Universitat Autònoma de Barcelona

Facultad de Ciencias Políticas y Sociología

Trabajo de Final de Grado
Resumen Ejecutivo

Título: La evolución de la política contra el ciberterrorismo de Francia en los últimos diez años

Autora: Paula González Sabariego

Tutor: Alessandro Demurtas

Fecha: Mayo de 2019

Grado en: Ciencia Política y Gestión Pública

Los ciberataques terroristas son, a día de hoy, una preocupación global debido a su fuerte impacto en las instituciones de todos los países. Concretamente, Francia, se ha visto afectada por este tipo de amenazas en la última década.

Por eso, el trabajo tiene como objetivo conocer cuáles han sido las estrategias y medidas del Gobierno francés para hacer frente al ciberterrorismo. Para ello, se va a establecer una cronología acerca de las política contra el ciberterrorismo que se han llevado a cabo.

Para situar al lector, el primer ciberataque se dio en Estonia en 2008 y fue realizado por Rusia tras una disputa por una estatua. A su vez, Francia sufrió en 2011 un ciberataque contra el Ministerio de Economía y Finanzas. Y, en 2015 sufrió su primer ciberataque terrorista contra un medio de comunicación (*TV5 Monde*). Por estos motivos, en el trabajo se analizan las estrategia y leyes promulgadas sobre seguridad interior y terrorismo des de 2011 hasta 2018.

En base a diferentes definiciones, se puede concluir que el ciberterrorismo consiste en el uso del ciberespacio, las tecnologías y, concretamente, de Internet por parte de organizaciones terroristas para lograr sus objetivos, creando pánico en las sociedades, a través de ataques a sus sistemas de información y comunicación.

Aunque es a partir de 2015 cuando hay cambios significativos en la ciberseguridad francesa, hay reacciones tras el ciberataque en 2011. Ese año, se redacta la primera estrategia de ciberdefensa: "Defensa y Seguridad de los Sistemas de Información". En ella no hay mención al ciberterrorismo, sino medidas de carácter informativo sobre ciberdelincuencia o delitos cibernéticos con fines económicos, e intenciones de legislar sobre el ciberespacio en un futuro.

En 2012, se pretende proteger los sistemas de procedimiento de datos implementados por el Estado a través de la modificación de diferentes artículos del Código Penal, los cuales no hacían referencia a sistemas de datos públicos. Esta protección va dirigida a posibles ataques cibernéticos de cualquier índole, incluida la terrorista.

En 2013, hay una extensa legislación en la ley 2013-1168 relativa a la programación militar para los años 2014-2019. En esta, aparecen nuevos artículos en el Código Penal para dar respuestas y establecer líneas de actuación ante posibles ciberataques terroristas. Además, se refuerzan las competencias de la Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI) y se incrementan los recursos humanos a través de un aumento de especialistas en ciberdefensa (500 agentes en ANSSI).

En 2014, se hace especial atención a la apología del terrorismo en servicios de comunicación en línea y al uso de documentos o sitios web de forma fraudulenta para la

realización de actos terroristas (artículos 4212-2-6 y 421-2-5 del Código Penal). De esta forma, se orienta la legislación a evitar la radicalización en Internet y la propaganda del terrorismo.

En 2015 se publica la estrategia más reciente de ciberdefensa: "Estrategia Nacional Francesa para la Seguridad del Ámbito Digital". En ella, el objetivo es divulgativo promoviendo la protección a los jóvenes de la radicalización en Internet. Iniciativas como la creación de una pagina web (stop.djihadisme.gouv.fr) o formación en los colegios y universidades sobre el ciberterrorismo, son algunas de las que aparecen. Además, se incrementan las penas relacionadas con delitos informáticos considerados actos terroristas, y se pretende aumentar los medios dedicados a la ciberdefensa en, al menos, 1000 efectivos.

En 2016, se añaden dos artículos en el Código Penal (421-2-5-1 y 421-2-5-2) en los que se consideran delitos terroristas el uso fraudulento de datos y la consulta de sistemas de comunicación provocando, en los dos casos, la apología al terrorismo.

En 2017, se legisla sobre el uso de menores para cometer cualquier acto terrorista, incluidos los delitos informáticos (art. 421.2.4.1 Código Penal). Y, también, se introduce un artículo sobre el control a personas consideradas sospechosas por visitar o estar en contacto con grupos terroristas (art. 228-1 del Código de Seguridad Interna).

Para acabar, el último año con la ley sobre "Programa Militar para los años 2019-2025 y disposiciones relevantes para la defensa", se introduce un aumento en los recursos de 1500 efectivos en las áreas de inteligencia y de ciberdefensa. Y, se proporcionan medios técnicos para la protección de sistemas y prevención de los ciberataques tanto a las Fuerzas Armadas, como a ANSSI.

Para terminar, las conclusiones a las que se han llegado son que la estrategia de ciberdefensa francesa contra el ciberterrorismo de los últimos años se basa en cuatro pilares claves: primero una nueva legislación y modificación de artículos sobre el ciberespacio y el ciberterrorismo, así como endurecimiento de las penas. Seguido del refuerzo de los órganos de ciberseguridad y sus competencias. Tercero, la aportación de nuevos recursos tanto financieros como humanos de forma progresiva. Y, por último, la intención de prevenir la radicalización, en especial en los jóvenes, a través de la red e Internet.