ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

61/2013 12 noviembre de 2013

Mª José Caro Bejarano

DELINCUENCIA ORGANIZADA E INTERNET

DELINCUENCIA ORGANIZADA E INTERNET

Resumen:

La delincuencia cibernética es un tema preocupante que inquieta por igual a la industria y a los gobiernos. Sin embargo, habría que distinguir si un específico uso delictivo organizado de Internet supone una amenaza para la seguridad nacional o internacional. Se puede determinar que depende de dos aspectos básicos: la seguridad y la delincuencia organizada. Ya se han dado algunas situaciones en las que la seguridad nacional e internacional ha sido amenazada por la actividad de ciberdelincuencia organizada. La extensión de las nuevas tecnologías a todos los ámbitos de la vida cotidiana hace inevitable su explotación continua con fines delictivos. Parte de esta actividad puede poner en peligro la seguridad, mientras que otra no. Es importante distinguir qué actos ciberdelincuentes pertenecen a cada categoría para encontrar las respuestas adecuadas.

Abstract:

Cyber-crime is a concern that worries equally to industry and governments. However, one should distinguish whether a specific organised criminal use of the Internet poses a threat to national or international security. It may be set that depends on two basic issues: security and organised crime. There have already been some situations in which national and international security have been threatened by organised cyber-criminal activity. The extension of new technologies in all areas of everyday life makes its continuous exploitation for criminal purposes inevitable. Some of this activity may compromise security, while some of it may not. It is important to distinguish which acts cyber-criminal acts belong to each category to find out the right answers.

Palabras clave:

Ciberdelincuencia, Tecnologías de la Información y Comunicación, TIC, seguridad nacional e internacional, ciberamenaza, ciberataque, ciberseguridad, infraestructuras críticas.

Keywords:

Cyber-crime, Information and Communication Technology, ICT, national and international security, cyber threat, cyber-attack, cyber security, critical infrastructures.

DELINCUENCIA ORGANIZADA E INTERNET

En los últimos años la delincuencia cibernética se ha convertido en un tema preocupante que inquieta por igual a la industria y a los gobiernos. El hecho de que el uso delictivo organizado de Internet suponga una amenaza para la seguridad nacional o internacional depende de dos aspectos básicos: la seguridad y la delincuencia organizada. Ya se han dado algunas situaciones en las que la seguridad nacional e internacional, han sido amenazadas por la actividad de ciberdelincuencia organizada. La extensión de las nuevas tecnologías digitales a todos los ámbitos de la vida cotidiana hace inevitable su explotación continua con fines delictivos. Parte de esta actividad puede poner en peligro la seguridad, mientras que otra no. Es importante distinguir qué actos ciberdelincuentes pertenecen a cada categoría para encontrar las respuestas adecuadas.

El concepto de seguridad nacional se ha ampliado en los últimos años para abarcar aspectos como la seguridad humana, centrado en los grupos y las personas; la seguridad ambiental, la preocupación por las pandemias, etc. Cada vez más, la capacidad de penetración de la tecnología digital tiene también profundas implicaciones para la seguridad, como son las infraestructuras críticas, tales como la generación de energía, las telecomunicaciones, los sistemas financieros y de defensa, etc., que dependen y se apoyan en la tecnología digital.

La expansión de la noción de seguridad en la era posterior a la Guerra Fría ha ido paralela a una mayor atención a la delincuencia convencional que - impulsada por el importante aumento en el uso de drogas en las naciones occidentales, con el consiguiente perjuicio a la salud, la productividad económica y a la cohesión social; y la creciente fuerza de las redes de delincuencia organizada que controlan el narcotráfico - ha adquirido mayores implicaciones para la seguridad. La delincuencia transnacional (la mayoría de ella organizada) ya se consideró una amenaza de seguridad prominente en el discurso del Presidente Clinton en la Asamblea General de la ONU en 1995. En los últimos tiempos, la actividad organizada denominada “ciberdelincuencia” también ha sido incluida entre las amenazas a la seguridad nacional. Algunas de estas consideraciones de hecho, pueden ser válidas, pero no deben aceptarse plenamente, sin ninguna crítica, para no caer en el riesgo de lo que se ha denominado “hipersecurización” o exceso de seguridad.

Las múltiples facetas de la seguridad internacional resultan difíciles de definir, de igual manera, la delincuencia organizada carece de una definición universalmente aceptada. El concepto común de la delincuencia organizada se ha visto superado por la evolución del fenómeno en sí. Hace cuatro décadas se analizaba el clásico "modelo mafia”. En la década de 1990, los observadores de las organizaciones criminales informaban de que en lugar de estructuras formales y permanentes, una cantidad importante de la actividad delictiva se

realizaba por coaliciones independientes de grupos más pequeños que convergían temporalmente para intercambiar bienes y servicios. La idea de empresas integradas verticalmente dio paso, por lo tanto, a la metáfora de "redes", que proporcionaban una base para el pensamiento contemporáneo sobre las relaciones tanto dentro de los grupos delictivos organizados como en grupos de individuos.

Las definiciones tradicionales de la delincuencia organizada se han basado en el ánimo de lucro. Sin embargo, incluso la mayoría de los observadores de la delincuencia organizada tradicional señalan el atractivo intrínseco de la emoción, el compañerismo y otros valores no materiales. Actualmente, hay muchas organizaciones criminales (como las especializadas en el fraude y el robo de vehículos) que no practican la violencia, ni el soborno. Por otra parte, una gran cantidad de actividades de la delincuencia organizada en Internet está impulsada principalmente por consideraciones no monetarias, como la búsqueda de desafío intelectual, notoriedad individual o del grupo, la lujuria (en el caso de la actividad pedófila organizada), la ideología, la rebelión y la curiosidad.

La visión tradicional de las organizaciones delictivas como delincuentes profesionales a tiempo parcial o completo es también algo simplista. Algunas organizaciones criminales requieren pertenencia explícita o implícita, pero también pueden incluir una variedad de simpatizantes, seguidores y cómplices, algunos de los cuales serán muy conscientes de su complicidad en la empresa delictiva, mientras que otros no. Además, así como la distinción entre los sectores público y privado se ha desdibujado en los últimos años con respecto a las actividades legítimas como las asociaciones público-privadas, la subcontratación y otros mecanismos para la prestación conjunta de gobernanza, así también hay un larga tradición de colaboración público-privada en la actividad criminal en apoyo de los intereses del Estado.

Como tal, algunos Estados también son capaces de actos delictivos directa o indirectamente. Una vez más, esto no es un fenómeno nuevo: a lo largo de la historia, los delitos cometidos por agentes del Estado han ocurrido en tiempos de paz, así como durante los conflictos armados.

Las formas híbridas de colaboración público-privada en actividades de crimen organizado pueden estar situadas a lo largo de un continuo, cuyos polos representan a la actividad privada "puramente" por un lado, y el propio Estado directamente involucrado en ese tipo de actividad, o incluso por sí solo, por el otro lado. Entre estos polos opuestos, se puede observar situaciones en las que el Estado hace la vista gorda a la delincuencia privada, donde se condona implícitamente la actividad delictiva; donde se promueve activamente esta actividad, pero a distancia, o cuando de forma sistemática colabora con sus socios delictivos

privados. La imagen de los actores de la delincuencia organizada y su relación con la seguridad, es por tanto, bastante numerosa y compleja, incluso antes de que el delito cibernético apareciera.

CONCLUSIÓN. EL DELITO CIBERNÉTICO ORGANIZADO

Gran parte de las comunicaciones ordinarias actuales y el mantenimiento de los registros se basa en Internet y en las tecnologías relacionadas. Al tiempo que la tecnología digital mejora la eficiencia de las actividades legítimas ordinarias, también mejora la eficiencia de las actividades delictivas. El delito cibernético o ciberdelito se refiere en términos generales a la actividad delictiva que utiliza los sistemas de información como instrumentos u objetivos de una ilegalidad. Esto supone el acceso ilícito a los sistemas, la interferencia con su uso legal y el robo o la destrucción de la información contenida en ellos. También puede implicar la posesión o transmisión de contenido prohibido.

Para nuestros propósitos, la cuestión fundamental es si la ciberdelincuencia organizada ha alcanzado una escala e intensidad que pudiera amenazar la seguridad nacional e internacional. Sin embargo, es necesario en primer lugar, establecer una definición de la ciberdelincuencia organizada. Al hacerlo, es importante analizar los diferentes tipos de ciber-actividad que podrían considerarse "delictiva", los tipos de actores y organizaciones que persiguen los mismos, y la cuestión de si todos los actos realizados por las organizaciones y que son ilícitos pueden, de hecho, ser clasificados como “ciberdelincuencia organizada".

En un posterior documento de análisis se complementarán y estudiarán estas cuestiones para intentar tener una visión clara y organizada de las mismas.

Mª José Caro Bejarano
Analista Principal IEEE