


**Introducción: Especial Ciberespacio**

# Introducción: Especial Ciberespacio

El ciberespacio es un ámbito muy extenso que se fundamenta principalmente en el uso intensivo de la tecnología en el día a día incluso en cuestiones que poco tiempo atrás se mantenían muy alejadas de estos ámbitos. Constituye herramienta, medio y fin en un gran número de cuestiones, lo que hace que cada vez resulte más complicado establecer de forma clara cuándo una cuestión está relacionada con el ciberespacio o no. El fenómeno de las redes sociales y el uso que se hace de ellas es un ejemplo de esta falta de definición pues, mientras para muchas personas se trata de una cuestión eminentemente cibernética, son también muchos los autores que lo separan de este ámbito más tecnológico y lo enfocan bajo una perspectiva más relacionada con la comunicación, la política o incluso las relaciones internacionales. Los fundamentos tecnológicos que soportan o dan lugar al ciberespacio también hacen que cuestiones de naturaleza tecnológica se incluyan dentro de este ámbito, lo que viene reforzado por la creciente necesidad de conectividad asociada a todas las tecnologías.

Se ha hecho un ejercicio de selección de los documentos publicados en este periodo de dos años que se ha considerado lo suficientemente extenso como para disponer de una visión global a la vez que no demasiado extenso ya que, ante la acelerada evolución que está experimentando este ámbito, las cuestiones, propuestas y visiones quedan

rápidamente obsoletas. En aquellas áreas donde no existían publicaciones, se ha pedido la colaboración de autores externos con el fin de completar una visión global de este campo que permita cubrir las áreas que, sin duda, serán tratadas a lo largo del curso.

La recopilación cuenta con un total de 20 documentos que se han organizado empezando por aquellos documentos de carácter más general y que tratan cuestiones de naturaleza más amplia en el ámbito del ciberespacio.

El primer documento, elaborado por Javier Candau, aborda la ciberseguridad, una de las cuestiones más importantes del ciberespacio. Internet es una tecnología que se ha desarrollado de forma incremental sobre una base que inicialmente primaba la capacidad de comunicación sobre cuestiones como la privacidad, la seguridad de la información y la disponibilidad. Son muchas las medidas que a lo largo de los años se han ido incorporando para conseguir estos fines mientras que los actores maliciosos han aprovechado las vulnerabilidades para fines ilícitos como el robo de la información, el secuestro de los sistemas o la desconexión digital de empresas. En el documento se introduce el concepto de ciberseguridad, se describe cómo a lo largo de los años se ha abordado y ha ido evolucionando esta cuestión desde los ámbitos de la defensa y la seguridad y se hace un análisis de la evolución de este problema creciente en el mundo conectado actual. Se describen las principales amenazas actuales de forma general proporcionando una visión general de los riesgos de las redes. El autor cierra el documento describiendo la aproximación institucional que ha adoptado España para proporcionar a sus ciudadanos, organismos y empresas un entorno de red que satisfaga las nuevas necesidades de conectividad.

Los Estados no son ajenos a los riesgos y posibilidades que proporciona el nuevo modelo de relación a través de las redes. El ciberespacio se ha convertido en un nuevo ámbito de confrontación en el que, como indica Enrique Cubeiro, los Estados persiguen objetivos muy diversos. En el documento se plantean preguntas sencillas de hacer y que todos deberíamos plantearnos al abordar una cuestión: por qué, para qué, cómo y quién; y en las respuestas a estas preguntas se van desgranando las complejidades de un espacio

caracterizado por la posibilidad de actuar de forma anónima y la dificultad de atribuir las acciones llevadas a cabo a su autor real.

El coronel José Luis Pontijas profundiza en la cuestión del anonimato y la dificultad de atribución describiendo las acciones por delegación, un fenómeno que se da en todos los ámbitos pero que cobra especial relevancia en el ciberespacio. El Estado que desea llevar a cabo una acción puede recurrir a organizaciones externas para desarrollar sus acciones escalando un peldaño en la complejidad de los conflictos al incluir actores tanto del ámbito público como privado.

La disuasión es una herramienta utilizada a lo largo de la historia tanto para prevenir como para limitar la escalada de los conflictos. En el ciberespacio es complicado establecer e implementar medidas de disuasión debido a la dificultad para ponerlas en práctica. Gabriel Sánchez-Román presenta las APT, amenazas persistentes avanzadas, como las herramientas de disuasión en el ciberespacio. Se trata de complejas herramientas que los actores pueden desplegar para tomar el control de una red, robar información o inutilizar los sistemas telemáticos de un gobierno, organismo o empresa mediante tecnologías punteras que explotan las vulnerabilidades conocidas y no conocidas de los sistemas. El autor hace un interesante paralelismo sobre la función disuasoria que suponen estas herramientas frente a la que se consiguió mediante el uso de los submarinos en las grandes guerras.

El ciberespacio es un espacio relevante en términos geopolíticos y los actores que, tras conseguir su presencia en ese espacio, pueden utilizarlo para ganar relevancia internacional. Águeda Parra describe en su documento cómo China está llevando a cabo acciones para reforzarse en su posición de actor global extendiendo sus capacidades tecnológicas para el mercado nacional con el objetivo de perseguir el liderazgo del ecosistema tecnológico mundial. Proporciona datos muy interesantes sobre la relevancia del ecosistema digital en el contexto mundial y analiza las medidas que China está llevando a cabo para ganar relevancia en este área utilizando sus principales empresas nacionales como caballos de batalla.

El complejo escenario que supone el ciberespacio requiere aproximaciones que permitan un análisis estructurado de su naturaleza. El documento de Francisco Marín se centra en las acciones de desinformación y decepción y, para ello, presenta un análisis previo que segmenta el ciberespacio en capas para acotar las áreas de estudio dentro de este amplio concepto. Esta segmentación proporciona una imagen algo más clara sobre las difusas fronteras que caracterizan este ámbito y redunda en los criterios que se han utilizado para la selección de los documentos que figuran en esta obra.

No se puede olvidar el aspecto normativo que a toda velocidad intenta seguir el ritmo de evolución del ciberespacio para establecer unas normas mínimas que permitan su uso seguro por todas las partes. Margarita Robles trata las medidas poco convencionales que está adoptando la Unión Europea para hacer frente a medidas maliciosas en el ciberespacio. El documento constituye una puesta al día de la legislación de la UE sobre el ciberespacio, analiza el modelo sancionador implantado y hace un análisis jurídico de las medidas implantadas en el contexto de los principios y políticas que rigen el funcionamiento de la Unión Europea.

La relevancia de las redes sociales en todos los ámbitos de la sociedad no deja de crecer tanto por la rápida adopción por la población como por el impacto que tienen como herramientas de información y desinformación que pueden afectar incluso a la seguridad de los Estados. Son varios los artículos que se han incluido en esta obra sobre las redes sociales que proporcionan visiones desde puntos de vista complementarios sobre este fenómeno social. La presencia de varios artículos en esta línea refleja a su vez su importancia y los múltiples enfoques que deben aplicarse para poder comprender con mayor profundidad su naturaleza y capacidades.

El ciberespacio está siendo usado de manera efectiva por las organizaciones terroristas como se refleja en el completo documento que Sandra López, Gorane Mendieta y Jacobo Miró han elaborado. Se trata de un análisis profundo desde la perspectiva de la comunicación donde se identifican las estrategias comunicativas utilizadas, mostrando un trabajo elaborado más allá de iniciativas individuales. Hacen un análisis sociocultural de la sociedad española para identificar cómo las labores que están llevando estas

organizaciones pueden impactar sobre esta sociedad y analizan la presencia de diferentes organizaciones así como los mensajes que intentan hacer llegar a la población.

El documento de Sara Herrero trata hasta qué punto los grupos terroristas también se han visto influenciados por la digitalización hasta el punto de que incluso sus estructuras se han visto modificadas. Se presentan las aproximaciones con las que Al Qaeda y Estado Islámico han afrontado el uso del ciberespacio sacando a relucir las diferencias entre estos dos grupos terroristas.

Sobre el ciberterrorismo, Amanda Pérez presenta en su documento las capacidades del ciberespacio que las organizaciones terroristas pueden utilizar para sus fines y cómo están haciendo uso del ciberespacio con fines de distribución de propaganda, publicación de videos, adoctrinamiento y captación de fieles. Destaca también la prácticamente inexistente actividad ciberterrorista, entendida esta como acciones realizadas a través del ciberespacio con fines terroristas. En todo caso, indica que no existe una definición clara de qué constituye ciberterrorismo y que esta falta de definición conlleva también una dificultad a la hora de asignar medios para luchar contra estas actividades. Asimismo, Luis Miguel Sánchez-Gil plantea en su documento la necesidad de repensar el concepto de ciberterrorismo para facilitar la implementación de medidas contra aquellas actividades que, si bien no constituyen un ataque terrorista, ciberterrorista en este caso, son actividades que sirven a los fines que persiguen las organizaciones terroristas.

El psicólogo Raúl Sampedro analiza en su documento los fundamentos del éxito de las redes sociales para llegar a un espectro tan amplio de la población, conseguir la permanencia de los usuarios y alcanzar la capacidad de convertirse en herramientas que, con el uso inconsciente por parte de los usuarios, facilitan las operaciones de desinformación. Plantea líneas de acción para hacer frente a esta amenaza que traspasa las fronteras del ciberespacio y puede dar lugar a riesgos para la seguridad nacional y muestra de qué forma las redes sociales están presentes en los documentos de más alto nivel estratégico y doctrinal.

Desde un punto de vista sociológico, Claudio Feijóo, Juan Miguel Aguado y Ángel Gómez ponen en contraste los regímenes autoritarios y democráticos en el abordaje tecnológico de las crisis y pandemias utilizando la COVID-19 como ejemplo. Llevan a cabo un análisis exhaustivo de la importancia que han tenido las redes sociales en la gestión de la comunicación bajo los distintos modelos y se identifican los factores que han permitido o no desarrollar determinadas acciones en el contexto de las diferentes culturas y regulaciones.

Una vez más se utiliza la COVID-19 como estudio de caso sobre la capacidad que proporcionan las redes sociales para llevar a cabo acciones de desinformación e influencia en un contexto en el que las redes sociales han experimentado un incremento de uso desaforado. Nuria Portero analiza las campañas de desinformación aparecidas en el contexto de la pandemia desde un enfoque europeo y extrae conclusiones sobre las implicaciones sociopolíticas de estas campañas en el contexto internacional.

También centrado en las redes sociales, Jesús Alberto García, expone cómo han resultado ser el medio para pasar de la propaganda persuasiva, con la que la alianza de la Administración estadounidense y los estudios de cine Washington-Hollywood motivó a las sociedades occidentales para ganar las dos guerras mundiales, a la propaganda participativa. Atribuye a la alianza entre Estado liberal y Silicon Valley, las grandes corporaciones, el éxito de esta nueva estrategia que, si bien exitosa, no está exenta de un alto precio al requerir la cesión de nuestra intimidad. La frontera entre el liberalismo y el autoritarismo cuando se dispone de esta información tan útil para unos como controvertida para otros se construye a partir de la moralidad con la que se trata la información.

Continuando con la línea de la protección de datos, Lorenzo Cotino hace saltar las alarmas sobre el riesgo de vigilancia masiva que acompaña a las diferentes herramientas que se plantean para luchar contra la COVID-19. Aplicaciones, geolocalización masiva y pasaportes biológicos pueden proporcionar información muy sensible que, utilizada de forma inapropiada puede suponer un riesgo para la seguridad. Describe cómo la solución

de la iniciativa europea a la que España se sumó fue diseñada para evitar las tentaciones de acumular datos, usarlos con fines distintos y evitar el control de la población.

Fernando Ruiz alerta en su documento sobre los riesgos de la identificación biométrica y cómo el robo de esta información puede suponer un problema. Presenta la ciberbioseguridad como una cuestión de seguridad nacional y analiza las vulnerabilidades que motivan la existencia de este riesgo. Presenta diversos escenarios donde la falta de seguridad biológica puede suponer un riesgo para la población y cómo estas tecnologías se pueden utilizar con fines más allá de la biología, como puede ser el almacenamiento de información o el cifrado utilizando moléculas de ADN. Plantea la necesidad de que las fuerzas y cuerpos de seguridad adquieran conciencia sobre estos riesgos y que se desarrollen las medidas jurídicas ante un reto que, en un futuro próximo, pudiera afectar a la sociedad.

El ciberespacio es un ámbito sustentado por la tecnología y la propia tecnología constituye uno de los aspectos más importantes a analizar. Además de cuestiones puramente científicas y tecnológicas, el desarrollo de la tecnología que da soporte al ciberespacio también se está viendo afectada por decisiones estratégicas y geopolíticas. Se están produciendo carreras tecnológicas porque son muchas las voces que atribuyen el poder al dominio tecnológico. Los documentos que siguen profundizando en estas cuestiones analizando la tecnología 5G que proporcionará la comunicación inalámbrica de gran parte del ciberespacio; y la inteligencia artificial que proporcionará capacidades difíciles de conseguir por otros medios.

Actualmente se encuentra en proceso de implantación la tecnología 5G, cuyas características van a posibilitar un amplio abanico de nuevas aplicaciones y usos de los sistemas interconectados. Las principales diferencias que introduce son la reducción de la latencia de las comunicaciones, el mayor ancho de banda y la flexibilidad para gestionar mayor número de usuarios con perfiles más distintos en términos de volumen y velocidad de datos. Se está planteando una revolución total basada en las prestaciones de esta tecnología que ha trascendido los términos económicos y de mercado y ha alcanzado la política y la geopolítica. David Corral hace un exhaustivo análisis de la

tecnología y de las implicaciones geopolíticas que se han producido a su alrededor en su documento.

De este mismo autor se ha incluido el documento sobre inteligencia artificial en el que se realiza un análisis del estado del arte y de las aproximaciones que las principales potencias están haciendo para su desarrollo y su implantación. Se trata de una tecnología que presenta numerosas virtudes y ventajas potenciales, pero que no está exenta de riesgos, especialmente cuando se tratan cuestiones éticas y morales como la eliminación del ser humano del proceso de decisión.

Finaliza este volumen el documento de Carlos Frías en el que se analiza el campo de batalla futuro donde las tecnologías van a tener un impacto fundamental. Muchas de estas tecnologías se apoyarán en un uso intensivo del ciberespacio, motivo por el cual se ha incluido en esta recopilación. Disponer de capacidades para estar en el ciberespacio, incluso en episodios de confrontamiento, resultará fundamental para que los sistemas funcionen y proporcionen la superioridad necesaria para hacer frente de forma efectiva al conflicto.

Por último, aunque no se incluye en esta compilación, cabe también mencionar una publicación realizada por el IEEE cuyo contenido, aunque publicado con anterioridad, sigue siendo de plena actualidad. El Cuaderno de Estrategia 185 "Ciberseguridad: la cooperación público-privada" fue elaborado con la colaboración de autores de los principales organismos públicos de ciberseguridad españoles así como representantes del ámbito académico y de la empresa privada[1].

[1] Disponible en: http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2017/Cuaderno_185.html