acciones desplegadas como consecuencia de los productos de inteligencia obtenidos mediante el análisis estratégico están orientadas a alcanzar resultados a largo plazo. Dentro de sus procedimientos, identifica a los actores y las variables que afectan la seguridad o que pueden ser potencialmente un riesgo o amenaza futura, para así intervenir en ellos monitoreando los resultados de las acciones aplicadas.

Como este tipo de inteligencia maneja rangos prospectivos amplios, tiene una visión macro de la problemática delictual y se enfrenta a ella con diferentes herramientas que le posibilitan captar y analizar grandes volúmenes de datos, que pueden provenir de los más diversos orígenes. Por esta razón, el estudio de esta información y su interrelación se convierte en una de las cuestiones más importantes en los análisis estratégicos, que debe enfocarse en encontrar las variables de mayor incidencia o que afecten la seguridad pública como modelo de convivencia pacífica (Delgado & Teano, 2019; 2020).

Inteligencia operativa

Al contrario de la inteligencia estratégica, la inteligencia operativa tiene una perspectiva micro y sus resultados se obtienen a largo plazo. Está orientada hacia problemáticas concretas o fenómenos delictuales específicos en los que la inteligencia estratégica, por el volumen de datos que analiza o por la complejidad de relaciones de los investigados, no consigue avanzar en la identificación y detención de los responsables criminales. Un ejemplo de cuándo se necesita esta inteligencia operativa es en los delitos relacionados con el blanqueo de capitales, donde las transacciones económicas son muy numerosas, lo que requiere, además, investigar el uso de empresas pantalla para dificultar la investigación. La investigación operativa también ofrece resultados óptimos en la investigación de delitos graves como asesinatos, secuestros, etc., ya que la cantidad de datos que se pueden generar a través de las distintas fases de la inteligencia ofrece productos con un gran valor para los responsables de la investigación.

La inteligencia criminal como concepto

La inteligencia como concepto es un pilar fundamental para la toma de decisiones. En este sentido, es importante destacar dos cuestiones: la primera es quién es el destinatario de este proceso, y la segunda es para qué necesita ese destinatario un determinado producto de inteligencia. A través de estas cuestiones, se puede definir la especialidad analítica más oportuna para la finalidad concreta. Así, hay procesos habituales de inteligencia que

abarcan desde una finalidad financiera, militar, estratégica o, como la que aquí interesa, la inteligencia criminal. La conceptualización de la inteligencia criminal contiene en su propia naturaleza un componente predelictual, lo que significa que algunos elementos preparatorios del delito pueden concurrir antes de que este se cometa, sin que estos aisladamente supongan un acto delictual. Es aquí donde la inteligencia criminal entra en escena explorando posibles escenarios para detectar amenazas y poder actuar antes de que estas lleguen a manifestarse. Aquí también es preciso aludir a las tareas investigativas que se despliegan una vez ocurrida la acción criminal, que se activan como respuesta reactiva ante la flagrante vulneración de derechos y libertades públicas. Así, la inteligencia criminal se sirve de ambas técnicas de investigación, esto es, las técnicas reactivas y las técnicas de inteligencia policial en la lucha contra la criminalidad, pues, aunque tienen objetivos distintos, comparten la finalidad esencial de contribuir al mantenimiento del orden.

Como se ha dicho, la inteligencia busca elementos tangibles en los cuales apoyar la toma de decisiones, con el fin de reducir los riesgos al máximo y evitar que se lleguen a materializar mediante acciones criminales. Por su parte, la investigación reactiva trata de identificar, detener y poner a disposición judicial a los autores de haber cometido determinado ilícito penal. La inteligencia criminal persigue el objetivo concreto de luchar contra el crimen en todas sus expresiones, para garantizar la seguridad de los ciudadanos, así como salvaguardar el orden democrático establecido (Payá-Santos & Delgado-Morán, 2017b).

Por este motivo, la sinergia entre ambas disciplinas puede encontrar puentes de comunicación mediante los resultados de las investigaciones (autores, *modus operandi*, fechas, víctimas, etc.), ya que estos constituyen una importante fuente de elementos tangibles para la elaboración de inteligencia criminal. Con esta finalidad, la inteligencia criminal se nutre de variadas fuentes de información que afectan o pueden afectar la seguridad pública. Esta amalgama de datos ayuda a la inteligencia policial de distintas FFCCSE en la toma de decisiones en la lucha contra el crimen.

A su vez, la inteligencia policial es lo suficientemente flexible para acomodar distintas disciplinas y fuentes de inteligencia criminal necesarias para obtener datos precisos en pro de lograr la mayor certidumbre en la lucha contra las nuevas formas de criminalidad. Es en este escenario donde la inteligencia policial, además de obtener información de personas (HumInt) a través de seguimientos con dispositivos de geolocalización (SigInt) o incluso mediante el análisis de imágenes de videocámaras (ImInt), también escruta fuentes mucho más difusas con base en el ciberespacio (CybInt), que no formaban parte de los ciclos clásicos de la inteligencia (Fernández-Osorio et al., 2019). A modo de ejemplo, se podría partir de la necesidad de adoptar ciertas medidas en el ámbito de la seguridad pública con relación a determinada delincuencia organizada. Una vez definida la finalidad del análisis, se especifica qué tipo de inteligencia se va a elaborar (inteligencia criminal o CrimInt). A partir de aquí, se deben recopilar datos para ser analizados, y es entonces donde se puede acudir a otras disciplinas, como la explotación de confidentes a través de técnicas HumInt, o un seguimiento con metodología SocInt o incluso OsInt.

Como se puede ver, las necesidades de inteligencia pueden ser dispares, por lo cual es necesario definir qué producto se necesita para poder determinar qué tipo de inteligencia se debe elaborar. Por ello, previo a cualquier prospectiva de inteligencia, se debe establecer unos objetivos que definan previamente cuál es la situación actual. Esto adquiere mayor sentido cuando se alude a la inteligencia policial respecto al ámbito de la seguridad publica. Así, por ejemplo, la inteligencia policial podría definir en su actuación diferentes objetivos parciales, como reducir la delincuencia en una zona concreta, prevenir una serie de delitos, luchar contra determinado crimen organizado, investigar ciberamenazas, etc. Todos estos objetivos se alinean bajo un objetivo general más amplio, como el que representa salvaguardar los derechos y libertades de los ciudadanos (Payá-Santos & Delgado-Morán, 2017a). Es entonces cuando el equipo directivo, en la fase inicial de dirección, debe decidir en qué ámbito quiere actuar, ya que esto determinará los requisitos necesarios para la elaboración de inteligencia, como el origen del dato a obtener y los procedimientos adecuados de su adquisición, que además puedan ser extraídos en los formatos válidos a tratar, etc. En este sentido, no será lo mismo establecer acciones para erradicar el tráfico de sustancias prohibidas que luchar contra estafas producidas en internet.

Inteligencia criminal ante las nuevas amenazas: el ciberespacio

En los procesos analizados, la inteligencia se elaboraba a partir de datos físicos, en un sentido analógico y no digital, esto es, procedentes de las entidades clásicas de producción, como las personas, los lugares, los hechos delictuales, etc. Para obtener estos datos, se utilizaban métodos igualmente clásicos como los seguimientos, los interrogatorios, entre otros (Payá-Santos et al., 2015).

Como se ha observado, los orígenes de la información eran muy diversos y cada producto de inteligencia, en su versión clásica, obligaba a destinar numerosos recursos tanto personales como materiales, lo que en ocasiones producía resultados poco eficientes a pesar de los medios empleados. Así, en este nuevo escenario, las tecnologías emergentes nos proporcionan un nuevo dominio, el ciberespacio. En este confluyen, además de muchos de los elementos de la inteligencia clásica, elementos novedosos para la elaboración de otros formatos de la inteligencia. Con esta novedad se puede tender a homogeneizar los procedimientos, según los intereses de cada organización, para obtener una "progresiva asunción de la necesidad de abordar la seguridad desde una perspectiva amplia e integradora" (Elías & Velázquez, 2014).

Definición de *ciberespacio*

Al revisar en la doctrina especializada el concepto de *ciberespacio*, se observa poca correspondencia entre distintas definiciones, y sobre todo mucha diseminación de conceptos, pues usualmente se constituyen con el objeto de darle carta de naturaleza según el objetivo que persiga su uso, que no siempre es el objetivo que persigue la inteligencia. La generali-

dad de las entradas al respecto confunde ciberespacio con internet o con el entorno web. Estos términos, que aparentemente son sinónimos, difieren sustancialmente, sobre todo cuando el interés de la materia es el que persigue la inteligencia. En este sentido, cada país e incluso cada organización con intereses en el quinto dominio ha publicado una estrategia o un memorando al respecto, que por espacio sería inoperante describir acá, pero sí se puede traer a colación Las primeras reacciones sobre el fenómeno del ciberespacio tienen su origen en los prolegómenos que dieron lugar al *Manual de Tallinn* de 2013, que, si bien está en constante evolución, con revisiones 2.0 y 3.0, cabe centrarse muy brevemente en su esencia para los intereses de este trabajo. Este manual, preparado por el grupo internacional de expertos invitados por el Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN, si bien no es un documento oficial, en su glosario de términos técnicos define *ciberdefensa* como "el entorno formado por componentes físicos y no físicos, caracterizado por el uso de ordenadores y el espectro electromagnético, para almacenar, modificar e intercambiar datos utilizando redes informáticas" (Schmitt, 2013; Delgado, 2017). Ante esta definición, es necesario recoger puntos en común para ayudar a delimitar una idea clara de qué determina el ciberespacio. Así, el ciberespacio comprende lo siguiente:

- Componentes tangibles o físicos, como el *hardware*, las redes, etc.
- Elementos intangibles, como la información, que se puede almacenar, transmitir o procesar por diferentes sistemas.
- Además de tener componentes reales, queda definido por ser un entorno virtual.
- Soporta actividades e interacciones entre sistemas y usuarios; esta es una de las cualidades más importantes de este entorno, que ha tenido su máxima expresión con el progreso de internet.
- Existencia de un componente humano sin el cual no existiría el ciberespacio, ya que es el encargado del mantenimiento y del desarrollo de su infraestructura, por lo cual es su elemento esencial y además constituye la base de su dinámica.

Como se desprende de esta relación, la ausencia de un espacio físico tangible lo diferencia de otros dominios de inteligencia convencional, ya que, al no tener un espacio geográfico asociado, sus conexiones e intercambios no entienden de fronteras, Estados ni husos horarios.

Estas acepciones son importantes porque nos ayudan a discernir los elementos de los cuales se extrae y con los que se elabora la inteligencia sobre las interacciones que se llevan a cabo en su dominio o con relación a la información que se genera o circula en este espacio virtual (Payá-Santos & Delgado-Morán, 2017a; 2017b).

Oportunidades del ciberespacio para la inteligencia criminal

El ciberespacio aporta a la inteligencia criminal una serie de herramientas que otras fuentes de datos no poseen. Por ello deben ser conocidas por el analista para poder usarlas y explotarlas. Con el adecuado uso de estas herramientas, se puede analizar y convertir en datos útiles todo lo obtenido. A grandes rasgos, las oportunidades que el ciberespacio aporta a la inteligencia criminal son las siguientes:

- *Inmediatez y actualización.* Los eventos y actividades generados en el ciberespacio presentan un gran dinamismo, ya que se producen constantes cambios tanto en sus componentes tangibles como intangibles. Sobre estos últimos, hay que señalar que la información se genera a una velocidad nunca experimentada, lo que obliga a los analistas a actualizar los datos constantemente. Como consecuencia de su dinamismo, todos sus componentes se modifican con una mayor velocidad que en otros dominios. Un ejemplo claro de ello es la actualización de la información que se genera o transmite casi en tiempo real, lo que hace que se vayan renovando los datos asociados con una gran celeridad.
- *Diversidad de fuentes.* Existen numerosas interconexiones y actividades en el ciberespacio que pueden provenir de los más diversos orígenes, como por ejemplo de servidores ubicados en diferentes países, de imágenes vía satélite, foros de mercados específicos, datos obtenidos a través del internet de las cosas (IoT), etc., lo cual genera un número de datos sin precedentes en la historia de la humanidad.
- *Universalidad y flexibilidad.* Las conexiones al ciberespacio cada vez se pueden realizar de más formas y más asequibles, apenas sin costo para el usuario; además, se puede incrementar el número de dispositivos utilizados en este dominio en interacción constante: ordenadores portátiles, tabletas electrónicas, teléfonos móviles e innumerables elementos, la mayoría bajo el paradigma del IoT. Esto genera un volumen de información difícil de calcular e incluso predecir, en un medio que se extiende a todo, sin fronteras, por lo que llega o puede llegar a todas las regiones de la Tierra (Mazurier et al., 2019). Esto permite interacciones entre sistemas o usuarios de todos los continentes, por lo que las fuentes de información a las que se puede acceder desde el ciberespacio son elevadísimas.
- *Volumen de información.* Para un analista, la información es la materia prima con la que se trabaja. El ciberespacio ofrece una ingente cantidad de datos que podrían ser utilizados para realizar todo tipo de análisis de inteligencia criminal, desde actuar contra las ciberamenazas, pasando por la seguridad en el propio entorno web, hasta incluso investigar delitos cometidos en el mundo real. Si bien el volumen de información es tanto que también dificulta las

acciones de depuración, criba, selección y síntesis, como se analiza en el punto correspondiente a la evaluación de la información.

- *Transversalidad y sencillez.* El ciberespacio se ha extendido a todos los ámbitos sociales. Desde las administraciones públicas hasta las empresas privadas, cada vez hacen más uso de este espacio por las ventajas que ofrece, ya que no se requiere formación alguna para poder interactuar en él, de modo que es accesible a individuos de todas las edades.

Amenazas del ciberespacio para la inteligencia criminal

Así como ofrece oportunidades, el ciberespacio también presenta amenazas que hay que conocer para que no fracase la labor del analista y pueda extraer la información necesaria para los productos de inteligencia que se requieran (Ruiz-Ruano et al., 2019). Entre estas desventajas se encuentran las siguientes:

- *Volatilidad.* Lo que se puede considerar una virtud también es una desventaja para el analista, pues los datos se generan a una gran velocidad debido a las diferentes fuentes que interactúan constantemente en este dominio. Esto lleva a que continuamente se estén actualizando y, por ello, también tienden a desaparecer o transformarse de forma muy rápida, lo que dificulta el conocimiento de su origen o de su contenido.
- *Legalidad.* La rapidez del desarrollo de este nuevo dominio hace que se encuentren nuevos escenarios por explorar. Algunos de ellos, aun siendo desconocidos, pueden presentar semejanzas a otros existentes. Otros serán totalmente desconocidos y a la hora de actuar con ellos se tendrá que examinar en profundidad las implicaciones de los actos que se lleven a cabo allí. Ello se puede apreciar con la legislación del agente encubierto, que durante un tiempo no tuvo un respaldo legal definido.
- *Evaluación de la información.* Trabajar con datos veraces hace que las conclusiones de los análisis tengan un alto grado de solidez y, por lo tanto, la toma de decisiones esté bien orientada. Cuando estos datos provienen de un entorno controlado y su cantidad es razonable, la fiabilidad se puede validar mediante diferentes técnicas de inteligencia. Ahora bien, cuando el volumen de datos aumenta notablemente, puede producir "infoxicación", que se refiere a una sobrecarga de *inputs* (datos) que impide que se puedan procesar a la velocidad que han sido adquiridos, lo que puede hacer colapsar los procesos siguientes. Así, el exceso de información, al igual que su falta, implica desventajas.
- *Anonimato.* Aunque el acceso al ciberespacio es público, las especiales circunstancias que presenta, a priori, favorecen el anonimato de los usuarios que pueden interactuar en él. Este hecho puede tener un importante impacto, por ejemplo, en la evaluación de la información o en la localización de objetivos.

El sistema clásico de inteligencia ante las nuevas amenazas a la seguridad

Si bien se puede definir la existencia de distintos métodos clásicos de extracción de inteligencia, no existe consenso sobre un protocolo específico para elaborar inteligencia del ciberespacio, independientemente de que existan procedimientos diversos, fundamentalmente desde el sector privado, para explotar las denominadas "fuentes abiertas". Los métodos clásicos OsInt de inteligencia en fuentes abiertas se enfrentan a un nuevo paradigma de investigación que aparentemente se aleja de su concepción, dado que se concibieron como método de extraer datos procedentes de los medios masivos de comunicación de entonces: la prensa, la radio, la televisión, etc. En la actualidad, en cambio, ese paradigma de investigación alcanza un espectro amplio de difícil asunción con un OsInt basado en la técnica original. Ante este escenario, algunas voces especializadas, como las que se expresan desde la Corporación RAND (Williams, & Blum, 2018), defienden que el ciclo clásico de la inteligencia puede enfrentar, con las necesarias ampliaciones del propio ciclo OsInt, los fenómenos criminales ubicados en el ciberespacio. Esto se puede conseguir estableciendo cuatro subfases dentro del propio ciclo clásico de la inteligencia, dentro de OsInt, que serían la "adquisición, el procesamiento, la explotación y la producción", como una adaptación a las nuevas tecnologías (Treverton & Ghez, 2012).

Ante este escenario, la primera pregunta sería por qué forzar las técnicas de OsInt para aplicarlas en internet. La creación de una nueva disciplina de ciberinteligencia (CybInt) planteada desde cero para este ámbito, más amplio que el que concibió en su momento OsInt, podría solucionar los problemas que se han presentado en los procedimientos habituales utilizados en la elaboración de inteligencia en fuentes abiertas. Por todo lo anterior, se debe resaltar que la inteligencia que se puede desarrollar en el ciberespacio no es únicamente la relacionada con OsInt, esto es, las fuentes abiertas, sino que también se puede explotar la información proveniente de redes no públicas, de las interacciones que se producen entre diferentes componentes intangibles o de las vulnerabilidades del hardware (Mazurier et al., 2019). Asimismo, tampoco se debe circunscribir la CybInt a la inteligencia generada desde y para el ciberespacio, puesto que constreñir este tipo de inteligencia a la toma de decisiones en este ámbito limita de manera sorprendente otros espacios en los que la inteligencia proveniente del entorno cibernético aportaría un gran conocimiento del mundo criminal. Por este motivo, desde la perspectiva de la elaboración de inteligencia criminal en el ciberespacio, las metodologías OsInt son insuficientes, ya que, como se ha mencionado, no abarcan el amplio espectro que cubre este escenario.

Conclusión

En los últimos años se ha intentado desarrollar metodologías de inteligencia como OsInt con mayor profundidad, orientadas cada vez más al ciberespacio. A través de estas metodologías se elabora inteligencia de datos que se encuentran abiertos al público en general,

pero cuyos procedimientos provienen de épocas en que el ciberespacio no existía ni como concepto. Entendiendo que ciberinteligencia es la inteligencia elaborada a partir de cualquier ámbito del ciberespacio para responder a las actividades delincuenciales, localizadas tanto dentro como fuera de este dominio, este análisis ha recorrido fase a fase los procesos comunes en el desarrollo de la inteligencia criminal, para analizar cómo se pueden explotar en cada fase las oportunidades que el ciberespacio ofrece. Con esto se ha demostrado que el ciberespacio modifica transversalmente las acciones desarrolladas en los procesos clásicos de inteligencia.

Desde esta óptica, en la elaboración de inteligencia criminal, el ciberespacio se presenta como una gran oportunidad, no solo para analizar las posibles ciberamenazas que podrían llevarse a cabo y afectar la seguridad dentro y fuera del quinto dominio, sino también como un espacio que ofrece grandes recursos para recopilar información de toda índole, y en el que se pueden obtener y utilizar herramientas para hacer análisis delincuenciales con mucho mayor alcance (Payá-Santos et al., 2017).

Así, conocer las interacciones que se producen y los datos que se comparten en este escenario ofrece unas oportunidades nunca antes vistas en la historia para cualquier actor que tenga necesidad de información y conocimiento. Todo ello, máxime en el ámbito de la inteligencia criminal, favorece la toma de decisiones orientada a garantizar, entre otras cosas, la seguridad pública. Este nuevo dominio está en constante expansión, de modo que se ha generado un espacio infinito de información donde solo los analistas mejor formados y con las herramientas tecnológicas más avanzadas podrán analizar todos los componentes del ciberespacio, y así prestar atención al gran número de ciberamenazas que pueden llegar a tener un impacto notable en la seguridad y en los derechos de los ciudadanos.

Agradecimientos

Los autores desean agradecer a la Universidad Isabel I de Castilla y al Instituto Internacional de Estudios en Seguridad Global (Iniseg) por su apoyo en la realización de este artículo.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre los autores

Claudio Payá-Santos es doctor *cum laude* en ciencias humanas, sociales y jurídicas por la Universidad Internacional de Cataluña, doctor en teoría política por la LUISS de Roma,

máster en inteligencia y en grafoanálisis europeo, y licenciado en criminología. Es investigador invitado en la Scuola Universitaria Superiore Sant´Anna de Pisa y profesor visitante en la Universidad de Florencia.

https://orcid.org/0000-0002-1908-9960 - Contacto: claudio.paya@ui1.es

José María Luque Juárez es doctor en ciencias sociales por la UCAM, licenciado y título superior de criminología por la Universidad de Alicante y graduado en seguridad por la Universidad Nebrija. Especialización profesional universitaria en ciencias policiales por la Universidad de Valencia. Docente de la Universidad Nebrija y de la Conselleria de la Generalitat Valenciana.

https://orcid.org/0000-0002-3707-7621 - Contacto: jluque@iniseg.es

Referencias

Calleja, G., & Delgado, J. J. (2017). Cuba vs. Estados Unidos: el contencioso de la base naval de Guantánamo. En A. M. Alija (Coord.), *Territorio y conflicto en América Latina* (pp. 313-359). Thomson Reuters.

Centro Criptológico Nacional (CCN). (2015). *Guía de seguridad (CCN-stic-425). Ciclo de inteligencia y análisis de intrusiones*. Ministerio de la Presidencia, Gobierno de España. https://bit.ly/3v9y2pU

Delgado, J. J. (2017). *Las relaciones internacionales del siglo XXI: transformar el mundo*. Thomson Reuters.

Delgado, J. J., Jiménez Reina, J., & Jiménez Reina, R. (2019). Transporte aéreo estratégico militar en las operaciones militares modernas. *Ciencia y Poder Aéreo, 14*(1), 114-147. https://doi.org/10.18667/cienciaypoderaereo.625

Delgado-Morán, J. J., Jiménez-Reina, J., & Cremades-Guisado Á. (2020a) Analytical approach to emergent hybrid threats phenomena. Case study: EU and Colombia. En J. Ramírez & J. Biziewski (Eds.), *A shift in the security paradigm* (pp. 49-68). Springer. https://doi.org/10.1007/978-3-030-43253-9_5

Delgado-Morán, J. J., Jiménez Reina, J., & Jiménez Reina, R. (2020b). Seguridad cooperativa como medida de prevención y respuesta de la Unión Europea. *Revista Científica General José María Córdova, 18*(29), 61-85. https://doi.org/10.21830/19006586.520

Delgado, J. J., & Teano, F. (2019). El concepto de hidrohegemonía como marco de análisis de los conflictos transfronterizos por el agua. Pensando en el caso chino. *Agua y Territorio, 14*, 97-104. https://doi.org/10.17561/at.14.4437

Delgado, J. J., & Teano, F. (2020). Gendering migration: securitization and integration media narratives in Europe. *Vergentis. Revista de Investigación de la Cátedra Internacional Conjunta Inocencio, 3*(11), 93-126. https://bit.ly/3DVkOQy

Elías, C. A., & Velázquez O., A. (2014). La ciberdefensa y sus dimensiones global y específica en la estrategia de seguridad nacional española. *Icade. Revista de la Facultad de Derecho, 92*, 59-76. https://doi.org/10.14422/icade.i92.y2014.002

Fernández-Osorio, A., Cufiño-Gutierrez, F., Gómez-Díaz, C., & Tovar-Cabrera, G. (2019). Dynamics of State modernization in Colombia: The virtuous cycle of military transformation. *Democracy and Security, 15*(1), 75-104. https://doi.org/10.1080/17419166.2018.1517332

Fernández-Rodríguez, J. C., & Delgado, J. J. (2016). La mujer en el terrorismo suicida. *Estudios en Seguridad y Defensa, 11*(22), 75-89. https://doi.org/10.25062/1900-8325.210

Joyanes Aguilar, L. (2011). Introducción. Estado del arte de la ciberseguridad. *Cuadernos de Estrategia, 149*, 11-46. https://dialnet.unirioja.es/servlet/articulo?codigo=3837217

Kent, S. (1949). *Strategic intelligence for American world policy*. Princeton University Press.

Mazurier, P., Delgado-Morán, J., & Payá-Santos, C. (2019). Gobernanza constructivista de la internet. *Teoría y Praxis, 17*(34), 107-130. https://bit.ly/3oXOs3A

Payá-Santos, C., Cremades Guisado, Á., & Delgado, J. (2017). El fenómeno de la ciberdelincuencia en España: la propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. *Revista Policía y Seguridad Pública, 7*(1), 237-270. https://doi.org/10.5377/rpsp.v7i1.4312

Payá-Santos, C. A., & Delgado-Morán, J. J. (2016). El uso del ciberespacio para infringir el terror. *Estudios en Seguridad y Defensa, 11*(22), 91-108. https://doi.org/10.25062/1900-8325.211

Payá-Santos C. A., & Delgado-Morán, J. J. (2017a). Use of cyberspace for terrorist purposes. En J. Ramírez & L. García-Segura (Eds.), *Cyberspace* (pp. 197-209). https://doi.org/10.1007/978-3-319-54975-0_12

Payá-Santos, C., & Delgado-Morán, J. J. (2017b). Incertidumbres del análisis dimensional de la inteligencia. *URVIO. Revista Latinoamericana de Estudios de Seguridad, 21*, 225-239. https://doi.org/10.17141/urvio.21.2017.2962

Payá-Santos, C., Delgado-Morán, J. J., & Fernández Rodríguez, J. (2015). Los medios de producción de inteligencia, en el análisis actual de los conflictos. *Estudios en Seguridad y Defensa, 10*(20), 5-17. https://doi.org/10.25062/1900-8325.31

Ruiz-Ruano, A., Puga, J. L., & Delgado-Morán, J. J. (2019). El componente social de la amenaza híbrida y su detección con modelos bayesianos. *URVIO. Revista Lationamericana de Estudios de Seguridad, 25*, 57-69. https://doi.org/10.17141/urvio.25.2019.3997

Schmitt, M. (2013). *Tallinn Manual on the international law applicable to cyber warfare gen*. Cambridge University Press. https://ccdcoe.org/research/tallinn-manual/

Townsend T., Ludwick, M., McAllister, J., Mellinger, A., & Ambrose, K. (2013, enero). *Cyber Intelligence Tradecraft Project. Summary of key findings* (SEI Innovation Center Report). Emerging Technology Center; Carnegie Mellon University. https://bit.ly/3BDLcO3

Treverton, G. F., & Ghez, J. J. (2012). *Making strategic analysis matter*. RAND Corporation. https://www.rand.org/pubs/conf_proceedings/CF287.html

Williams, H., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise*. RAND Corporation: https://bit.ly/2YJL29f