

Proyecto JEAN MONNET

La Unión Europea y la seguridad: defensa de los espacios e intereses comunes



Numero de proyecto: 565277-EPP-1-2015-1-ES-EPPJMO-PROJECT

Duración: 01/09/2015 – 31/08/2017

Universidad Complutense de Madrid

Cofinanciado por el Programa ERASMUS +
de la Unión Europea



RESÚMENES

Taller 3 “Ciberespacio: desafíos contemporáneos”

PARTE 1:

Yaiza RUBIO VIÑUELA Y Félix BREZO

“La posición de la industria ante el contexto de las ciberamenazas”.

Uno de los principales retos para cualquier unidad de inteligencia que opera en el sector de la ciberseguridad, tanto si pertenece al sector público como el privado, es la obtención de información referente a aquellas amenazas que proceden de la red. La dificultad de detección se debe principalmente a cómo se encuentra estructurada internet, así como a la escasez de recursos que tiene cualquier organización para poderles hacer frente, especialmente si se tiene en cuenta que en ocasiones se considera dicha protección más como un gasto que como una inversión.

A esta complejidad se le suma el aumento de las herramientas orientadas a proporcionar anonimato en la red, que desde el punto de vista del usuario, son necesarias si queremos que nuestra información no sea interceptada por un tercero, pero que si son utilizadas por cibercriminales hacen muy difícil que se pueda llegar a una atribución real por parte del investigador.

La cibercriminalidad es una parte muy importante a tener en cuenta debido a su crecimiento en los últimos años. Sin embargo, en la actualidad, nos encontramos ante un nuevo contexto de amenazas avanzadas mucho más sofisticadas tecnológicamente e incluso más propias de organismos estatales que no son posibles de detectar por las soluciones y servicios tradicionales de seguridad. En este sentido, los ponentes expondrán su

visión del problema a partir de investigaciones reales llevadas a cabo, así como esbozarán los caminos que están tomando tanto la industria como los organismos públicos para minimizar este tipo de amenazas.

XESÚS PÉREZ LÓPEZ

“La Unión Europea, entre la espada de la incertidumbre y la pared de los hechos: la regulación de las criptomonedas”.

Aún a día de hoy, las criptomonedas son consideradas por los analistas de la evolución de las tecnologías de la información como una de las aplicaciones en devenir de la tecnología de registros distribuidos (TRD), cuya madurez definitiva requerirá aún varios años. A pesar de ello, su presencia social y económica es un ya hecho, que impone al legislador la necesidad de regular un fenómeno aún en desarrollo, con los inevitables inconvenientes que ello implica. Puesto que las aplicaciones financieras de las criptomonedas participan de la naturaleza transfronteriza y desmaterializada propia de las tecnologías de la información, la Unión Europea está llamada a jugar un papel protagonista en esta difícil tarea regulatoria.

El ponente ofrecerá un análisis de las incipientes acciones admonitoras, jurisprudenciales y legislativas de las instituciones europeas, el cual partirá de la percepción de las criptomonedas por parte de los principales actores sociales e institucionales implicados. Seguirá una alusión a los factores que han determinado que las distintas reacciones por parte de agencias, supervisores y legisladores presten una atención especial en los riesgos de empleo de las criptomonedas en el ámbito de las finanzas criminales. Por último, el ponente analizará los grandes rasgos de la incipiente jurisprudencia nacional y europea sobre la materia, y en particular el proyecto de reforma de la Directiva de prevención del

blanqueo de capitales, el cual, entre otras medidas ad hoc, prevé extender sus obligaciones específicas de información a los cambistas de criptomonedas.

PARTE 2:

Rosario DUASO CALÉS

“Los principios de ‘*Privacy by Design*’ y ‘*Privacy by Default*’ como mecanismos de protección de los datos personales en el ciberespacio”

El nuevo Reglamento general de protección de datos, establece a nivel europeo, un nuevo dispositivo de protección de los datos personales en un contexto caracterizado por el uso generalizado de Internet y por un desarrollo jamás conocido en el pasado en lo que respecta a la innovación tecnológica.

El texto europeo establece los principios de la protección de datos desde el diseño y por defecto, que responden a esta realidad y que además se alinean con la idea de que la propia tecnología puede jugar un papel esencial en la protección de los datos personales.

En la presentación analizaremos los orígenes de los conceptos de *Privacy by Design* y *Privacy by Default*, desarrollados desde hace varios años, para entender así cómo y por qué estos principios se han convertido en la actualidad en unos de los instrumentos fundamentales de la protección de datos personales en el ciberespacio.

Manuel J. GAZAPO LAPAYESE

“Amenazas Virtuales: Terrorismo y Crimen Organizado en el Ciberespacio”

Los conflictos entre seres humanos han ido evolucionado conforme el paso

del tiempo. La comisión de actos delictivos y bélicos han ido conociendo diferentes escenarios, como la tierra, el mar, el aire y el espacio. Todas estas dimensiones de conflicto pertenecen a un plano material o tangible. La llegada del siglo XXI y el desarrollo de Internet han hecho posible la aparición de una nueva dimensión de carácter intangible en la que los actores de la Sociedad Internacional pueden combatir sin la necesidad de enfrentarse cuerpo a cuerpo: el ciberespacio.

De la misma manera que los conflictos entre Estados-Nación se trasladan hacia el ciberespacio, las organizaciones criminales y grupos terroristas también están trasladando sus operaciones a esta nueva dimensión. Esto provoca que el ciberespacio se esté convirtiendo en la primera línea de batalla de los principales conflictos contemporáneos. El aumento de la interdependencia y la interconexión entre todos los actores de la escena internacional ha traído consigo un aumento de las vulnerabilidades del sistema.

El cibercrimen y el ciberterrorismo evidencian la compleja situación en la que nos encontramos, en tanto, los conflictos clásicos se trasladan y metamorfosean en la red. A través del estudio de algunos casos paradigmáticos se analizarán las condiciones de campo de este nuevo ciberterritorio y sus lógicas operativas.

Se llegará a la conclusión de que para poder hacer frente a este nuevo panorama, se hace innegable la necesidad de una acción multidimensional que englobe a todos los actores de la Sociedad Internacional e implique de forma directa a la sociedad civil para desarrollar una cultura de ciberseguridad proactiva y no solo reactiva.