EVOLUCIÓN DE LA POLÍTICA CONTRA EL CIBERTERRORISMO EN FRANCIA (2010-2018)

Autora: Paula González Sabariego

Tutor: Alessandro Demurtas

INTRODUCCIÓN

Objeto de estudio: los políticas contra el ciberterrorismo en Francia.

Pregunta de estudio: ¿Qué estrategias o políticas de defensa y seguridad nacional se han implementado para afrontar el ciberterrorismo en Francia en los últimos años?

CIBERTERRORRISMO

Ciberterrorismo: uso del ciberespacio por organizaciones terroristas para causar miedo y lograr sus objetivos.

Ciberyihadismo: utilización de medios cibernéticos para realizar ataques con una motivación ideológica yihadista (CCN, 2019)

Ciberataque terrorista en Francia (2015) contra la cadena internacional "*TV5 Le Monde*".

EVOLUCIÓN DE LA POLÍTICA FRANCESA CONTRA EL CIBERTERRORISMO

2011
"Défense et sécurité des systèmes d'information":
Medidas divulgativas hacia ciberdelincuencia e intención de legislar el ciberespacio.

2012
Cambios en artículos:
323-1,323-2, 323-3.
Delitos informáticos contra sistemas de datos públicos = actos de terrorismo.

2013
Ley sobre "Programación Militar para los años 14-19": Líneas de actuación técnicas a ataques cibernéticos. Refuerzo de la seguridad y aumento de efectivos en sistemas de información.

2014:
Art. 421-2-6: consulta sititos web o documentos relacionados con el terrorismo (= actos terroristas).
Art. 421-2-5: castiga la apología del terrorismo en servicios de comunicación en línea.

2015
"Stratégie nationale pour la sécurité du numérique":
Protección de jóvenes de la radicalización en Internet. Y aumento de las penas en los delitos cibernéticos.

2016
Art. 421-2-5-1 y 421-2-5-2:
Delitos el uso fraudulento de datos y consulta de sistemas de comunicación provocando la apología al terrorismo.

2017
Art. 421-2-4-1: uso de menores para cometer delitos informáticos (actos terroristas).
Art. 228-1: comportamiento sospechoso (estar en contacto con grupos que incitan al terrorismo).

2018
Ley sobre "Programa Militar para los años 19-25" incremento de:
- 1500 efectivos en ciberdefensa.
- Capacidades FFAA en ataques cibernéticos.

CONCLUSIONES

1) Nueva legislación sobre ciberterrorismo y endurecimiento de las penas.
2) Refuerzo de órganos ya existentes como la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI).
3) Aportación de nuevos y más recursos financieros y humanos.
4) Objetivo: prevención de la radicalización, en especial en jóvenes, y de la apología en la red.

BIBLIOGRAFIA CLAVE

- Ley Nº 2012-410, ley Nº 2013-1168, ley Nº 2014-1353, ley Nº 2015-917, ley Nº 2016-731, ley Nº 2017-1510 y ley No 2018-607. Journal officiel de la république française, Paris, France.
- SGDSN, Secrétariat général de la défense et de la sécurité nationale (2015), "Stratégie nationale pour la sécurité du numérique".
- ANSSI, (2011), "Défense et sécurité des systèmes d'information - Stratégie de la France"