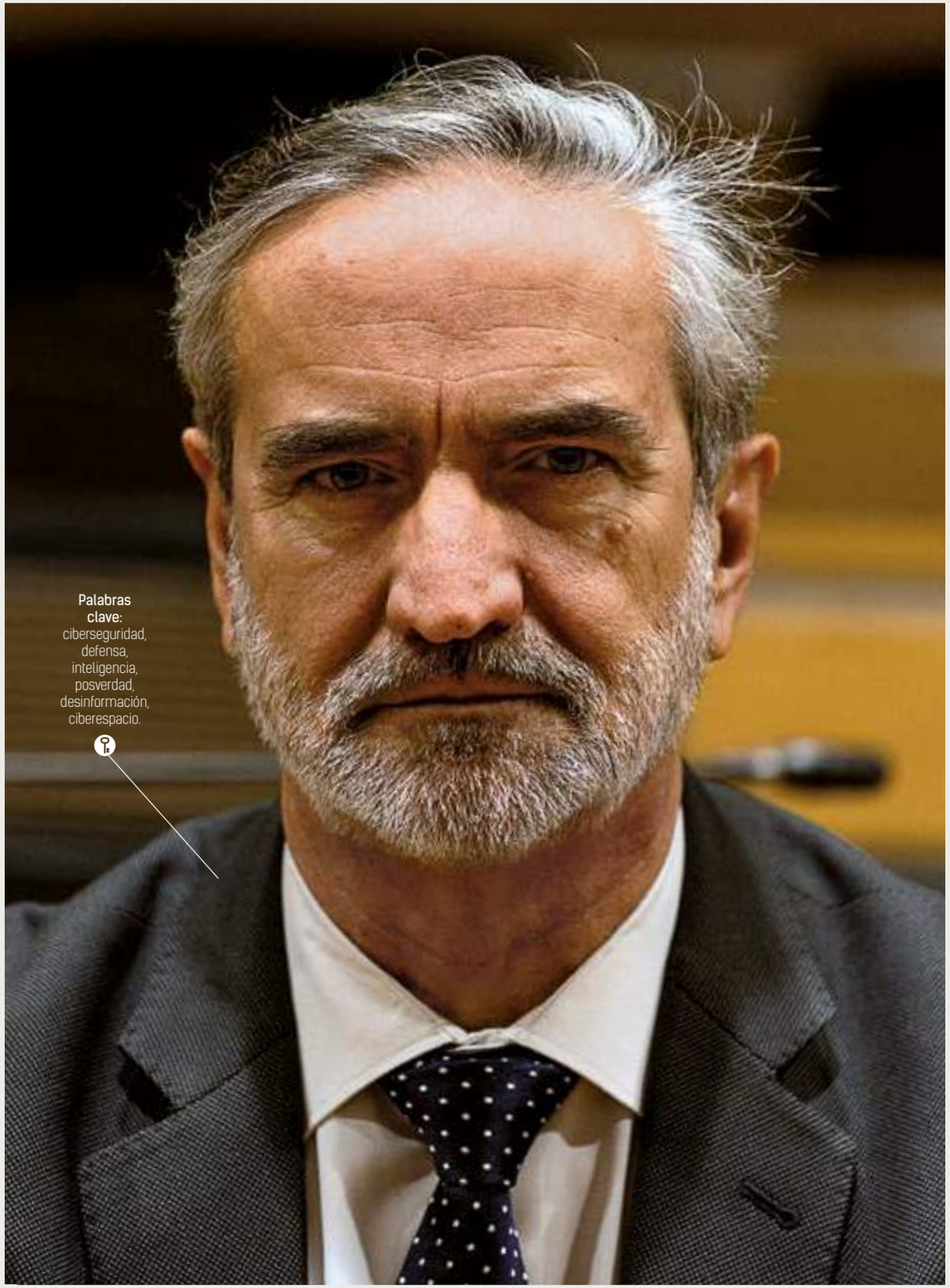


Palabras clave: ciberseguridad, defensa, inteligencia, posverdad, desinformación, ciberespacio.

“LOS CIBERATAQUES SON PARTE DE LA GUERRA **HÍBRIDA** QUE PERSIGUE CAUSAR INESTABILIDAD Y DESCONFIANZA”

Luis Jiménez Muñoz

MÁXIMA AUTORIDAD EN MATERIA DE CIBERSEGURIDAD NACIONAL

El teniente coronel es subdirector general del Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia (CNI) que se encarga de coordinar e implementar la Estrategia de Ciberseguridad Nacional. “La capacidad de los Estados para hacer frente a los retos de ciberseguridad es un elemento estratégico de primer orden, tanto para protegerse como para progresar en el complejo panorama geopolítico actual”, sostiene este experto en tácticas de guerra digital.

UNA CONVERSACIÓN CON **JUAN M. ZAFRA** FOTOS: **ENRIQUE TORRALBO**

Top national cibersecurity authority
“CYBERATTACKS ARE PART OF HYBRID WARFARE THAT AIMS TO CAUSE INSTABILITY AND MISTRUST”

The lieutenant colonel Luis Jiménez is deputy general manager at the National Cryptologic Center (CCN), a body attached to the National Intelligence Center (CNI) that is responsible for coordinating and implementing the National Cybersecurity Strategy. “The ability of states to meet cybersecurity challenges is a strategic element of the first order, both to protect themselves and to make progress in today’s complex geopolitical landscape,” maintains this expert in digital warfare tactics..

Keywords: *cybersecurity, defense, intelligence, post-truth, disinformation, cyberspace.*

Luis Jiménez es teniente coronel "en situación de servicios especiales", según consta en su currículum profesional. Su cometido, sin embargo, se ha convertido en los últimos tiempos en algo cotidiano, aunque, eso sí, en el desempeño de su tarea se detectan cada día más situaciones muy especiales, complejas y de alto riesgo. "Mi peor pesadilla es el ciberespionaje sofisticado que determinados Estados tienen capacidad de realizar. Esos son los incidentes más complejos a los que nos enfrentamos, los que más recursos nos exigen y que ponen de manifiesto un conflicto entre países ante el que hay que estar muy alerta", afirma.

Al mando del Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia (CNI), entre sus principales cometidos se encuentran el desarrollo de la Estrategia Nacional de Ciberseguridad, el apoyo a la implementación del Esquema Nacional de Seguridad en el sector público, la mejora de las capacidades de Respuesta ante Incidentes de Seguridad y la mejora de las capacidades de Evaluación y Certificación de la Seguridad de las TIC. En su desempeño confluyen tecnología, ciberseguridad, información y conocimiento, una combinación sobre la que se construyen las economías y las sociedades modernas.

El Centro que usted dirige es responsable de desarrollar e implementar un esquema general de ciberseguridad. En resumen...
Nuestro objetivo se resume en hacer que España tenga un ciberespacio seguro y confiable. A partir de ahí se desarrollan unas líneas de acción que son, básicamente, de concienciación, de capacitación de los ciudadanos, de las empresas y de las fuerzas de seguridad, y de despliegue de herramientas de ciberseguridad.

Es usted el guardián del nuevo espacio digital en el que habitamos. ¿Quiénes formamos parte de ese ciberespacio?
Todos. Ciudadanos, Administraciones públicas y empresas. El ciberespacio es donde tenemos ya nuestra vida pública y privada. Nuestros negocios, nuestro teléfono móvil, nuestro ordenador y hasta el televisor; nuestras aplicaciones corporativas o las que utilizamos a título personal son ya parte del ciberespacio. Ya quedan muy pocas redes aisladas del ciberespacio.

En un número anterior de *TELOS* afirmamos que somos más digitales que físicos o analógicos.
No somos conscientes de que habitamos en el ciberespacio. Necesitamos desarrollar una cultura de ciberespacio y ciberseguridad. Aún no hemos tomado conciencia de la cantidad de información que volcamos en el ciberespacio y de los riesgos que asumimos con ello. Pero estoy convencido de que esta cultura de la ciberseguridad irá calando en la sociedad, de la misma forma que fuimos tomando conciencia de la necesidad de la seguridad vial.

A muy corto plazo tendremos mayor vinculación con la tecnología y más necesidad de preservar nuestra ciberseguridad.
La dependencia de las infraestructuras críticas y de las tecnologías con las que se gestionan va a ser absoluta en la sociedad del 5G y del internet de las cosas. Será necesario fortalecer los sistemas de ciberseguridad. Los ciudadanos van a tener que ser más hábiles, las empresas habrán de formarse y las Administraciones públicas deberán aprender a gestionar riesgos mayores.

¿Se han incrementado los ciberataques con motivo de la guerra en Ucrania?
Ya se venía produciendo un incremento muy significativo de los ciberataques desde hace cinco o seis años y la realidad es que cada vez tenemos ataques más graves y críticos. La guerra de Ucrania ha incrementado principalmente los ataques de denegación de servicio. Al inicio, su objetivo era que las fuerzas armadas ucranianas no pudieran utilizar sus sistemas, sus ordenadores, sus redes de comunicación o manejar sus drones, por ejemplo. Esos ataques se han producido siempre en Europa.

¿Qué persiguen esos ataques?
Intentan limar la confianza de los ciudadanos europeos en sus instituciones y en sus empresas. Atacan a la estabilidad de las democracias y de las economías. Hemos recibido ataques de denegación de servicio a webs del Ministerio de Defensa o de la Presidencia del Gobierno. Desde el punto de vista técnico es fácil responder porque en cuanto lo detectas, en colaboración con las operadoras de telecomunicaciones, tenemos herramientas para reanudar muy rápidamente el servicio en las webs afectadas. Hemos aprendido a defendernos de los ataques de denegación de servicio.

Esos ciberataques forman parte de la cada vez más intensa estrategia de guerra híbrida[1].
Así es. El objetivo de estos ataques es generar una sensación de inseguridad a la ciudadanía. No buscan una compensación económica ni pueden considerarse una acción de guerra, ni siquiera una neutralización de la infraestructura; persiguen causar inestabilidad y desconfianza. De hecho, dentro de las acciones de guerra híbrida se contemplan estos ciberataques, que buscan complementar otras acciones de guerra como la desinformación o los sabotajes.

¿De qué forma estas prácticas combinadas están condicionando su trabajo?
Cada vez con más frecuencia analizamos los ciberataques como acciones complementarias que se enmarcan dentro de un conflicto híbrido y que incluye otras como pueden ser las *fake news* o la manipulación informativa. Esto hace que la estrategia de seguridad sea cada vez más compleja.

¿Cómo abordáis esta guerra híbrida, que combina aspectos técnicos y sociológicos, herramientas tecnológicas y contenidos?
Desde la inteligencia, fundamentalmente. Cuando se estudia y se analiza la amenaza lo más relevante es la trazabilidad El estudio de estas amenazas es una de las misiones fundamentales del Centro Nacional de Inteligencia. Nosotros [CCN y el CNI al que está adscrito] analizamos estas amenazas cuando vienen desde un Estado; no entramos en el análisis de asuntos políticos antropológicos o sociales. No analizamos un meme de actualidad, lo que hacemos es ponerlo en un contexto y analizar si forma parte de un conjunto de ciberamenazas. Cuando detrás de esa amenaza hay un Estado siempre hace saltar las alarmas.

¿Por qué es tan evidente si hay un Estado detrás?
Porque hay indicadores y porque hay analistas de inteligencia que tienen mucha experiencia, información y acceso a fuentes de información que, estableciendo correlaciones y contexto, pueden permitir identificar el origen de la amenaza.

Un titular, un tuit, un GIF, un vídeo de unos segundos puede generar ahora muchísima inestabilidad en la opinión pública. ¿Cómo actuáis en estos casos?
Un tuit con capacidad de desestabilización tiene que pasar de 100.000 o 200.000 personas. Necesitas herramientas que extiendan ese tuit, que ese tuit se haga viral y consiga ese alcance.

"La IA va a exigir un nivel de madurez muy alto a nuestra sociedad"

1 Guerra híbrida es una teoría de la estrategia militar en la que se utilizan toda clase de medios y procedimientos, ya sea la fuerza convencional o cualquier otro medio irregular como la insurgencia, el terrorismo, la migración, los recursos naturales, e incluso otros más sofisticados mediante el empleo de las últimas tecnologías con otros métodos de influencia como las noticias falsas, diplomacia, guerra jurídica e intervención electoral del extranjero y en las que la influencia sobre la población resulta vital.

¿Entonces, sin máquinas no son posible las campañas de desinformación?
Ninguna campaña de desinformación se hace sin organizarla previamente y sin usar máquinas para que sea efectiva. Nuestro objetivo es detectar cómo se ha organizado y qué máquinas se han utilizado. El gran reto es la trazabilidad.

¿Cómo afecta el desarrollo de tecnologías como el *blockchain* en vuestra estrategia de ciberseguridad?
Blockchain permite, básicamente, el anonimato; rompe la trazabilidad de las operaciones. Pero lo cierto es que conforme se ha ido desarrollando y se ha producido una concentración de nodos dedicados al *blockchain*, es más fácil la trazabilidad.

¿Y las inteligencias artificiales?
No sabemos hacia dónde va a evolucionar la inteligencia artificial, hacia el lado bueno o hacia el lado del mal. Una cosa es cierta: va a aumentar muchísimo la capacidad de manipular, de engañar. Ya lo estamos viendo. Con la IA se manipulan imágenes, vídeos, la voz… El desarrollo de la IA va a exigir un nivel de madurez muy alto en la sociedad para poder discernir; va a exigir tener muy presente el contexto. Y eso exige más formación. La inteligencia artificial tiene unas ventajas enormes, pero nos plantea unos retos que aún ni siquiera conocemos.

Ayuda al mal, pero también tiene aspectos muy positivos.
Por supuesto. Uno de los grandes retos que tenemos en ciberseguridad es detectar los ciberataques en tiempo real. La inteligencia artificial nos permite inferir que una serie de evidencias se corresponden con un ciberataque, hacer saltar las alarmas y actuar con anticipación al propio ataque. Los malos también utilizarán la IA para generar patrones indetectables.

¿Vamos a un escenario de batalla entre máquinas que interactúan?
Ha sido así siempre. Detrás de las máquinas hay humanos, pero la tecnología —las máquinas— determinaba siempre el curso de los enfrentamientos.

Con lo que veis en vuestras pantallas, ¿podría hacernos una estimación de hasta qué punto vivimos engañados o amenazados?
Puedo hablar desde una perspectiva personal en este caso. Yo tengo redes sociales. Tengo una vida digital, pero también tengo una vida analógica y puedo discernir la emoción y el sentimiento que se pone en las redes sociales del sentido común, la objetividad y los hechos reales que compartimos en el día a día. Pero no podemos ocultar que cada día vivimos más en las redes sociales, condicionados por el algoritmo en las plataformas. Ese metaverso es el mundo donde habitan muchos jóvenes y ahí no hay objetividad y sí mucha emoción. Y eso hace que esos jóvenes, esas personas, sean emocionales y, por tanto, más vulnerables que quienes estamos más pegados al mundo físico.

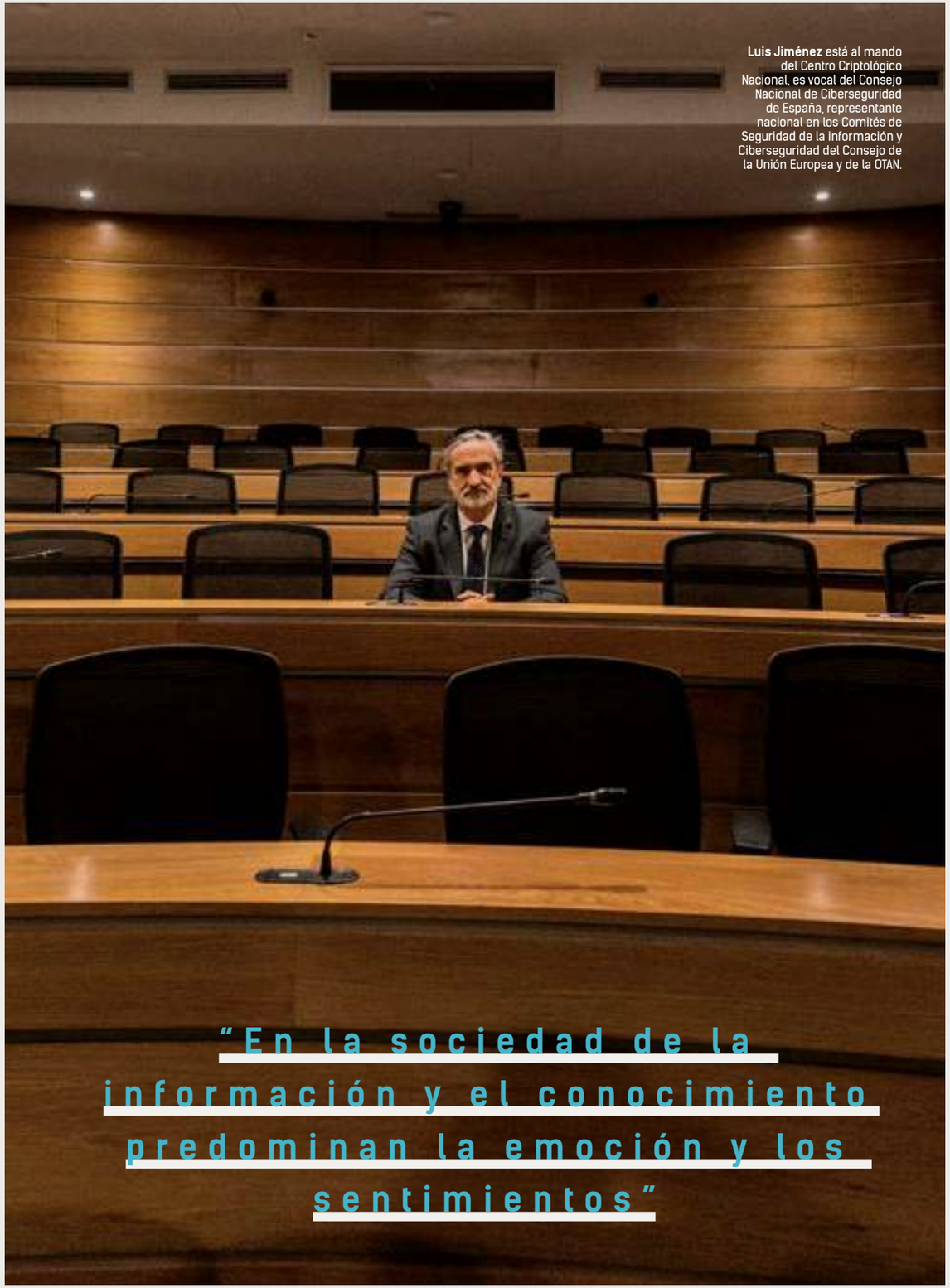
Desde esa perspectiva, en el metaverso es más difícil discernir entre hechos reales y falsos; la emoción y los sentimientos anulan la razón.
Es una paradoja enorme que en la sociedad de la información y el conocimiento sean la emoción y los sentimientos los que predominan.

¿Cómo se combate la posverdad?
Es una cuestión de formación, de cultura y de madurez. Además, tenemos que plantearnos si establecemos limitaciones al mundo virtual. Y es también muy importante la responsabilidad de quienes generan contenidos en ese metaverso, de los *influencers*. Son muy importantes iniciativas como la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), que abordará cuestiones éticas y legislativas.

¿Quiénes son los peores malos?
Los malos son los que nos agreden. En el mundo en el que vivimos, no existen amigos o enemigos, sino intereses comunes o encontrados.

¿Su peor pesadilla?
Un *malware* desconocido que, de repente, lo encuentras en un sistema informático de la Administración pública en el que ha estado alojado varios años extrayendo información en contra de nuestros intereses políticos, estratégicos o económicos. Mi peor pesadilla es el ciberespionaje sofisticado que determinados Estados tienen capacidad de realizar.

Al final, ya sea mediante la manipulación o la extracción de información, se trata de condicionar la toma de decisiones.
Esos son los incidentes más complejos a los que nos enfrentamos, los que más recursos nos exigen. Ponen de manifiesto un conflicto entre países ante el que hay que estar muy alerta. Hay mucho más ciberespionaje del que nos podemos imaginar y no solo para cuestiones de tipo político o geopolítico —como puede ser obtener información sobre la posición de un país por anticipado—, también hay mucho robo de información empresarial y de patrimonio tecnológico, de *know-how*, de conocimiento del interior de nuestras empresas, de los centros tecnológicos y de las universidades.



Luis Jiménez está al mando del Centro Criptológico Nacional, es vocal del Consejo Nacional de Ciberseguridad de España, representante nacional en los Comités de Seguridad de la información y Ciberseguridad del Consejo de la Unión Europea y de la OTAN.

"En la sociedad de la información y el conocimiento predominan la emoción y los sentimientos"