

## Nota de actualidad: Síntesis de la I Jornada sobre “Prospectiva Tecnológica en Seguridad” ISDEFE

*En este documento se presenta un resumen de las ideas expuestas en la I Jornada sobre «Prospectiva Tecnológica en Seguridad», celebrada en la sede de ISDEFE el pasado 20 de junio de 2017\*.*

### Contenidos

El primer panel de esta Jornada, relativo a la prospectiva tecnológica, corrió a cargo de Almudena Agüero, de la Secretaría de Estado de Investigación, Desarrollo e Innovación, perteneciente al Ministerio de Economía, Industria y Competitividad. La ponente comenzó su intervención explicando que, en la actualidad, los gobiernos se deben enfrentar a una amplia gama de problemas complejos e interdependientes, tales como el cambio climático, el envejecimiento de la población o la cuestión de la seguridad energética, y que la ciencia puede aportar soluciones u opciones de actuación respecto a esos problemas.

A continuación, presentó al público la existencia del Joint Research Centre (Centro Conjunto de Investigación), una institución dependiente de la Comisión Europea y que se dedica a utilizar la ciencia para, por ejemplo, diseñar políticas anticipatorias o hacer enmiendas a propuestas del Consejo o del Parlamento. El JRC también colabora con otras organizaciones de investigación y desarrolla sus actividades en torno a diez áreas, entre las que se encuentran la economía, la seguridad civil, la educación o la transformación digital. Por otro lado, existen diversos acuerdos de colaboración entre el JRC y el Gobierno de España.

Almudena Agüero también mencionó algunas de las prioridades de la Comisión Europea, incluyendo la ciberseguridad, las tendencias actuales en movimientos migratorios y el estudio del espacio. Concluyó su ponencia mostrando el portal de comunicaciones del JRC, donde los usuarios pueden encontrar información y documentación sobre los proyectos y áreas estratégicas de esta institución.

En el segundo panel de la Jornada, titulado «Cartografía de tecnologías», varios ponentes analizaron el papel de las nuevas tecnologías en cuestiones actuales de seguridad. El primero de ellos, José María Blanco, director del Centro de Análisis y Prospectiva de la Guardia Civil, explicó que, en materia de seguridad, la tecnología puede constituir una importante fuente de nuevas amenazas, tales como la comisión de delitos en diversos ámbitos o la propagación de informaciones falsas. Por este motivo, es necesario estudiar las tecnologías existentes en la actualidad y determinar cuáles pueden ser una amenaza, cuáles pueden ser una oportunidad y cuál es el estado de la cuestión en el momento presente. Por último, planteó la cuestión de si realmente se está midiendo el impacto de las nuevas tecnologías en nuestras vidas.

---

\* Analistas y becarias del CAP

\* Ver información en: <http://iuisi.es/?p=551>

Posteriormente, Enrique Ávila, jefe de Seguridad de Información de la Jefatura de Servicios Técnicos de la Guardia Civil, incidió en la necesidad de recuperar el pensamiento profundo para crear nuevas formas de entender el mundo y para compensar el creciente papel que ya tiene la tecnología en nuestra vida diaria. Explicó, además, que uno de los principales problemas a los que se enfrenta nuestra sociedad es la falta de formación necesaria para evitar y controlar ataques cibernéticos.

Por su parte, Igor de la Casa, comandante de la Jefatura Fiscal y de Fronteras de la Guardia Civil, enumeró las amenazas a las que debe hacer frente España debido a su posición geográfica como frontera sur de la Unión Europea, incluyendo el tráfico de drogas, el tráfico de seres humanos, la inmigración irregular o el terrorismo. La Guardia Civil comenzó a estudiar los posibles usos de la tecnología para combatir esas amenazas en el año 1997 y ha participado desde entonces en numerosos proyectos de investigación y cooperación sobre temas de vigilancia litoral y de fronteras.

A continuación, Raquel Pastor, consultora principal en Tecnologías de Vigilancia de ISDEFE, habló sobre la inteligencia de fuentes abiertas y explicó que gracias a Internet disponemos de demasiada información para hacer este tipo de inteligencia, lo cual puede suponer un problema. No obstante, la inteligencia de fuentes abiertas mejora considerablemente la capacidad de decisión y actuación de las fuerzas policiales y está presente en todas las esferas de la Unión Europea. Por último, presentó algunos de los proyectos de colaboración europeos sobre inteligencia de fuentes abiertas en los que ha participado ISDEFE en los últimos años.

Más tarde, Ana Ortega, consultora senior en Tecnologías de Vigilancia de ISDEFE, puso de manifiesto que las amenazas a las que se enfrentan las sociedades actuales son muy cambiantes y, por lo general, avanzan más rápido que las tecnologías que se encuentran a disposición de los Estados. En este sentido, el usuario final de la tecnología se considera el motor de la innovación y su presencia es necesaria en todas las fases del desarrollo tecnológico.

Por último, Juan Carlos Iravedra, jefe del Área de Tecnologías de Vigilancia para la Seguridad Pública de ISDEFE, comenzó su intervención defendiendo la necesidad de conocer el pasado para poder crear posibles escenarios de futuro y tomar decisiones conforme a ellos. También explicó que la tecnología siempre ha sido un factor disruptivo a lo largo de la Historia y que el futuro estará condicionado por el *big data*, el Internet de las cosas y la inteligencia artificial. Por último, afirmó que la condición clave para mantener la seguridad de una sociedad es el estudio y desarrollo de sistemas de alerta temprana para poder adelantarnos a los acontecimientos.

El tercer y último panel recogido bajo el título «Experiencia y buenas prácticas», comenzó con la ponencia de Rosalía Machín, teniente del Servicio de Innovación de la Guardia Civil, creado entre los años 2012-2014 y dependiente de la Jefatura de Servicios Técnicos de la Guardia Civil. La intervención empezó con la presentación del objetivo de este Servicio que consiste en prestar apoyo y soporte de gestión, administración y técnica a diferentes unidades y servir como nexo de unión entre ISDEFE, las administraciones públicas y las unidades de especialidades de la Guardia Civil. Destacando la importancia de la investigación en innovación y la especialización en diferentes áreas (como por ejemplo en el desarrollo financiero, el desarrollo propio de aspectos ético-legales, la lucha contra el crimen organizado, la protección de fronteras, la compra pública innovadora, etc.), para conseguir una lucha más efectiva de presentes y futuras amenazas en la seguridad.

Además Rosalía señaló diferentes proyectos de investigación y cooperación en los que participan con entidades tanto nacionales como internacionales para el impulso de I+D+i en la Guardia Civil y, por ende, en el Ministerio del Interior para un mejor posicionamiento.

El cierre del panel fue a cargo de Daniel Mosquera, jefe de Área de I+D+i de ISDEFE, el cual destacó la apuesta de ISDEFE por el compromiso en la investigación, innovación y la optimización del I+D+i en seguridad, con el objetivo de desarrollar productos y servicios innovadores que ofrecen soluciones a las necesidades de sus clientes con el fin último de que las sociedades sean más seguras. Asimismo subrayó la participación y colaboración de ISDEFE en diferentes proyectos europeos para dar apoyo y crear una red de expertos al servicio, principalmente, de los Ministerios de Defensa e Interior.

## Conclusiones

En julio de 2004 el ejército norteamericano publicaba un documento titulado "Assessment of the Think Like a Commander Training Program", en el que se destacaba que "el éxito en operaciones futuras dependerá de las capacidades de líderes y soldados de pensar creativamente, decidir con prontitud, aprovechar la tecnología disponible, adaptarse con facilidad y actuar en equipo".

## Decálogo sobre tecnología y seguridad (CAP de la Guardia Civil):

1. La tecnología es una clave del futuro de nuestras sociedades, contribuyendo al desarrollo y la sostenibilidad. Sin perjuicio de ello es evidente la utilización perversa de la misma por terroristas y criminales, o su combinación con procesos de ingeniería financiera para la comisión de delitos financieros y corrupción. Presenta amenazas para la seguridad de los estados, pero a su vez, genera nuevas oportunidades.
2. La tecnología es un medio, no es el fin. Hay que evitar un exceso de "tecnocentrismo", definido por Eugeny Morozov y otros autores como aquella situación en que se busca una solución tecnológica para cada problema, incluso para los que no son tal.
3. El factor humano, con sus pros y contras, sigue y deberá seguir siendo central en el campo de la seguridad. La tecnología es un apoyo, sin perjuicio del recurso a desarrollos, como es el caso de Blockchain, que ofrecen multitud de oportunidades a través de sistemas descentralizados que no precisan la intervención humana (útiles, por ejemplo, para la lucha contra el blanqueo de capitales, o para asegurar la transparencia de las Administraciones Públicas).
4. La tecnología cambia al ser humano. Afecta a sus formas de comunicación pero, de la misma manera, al cerebro. Hace que posiblemente se pierdan capacidades (como el denominado efecto Google, que evita memorizar tanta información como en década anteriores), que la información sea más superficial, como señala Nicholas Carr (en una sociedad actual de titulares e imagen), pero también puede permitir que sea más sencillo conectar informaciones diversas. La plasticidad del cerebro asegura los precisos procesos adaptativos.
5. Se debe prestar atención a la "desigualdad tecnológica", menos tratada que la social o la económica. Se producen brechas generacionales en el uso de las tecnologías, además de desigualdad entre quienes proveen los datos (ciudadanos) y quienes sacan partido de los mismos.
6. El desarrollo tecnológico avanza a tal velocidad que juristas y expertos en ética tendrán que mantener un elevado grado de alerta. Se deberá reducir la brecha temporal entre el momento en que

una tecnología está disponible, y puede generar dobles usos no deseados, y la respuesta normativa precisa para que no afecte a los derechos y libertades.

7. Los tiempos actuales exigen nuevo pensamiento para nuevas formas de hacer. No se puede gestionar el futuro con hábitos del pasado. Ello exige una formación, nuevas habilidades, nuevo "saber hacer". Para construir el futuro, no adaptándose sino creando nuevas reglas de juego, es preciso invertir en creatividad y en pensamiento crítico.

8. La tecnología no es magia, ni tiene todas las soluciones. El ciclo de vida de la innovación tecnológica suele ser corto, hasta que nuevos proveedores acceden a la misma. Ello puede generar que el coste de una tecnología incipiente sea muy elevado, pero que su madurez no sea aún la precisa. Una situación que a su vez puede llevar a la parálisis tecnológica, ante las dificultades de los clientes para optar por una solución. Desde este punto de vista la prospectiva tecnológica no es un opción, es una obligación para toda organización que pretenda liderar un sector.

9. Nuestro mundo debe volver a poner el foco en las personas y las estructuras sociales. Existe una urgente necesidad de un nuevo humanismo, ante una sociedad que dota de características humanas a los objetos (son inteligentes los móviles, las ciudades, los contratos, o se insiste en la inteligencia artificial, pero poco se trata sobre la inteligencia humana, con el riesgo de que una mayor inteligencia de las cosas lleve a una mayor imbecilidad del ser humano), incluso de sentimientos (son los mercados quienes "sufren" o se sienten "nerviosos"), mientras que las personas se convierten en números (número de desempleados, número de asesinados en atentados, número de desahuciados, número de desplazados, etc.). Riesgos como la "singularidad" se asoman a nuestro futuro, o sus formas más light como la cesión de decisiones en máquinas. El riesgo es perder la naturalidad de la vida humana, la belleza del caos de nuestro devenir por este mundo. Por tanto, es preciso realizar un llamamiento a la SERENDIPIA, y a su provocación, aquellas circunstancias no buscadas pero que nos cambian la vida.

10. Siguiendo la anterior argumentación, y en base a los principios de Peter Senge en "La Quinta Disciplina", la tecnología debe ayudar a que las personas y las organizaciones sean cada vez más inteligentes, característica que Senge atribuye a "quienes aprenden". Porque la ciencia, el conocimiento, la innovación y la inteligencia, especialmente como resultado de una acción colectiva, son el futuro de nuestras sociedades, de unas sociedades más justas y más libres.

#### **Bibliografía recomendada en Biblioteca del Centro de Análisis y Prospectiva y Academia de Oficiales de la Guardia Civil:**

- <http://gccap.bage.es/cgi-bin/koha/opac-shelves.pl?op=view&shelfnumber=89&sortfield=title>