

La inteligencia de comunicaciones contra el crimen organizado: un arma fundamental ante la amenaza híbrida

TENIENTE CORONEL DE LA GUARDIA Civil
Juan de Dios GÓMEZ GÓMEZ

RESUMEN

Recientemente han visto la luz dos documentos de la máxima trascendencia estratégica en lo que se refiere a la seguridad de la UE y de España, la Brújula Estratégica (UE) y la Estrategia de Seguridad Nacional (España). Ambos identifican la amenaza híbrida como una de las más relevantes a las que la UE y sus Estados Miembro deben hacer frente con nuevas estrategias y medidas. En esta línea, una reciente resolución del Parlamento Europeo llama a la Comisión Europea a tomar medidas para identificar y neutralizar este tipo de amenazas. Esta investigación trata de determinar nuevas maneras de explotar las capacidades de inteligencia de comunicaciones (COMINT) desde el escrupuloso respeto a los DDFF de los ciudadanos y con el máximo impacto neutralizador y disuasorio que el Parlamento Europeo busca. La investigación concluye con una serie de propuestas de medidas concretas para alcanzar dicho objetivo y de nuevas líneas de investigación.

PALABRAS CLAVE: Interceptación de comunicaciones, zona gris, conflictos actuales, Derechos Fundamentales, garantías jurídicas.

SUMMARY

Two documents of the utmost strategic importance in terms of the security of the EU and Spain have recently been published: the Strategic Compass (EU) and the National Security Strategy (Spain). Both identify the hybrid threat as one of the most relevant threats that the EU and its Member States must face with new strategies and measures. Along these lines, a recent European Parliament resolution calls on the European Commission to take measures to identify and neutralize this type of threat. This research seeks to determine new ways to exploit communications intelligence (COMINT) capabilities while scrupulously respecting the DDFF of citizens and with the maximum neutralizing and deterrent impact that the European Parliament seeks. The research concludes with a series

of proposals for concrete measures to achieve this objective and for new lines of research.

KEY WORDS: communications Interception, gray zone, current conflicts, Fundamental Rights, legal guarantees.

INTRODUCCIÓN

La amenaza del Crimen Organizado en el ámbito de conflictos híbridos sostenidos en estados vulnerables, desestabilizados, caídos, en situación poscrisis o en proceso de recuperación, puede contribuir a la ausencia o pérdida de confianza en los poderes públicos de dichos países. En ocasiones, incluso entrelazando sus actividades y fines con el terrorismo o la subversión. También en estados democráticos consolidados, el Crimen Organizado puede erigirse en una herramienta al servicio de intereses desestabilizadores o, por qué no, de agresión manifiesta, operando en una zona gris del conflicto. Las organizaciones criminales tienen a su alcance muy relevantes capacidades para proveer de seguridad sus sistemas de comunicaciones y preservar así, fuera del alcance de las agencias implicadas en combatirlos y los poderes públicos legales y de justicia, sus actividades e informaciones más sensibles.

ANTECEDENTES

En este escenario es necesaria una estrategia coordinada contra la injerencia extranjera en la UE. El Parlamento Europeo está profundamente preocupado por la creciente y cada vez más sofisticada naturaleza de estas actividades de injerencia y de los intentos de manipulación de la información llevados a cabo por Rusia y China. Estas acciones han tenido como objetivo todo el espectro del funcionamiento democrático de la UE y de sus Estados Miembro. Por ello, la intención en la UE es la de implementar políticas y herramientas de previsión, resiliencia y disuasión para hacer frente a estos ataques híbridos orquestados por agentes estatales y no estatales extranjeros. Estas políticas y herramientas habrán de basarse, entre otros aspectos, en el establecimiento de una terminología y una metodología común, evaluaciones de impacto de la legislación adoptada hasta la fecha, un sistema de inteligencia compartida, sistemas de alerta temprana y conciencia situacional, políticas de construcción de resiliencia, sanciones, contramedidas y apropiadas capacidades de disrupción y defensa (Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación, 2022).

En este artículo se tratan los efectos positivos que las capacidades de inteligencia de comunicaciones puede tener en la mejora de la cooperación para el alcance de los objetivos de la Estrategia de Seguridad Nacional (2021)I y de la Seguridad Cooperativa Europea en los escenarios en los que España esté involucrada, en concreto, proponiendo nuevas líneas de aprovechamiento de capacidades de inteligencia de comunicaciones en el marco de la lucha contra el Crimen Organizado ante la amenaza híbrida.

EXPOSICIÓN

En la actualidad, existen capacidades de inteligencia de comunicaciones tecnológicamente innovadoras de aplicación a la lucha contra el Crimen Organizado. Más allá de las técnicas de interceptación de comunicaciones empleadas en las investigaciones contra el Crimen Organizado de manera rutinaria en escenarios no bélicos, que no son masivas y que precisan de la cooperación de las compañías proveedoras de servicios de comunicación o de la información, existen otras que, desde la perspectiva técnica, pueden ser también de aplicación en el ámbito de los conflictos híbridos. Es el caso de técnicas de interceptación dirigida innovadoras como las técnicas de interceptación tácticas y las técnicas de interceptación EPI [1], y técnicas de interceptación masiva como la interceptación del Internet Back Bone (Gran Sala del Tribunal Europeo de Derechos Humanos, 2021) o las técnicas ISR aeroespaciales. También se han identificado técnicas de análisis de datos asociados a comunicaciones electrónicas conservados (CDR) (Gómez Gómez, 2019), metadatos, que pueden ser de gran interés en la lucha contra el Crimen Organizado en todos los escenarios.

El Crimen Organizado es un vector de desestabilización que puede ser empleado de forma deliberada por actores hostiles en el marco de conflictos híbridos dentro de la zona gris de su espectro, como proxi para contribuir decisivamente a la consecución de sus objetivos maliciosos (Ministerio de Defensa., 2018). En México, por ejemplo, se ha constatado como las redes de crimen transnacionales emplean los cárteles mexicanos de la droga para desestabilizar al gobierno del país y parasitar el Estado con el objeto de garantizar sus objetivos lucrativos. En el caso de Rusia la guerra híbrida está contemplada en su forma de dirimir conflictos internacionales, y el Crimen Organizado y la corrupción son deliberadamente empleados para injerir e influir de manera contraria a la buena fe en asuntos internos de determinados países, todo ello en escenarios ajenos al espectro bélico del conflicto (Fridman, 2017).

La explotación de capacidades de inteligencia de comunicaciones tiene una afectación directa en los Derechos Fundamentales de los ciudadanos cuando se emplean en escenarios catalogados como de zona gris. El derecho al secreto de

las comunicaciones queda protegido por un gran abanico de normativas nacionales y, sobre todo, de Derecho Internacional, habiendo sido ratificado también por jurisprudencia de los más altos tribunales de ambos ámbitos. Esta alta protección está fundamentada en el uso privado de las comunicaciones por parte de los individuos, relativo a su vida privada y familiar (Convenio Europeo de Derechos Humanos, 1950, Art. 8), y en la expectativa de privacidad que albergan para estos asuntos cuando los tratan por dicho medio de comunicación. Si bien es cierto que el uso relativo a la vida privada y familiar de medios de comunicación de sistemas de mando y control militar por parte de unidades desplegadas en un conflicto bélico sería discutible, no lo es en caso de actores como el Crimen Organizado, en especial cuando actúan en el espectro no bélico del conflicto, como es la zona gris, y pese a que lo hagan como vector de injerencia o proxi de un actor estatal hostil.

Existe una falta de preparación generalizada en los actores nacionales e internacionales a nivel europeo para hacer frente a la amenaza híbrida. De ello se hace eco la reciente Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación. Se pone de manifiesto una falta de aprovechamiento de las capacidades de inteligencia de comunicaciones para identificar y neutralizar la amenaza híbrida cuando progresa empleando el Crimen Organizado como proxi. Esta faceta del Crimen Organizado, que implica una amenaza a bienes jurídicos superiores, como son la seguridad nacional, más allá de la protección del patrimonio, o la salud pública, no encuentra un reflejo proporcional en la modulación de las garantías jurídicas que protegen el DDFD al secreto de las comunicaciones en escenarios de paz formal.

Es perentorio analizar las vulnerabilidades del Estado de Derecho en los países democráticos ante estas amenazas en la zona gris y, en particular, en lo que atañe al aprovechamiento que los actores hostiles pueden pretender explotar de las garantías que el marco jurídico en tiempo de paz exige para la protección de los DDFD de los ciudadanos, en concreto el derecho al secreto de las comunicaciones. Es decir, es necesario evitar que actores hostiles, injiriendo en los asuntos de un país democrático a través del vector Crimen Organizado, se aprovechen de un marco jurídico de garantías procesales que no permita una acción investigadora contundente contra esas actividades. Por una parte, esta falta de contundencia podría ser consecuencia de una falta de capacidad legal para identificar y atribuir al Crimen Organizado fines distintos del lucro económico, como serían los de injerencia extranjera en caso de darse. Por otra, por una falta de herramientas o medidas de investigación suficientes para contrarrestar dicha acción hostil.

Por tanto, se considera oportuno que los estados democráticos acometan las siguientes acciones a fin de protegerse ante las amenazas híbridas por medio del aprovechamiento de capacidades de inteligencia de comunicaciones:

- Analizar de forma graduada y honesta el empleo de sus capacidades de inteligencia de comunicaciones antes de considerar respuestas institucionales y operativas contra el Crimen Organizado en la zona gris o de guerra híbrida.
- Contribuir al desarrollo internacional de una nueva teoría del conflicto, fruto de una asociación de los estados democráticos basada en un entendimiento común y en definiciones compartidas, con vistas a establecer normas y principios internacionales comunes (Resolución del Parlamento Europeo, de 9 de marzo de 2022). Para ello, será necesario definir lo que puede entenderse como un hecho internacionalmente ilícito desde el enfoque de la injerencia extranjera y los umbrales mínimos para la activación de contramedidas. Así, habrán de establecerse estándares suficientes y apropiados de procedimientos de alerta, y de medidas para identificar y responder ante actos de injerencia. Se propone, como indica el Parlamento Europeo, el establecimiento de un registro de injerencias extranjeras y la creación de un registro de las actividades declaradas realizadas para un Estado extranjero o en su nombre, gestionado por los gobiernos. Y todo ello habrá de hacerse teniendo presente que esta nueva teoría y su desarrollo, como dice Baqués (2017), ha de ser: “capaz de integrar en un *continuum* la propia zona gris, la guerra híbrida y la guerra convencional, contando con sus solapamientos y con sus intersecciones, llegado el caso” (p.11). Como dice Tenzer, (2021), será fundamental que la nueva teoría y su desarrollo permita descubrir y atribuir acciones, en este caso del Crimen Organizado, que caigan bajo el paraguas de las agresiones híbridas, lo que es el fundamento más esencial para la lucha contra estos ataques.
- Promover los cambios legales y la adaptación de las garantías legales aplicables a la lucha contra el Crimen Organizado, tanto en zona gris como en tiempo de conflicto armado, cuando actúa en beneficio de la injerencia extranjera. Remover las limitaciones legales que impidan la compartición eficiente de información entre agencias de información o inteligencia. Tipificar como delitos nuevos ciertas actividades vinculadas al Crimen Organizado y la corrupción cuando respondan a injerencias extranjeras. Siguiendo a Tenzer (2021), también se propone desarrollar medios de castigo adecuados para el Crimen Organizado, cuando contribuye a la consecución de objetivos de esta naturaleza en línea con las propuestas del Parlamento Europeo (Resolución del Parlamento Europeo, de 9 de marzo de 2022). En este sentido recalamos que ya existen interpretaciones legales en las que se relajan las garantías jurídicas del secreto de las comunicaciones cuando afecta a bienes

jurídicos como la seguridad nacional (ver Sentencia del Tribunal De Justicia (Gran Sala), de 6 de octubre de 2020).

- Plantear cambios organizativos y adecuación de servicios policiales y de contrainteligencia. Impulsar la cooperación en inteligencia a nivel global y multilateral (Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación). Mitigar la falta de cooperación entre departamentos señalada por Baques (2017), creando grupos de trabajo conjuntos que reúnan servicios de inteligencia internos y externos, a la policía y a los servicios aduaneros y fiscales para identificar a las personas que trabajan para una potencia extranjera en línea con la propuesta de Tenzer (2021), en este caso enfocándolos a la explotación conjunta de capacidades de inteligencia de comunicaciones.
- Afrontar el estudio de la explotación en concreto de las capacidades de inteligencia de comunicaciones en la lucha contra el Crimen Organizado en la zona gris no solo en una dinámica precrisis, sino también de crisis y de poscrisis, en línea con lo propuesto por Baqués en términos generales (2017).

CONCLUSIONES

La explotación eficaz, siempre respetuosa con los Derechos Fundamentales, de capacidades de inteligencia de comunicaciones representan una oportunidad fundamental para el éxito de la lucha contra la injerencia extranjera y la amenaza híbrida, especialmente en el ámbito de la lucha contra el Crimen Organizado en la zona gris del espectro de los conflictos. La Unión Europea y sus Estados Miembro no deben olvidar este aspecto en el camino emprendido de adopción de nuevas estrategias y medidas contra la inferencia extranjera, teniendo presente en todo momento como estas capacidades pueden contribuir a la detección, neutralización y disuasión de la amenaza híbrida.

NOTAS

[1] Siglas de interceptación en el punto final en inglés. Se refiere a la interceptación de comunicaciones llevada a cabo mediante la instalación de un software de monitorización remota en el terminal de comunicaciones del objetivo de la investigación de que se trate. Esta técnica pretende interceptar la comunicación antes de que tenga lugar el cifrado de su contenido. Es la técnica empleada por soluciones como la tristemente conocida PEGASUS (Peñalosa, 2022).

(2006)

BIBLIOGRAFÍA

- Baqués, J. (2017). Hacia una definición del concepto «Gray Zone» (GZ). *Instituto Español de Estudios Estratégicos*. [Accessed 2 April 2022].
- Consejo de Europa. (1950). *Convenio Europeo de Derechos Humanos*. Sitio web Tribunal Europeo de Derechos Humanos. [Online]. Available at: http://www.echr.coe.int/Documents/Convention_SPA.pdf.
- Fridman, O. (2017). Hybrid warfare or Gibrinaya Voyna?: Similar, but different. *RUSI Journal*, 162 (1), pp.42–49. [Online]. Available at: doi:10.1080/03071847.2016.1253370 [Accessed 12 March 2022].
- Gobierno de España. (2021). *Estrategia de Seguridad Nacional*. España: BOE.
- Gómez Gómez, J. de D. (2019). La geolocalización diferida. In: *Los medios técnicos e investigación criminal*. Delta Publicaciones. pp.119–153.
- Gran Sala del TJUE. (2020). *Sentencia del Tribunal De Justicia (Gran Sala), de 6 de octubre de 2020*.
- Gran Sala del Tribunal Europeo de Derechos Humanos. (2021). *Grand Chamber Case of Big Brother Watch and others v. the United Kingdom*.
- Ministerio de Defensa. (2018). *Doctrina para el empleo de las FAS*. España. [Online]. Available at: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/PDC-01_A_Doctrina_empleo_FAS_27feb2018.pdf [Accessed 30 December 2021].
- Parlamento Europeo. (2022). Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación. <https://www.europarl.europa.eu/>, Unión Europea. [Online]. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_ES.html [Accessed 28 May 2022].
- Peñalosa, G. (2022). El móvil de Marlaska fue espiado con Pegasus en junio y el ministro de Agricultura fue víctima de un hackeo frustrado. [Online]. 10 May. Available at: <https://www.elmundo.es/espana/2022/05/10/627a3f0fe4d4d8e2258b45a2.html> [Accessed 16 May 2022].
- Tenzer, N. (2021). Countering hybrid threats between common resistance and legal measures. *GLOBSEC*. [Online]. Available at: <https://www.globsec.org/publications/countering-hybrid-threats-between-common-resistance-and-legal-measures/> [Accessed 2 April 2022].
- A Strategic Compass for Security and Defence | EEAS Website*. [Online]. Available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en [Accessed 28 May 2022].