Ángel Gómez de Ágreda
Coronel del Ejército del Aire

E-mail: agomde@ea.mde.es

RESEÑA

EL QUINTO ELEMENTO

Autor: Alejandro Suárez Sánchez-Ocaña. Editorial Deusto, Grupo Planeta. Primera edición. Octubre de 2015. ISBN: 978-84-234-2178-7. 267 páginas.

«El quinto elemento», de Alejandro Suárez Sánchez-Ocaña es un relato sobre espionaje, guerra y terrorismo desde la perspectiva de la utilización de las nuevas tecnologías digitales y de sus consecuencias. Escrito en un estilo ágil y desenfadado, Suárez va hilando un ejemplo tras otro de agresiones cibernéticas para ilustrar los riesgos y amenazas que introduce el ciberespacio en la sociedad del siglo xxi.

Correcto en la mayor parte de las apreciaciones y los datos que aporta, Alejandro Suárez consigue despertar la conciencia del lector respecto de las vulnerabilidades del mundo digital y, acertadamente, incluye una sección en la que se apuntan factores de mitigación de las mismas. Publicado en el año 2015, el libro relata ataques que ya se han convertido en clásicos en un mundo en vertiginosa evolución. Si bien sus conclusiones siguen siendo válidas, el año y medio transcurrido desde su primera edición hace que queden fuera, irremediablemente, numerosos y muy significativos acontecimientos.

El texto parte de las filtraciones de material del Departamento de Defensa de Estados Unidos que publicó *Wikileaks* en 2010. Un modelo que —aunque, evidentemente, no se recoge en el libro— vuelve a estar de actualidad a raíz de la utilización de este mismo medio para la difusión de documentos durante la reciente campaña presidencial norteamericana.

Los cuatro siguientes capítulos se dedican al espionaje económico e industrial, el crimen, el terrorismo y la guerra, siempre en el entorno *ciber*. Finalmente, Suárez ofrece algunas medidas de protección frente a las agresiones en el ciberespacio y dedica un último capítulo a un intento de prospectiva.

Más allá de su estilo, en ocasiones apocalíptico, arrogante y mesiánico[1], se trata de una lectura que permite acercarse cómodamente a los rudimentos de lo que significa «El quinto elemento», el quinto entorno, tras la tierra, el mar, el espacio aéreo y el espacio exterior.

Así, como un quinto ámbito del teatro de operaciones, ha sido también definido por la Alianza Atlántica y, de forma pionera, por España. En este sentido, cabe recordar que, aunque no se recoja en la obra, el Ministerio de Defensa español fue de los primeros en considerar al ciberespacial como un Mando Componente diferenciado de los tradicionales. La creación del Mando Conjunto de Ciberdefensa, de forma casi simultánea a la publicación de la Estrategia de Ciberseguridad Nacional en 2013, vino a dar carta de naturaleza y aplicación práctica a esta visión doctrinal.

A pesar de todo el reconocimiento de la importancia del entorno digital por parte de España y de la práctica totalidad de los países y organizaciones internacionales, sí podemos estar de acuerdo con el autor en la relativa inconsciencia existente en relación con el alcance real de los cambios que introduce internet y el conjunto del ciberespacio.

1 Como cuando afirma en la dedicatoria «a todos los miembros de las fuerzas y cuerpos de seguridad del Estado, que apenas intuyen los duros años que se les vienen encima».

Como demuestran los acontecimientos que se relatan en las 267 páginas del libro y, de forma incluso más reveladora, los últimos sucesos y su reiteración casi diaria, el ciberespacio resulta algo más que un entorno diferenciado respecto de los espacios físicos, se trata de un ámbito trasversal a todos ellos y con un carácter más habilitante que complementario a los mismos. Se hace preciso abandonar la visión de las tecnologías digitales y de las comunicaciones como un servicio de apoyo para la consecución de los fines a alcanzar por los actores físicos y empezar a considerarlas como un prerrequisito para la explotación de las capacidades físicas y lógicas.

En una sociedad posindustrial que evoluciona hacia un «coste marginal cero»[2], el verdadero valor añadido está en la innovación, en las ideas y en los conceptos. La protección de la propiedad intelectual, los planes y proyectos, y la preservación de la privacidad se convierten en valores fundamentales tanto para las personas como para las instituciones. Ambos —entes privados y públicos— ven cómo son objeto de atención y de ataques desde todo el espectro de actores estatales, empresariales, criminales o particulares. La transversalidad se traduce también en simetría de capacidades.

En la era global, todos atacan y son atacados por todos. El orden westfaliano que atribuía a los Estados el monopolio en el uso de la fuerza se desmorona por momentos. Así, criminales o individuos aislados convierten a poderosas naciones en sus blancos, Estados Unidos reacciona contra el ataque a la empresa Sony —atribuido en su momento a Corea del Norte— como si fuera una empresa nacional, el Estado Islámico proporciona servicios administrativos on-line o, incluso, grupos tan desestructurados como puede ser *Anonymous* declaran abiertamente la guerra a Israel o Canadá.

El robo de los planos del avión F-35, diseñado por Lockheed Martin, dio lugar a la fabricación de dos modelos de aeronaves de quinta generación en China tras un inmenso y repentino salto cualitativo en su industria de defensa nacional en lo que los americanos, en un alarde de sentido del humor, han catalogado como «la mayor transferencia de propiedad intelectual de la Historia». Contra lo que podría pensarse, el trasvase de conocimientos entre actores estatales y privados no se limita a países con economías dirigidas, según nos señala el autor en alguno de los ejemplos. Transferencias y externalizaciones similares también tienen lugar entre terroristas y criminales.

De hecho, señala Alejandro Suárez, las grandes multinacionales del sector no surgen simplemente amparadas por la excelencia de sus productos, sino también por la utilidad que estos tienen para los servicios de inteligencia de sus países, con los que compartirían aquellos datos que les sean requeridos. El caso judicial del FBI contra Apple, que tuvo lugar dos meses después de la publicación del libro, podría parecer desmentir esta vinculación entre los Estados y las corporaciones. Conviene recordar que el *bureau* solicitó de una juez californiana una orden para que la compañía que lideró Steve Jobs desbloquease el acceso a un teléfono perteneciente a uno de los terroristas

2 RIFKIN, Jeremy, «La sociedad de coste marginal cero», Espasa Libros, septiembre de 2014. ISBN 978-84-493-3051-3.

del atentado de San Bernardino. La negativa de Apple —basada en la cerrada defensa de la privacidad de sus clientes— pudo sostenerse con la supuesta colaboración de un tercero en el descifrado del aparato. Más allá del carácter comercial y propagandístico que la defensa de la privacidad tenía para la compañía de la manzana, el caso ilustra la contraposición entre dos modelos de seguridad: el público estatal, representado por el FBI, y el privado, que dejaría en manos de las multinacionales la responsabilidad de proporcionar este servicio a sus clientes.

En fecha tan reciente como 1982 se forzaba la ruptura de la compañía telefónica Bell —que ostentaba el monopolio de estas comunicaciones en Estados Unidos y Canadá— en defensa de la libre competencia y la libertad de elección en el mercado. Apenas unos años después, no ya a nivel nacional, sino global, se permitió y promovió, sin embargo, la creación de grandes monopolios digitales en un movimiento que no deja de ser llamativo. Evidentemente, las consideraciones económicas pesarían en el cambio de modelo, pero es más que probable que el acceso universal a datos de miles de millones de «abonados» también jugara su papel en la decisión.

El libro no entra de lleno a analizar el modo en el que la hiperconectividad está afectando a nuestra forma de vivir. Ubicuidad e inmediatez son requisitos inexcusables en el siglo XXI. *I want it all, and I want it now* rezaba el estribillo del tema de Queen hace ahora 18 años. Ese estribillo se ha convertido en el modo de entender la vida de la generación que estaba naciendo en aquellos momentos. El acceso universal e instantáneo a cualquier contenido ha llegado a plantearse como un derecho humano mientras que la cultura del esfuerzo, de la planificación, de la paciencia y la ilusión mantenida se ha ido quedando atrás.

Esa misma ubicuidad que amplía los horizontes en los que nos movemos a diario relativiza también el valor de la proximidad. El ser humano contemporáneo tiene la capacidad aparente de individualizar su vida más que en ningún otro momento de la historia. Puede generar tantos grupos, tantas pandillas, como desee para atender cada uno de los aspectos de su vida, pero al mismo tiempo, cada uno de esos grupos le encierra cada vez más en la reafirmación de sus creencias con un pensamiento acrítico que no busca más que obtener el aplauso y el «me gusta» de tantos internautas como sea posible.

Las últimas páginas de «El quinto elemento» nos acercan a un futuro distópico con tintes orwellianos. 2017 parece aproximarse velozmente a 1984, con la diferencia de que lo que en la novela de Orwell venía impuesto por un Estado tiránico está siendo incorporado a nuestras vidas a nuestras propias expensas. El libro ofrece numerosos ejemplos de monitorización de las comunicaciones y los datos —especialmente, la geolocalización, pero también el reconocimiento facial o los hábitos de consumo— que se basan en tecnologías que adquirimos, habilitamos y utilizamos voluntariamente todos los días.

No solo nuestra forma de ser se está viendo afectada por las tecnologías digitales, el ciberespacio también se ha convertido en un escenario preferido para las relaciones sociales. La forma en que estas se desarrollan difiere sustantivamente de las tradicionales.

El hombre sigue siendo el centro de gravedad de las relaciones sociales y políticas, pero el papel que juega en ellas es fundamentalmente distinto. La incorporación al ciberespacio de miles de millones de objetos conectados, lo que se ha dado en llamar el *internet de las cosas*, incrementará exponencialmente el control centralizado de nuestras decisiones —o, al menos, la influencia sobre ellas— a quién controle los contenidos digitales.

En este escenario, las ciudades se vuelven nodos inteligentes de población. Lo rural prácticamente desaparece de la imagen del futuro si no se mantiene conectado. Todo está regulado por algoritmos que optimizan las opciones disponibles. Todavía embrionarios en el momento de publicarse el libro, los coches autónomos se empiezan a imponer en los últimos meses como una alternativa clara a medio plazo. Sus decisiones también estarán guiadas por la mejor opción para los transeúntes, incluso si supone una alternativa subóptima para el pasajero. ¿Será necesario redefinir las leyes de la robótica de Asimov?

Los capítulos centrales del libro se entretienen en ilustrar al lector sobre múltiples ejemplos de criminalidad, terrorismo y guerra en el ámbito cibernético. Los tres aspectos, sin embargo, están íntimamente vinculados entre sí y, en numerosas ocasiones, hay que acudir a la interpretación de la intención del autor para calificar una acción de un modo u otro.

En un entorno tecnológico como el ciberespacio, la capacidad para perpetrar una agresión se basa, en buena medida, en el conocimiento técnico de las herramientas. Los individuos con capacidad para *hackear* un sistema podrán después explotar personalmente sus habilidades para la obtención de beneficios directos o convertirse en proveedores cualificados de servicios para criminales, terroristas o agentes estatales.

Alejandro Suárez describe en el libro algunas de las posibilidades que ofrece la *internet profunda*, la *Deep web*, en la que se alojan desde códigos de virus y otro *malware* hasta servicios de mercenarios cibernéticos que, por un módico precio, proporcionan acceso a las páginas o los correos de rivales, adversarios o enemigos.

«El quinto elemento» es un relato actual, trata temas candentes que afectan a la Seguridad Nacional y a la seguridad de cada uno de nosotros. Sin entrar en tecnicismos, transmite la necesidad de adoptar medidas ante las vulnerabilidades de nuestro mundo digital. Quizás uno de los elementos más interesantes sea ver cómo, tras solo un año y medio después de su publicación, no solo han evolucionado tremendamente las técnicas descritas en el libro, sino incluso el grado de penetración y la gravedad de sus efectos en la sociedad.

Artículo recibido: 18 de enero de 2017.
Artículo aceptado: 15 de febrero de 2017.