
XIV JORNADAS DE SEGURIDAD, DEFENSA Y COOPERACIÓN
EL CIBERESPACIO
RETOS Y OPORTUNIDADES EN EL MUNDO VIRTUAL
17-19 DE NOVIEMBRE DE 2020
LIBRO DE ACTAS DE LAS JORNADAS
Resúmenes
Ponencias
Vídeos
Presentaciones
Recursos
PATROCINADO POR
PROMÁLAGA
FORO PARA LA PAZ EN EL MEDITERRÁNEO
Ayuntamiento de Málaga
cifal
Unicaja Banco
Fundación Unicaja
UNIVERSIDAD DE MÁLAGA
Cámara
AECYR
REAL CLUB EL CANDADO

FORO PARA LA PAZ
EN EL MEDITERRÁNEO

Edición: Foro para la Paz en el Mediterráneo
ISBN: 978-84-09-30174-4

XIV JORNADAS DE SEGURIDAD, DEFENSA Y COOPERACIÓN. FORO PARA LA PAZ EN EL MEDITERRÁNEO.

EL CIBERESPACIO: RETOS Y OPORTUNIDADES EN EL MUNDO VIRTUAL.

FORO PARA LA PAZ
EN EL MEDITERRÁNEO

XIV JORNADAS DE SEGURIDAD, DEFENSA Y COOPERACIÓN. FORO PARA LA PAZ EN EL MEDITERRÁNEO.

EL CIBERESPACIO: RETOS Y OPORTUNIDADES EN EL MUNDO VIRTUAL.

Director Comisión Jornadas: Carlos de Palma Arrabal.
Coronel (Rva.), Piloto aviación militar. Ingeniero de organización industrial.
carlosdepalmaarrabal@gmail.com

Coordinación institucional: Deborah Salafranca, Francisco Pastor, Luis Macua.
Centro CIFAL Málaga de UNITAR (United Nations Institute for Training & Research).

Redacción: Roberto López Pensado.
Ingeniero Técnico de Telecomunicaciones. Especializado en Electrónica y Telecomunicaciones.

Oficina apoyo a la dirección: Iñaki Benedicto Marqués.
Máster en Ciberseguridad. Universidad Católica de Murcia y Telefónica.

Equipo Técnico de producción: Enrique A. Martínez y José Manuel Fernández
Unidades Audiovisuales Universidad Internacional de Andalucía.

GUÍA DE LAS JORNADAS.

0. **SALUDO Y PRESENTACIÓN INSTITUCIONAL.**
1. **PROGRAMA DE LAS JORNADAS DEDICADAS AL CIBERESPACIO.**
2. **ACTAS, ENLACES A LOS VIDEOS, INTRODUCCIÓN, BIBLIOGRAFÍA Y TEXTOS PONENTES.**
3. **DICCCIONARIO DE LA ADMINISTRACIÓN ELECTRÓNICA. (Ver en Anexos).**
4. **PRESENTACIONES USADAS DURANTE LAS INTERVENCIONES. (Ver en Anexos).**

TODO ESTE MATERIAL EN SU CONJUNTO, OFRECE UN CONOCIMIENTO AMPLIO Y COMPRENSIBLE SOBRE EL PANORAMA ACTUAL DEL CIBERESPACIO, DE SUS RETOS Y SUS OPORTUNIDADES, TODO LO CUAL FUE EXPUESTO POR EXPERTOS EN CADA ÁREA, EN NOVIEMBRE DE 2020 EN FORMATO VIRTUAL.

INVITAMOS A TODOS LOS LECTORES A DISFRUTAR Y COMPARTIR LIBREMENTE ESTA ATRACTIVA INFORMACIÓN CON SUS CONTACTOS.

ENLACES A LA COLECCIÓN DE VIDEOS DE LAS JORNADAS

XIV Jornadas de Seguridad, Defensa y Cooperación. "El Ciberespacio. Retos y oportunidades en el mundo virtual". 17-19 noviembre 2020.

Enlace a la colección de vídeos XIV Jornadas de Seguridad, Defensa y Cooperación
https://vimeo.com/showcase/7942138

Sesión Inauguración XIV Foro para la Paz en el Mediterráneo
https://vimeo.com/497907737

1ª JORNADA. 1ª Mesa redonda: Diplomacia digital y cooperación internacional.
https://vimeo.com/497908793

1ª JORNADA. 2ª Mesa redonda: Panorama de Utilidades cibernéticas e Inteligencia Artificial.
https://vimeo.com/497910937

2ª JORNADA. 1ª Mesa redonda: Usos y abusos en el ciberespacio. Defensa, seguridad y protección.
https://vimeo.com/494049004

2ª JORNADA. 2ª Mesa redonda: Identidad Digital, Comunicación y Manipulación.
https://vimeo.com/498313436

3ª JORNADA. 1ª Mesa redonda: Mundos Físicos y Virtuales, Málaga como Ciudad-Región. https://vimeo.com/498182383

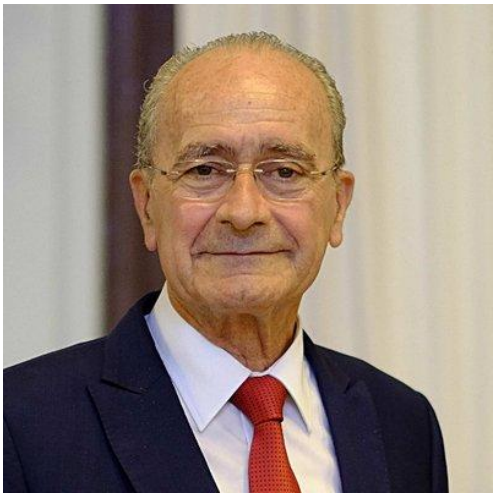
3ª JORNADA. 2ª Mesa redonda: Perspectivas y estrategias para el mundo virtual.
https://vimeo.com/498183143

Sesión Clausura de las XIV Jornadas del Foro para la Paz en el Mediterráneo
https://vimeo.com/498169230

SALUDOS Y PRESENTACIÓN INSTITUCIONAL

D. FRANCISCO DE LA TORRE PRADOS, ALCALDE DEL AYUNTAMIENTO DE MÁLAGA:

FORO PARA LA PAZ EN EL MEDITERRÁNEO.
XIV EDICIÓN JORNADAS DE SEGURIDAD, DEFENSA Y COOPERACIÓN:
EL CIBERESPACIO, RETOS Y OPORTUNIDADES EN EL MUNDO VIRTUAL.



Me resulta muy grato introducir estas Jornadas que cada año desarrolla el Foro para la Paz en el Mediterráneo, dedicadas en esta ocasión a la dimensión del ciberespacio, y que debido a condicionantes sanitarios por la pandemia de la COVID-19 hemos tenido que celebrar en formato virtual, aunque despertando gran interés entre sus asistentes.

Málaga es una ciudad abierta, con una larga historia como puente entre continentes y culturas; sus habitantes son acogedores y disfrutan de un clima y unas condiciones envidiables. También son laboriosos, solidarios y muy amigos del conocimiento, permaneciendo siempre atentos a los avances que la cultura, las ciencias o la tecnología nos ofrecen. Por ello, el tema al que se dedican las jornadas de este año, tituladas “El Ciberespacio, retos y oportunidades en el mundo virtual”, se ha preparado con especial atención y cariño.

Ya no existen mundos físicos y virtuales que puedan considerarse separados, ni siquiera complementarios. Ambos mundos se han fundido en uno sólo, y conforman nuestra realidad actual y de futuro. La informática, las telecomunicaciones, los dispositivos basados en tecnologías digitales, la inteligencia artificial y el Ciberespacio, forman parte integral de nuestras vidas y amplían cada día el entorno con el que debemos convivir.

Queremos que esta nueva dimensión, más intangible o impersonal aparentemente, se humanice en lo posible. Las habilidades y competencias digitales deben enriquecer las relaciones profesionales y personales, y orientarse por un lado al mejor servicio público a los ciudadanos, y por otro a reducir la brecha digital, mejorar la formación en todos los campos, y facilitar la igualdad de oportunidades.

Por todo ello, las instituciones de nuestra ciudad, Junta Directiva del Foro para la Paz en el Mediterráneo, Secretaría de CIFAL-Málaga, director de las Jornadas, técnicos, moderadores e ilustres ponentes que han participado o apoyado el desarrollo de estas jornadas, han trabajado con enorme ilusión. A todos les traslado mi sincera felicitación por el resultado, y desde esta ciudad quedamos a la espera de poder celebrar la próxima edición en condiciones más favorables, así como compartir nuestro variado y maravilloso patrimonio con quienes nos visiten.

D. JULIO ANDRADE, VICEPRESIDENTE DEL FORO PARA LA PAZ EN EL MEDITERRÁNEO. DIRECTOR DEL CENTRO INTERNACIONAL DE FORMACIÓN DE AUTORIDADES Y LÍDERES CIFAL MÁLAGA, Y FELLOW DEL INSTITUTO DE NACIONES UNIDAS PARA LA FORMACIÓN PROFESIONAL E INVESTIGACIONES (UNITAR).

La edición de estas XIV Jornadas ha estado muy condicionada por la pandemia que nos azota, pero hemos redoblado nuestros esfuerzos e ilusión para poder celebrar este encuentro, compartir virtualmente conocimientos y debatir estrategias y proyectos de vanguardia en el campo del ciberespacio y la digitalización. Desde comienzos del presente año 2020, las videoconferencias tanto personales como públicas se han instalado en nuestras agendas y modos de vida, y ello nos ha permitido disfrutar de los interesantes temas seleccionados para cada jornada junto a un plantel multidisciplinar de expertos ponentes.

Quisiera señalar que una docena de representantes institucionales, veinticinco expertos en sus respectivos campos entre moderadores y ponentes, y una decena de patrocinadores, han logrado ofrecer sus aportaciones por medio de dispositivos portátiles desde sus respectivas oficinas o domicilios, a modo de estudios de televisión domésticos improvisados, lo cual ha supuesto un reto de coordinación muy importante para el director y equipo organizador de las Jornadas, incluyendo a los técnicos de realización de la Universidad Internacional de Andalucía.

Sin duda, necesitamos conocer mejor esta nueva dimensión del Ciberespacio, dominar las posibilidades, limitaciones y riesgos de los dispositivos digitales, y asumir el reto de integrar todo ello en nuestras vidas, junto a los avances en inteligencia artificial. El reto se nos presenta tanto a nivel individual como profesional, corporativo, nacional e incluso supranacional, pues las oportunidades y riesgos que el uso del ciberespacio nos plantea son sin duda globales y apasionantes. A las enormes oportunidades que nos brinda la cibernética y el uso del ciberespacio, bien sea para comunicarnos, aprender, trabajar, comerciar, ayudar, curar, etc. hay que superponer su regulación y protección, pues como toda herramienta humana presenta multitud de ventajas e inconvenientes que hay que aprovechar y prevenir.

Esta XIV Edición del Foro para la Paz en el Mediterráneo se ha conformado en tres jornadas, celebradas entre el 17 y el 19 de noviembre de 2020:

- La primera jornada dedicada a introducirnos en las múltiples oportunidades y facetas positivas del actual Panorama cibernético y virtual, incluyendo la temática de la diplomacia digital y cooperación internacional, así como las actuales utilidades cibernéticas y de inteligencia artificial.

- La segunda centrada en la cara negativa que suponen los graves Riesgos presentes y futuros que afectan a la seguridad, incluyendo los usos y abusos presentes en el ciberespacio, así como la identidad digital y la manipulación de nuestras mentes.

- La tercera jornada apunta a la idea de Ciudad como polo de una provincia o región ampliada, y como sus entornos urbano y rural se enfrentan al ciberespacio. Se ha debatido sobre los mundos físico y virtual, y las perspectivas y estrategias aplicadas en la ciudad de Málaga que pudieran ser de utilidad para otras ciudades o zonas ampliadas.

Estas Jornadas se ponen ahora al alcance de una comunidad más amplia e interesada en el tema, en forma de Actas que resumen sus contenidos en nuestra Web del Foro para la Paz en el Mediterráneo con el siguiente índice disponible:

- Presentación XIV Jornadas del Foro para la Paz en el Mediterráneo.
- Programa. El Ciberespacio: Retos y oportunidades en el mundo virtual.
- Introducción al Ciberespacio.
- Colección de Videos con las intervenciones de los ponentes.
- Presentaciones con imágenes y textos que completan las intervenciones.
- Anexos de interés.

Finalmente, solo me queda decir que seguiremos en contacto, y esperando contar con el apoyo de las entidades patrocinadoras a las que traslado mi más sincero agradecimiento: Ayuntamiento de Málaga, Promálaga, Unicaja Banco, Fundación Unicaja, CIFAL Málaga-UNITAR, Universidad de Málaga, Universidad Internacional de Andalucía, Cámara de Comercio, Real Club Mediterráneo, Real Club el Candado, Asociación Española de Capitanes de Yate para la Reserva Civil, y Real Hermandad de Veteranos de las Fuerzas Armadas y la Guardia Civil de Málaga.

FORO PARA LA PAZ EN EL MEDITERRÁNEO

XIV JORNADAS DE SEGURIDAD, DEFENSA Y COOPERACIÓN

EL CIBERESPACIO: RETOS Y OPORTUNIDADES EN EL MUNDO VIRTUAL

FECHAS: 17 al 19 noviembre 2020.

MARTES 17 NOVIEMBRE: PANORAMA CIBERNÉTICO Y VIRTUAL

17:45 h. <u>Inauguración de las XIV Jornadas dedicadas al Ciberespacio</u>:

- **José Ignacio García Pérez**. Rector de la Universidad Internacional de Andalucía (UNIA).
- **Salvador Molina Ruíz**. Subdirector de la sede de la UNIA en Málaga.
- **Rosa Sánchez Jiménez.** Tte. Alcalde de Turismo y Promoción de la Ciudad.
- **José María López Jiménez.** Director Responsabilidad Social Corporativa UNICAJA Banco.
- **Rafael Vidal.** Representante Real Club Mediterráneo de Málaga.
- **Julio Andrade**. Director de CIFAL MÁLAGA-UNITAR y Vicepresidente del Foro para la Paz en el Mediterráneo.
- **Ricardo Nandwani.** Vocal del Pleno y Presidente de la Comisión de Empresa y Economía Digital de la Cámara de Comercio de Málaga.

Moderador Jornada: José María López Jiménez. *Director Responsabilidad Social Corporativa de UNICAJA Banco.*

18:10 h. <u>Diplomacia digital y cooperación internacional</u>:

Digitalización en ámbitos de la Unión Europea y las relaciones internacionales. Diplomacia Digital. Agencia andaluza y Foros de Cooperación europeos y mediterráneos. Málaga como puente de cooperación entre Europa y África.

- ***Embajador Juan José Escobar Stemmann.*** *Ministerio de Asuntos Exteriores y Cooperación en Madrid. Embajador del Reino de España en Irak.*
- ***Dr. Jamal-Eddine Mechbal.*** *Antiguo Diplomático de la Embajada del Reino de Marruecos en España.*
- ***Ricardo Nandwani****, Vocal del Pleno y Presidente de la Comisión de Empresa y Economía Digital de la Cámara de Comercio de Málaga.*

19:10 h. Descanso.

19:20 h. <u>Panorama de Utilidades cibernéticas e Inteligencia Artificial</u>:

El Ciberespacio y la interacción de la informática con las telecomunicaciones, bases tecnológicas de las TIC (Tecnologías de la Información y las Telecomunicaciones). Computación cuántica. Dispositivos digitales. El Internet de las cosas (IoT). Big Data. Realidad aumentada. Herramientas 3D. Digitalización y Administración electrónica. Utilidades cibernéticas y necesidades sociales y económicas. Telemedicina y biotecnología. Digitalización de procesos judiciales. Industria 4.0. Empresas y teletrabajo. Robots. Mercado laboral y

aspectos fiscales. Comercio electrónico y mercado digital. Banca y finanzas 0n-line. Criptomonedas. Blockchain. Turismo. Administración digital. Conservación e integridad de archivos digitales. Transporte inteligente. La Inteligencia artificial dedicada de hoy y la multifunción del mañana. Red 5G. Ciudad inteligente (Smart City). Educación on-line. La religión en Redes e Internet. Juegos virtuales en red. Ciberespacio para Jóvenes y Mayores. Brechas digitales entre generaciones y regiones. Necesidades de formación continúa.

- ***Víctor Manuel Solla:*** *Director General Innovación y Digitalización Urbana. Ayuntamiento de Málaga.*
- ***José María López Jiménez.*** *Director Responsabilidad Social Corporativa UNICAJA Banco*.
- ***Carlos de Palma.*** *Coronel (Rva.), Ingeniero organización industrial, Piloto aviación militar.*
- ***Francisco López.*** *Investigador responsable Laboratorio Inteligencia Artificial Aplicada, E.T.S de Informática de la Universidad de Málaga.*
- ***Belén Bahía.*** *Profesora Titular Derecho Financiero y Tributario. Universidad de Málaga.*
- ***María Gómez.*** *Abogada. Coordinadora Sección Derecho Digital, Innovación y Gestión. Colegio de Abogados de Málaga.*

20:30h. Fin de la primera jornada

MIÉRCOLES 18 NOVIEMBRE: RIESGOS PRESENTES Y FUTUROS

Moderador: F. Javier López Muñoz, *Vicerrector de Empresa, Territorio y Transformación digital de la Universidad de Málaga****.***

17:45 h Saludo participantes.

18:00 h. <u>Usos y abusos en el ciberespacio. Defensa, seguridad y protección</u>:

Las dimensiones terrestre, marítima, aérea, espacial y ciberespacial. Estrategia de Seguridad Nacional 2017, Integración del mundo virtual en la Estrategia Nacional de Ciberseguridad 2019. Foro Nacional de Ciberseguridad 2020. Proyectos digitales de la Defensa. Actualidad de los ataques informáticos, hackers y virus. Seguridad de Infraestructuras críticas y Redes de servicio público. Centros de respuesta nacionales. Conflictos regionales, crimen organizado, terrorismo y Ciberdelincuencia. Ciberinteligencia y Ciberespionaje. Ciberseguridad doméstica, empresarial y corporativa. Papel del factor humano y tecnologías disponibles para la seguridad digital. Iniciativa y velocidad de respuesta en los procesos de defensa frente a Ciberataques. Derecho digital, juicios telemáticos y legislación relacionada.

- ***Mar López.*** Jefa de la Oficina de Ciberseguridad del Departamento de Seguridad Nacional**.**
- ***Carlos Seisdedos.*** Internet Security Auditors, responsable Ciberinteligencia.
- ***General Raimundo Rodríguez.*** Mando Operaciones Especiales del Ejército (MOE).
- ***Coronel Francisco Palomo.*** Mando Conjunto del Ciberespacio (MCCE). Ministerio de Defensa.
- ***Inspector Antonio Gómez.*** Grupo Ciberdelincuencia. Jefatura Provincial del Cuerpo Policía Nacional de Málaga.
- ***Teniente Coronel José Durán***. Unidad de Coordinación en Ciberseguridad de la Guardia Civil. Dirección General. Madrid.
- ***José Miguel Ruiz.*** Director Servicios Gestionados y Ciberseguridad. Ingenia. Málaga Tech Park.

19:50 h. Descanso

20:00 h. <u>Identidad Digital, Comunicación y Manipulación</u>:

Redes sociales informales, aplicaciones y canales profesionales de comunicación. Publicidad, influencers, propaganda y control de contenidos. Identidad digital y Reputación on-line. El factor Google. Marcos mentales y toma de decisiones en la era digital. Defensa frente a la manipulación. Lobbies, campañas electorales y gobernanza. Gestión y servicio público, Partidismo, Populismo, Globalismo y Sociedad Civil.

- ***Vicente Díaz**. Ingeniero de Seguridad de Google.*
- ***Alex Borrás.** Director de Comunicación. Agencia comunicación Digital Site 360.*
- ***Carlos de Palma.** Coronel (Rva.), Ingeniero Organización Industrial, Piloto aviación militar.*

20:30 h. Fin de la Segunda jornada

JUEVES 19 NOVIEMBRE: CIUDADES FRENTE AL CIBERESPACIO

17: 45h. Saludo participantes

***Moderador: Carlos de Palma.** Director Comisión XIV Jornadas sobre el Ciberespacio.*

18:00 h. <u>Mundos físicos y virtuales. Málaga como Ciudad-Región</u>:

Realidad y virtualidad. Fronteras físicas e interacción con el Ciberespacio. Retos y futura transformación de los espacios urbanos, rurales y extendidos. Movilidad, conectividad y mercados en la transformación del modelo Ciudad-Región. Apuntes para Málaga.

- ***Salvador Moreno Peralta.** Arquitecto y Urbanista.*

18:15 h Descanso

18:20 h. <u>Perspectivas y estrategias para el mundo virtual:</u>

Estrategias, foros y proyectos de desarrollo y digitalización urbanos y rurales. Redes y oficinas de apoyo, servicios cooperativos, incubadoras, infraestructuras y recursos. Experiencias para compartir entre ciudades. El caso de Andalucía, Málaga y provincia.

- ***Susana Carillo.** Primer Teniente Alcalde y Concejala Innovación y Digitalización Urbana Ayuntamiento de Málaga*
- ***Felipe Romera.** Director General Parque Tecnológico de Andalucía.*
- ***Yolanda De Aguilar.** Directora General Palacio Ferias y Congresos de Málaga (FYCMA).*
- ***Carmen García.** Directora Gerente Fundación CIEDES (Centro Investigaciones Estratégicas y Desarrollo Económico y Social).*
- ***Francisco Salas.** Director de Promálaga.*

20:00 h. <u>Cierre de las XIV Jornadas del Foro para la Paz en el Mediterráneo</u>

- ***Olga Guerrero.** Vicerrectora Adjunta de Proyectos. Universidad de Málaga.*
- ***Rafael Muñoz.** Director de Actuaciones Socioculturales de la Fundación UNICAJA.*
- ***Manuel Calderón de Bonis.** Presidente Real Club del Candado.*
- ***Alfredo Escudero y Díaz.** Presidente AECYR.*
- ***Francisco de la Torre Prados.** Alcalde de Málaga*

ACTAS, ENLACES, INTRODUCCIÓN, BIBLIOGRAFÍA Y TEXTOS PONENTES

INTRODUCCIÓN, GLOSARIO Y BIBLIOGRAFÍA SOBRE EL CIBERESPACIO.

Roberto López Pensado.

Ingeniero Técnico de Telecomunicaciones. Especializado en Electrónica y Telecomunicaciones. Certificado Profesional en Seguridad Informática. Técnico Superior en Sistemas Automáticos y Programables. Quince años experiencia en Multinacionales Tecnológicas Norteamericanas, Australianas, Suecas y Holandesas. Máster en Formación para el Profesorado de Tecnología. Condecorado por cooperar en la Operación Balmis contra la COVID-19 por el Hospital Central de la Defensa (Electromedicina).

A) Preámbulo.

La historia de la humanidad siempre se ha visto afectada por los avances tecnológicos, y en especial por la irrupción en nuestras vidas de la electricidad y electrónica, las telecomunicaciones, la informática y los dispositivos basados en tecnologías digitales. Y sus efectos se han multiplicado recientemente con los avances en la velocidad de tratamiento de datos, la inteligencia artificial, la computación cuántica o las redes sociales.

Durante décadas se ha considerado que existía una separación o paralelismo entre los mundos físico y virtual, pensando incluso algunas personas que se podía vivir sin teléfonos, ordenadores, mensajería o aplicaciones informáticas varias. La informática, Internet, etc. no sólo han llegado para quedarse, sino también para sustituir hábitos y procedimientos pasados, formando parte integral de nuestras vidas. Es más, en muchos casos han dejado obsoletas y fuera del mercado a las herramientas tradicionales de trabajo, cambiando nuestra realidad actual y evolucionando muy rápidamente hacia un futuro impredecible. Un futuro que no tiene porqué ser caótico, pero siempre y cuando le prestemos la atención adecuada.

La Real Academia de la Lengua Española (RAE) define el Ciberespacio como un "ámbito virtual creado por medios informáticos". Y en los ANEXOS que acompañan a este documento se encontraran las definiciones y significado del vocabulario especial que se emplea en este nuevo ámbito.

La siguiente infografía muestra, en su círculo interior. los ámbitos tradicionales y más importantes de nuestro entorno y, en el círculo exterior, las nuevas tecnologías y servicios digitales complementarios que están surgiendo. No hay marcha atrás, lo cual no quiere decir que nos dejemos arrastrar por el vértigo tecnológico, sino que habría que encauzar su evolución y controlarlos adecuadamente.

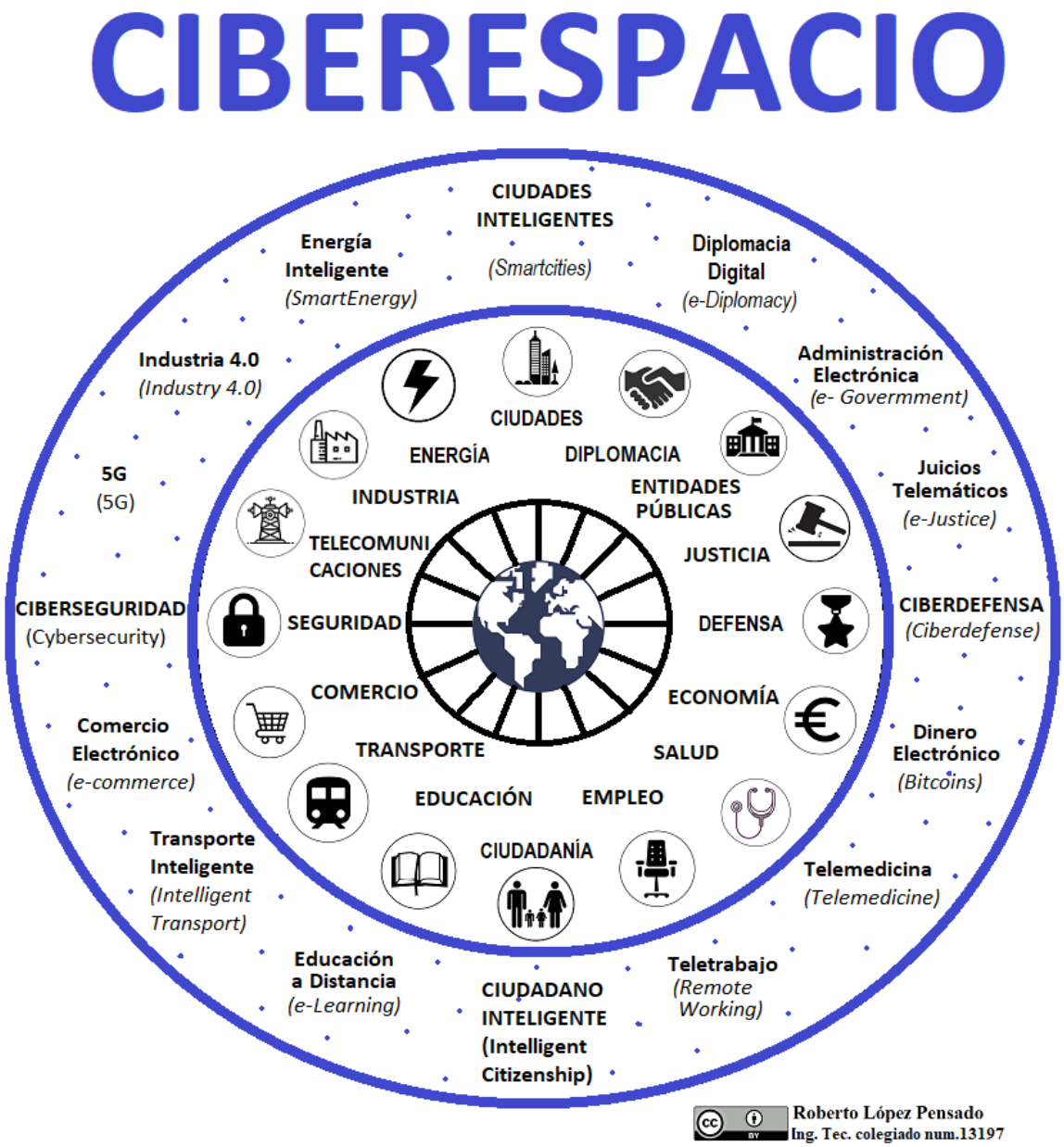


Figura: *Infografía sobre el Ciberespacio.* ***Fuente:*** *propia – Roberto López Pensado. Ingeniero Técnico colegiado COITT núm. 13197.* ***Ilustraciones:*** *free icons (www.icon-icons.com)*

B). Hitos y Evolución tecnológica.

En el Siglo XX se han sucedido varios hitos importantes desde el punto de vista de la Electrónica, la Informática, el Internet y las Telecomunicaciones que son considerados como la base tecnológica de desarrollo y uso del Ciberespacio. Y en el Siglo XXI se han seguido desarrollando de modo imparable nuevas tecnologías que permiten dar forma a estructuras y redes más complejas.

A continuación se muestran en una tabla varios hitos tecnológicos que han contribuido a la evolución del actual Hardware, del Software y de las Comunicaciones:

Año	Hito Tecnológico	Nombre	Descripción
1945	Primera computadora electrónica con memoria para 64 palabras y una unidad de cálculo.	ENIAC	
1950	Primer código de programación electrónica o lenguaje de programación a bajo nivel.	ENSAMBLADOR	
1957	Primer Satélite artificial que funcionó como GPS.	SPUTNIK	
1958	Primer circuito electrónico integrado.	CHIP	
1958	Primeros lenguajes de programación informáticos.	FORTRAN, COBOL	
1971	Primer procesador de datos informáticos.	MICROPROCESADOR	
1981	Primer ordenador personal.	PC	
1983	Primera red informática que comparte datos entre PC´s.	ArpaNET	
1988	Primer virus o código malicioso informático en Red.	Gusano MORRIS	
1994	Primer teléfono móvil con pantalla táctil, aplicaciones y transmisión de datos.	SMARTPHONE	
1998	Primer buscador consolidado en Internet.	GOOGLE	
2001	Inicio de las Telecomunicaciones multimedia y tarifa plana de datos móviles.	3G	
2001	Datos masivos en volumen, variedad y velocidad.	BIG DATA	
2008	Primer Sistema Operativo consolidado para móviles inteligentes.	ANDROID 1.0	
2009	Los dispositivos conectados (Internet de las cosas) superan en cantidad al número de habitantes del mundo.	IoT	
2012	Primeros algoritmos de aprendizaje automático complejos basados en datos masivos.	INTELIGENCIA ARTIFICIAL	
2019	Quinta generación de Telecomunicaciones para dispositivos móviles.	5G	

Tabla: *Hitos y Tecnologías relevantes para el Ciberespacio.* ***Fuente:*** *propia – Roberto López Pensado. Ingeniero Técnico colegiado COITT num. 13197.* ***Ilustraciones:*** *free icons (www.icon-icons.com)*

El conocimiento necesario para el nacimiento y uso de la dimensión del Ciberespacio se ha ido moldeando durante décadas, gracias a proyectos de investigación universitarios, y a la inversión y colaboración público-privada y empresarial. Este desarrollo tecnológico y su evolución se podrían entender con las siguientes premisas:

- La Ciencia, la Ingeniería y la Física son el origen de su base técnica.

- La Electrónica, la Informática y las Telecomunicaciones son las ramas en las que se basan las nuevas tecnologías y los servicios telemáticos digitales del Ciberespacio.

- Todo Sistema Telemático consta de una componente Hardware, de un Software, de un medio de transmisión y de una red de transmisión y almacenamiento de datos.

- La mayoría de patentes de las nuevas tecnologías están en manos de empresas privadas internacionales que fabrican Hardware o desarrollan Software, como Siemens, Intel, Thosiba, AMD, Nokia, Cisco, Microsoft, Huawei, GE, Google, Sony, IBM, Apple, Dell, Amazon, Oracle, Mitshubishi Electric, Ericsson, Canon, IBM, Qualcomm, Texas Instruments, Airbus, Bosch, 3M, Fujitsu, NEC, Rockwell, HP, Adobe, Philips, Sun Microsystem o Xerox.

- Diferentes organismos Europeos e Internacionales regulan la estandarización y la normalización de procesos, de lenguajes de programación y de protocolos de comunicaciones industriales (como Profinet, CAN o Fieldbus), informáticos (Java, SQL, C++, Phyton), de redes (TCP/IP, SS7, HTTP) o de Comunicaciones (Bluetooth, ADSL, GPS, GSM o 802.11 /Wifi, 5G).

- En los últimos veinte años se han desarrollado multitud de tecnologías innovadoras como la Inteligencia Artificial, el Big Data, el diseño 3D, la realidad virtual aumentada, el certificado digital, el internet de las cosas, almacenamiento en la nube, el blockchain, la nanotecnología, los ordenadores cuánticos, el machine learning o la ciberseguridad que permitirán en un futuro próximo la digitalización de datos o parámetros relevantes que representen a las ciudades, la industria o la sociedad. A veces se usarán para facilitar sus vidas y otras para intentar su control.

Evolución y Bases Tecnológicas del Ciberespacio

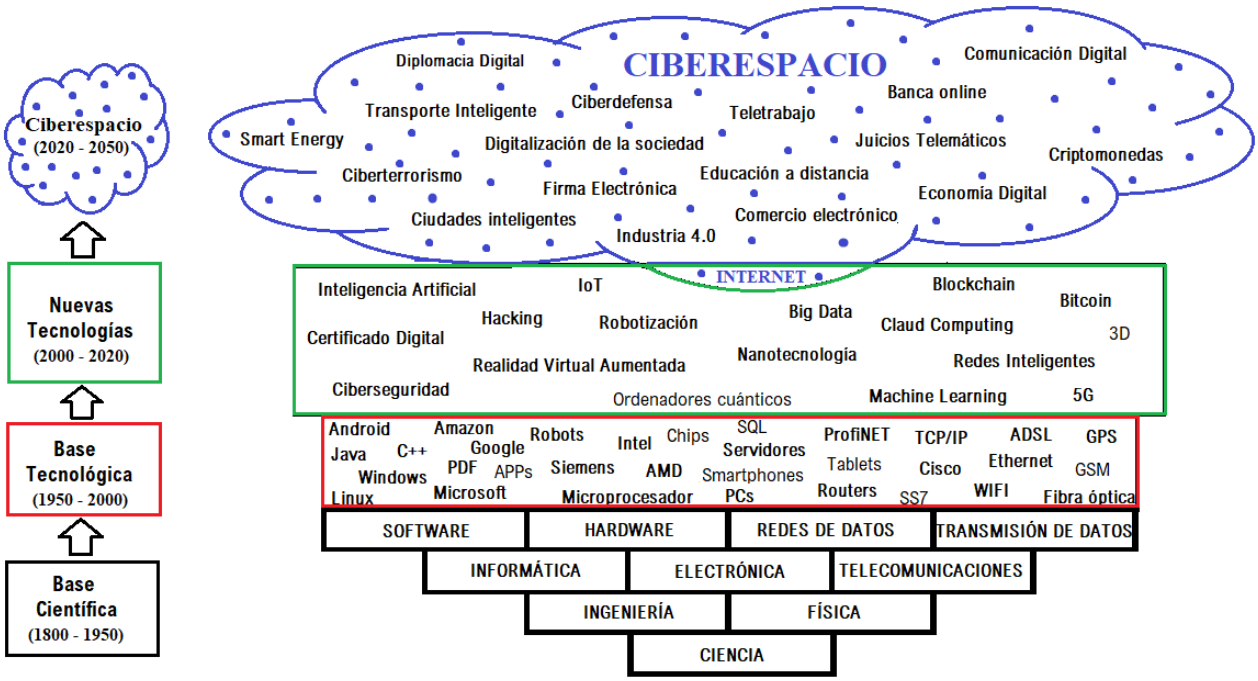


Ilustración: *Evolución y base tecnológica del Ciberespacio.* ***Fuente:*** *propia – Roberto López Pensado. Ingeniero Técnico colegiado COITT num. 13197*

A) **Organismos reguladores en la Tecnología y la Ciberseguridad.**

A nivel tecnológico, entre otros, existen los siguientes Organismos Internacionales que se encargan de regularizar el diseño y la fabricación de componentes electrónicos y equipos informáticos así como de estándares de comunicaciones:

- ITU (International Telecommunications Union, 1932): Organismo de las Naciones Unidas especializado en telecomunicaciones y encargado de regular las telecomunicaciones a nivel internacional. Por ejemplo, la Recomendación UIT-T H.264 (MPEG-4) ha contribuido a estandarizar uno de los formatos comprimidos de Video más utilizado del mundo: el MP4.
- ISO (International Organization for Standarization, 1947): Organismo para la creación de estándares internacionales compuesto por diversos organismos nacionales estandarizados , como por ejemplo ANSI en Estados Unidos, DIN en Alemania o AENOR en España .
- CEPT (Conférence Européenne des administrations des Postes et des Télécommunications, 1959): Organismo interno que agrupa a las entidades responsables en la administración pública de cada país europeo de las políticas y la regulación de las telecomunicaciones.
- ECMA (European Computer Manufacturers Association, 1961): Organización internacional basada en membrecías de estándares para la comunicación, los ordenadores y la informática.
- IEEE (Institute of Electrical and Electronics Engineers, 1963): Asociación mundial de ingenieros dedicados a la estandarización y desarrollo de área técnicas. Los estándares Ethernet 1.0 (redes LAN) y el estándard IEEE 802.11 (WIFI) fueron desarrollados por esta organización en 1979 y 2004 respectivamente.
- IETF (Internet Engineering Task Force, 1986): Organización internacional abierta de normalización, que tiene entre sus objetivos contribuir a la ingeniería del Internet y en concreto en áreas como el transporte, enrutamiento y seguridad.
- ISOC (Internet Society, 1992): Organización gubernamental sin ánimo de lucro y de carácter internacional dedicada exclusivamente al desarrollo mundial de Internet y a asegurar que siga siendo abierta y transparente.
- AUI (Asociación de Usuarios de Internet, 1995): Entidad sin ánimo de lucro de ámbito nacional, que realiza actividades para promover el desarrollo y buen uso de Internet, a la vez que defiende los intereses y derechos de los usuarios y práctica de las nuevas tecnologías.
- W3C (World Wide Web Consortium, 1994): Comité fundado por Tim Berners-Lee, el arquitecto inicial del World Wide Web (WWW). El propósito de esta organización es desarrollar estándares abiertos, como por ejemplo HTTP, HTML o XML que son los lenguajes de programación que se utilizan para el diseño de páginas Web.
- ENISA (European Network and Information Security Agency, 2004): Agencia Europea de Seguridad de las Redes y de la Información es el organismo público de ámbito europeo encargado de promover mejoras en cuestiones de seguridad en internet.

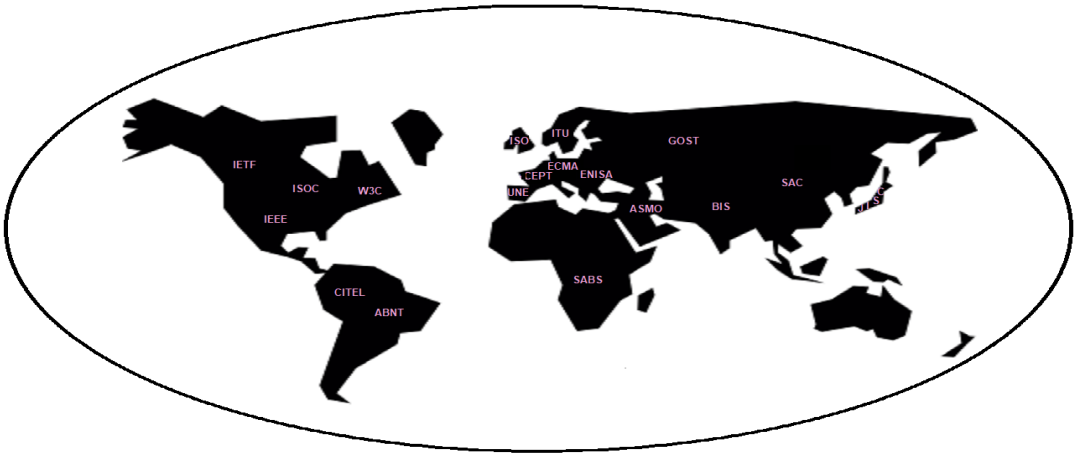


Figura: *Organismos internacionales de Normalización.* ***Fuente:*** *propia – Roberto López Pensado. Ingeniero Técnico colegiado COITT num. 13197.* ***Ilustraciones:*** *free icons (www.icon-icons.com)*

B) Glosario de términos: Tecnología, electrónica, informática y telecomunicaciones.

Concepto	*En inglés*	*Descripción*
4ª Revolución industrial ó Industria 4.0	Industry 4.0	Cuarta etapa de evolución técnico-económico-industrial de la humanidad. Incluye tecnologías como las fábricas Inteligentes (SmartFactories), la Robótica, Internet de las Cosas (IoT), Big Data, Inteligencia Artificial (AI), la nube (Cloud Computing) , Comunicación Máquina-Máquina (M2M), Lenguaje Máquina (ML), Software 3D, Realidad aumentada, Visión Artificial, Ciberseguridad, la NanoTecnología, los sensores inteligentes (Smartsensors), la Digitalización y la Automatización.
5G	5G	Quinta generación de tecnologías móviles, inalámbricas y de telecomunicaciones. Con respecto al 3G y al 4G se aumenta la velocidad de conexión (ultravelocidad de subida y de bajada), se reduce el tiempo de latencia (tiempo de respuesta) y mayor capacidad de conexión de múltiples dispositivos y servicios simultáneos (teóricamente hasta 1 millón de dispositivos conectados por Km2). Para conseguir esta funcionalidad se requiere la utilización de diferentes medios de comunicación como antenas GSM de radiofrecuencia, redes informáticas, redes WIFI, fibra óptica, cables submarinos, sistemas GPS y comunicaciones satelitales en el espacio.
Bit	Binary Digit	Es la unidad de medida de datos en Sistemas Digitales. En el sistema binario un bit puede tener dos valores: 0 ó 1
Cadena de Bloques	Blockchain	División de un documento con datos digitales en bloques codificados. Al estar basado en un sistema descentralizado y distribuido, en el caso de que se cayesen varios nodos, la red seguiría funcionando y la información no se perdería. Ejemplos de tecnologías que utilizan estas tecnologías Blockchain son las criptomonedas, los juegos en red y la distribución de energía inteligente.
Ciber	Cyber	Prefijo, creado por acortamiento del adjetivo cibernético, que forma parte de términos relacionados con el mundo de las computadoras u ordenadores y de la realidad virtual: ciberespacio, cibernauta, ciberseguridad,etc.
Ciberdefensa	Cyberdefense	Capacidad militar plenamente integrada en todos los ámbitos de las Fuerzas Armadas (FAS) y del Ministerio de Defensa (MDEF) en general, así como el resto de actores civiles y militares del ámbito nacional e internacional que comparten riesgos y amenazas a nivel nacional e internacional.
Ciberdelincuencia	Cybercrime	Actividades delictivas que se llevan a cabo a través de medios informáticos o tecnológicos. Los ciberdelincuentes atacan a equipos, dispositivos, personas, empresas, industrias y entidades de distintos tipos incluyendo los gobiernos. Los ciberdelitos no encuentran fronteras ni físicas ni virtuales.

Ciberespacio	Cyberspace	Ámbito virtual creado por medios informáticos. Tejido complejo de redes informáticas y servicios telemáticos a nivel mundial que se ha desarrollado a partir de la llegada de la Microelectrónica, de las Telecomunicaciones, del ordenador personal, del teléfono móvil y de Internet a nuestra sociedad.
Ciberjusticia	Cyberjustice	Incorporación de nuevas tecnologías en el sistema judicial permitiendo realizar juicios a distancia (también llamados juicios telemáticos o juicios online)
Cibernauta	Netizen	Cibernavegante, persona que navega por el Ciberespacio. Ciudadano de la red.
Ciberseguridad	Cybersecurity	Seguridad Telemática y de las Tecnologías de la Información.
Criptomonedas	Cryptocurrency	Monedas virtuales y divisas digitales que utilizan la Criptografía (codificación y cifrado) y el Blockchain para asegurar las transacciones y los pagos por internet. Ejemplos de criptomonedas son Bitcoin y Ethereum (los dos mayores proyectos y comunidades blockchain del mundo)
Cookie	Cookie	Una cookie es un pequeño fichero de texto (*.txt) que guarda información enviada por los sitios web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario. Las funciones más comunes son llevar el control de usuarios (almacena el usuario y la contraseña) y recabar información sobre los hábitos de navegación del usuario. Esto puede significar un ataque contra la privacidad del cibernauta y por este motivo hay que tener cuidado con ellas.
Datos masivos	Big Data	Datos masivos, macrodatos, datos a gran escala.
Digitalización	Digitalization	Acción y efecto de digitalizar. Convertir o codificar información, datos, imágenes, videos o documentos números dígitos o en sistema digital binario (en formato digital)
Dinero electrónico	e-money	Todo valor monetario almacenado en medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita para realizar operaciones de pago y que sea aceptado por una persona física o jurídica distinta del emisor del dinero electrónico.
Electrónica	Electronics	Rama de la física que crea tecnología y productos destinados a aplicaciones de cálculo y transformación de información (informática), control de procesos (industria) y transmisión de la información a distancia (telecomunicaciones).
Electrónica digital	Digital Electronics	Basada en sistemas digitales binarios (2 dígitos = "0" y "1", también llamados bits). Componentes como los microprocesadores y las memorias de almacenamiento de los ordenadores y de los teléfonos móviles se consideran sistemas electrónicos digitales.
Electrónica analógica	Analog Electronics	Basada en sistemas analógicos (pueden tener infinitos valores). Los componentes de los cuadros eléctricos y los amplificadores de sonido para instrumentos musicales se consideran sistemas electrónicos analógicos.
Firma electrónica	Electronic Signature	Todas aquellas firmas mediante las cuales un firmante acepta las condiciones del documento que se está firmando. Se puede realizar a través de la firma manuscrita digitalizada, un botón aceptando las cláusulas de un contrato, una casilla de aceptación de derechos, nuestro usuario y contraseña para acceder al email, etc.… No todas las firmas electrónicas tienen validez jurídica.
Firma digital	Digital Signature	Tipo de firma electrónica que sí tiene validez legal. Se basa en sistemas de criptografía de clave pública (PKI-Public Key Infraestructures) que la dotan como una firma electrónica avanzada para informar, dar fe o mostrar validez y seguridad.
Firma digitalizada	Scanned Signature	Tipo de firma electrónica que consiste en la digitalización de la firma manuscrita.
Hardware (HW)	**H**ard**W**are	Componentes físicos (partes tangibles, "lo que se puede tocar"). Incluye los equipos, dispositivos, placas, componentes electrónicos que forman los sistemas informáticos, electrónicos e industriales.
HTML	**H**yper**T**ext **M**arkup**L**anguage	Lenguaje de programación que se utiliza para crear las páginas Web. Es sencillo y permite combinar gráficos, imágenes, textos y enlaces
HTTP	**H**yper**T**ext **T**ransfer **P**rotocol	Protocolo de transferencia de hipertexto. Es el protocolo de comunicación que se utiliza en la WWW
HTTPS	**H**yper**T**ext **T**ransfer **P**rotocol **S**ecure	Protocolo seguro de transferencia de hipertexto. Es la versión segura de HTTP. Protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web.

Hacker	Hacker	Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora. Persona con grandes conocimientos de Software, Hardware, Bases de datos, Lenguajes de Programación y comunicaciones que se dedica a encontrar fallos en los Sistemas y Redes Informáticas
Hipertexto	Hypertext	Texto relacionado. Formato de texto que te permite enlazar conceptos afines. El usuario, haciendo clic en la palabra subrayada o de distinto color, accede a la información relacionada dentro de las páginas web o del manual online.
Informática	Computing	Rama de la Ingeniería que estudia los métodos, técnicas y procesos para enviar, almacenar y procesar información y datos digitales. Entre otras especialidades se pueden mencionar el Software, Hardware, Sistemas Operativos, Redes de Ordenadores, Bases de Datos, Lenguajes de Programación y Ciberseguridad.
Interactivo	Interactive	Programa o dispositivo que permite una interacción, a modo de diálogo, entre la computadora y el usuario
Internet	**INTER**national **NET**work	Red internacional de ordenadores. Es un conjunto descentralizado de redes de comunicaciones y de dispositivos electrónicos e informáticos. Conjunto de ordenadores y servidores conectados en una red a nivel mundial y que comparten un mismo protocolo de comunicaciones (HTTP)
IoT	**I**nternet**O**f**T**hings	Internet de las cosas conectadas. Se refiere a la interconexión digital de aparatos cotidianos y de dispositivos industriales con internet. Reciben y transfieren datos mayoritariamente a través de redes inalámbricas sin intervención humana.
Microelectrónica	Microelectronics	Electrónica a nivel de micrómetros, a escala del grosor del cabello humano, a escala de un hilo de cobre o del tamaño de las bacterias). Los chips y los microscopios digitales utilizan esta tecnología.
Nanotecnología	Nanotechnology	Ciencia que consiste en manipular la estructura molecular de la materia a escala manométrica, es decir, a escala atómica, molecular o a nivel de ADN. La nanoelectrónica, los nanorobots y los nanomateriales son ejemplos de tecnologías que se están desarrollando actualmente.
Nube (almacenamiento en la nube)	Cloud Storage	Compañías privadas que ofrecen almacenamiento de datos en servidores conectados a Internet. Como ejemplos se pueden citar Google Drive, Dropbox, Microsoft Onedrive, Apple iCloud, Amazon Cloud Drive, etc., ...
Página Web	Web page	Portal electrónico en Internet que puede contener información en diferentes formatos: texto, sonido, enlaces, imágenes, hipervínculos, videos o programas. Su nombre siempre empieza por http://www.nombredelapaginaweb.xyz (donde xyz se denomina el dominio de internet)
PC	**P**ersonal **C**omputer	Ordenador Personal
Software (SW)	**S**oft**W**are	Componentes lógicos (no tangibles, "lo que no se puede tocar"). Programas informáticos
Telecomunicaciones	Telecomms	Sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos, por aire o por cable.
Telemática	Telematics	Telecomunicaciones aplicadas a la Informática.
TIC	Information Technology	Tecnologías de la Información y de las Comunicaciones.
Virtual	Virtual	Que tiene existencia en el contexto de una simulación. Representación digital de algo físico.
Web	Web	Forma abreviada de referirse a la WWW
WIFI	**Wi**reless **Fi**delity	Fidelidad inalámbrica. Tecnología que utiliza el protocolo 802.11x. y que permite a los dispositivo informáticos acceder a Internet desde un router de manera inalámbrica o conectarse a una red sin cables.
WWW	**W**orld **W**ide **W**eb	Red informática a nivel mundial. Sistema interconectado de páginas web públicas y accesibles a través de dispositivos informáticos (PCs, servidores, ordenadores portátiles), electrónicos (IoT, sensores inteligentes) y de telecomunicaciones (teléfonos inteligentes, tabletas)

C) BIBLIOGRAFÍA

- FUENTES: **BOE,** RED.ES **y Ministerio de Industria**
  https://www.boe.es/biblioteca_juridica/publicacion.php?id=PUB-NT-2018-97&tipo=L&modo=2
  - La persona en el Mundo Digital
  - Ciudadanía digital
  - Privacidad en el Mundo Digital
  - Igualdad en el Mundo Digital
  - Responsabilidad en la Red
  - Seguridad y Ciberdefensa
  - Trabajo en el mundo digital
  - Mercado digital y competencia
  - Deportes y Cultura Digital
  - Justicia y derechos digitales
  - Salud en el mundo digital
  - Relaciones internacionales en el mundo digital
  - Sostenibilidad (ciudades inteligentes, Turismo, Energía, Tecnología e Impacto Medioambiental)

- FUENTES: **Universidad de la Rioja y Guardia Civil**
  https://fundacion.unirioja.es/formacion_cursos/view/377/Inteligencia-y-seguridad-La-seguridad-en-el-ciberespacio

  - A nivel Económico: Blockchain y Bitcoin
  - A nivel Ciudad/País: Protección de infraestructuras críticas, Ciberterrorismo
  - A nivel Social: Ciberdelitos

- FUENTE: **Ministerio de Defensa (MDEF)**
  https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
  - Estrategia Nacional de Ciberseguridad 2019

- FUENTE: **Instituto Nacional de Ciberseguridad (INCIBE)**
  https://www.incibe.es/sala-prensa/notas-prensa/el-mercado-ciberseguridad-alcanzara-los-80000-millones-euros-2018

  - Big Data.
  - Cloud Computing.
  - IoT.
  - Smart Cities.
  - Smart Grids.
  - Industria 4.0
  - Redes sociales.
  - Tecnologías cognitivas.
  - Wifi óptico.
  - Sistemas ciber-físicos.
  - Tecnología móvil.
  - Redes 5G.
  - Nuevos modelos de pago.

- FUENTE: **Unión Internacional de Telecomunicaciones (ITU)**
  https://www.itu.int/es/Pages/default.aspx

- Guía de Ciberseguridad para los países en Desarrollo Digital
- Concienciación básica.
- Creación y promulgación de una legislación nacional eficaz.
- Creación de capacidades personales e institucionales.
- Puesta en vigor (dominio de creación de capacidad).
- Creación de estrategias y políticas nacionales sobre seguridad.
- Facilitar el intercambio de información entre países y entre las partes interesadas pertinentes.
- Establecimiento de coordinadores nacionales.
- Supervisión y evaluación del progreso de las iniciativas existentes.
- Implementación de soluciones de respuesta, vigilancia y alerta ante incidentes.
- Evaluación de las vulnerabilidades y amenazas a la ciberseguridad.
- Preparar herramientas y aplicaciones efectivas para la red y la ciberseguridad.
- Asociaciones.
- Cooperación internacional.

- FUENTES: **Instituto Español de Estudios Estratégicos (IEEE), Universidad de Málaga y MDEF**
  http://www.ieee.es/contenido/noticias/2018/05/DIEEEO60-2018.html

  - Geopolítica de la Diplomacia
  - Diplomacia Pública
  - Diplomacia Digital
  - Relación entre diplomacia e inteligencia

- FUENTE: **Universidad Nacional de Estudios a Distancia (UNED)**
  http://revistas.uned.es/index.php/EEII/article/view/23243/pdf

  - Ciberdiplomacia
  - Comunicación institucional

- FUENTES: **Centro de Ciberseguridad industrial (CCI) y Centro Criptológico Nacional (CCN)**
  https://www.cci-es.org/buscador/-/journal_content/56/10694/232182?p_p_auth=uVZ4d0AB

  - Smart Grid (Red de Eléctrica Inteligente)
  - Smart Cities (Ciudades Inteligentes)
  - Smart OT (Tecnologías de Operación inteligentes)

- FUENTES: **Ministerio de Justicia y Fujitsu Corporation**
  https://www.mjusticia.gob.es/cs/Satellite/Portal/es/ministerio/gabinete-comunicacion/noticias-ministerio/justicia-difunde-guia
  https://www.fujitsu.com/es/about/resources/case-studies/ministerio-justicia.html

  - Juicios telemáticos / Juicios virtuales
  - Protocolos de ciberseguridad
  - Sistema eFidelius de grabación de vistas
  - Expediente electrónico
  - Justicia digital

- FUENTE: **Instituto Nacional de Ciberseguridad (INCIBE) - Empresas**
  https://www.incibe.es/protege-tu-empresa/sectoriza2

- Cibersociedad: Los retos sociales y los sectores empresariales
- Ciberseguridad en Educación
- Ciberseguridad en Turismo y Ocio
- Ciberseguridad en Asociaciones
- Ciberseguridad en Construcción
- Ciberseguridad en Industria
- Ciberseguridad en Logística
- Ciberseguridad en Comercio minorista
- Ciberseguridad en Comercio mayorista
- Ciberseguridad en Oficinas

- FUENTE: **Congresos Internacionales de la Lengua Española (INSTITUTO CERVANTES)**
  https://congresosdelalengua.es/cartagena/ponencias/seccion_2/25/avila_raul.htm

  - El Español en el Ciberespacio
  - Terminología de Internet

- FUENTE: **Real Academia de la Lengua Española (RAE)**
  https://dle.rae.es/ciberespacio

  - Prefijo Ciber
  - Definición de Ciberespacio
  - Definición de Cibernauta

- FUENTE: **Universidad Autónoma de Barcelona (UAB) – Gabinete de Comunicación y Educación**
  http://www.gabinetecomunicacionyeducacion.com/en/noticias/el-espanol-se-digitaliza-la-rae-incorpora-terminos-del-ciberespacio-la-23o-edicion-del

  - Términos del Ciberespacio

- FUENTE: **Icon-Icons.com (Iconos gratis)**
  https://icon-icons.com/es/

  - Ilustraciones sobre tecnología, sociedad y Ciberespacio

- FUENTE: **Instituto Nacional de Ciberseguridad (INCIBE) – Glosario de Ciberseguridad**
  https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

  - Virus
  - Ciberseguridad

- FUENTE: **Ministerio de Defensa – Centro Conjunto de Desarrollo de Conceptos (CCDC)**
  https://www.defensa.gob.es/ceseden/en/ccdc/actividades/noticias/noticias/2018/2018_11_concepto_ciberdefensa.html

- Ciberdefensa
- Ciberdelincuentes

- FUENTE: **Ministerio de Defensa – Centro Superior de Estudios de Defensa Nacional (CESEDEN)**
  https://www.defensa.gob.es/ceseden/Galerias/ccdc/documentos/PDC00_GLOSARIO_DE_TERMINOLOGIA_DE_USO_CONJUNTO.pdf

  - Ciberdefensa
  - Ciberespacio

- FUENTE: **Diccionario Hispánico de dudas de la RAE**
  https://www.rae.es/obras-academicas/diccionarios/diccionario-panhispanico-de-dudas

  - Términos Informáticos
  - Términos Telemáticos
  - Términos Cibernéticos

- FUENTE: **Universidad Internacional de la Rioja (UNIR) – Revista Online**
  https://www.unir.net/derecho/revista/que-es-ciberdelincuencia/

  - Ciberdelincuencia

- FUENTE: **Universidad Politécnica de Madrid (UPM) – Archivo digital**
  http://oa.upm.es/cgi/search/advanced/

  - Ciberespacio
  - Telecomunicaciones

- FUENTE: **Agencia de la Unión Europea para la Ciberseguridad (ENISA)**
  https://www.enisa.europa.eu/

  - Legislación Europea
  - Ciberseguridad

TEXTOS COMPLEMENTARIOS APORTADOS POR LOS PONENTES.

1ª Mesa redonda. Diplomacia digital y cooperación internacional.

Moderador Jornada: José María López Jiménez.

Director Responsabilidad Social Corporativa UNICAJA Banco.

https://vimeo.com/497908793

Embajador Juan José Escobar Stemmann.

Embajador del Reino de España en Irak. Ministerio de Asuntos Exteriores y Cooperación.

C.V.: *Nacido en Málaga, ha desempeñado la Segunda Jefatura de las Embajadas de España en Bulgaria, Nicaragua y Jordania. Fue también Secretario de la Embajada de España en Marruecos y Cónsul de España en Buenos Aires. En 2011 fue nombrado Embajador en Misión Especial para Asuntos Mediterráneos en el Ministerio de Asuntos Exteriores español. Desde 2013 a 2016 fue Cónsul General de España en Jerusalén. En agosto de 2016 fue nombrado Vicepresidente del Comité Militar Permanente entre Estados Unidos y España en el Ministerio de Defensa. Desde abril de 2017 es Embajador de España en Irak.*
Es especialista en asuntos árabes e islámicos. Ha publicado varios libros colectivos y numerosos artículos sobre el activismo islámico, la reforma política en el mundo árabe y las relaciones Euro-Mediterráneas. Ha sido profesor de temas políticos árabes en el Instituto Gutiérrez Mellado para los Estudios de Defensa, en la Escuela Diplomática Española en Madrid y en el Centro de Estudios de Defensa del Ministerio de Defensa español. Es profesor colaborador honorario del departamento de derecho internacional público de la Facultad de Derecho de la Universidad de Málaga. En 2017 fue elegido miembro del Consejo Científico del Real Instituto Elcano. Desde 2018 es miembro del Consejo Científico de CIFAL Málaga (International Training Center for Authorities and Leaders) integrado en el Instituto de NNUU para la Formación Profesional e Investigaciones (UNITAR). Desde 2020 es miembro del Consejo Científico del Foro para la Paz en el Mediterráneo.

DIPLOMACIA DIGITAL.

1. En los dos últimos años se ha producido una verdadera eclosión en el uso de las redes sociales por parte de Ministerios de Asuntos Exteriores, Embajadas y Consulados, expansión que, en la arena internacional, se produce en paralelo a la utilización que de ellas hacen los políticos y muy especialmente los líderes mundiales. Todos competimos por la atención de una audiencia global ofreciendo nuestra propia narrativa, y los nuevos medios y plataformas digitales (sobre todo Tweeter y Facebook) se convierten en el nuevo campo de batalla político. A este uso de las redes sociales por parte de los diplomáticos se ha denominado DIPLOMACIA DIGITAL.

Sin embargo, el concepto va mucho más allá. El contexto internacional en el que operan los Ministerios de Asuntos Exteriores está cambiando rápidamente como consecuencia de una serie de factores que están transformando la diplomacia contemporánea.

En los últimos 25 años, el desarrollo de la globalización, la aparición de los grandes medios audiovisuales o más recientemente la consolidación de Internet y las nuevas plataformas digitales han provocado un aumento de la velocidad con la que ocurren los hechos en la sociedad internacional y han transformado el medio en el que la diplomacia clásica ejercía sus funciones.

2. La sociedad internacional del siglo XXI se caracteriza por la expansión del número y variedad de actores internacionales no estatales que obliga al establecimiento de nuevas redes de relaciones basadas en el conocimiento y en la experiencia; una nueva agenda de seguridad internacional centrada en la seguridad del individuo que ha ampliado el número y la complejidad de los temas que deben abordar los estados, y la aparición de las agendas diplomáticas regulatorias para hacer frente a situaciones de crisis globales que exigen soluciones globales.

Pero, paradójicamente, también caracteriza a esta nueva sociedad internacional el resurgimiento de las agendas políticas tradicionales, producto de la competencia entre estados, o la progresiva fragmentación de las normas y reglas que gobiernan sus relaciones políticas y económicas. En este contexto cambiante e incierto, la diplomacia juega cada vez un papel más relevante. Sigue siendo esencial para proteger y promover los intereses nacionales, pero también desempeña un papel fundamental para promover el desarrollo de la gobernanza global y la seguridad internacional.

3. En este nuevo entorno, algunos hablan de una diplomacia integradora, en la que los diplomáticos han dejado de ser los guardianes de las fronteras de lo exterior para convertirse en facilitadores que integran a los distintos actores y ambientes que conforman el nuevo medio diplomático. Otros prefieren hablar de diplomacia en red. La emergencia de nuevos actores con capacidad para influir en la agenda de las relaciones internacionales obliga a la creación de redes entre estados y actores no estatales para gestionar asuntos que exigen recursos comunes. Los diplomáticos deben desarrollar enfoques de red, adaptar los medios de trabajo a un contexto cambiante, y definir estrategias para acomodar intereses y demandas de otros participantes.

Tanto los defensores de la teoría de la diplomacia integradora como los de la diplomacia en red han tratado de establecer un marco para comprender, entre otras cuestiones, los cambios que ha provocado en la diplomacia el aumento de la complejidad de los modelos de comunicación, provocada por la irrupción de Internet y las nuevas plataformas digitales, ejes sustantivos del proceso de globalización.

4. Por ello, el término diplomacia digital, que utiliza por primera vez Wilson Dizard en un artículo publicado en 2001, ha terminado convirtiéndose en el concepto usado para tratar de explicar las transformaciones que está experimentando la diplomacia como consecuencia de los cambios arriba comentados.

Internet y las nuevas plataformas también han reducido drásticamente el tiempo de respuesta con el que cuentan los gobiernos para reaccionar ante un determinado evento, dando lugar a lo que el profesor de periodismo de la Universidad del Sur de California Philip Seib ha denominado diplomacia en tiempo real. Como ejemplo se menciona el tuit que publicó un ingeniero de Abbottabad en la noche en la que comandos norteamericanos asaltaban la casa en la que estaba escondido Bin Laden y que obligaron a la Casa Blanca a anunciar la operación mucho antes de lo que tenían previsto.

Las nuevas tecnologías también pueden potenciar los daños a la reputación de un país como consecuencia de la publicación en las redes sociales de un determinado suceso. Un ataque sufrido por un estudiante indio en Australia hace unos años, cuya noticia se extendió rápidamente por las redes sociales, provocó una drástica reducción del número de estudiantes indios en Australia al año siguiente.

5. Hay varios modelos de diplomacia con necesidades de comunicación diferentes. La diplomacia pública, actuación consular. Hoy nos vamos a detener en su componente político, que gira en torno a tres elementos básicos: la gestión del conocimiento, la negociación, y a lo que algunos autores han denominado nueva geoestratégica digital.

Uno de los elementos básicos a la hora de analizar los aspectos políticos de la diplomacia digital es el conjunto de ideas que dan forma y garantizan la gobernanza de Internet y los nuevos medios digitales. Fue la Secretaria de Estado Hillary Clinton la que en septiembre de 2009 lanza por primera la idea de la libertad de Internet como principio básico de la política exterior norteamericana, aunque sus contornos definitivos no quedarían establecidos hasta el año 2011.

Más complejas, y sobre las que nos vamos a centrar, son las cuestiones ligadas a la ciberseguridad, que también forman parte de la geoestratégica digital y cuya promoción se ha convertido en un elemento esencial de la acción exterior de los estados.

En España, la Estrategia de Acción Exterior sitúa a la ciberseguridad en un lugar prioritario de la política exterior española. Nuestro país está representado, en el Grupo de Expertos Gubernamentales de NNUU sobre los Avances en la Información y las Telecomunicaciones en el contexto de la Seguridad Internacional, por el Embajador en Misión Especial para la Ciberseguridad.

6. Los ataques cibernéticos se han convertido en una verdadera pesadilla para todos los gobiernos. El pasado verano, el Parlamento noruego, la Bolsa Aukcland, el Vaticano, fueron objeto de ataques, extorsión o espionaje. Pero son sólo la punta del iceberg, pues los ciberataques son diarios.

Desde hace años hay posibilidad de un ataque como Pearl Harbour contra las infraestructuras críticas digitales, pero con mayores riesgos y ataques menores. Ejemplos tenemos en 2017. Microsoft Windows. Virus WANACRY. 300.000 ordenadores en 150 países. Servicio Nacional de Salud de UK. Cancelación 19.000 citas. Pérdidas 100 m$. Total 4.000m$. Corea Norte. El problema es la facilidad con la que actores geopolíticos o criminales se aprovechan de las vulnerabilidades del mundo digital.

7. MARIETJE SCHAAKE, Presidenta del Instituto de Ciberpaz, Universidad de Stanford. Las Instituciones democráticas deben asegurar la seguridad en el ciberespacio. Para ello deben reconocer que han cedido demasiado espacio al sector privado. Las autoridades dependen de las compañías privadas. No tienen acceso a la forma en que éstas desarrollan el software de hospitales o compañías eléctricas. Esto les ha dado a estas una posición dominante. Incluso las agencias de seguridad nacional están en la difícil situación de depender de datos comerciales para cumplir sus deberes.

Las compañías privadas construyen la arquitectura del mundo digital y gobiernan el flujo de datos. Son a menudo las víctimas de estos ataques, pero también cómplices cuando no pueden proteger la información de sus clientes.

Ausencia de mecanismos que garanticen la cooperación internacional. Y los Estados son incapaces de controlar la actividad de las compañías privadas.

8. Ayudas a Estados totalitarios. Este desequilibrio entre el sector público y el sector privado en los países democráticos es obvio en otros ámbitos. La venta de armas cibernéticas a regímenes autoritarios. Lo que Yuval Noah Harari denomina las nuevas tecnologías de vigilancia.

No hay leyes que les impidan hacerlo. Cuando las empresas venden a gobiernos autoritarios minan los objetivos de la política exterior de sus países. Ejemplo empresa italiana AREA para controlar Facebook y búsquedas en Google ha vendido a Siria, Egipto, Irán, o Saudí Arabia.

Este es un mercado en alza, en el que se mueven cientos de miles de millones al año. China ha entrado con fuerza en ese mercado. Es líder en tecnologías que permiten la represión en la red, el reconocimiento facial y sistemas de predicción de comisión de delitos.

Estas tecnologías en manos de actores no estatales también pueden hacer mucho daño. En 2015 por ejemplo, JP Morgan sufrió el ataque de un hacker y comprometió 83 millones de cuentas. Este año un chico de 17 años hackeó las cuentas de 130 personalidades en Twitter, entre ellas Biden y Obama. Aunque lo que pretendía era enviar bitcoins a una cuenta podría haber hecho muchísimo más daño.

Los Estados tienen problemas para regular el mundo digital y el mercado de ciber armas. Hace poco Facebook demandó a la compañía israelí NSO por haber vendido las vulnerabilidades de WhatsApp para extraer información ilegalmente. NSO vendió este producto a 45 países entre ellos México y la propia España.

9. Necesidad de cooperación internacional y en el papel de la diplomacia. Las naciones democráticas deben dictar normas que garanticen la seguridad en el mundo digital. Deben firmarse acuerdos internacionales para hacer frente a las amenazas en el ciberespacio.

Los gobiernos democráticos deben tomar medidas para equilibrar el poder entre el estado y las compañías privadas. Hay que identificar qué sistemas digitales son vitales para el interés público y el funcionamiento de la sociedad. Por ejemplo, el sistema de voto o las infraestructuras críticas.

Hay que responsabilizar a las empresas privadas para que respondan por las consecuencias de sus productos. Hay que determinar también cuando las funciones estatales y los sistemas vitales no pueden ser gestionados por empresas privadas.

Un ejemplo aquí lo da la empresa CLEARVIEW, especializada en reconocimiento facial. Numerosos departamentos de policía se han convertido en clientes de esta empresa. Este mismo año un ataque contra la base de datos de dicha compañía demostró que estaba vendiendo su tecnología a otras empresas compartiendo información de los particulares sin su consentimiento. No se debería permitir obtener datos de rostros humanos en internet para venderlos a las agencias policiales.

La mayor parte de las compañías tecnológicas que operan en el ciberespacio mantienen secretos comerciales y acuerdos de no divulgación que impiden a los Estados saber cómo funcionan. Ello no permite a los gobiernos conocer las amenazas reales y los riesgos de sus actividades.

Estos obstáculos legales no permiten tampoco investigaciones sobre los efectos intencionados y no intencionados de los productos que venden. Los gobiernos deberían dictar normas para obligar a estas compañías a que permitan el acceso a esta información.

Los gobiernos deberían también cortar los lazos estrechos que existen entre estas compañías y los servicios de inteligencia. Limitar las exportaciones a los regímenes represivos. La adopción de multas importantes,

exigir responsabilidades criminales o prohibir la venta de determinados productos digitales podría tener un efecto inmediato.

La vigilancia, el robo de datos o el hackeo no deberían considerarse servicios comerciales legítimos. Hay que evitar que agentes de inteligencia sirvan un día al estado y al otro desarrollen sistemas de hackeo militar. DARKMATER, ex miembros de la NSA o del Mosad.

Las sociedades democráticas deben trabajar más para dar a conocer a la población el daño provocado por los ciberataques. Todos debemos ser conscientes de la importancia de la seguridad en el ciberespacio.

Dr. Jamal-Eddine Mechbal.

Antiguo Diplomático de la Embajada del Reino de Marruecos en España.

C.V.: *Estudió en la Escuela Nacional de la Administración Pública en Rabat y cursos monográficos para el doctorado en Derecho en la Universidad Autónoma de Madrid. En 1977 formó parte del Cuerpo Diplomático de la Embajada del Reino de Marruecos en Madrid. Ocupó varios cargos en Marruecos y fue sucesivamente Encargado de Estudios en el Gabinete del ministro de la Planificación y en el gabinete del Ministro de Transportes. Finalizó su carrera como Ministro Plenipotenciario en la Misión Diplomática del Reino de Marruecos en Madrid. Participa en varias conferencias y coloquios. Colabora en el diario digital Atalayar y tiene publicados en medios españoles y marroquíes gran cantidad de artículos y trabajos en varios temas, especialmente sobre cooperación bilateral y los movimientos migratorios.*

COOPERACIÓN ENTRE MARRUECOS Y ESPAÑA.

En este encuentro quiero resaltar la situación geoestratégica de Málaga, como capital de una provincia andaluza que, junto a la provincia de Cádiz, es la capital de provincia más próxima a Marruecos y del continente europeo a África. Estamos en el mundo de la globalización en el que se instauró la cooperación y en el que todos intentan salir ganando, repartiendo los dividendos y eliminando fronteras y barreras para levantar espacios económicos. El ciberespacio facilita mucho todo tipo de relación y comunicación.

Málaga, parte del espacio europeo, tiene justo enfrente dos espacios económicos, el Oriente Medio y Norte de África (MENA) junto a la Comunidad Económica de Estados de África Occidental (CEDAO). La primera formada por 19 países y una población de unos 380 millones de personas y la segunda formada por 15 países de África occidental que establecen una Zona de Libre Comercio en torno a un mercado de 261,13 millones de personas. Marruecos, que pertenece a la zona MENA, solicitó también su ingreso en la CEDAO. Además de estos dos importantes espacios, Málaga tiene enfrente el resto del continente africano. Todo un potencial económico y humano con gran futuro para el resto del mundo. Málaga es el puente entre Europa y esos grandes espacios económicos del futuro.

España y Marruecos, junto con Francia, son los únicos países del Mediterráneo con la ventaja de acceso marítimo al Océano Atlántico, y en este contexto, Málaga está en una situación privilegiada a pocos kilómetros del estratégico Estrecho de Gibraltar.

La posición política y económica de Marruecos, junto a su proximidad geográfica e histórica facilitó que, en 2008, la UE y Marruecos acordasen el reforzamiento de las relaciones bilaterales mediante un Estatuto Avanzado. Es una relación mucho más estrecha que una asociación, pero sin llegar a la adhesión. Esta

situación le permite contar con las ventajas de los miembros que componen la UE salvo su presencia en las instituciones. Con este acuerdo, por primera vez un país no europeo, puede beneficiarse de muchas ventajas, sin formar parte de las instituciones europeas.

El Monarca Hassan II a menudo repetía que "Marruecos parece un árbol cuyas raíces nutritivas se hunden profundamente en la tierra africana, y que respira gracias a su follaje susurrante a los vientos de Europa". Esta interesante parábola se concreta en la política de desarrollo y los grandes proyectos que se llevan a cabo aprovechando su proximidad a Europa donde respira, mientras consolida sus raíces africanas.

Por ello se fijó tres objetivos, conexos entre sí, sobre los cuales gravita su política de cooperación internacional en materia de desarrollo económico y social:

- Convertirse en una plaza privilegiada para atraer inversiones internacionales.
- Constituirse en inversor activo en el continente africano.
- Paralelamente, constituirse en el enlace perfecto para la circulación de los negocios, para operaciones triangulares en África.

Marruecos cuenta para tal fin con:

- Estatuto Avanzado en sus relaciones con la UE.
- Acuerdo de libre comercio con EE. UU.
- Otros importantes acuerdos con China, Rusia e India entre otros.

Así pues, se constituye para estos socios en un atractivo país para atraer inversiones y un perfecto enlace para acceder a África. Y todo lo que ha sido válido para el mundo tradicional, lo es ahora para el virtual.

La Región Tánger-Tetuán-Alhucemas

a) Puerto Tánger-Med.

Ubicado en el Estrecho de Gibraltar, entre el Mediterráneo y el Océano Atlántico, sobre la segunda ruta marítima más concurrida del mundo, con más de 100,000 embarcaciones al año entre Asia, Europa y América del Norte. Gran puerto de última generación a 40 km de Tánger y a solo 14 Km de Europa.

El puerto Tánger Med está clasificado como el primer puerto de África y clasificado en el puesto 20 de los puertos de contenedores más grandes del mundo. Su principal actividad es el trasbordo de contenedores cargados en buques portacontenedores gigantes que descargan sus mercancías sin desviarse de su ruta y parten de inmediato, luego cargan en él a barcos más pequeños para servir a puertos de segunda clase. África es el primer mercado de destino con el 38%, Europa el segundo con 27%, Asia con 26% y América con el 9%.

b) Zona Franca.

Junto al puerto se edificó una zona franca para más de 900 empresas en diversos sectores (automotriz, aeroespacial, logística, textiles y comercio), que cuenta con 70 mil empleados y representa una facturación anual de 8,000 millones Euros.

c) La ciudad tecnológica Mohamed VI de Tánger.

Es un proyecto creado en asociación entre el sector público y el privado marroquí y chino, para constituir un "hub" o nudo económico hacia los países africanos, con una inversión de unos diez mil millones de dólares.

Es una Smart City o ciudad inteligente, que albergará 300 mil habitantes. Creará 100 mil empleos y generará 11 mil millones de dólares en 10 años. Es una ciudad destinada a la industria del automóvil, la aeronáutica, las energías renovables, telecomunicaciones, fabricación de productos farmacéuticos, la agroindustria, los equipos de consumo, los transportes y el comercio, además de un espacio habitable con otras comodidades.

Tren de alta velocidad y la red ferroviaria

Paralelamente al proyecto Tánger Med y la ciudad tecnológica, hace menos de un par de años se inauguró el tren de Alta Velocidad. Es un tren AVE que une Tánger con Casablanca en 2h10, en vez de 5 horas y al final del 2020 ha quedado en solo 1 hora. Con ello mejora la conexión entre Tánger, puerta de entrada de Marruecos, y Casablanca como capital industrial, convertida en un importante centro financiero africano.

El proyecto del AVE prevé dos ejes; el de Casablanca-Oujda en 3 horas (línea Magreb, 600 km) y el de Tánger-Casablanca-Agadir en 4 horas (línea atlántica, 900 km). Por otro lado, los estudios preliminares de construcción del Túnel de Gibraltar prevén un enlace ferroviario África-Europa que hará posible el trayecto de AVE Rabat-Madrid en seis horas y Rabat-París en diez horas.

Red de autopista transmagrebí y aeropuertos

Es un proyecto de autopista magrebí que cruzará Mauritania, Marruecos, Argelia, Túnez y Libia. Se compone de un eje atlántico desde Nuakchot-Rabat-Tánger y otro mediterráneo desde Rabat hasta Trípoli a través de Argel y Túnez. La parte marroquí es (1.046) km, la argelina (1.216 km), la tunecina (780 km), la libia (200 km).

En Marruecos, la autopista ya está operativa entre Tánger-Rabat-Casablanca- Marrakech-Agadir y hacia el éste desde Rabat-Fez hasta Oujda ciudad fronteriza con Argelia. El impacto socio económico de la autopista transmagrebí enlaza a 55 ciudades con población total de más de 50 millones de habitantes (la población magrebí alcanza los 90 millones). Es una autovía estratégica para la economía y el desarrollo de cada región del Magreb, del mismo espacio magrebí y para el enlace de Europa - Magreb, gracias al tramo ya en funcionamiento en Marruecos a partir de Tánger y para África subsahariana. También cuenta con 22 aeropuertos operativos.

Marruecos en África

En los años setenta es cuando empieza el nacimiento de una burguesía marroquí que hoy día ya es dinámica y consolidada. Actualmente juega un papel decisivo en la economía y los mercados, no solo dentro de Marruecos sino en la cooperación internacional, junto con el sector público y el gobierno, sobre todo en África.

África cuenta hoy con la presencia de grupos y entidades marroquíes en sectores como la Banca, seguros, construcción, telecomunicaciones, minería. Se puede citar en el sector financiero Attijari Wafa Bank, la BMCE, la Banque Populaire y el holding Yenna, en seguros IAM, en el sector construcción Addouha, en telecomunicaciones la empresa de telefonía e internet Ittissalat Al Maghreb, en minería la sociedad Manajim y el grupo Oficina Jerifiana de Fosfatos OCP.

El grupo marroquí Telecom

Telecom está cumpliendo un papel importante en el desarrollo de las telecomunicaciones en África. Se encuentra implantado en países como Benín, Burkina Faso, África central, Costa de Marfil, Gabón, Mali, Mauritania Níger y Togo.

Extendió cables de fibra óptica en varios países de África enlazándolos con Europa dentro de un ambicioso plan global. En este contexto extendió desde Marruecos un tendido de cable óptico de 5.300 Km a través de Mauritania, Mali y Burkina faso llegando a Níger.

Office Chérifien des Phosphates (OCP)

Es uno de los principales exportadores de fosfato crudo, ácido fosfórico y de fertilizantes de fosfato en todo el mundo. Un mercado donde Marruecos controla el 70% de las reservas mundiales del mineral. (50 mil millones de toneladas, muy por delante de China, que ocupa el segundo lugar, con sus 3,3 mil millones de toneladas). De hecho, tal concentración de recursos minerales en un solo país es un caso único en el mundo.

Los investigadores del OCP están trabajando sobre las posibilidades de extraer del fosfato tierras raras y materiales como el flúor y el uranio. Tierras raras actualmente están en el corazón de una futura batalla por el posicionamiento global en el que China ya está jugando a ser líder, pues el juego bien vale la pena.

El grupo de fosfatos marroquí “Office Cherifiana des Phosphates” (OCP) creó en África una filial bajo el nombre de OCP África. Su objetivo es entrar en el mercado africano de fertilizantes, que cuenta con atractivas perspectivas ya que en África se consume diez veces menos que el promedio mundial de fertilizantes. Las perspectivas para el crecimiento y desarrollo de productos innovadores en África son enormes. En África se están llevando experimentos con nuevos fertilizantes de diseño en varios países.

También se han lanzado varias iniciativas: establecimiento de mapas de fertilidad del suelo en Etiopía y Costa de Marfil, desarrollo de fertilizantes adecuados para el maíz (Kenia, Nigeria), cacao (Costa de Marfil, Nigeria) y algodón (Malí, Burkina Faso, Costa de Marfil, Togo, Benin).

El OCP creó 14 filiales en un continente donde el crecimiento de la demanda es del 20% anual. También la construcción de dos unidades de producción a gran escala. En Nigeria y en Etiopía para una producción de 3.8 millones de toneladas por año. En el Cuerno de África, con el gigante saudí de aluminio y fosfatos Ma’aden, el objetivo es servir al enorme mercado de África Oriental

El Gaseoducto Nigeria-Marruecos

Nigeria (primer exportador de África de gas natural licuado y el quinto a nivel mundial) y Marruecos, siendo la puerta de salida hacia Europa, proyectan construir un gasoducto que atraviese 16 países de África occidental. Además de suministrar energía a Europa, el megaproyecto pretende electrificar las regiones africanas a su paso. Ello conlleva crear industrias: agroalimentaria, fábricas fertilizantes, y una cooperación interregional y de integración entre esos países. También permitirá desarrollar polos industriales integrados en subregiones africanas.

Es un gigantesco proyecto de cooperación entre África y Europa, que crea riqueza a su paso y mejorará el futuro de África Occidental, mediante su desarrollo socioeconómico, permitiendo mayor cooperación

regional entre sus miembros y su integración, creando con ello más riqueza y menos pobreza, generando empleo siendo estos el mejor remedio contra la emigración.

El sector de electricidad y energía renovable

Marruecos adoptó, desde 2009, un plan estratégico de transformación energética para alcanzar en el 2030 la integración de las energías renovables al 52%. El ambicioso objetivo no se limita a cubrir las necesidades internas del Reino, sino situarse también como el primer proveedor de energías renovables hacia Europa y convertirse en plataforma industrial para la energía limpia en África. Esta transición hacia energía limpia está centrada sobre el desarrollo de energías de origen solar, eólico e hidráulico.

Siete años después, en 2016, Marruecos puso en funcionamiento la primera fase de una planta generadora de energía solar, la más grande del mundo, situada en Ouarzazat sobre un área de 3 000 ha y lleva por nombre Noor-Ouarzazat. Hoy ya superó el 42% quedando a solo el 10% del objetivo marcado para el próximo decenio.

También en la localidad de Midelt empezaron los trabajos de otra planta, un proyecto llamado Noor – Midelt. El consorcio formado por la eléctrica francesa EDF, la compañía Masdar de Emiratos y la empresa marroquí Green of África ha seleccionado a la española TSK para el diseño y construcción de la planta solar. El proyecto contará con la financiación de entidades como el Banco Alemán de Desarrollo KFW, el Banco Mundial, el Banco Africano de Desarrollo (BAD), el Banco Europeo de Inversiones (BEI), la Agencia Francesa de Desarrollo, la Comisión Europea y el Clean Technology Fund.

Marruecos está desarrollando parques eólicos sobre todo en el norte de Marruecos, en la región Tánger-Tetuán- Alhucemas y en el sur en la región de Tarfaya. En los proyectos participan empresas españolas entre ellas ENDESA e Iberdrola. Por otra parte, en el marco de la extensión de la red eléctrica a la región sur de Marruecos, se está llevando a cabo un tendido de línea de 400 kV a lo largo de 1200 km que vincula la ciudad de Ágadir con varias ciudades y localidades del sur. Este proyecto es una verdadera autopista de electricidad que conectará Marruecos con Mauritania.

Partenariado Marruecos Mauritania

El importante incremento de la demanda de electricidad en Marruecos y Mauritania constituye un motivo para una cooperación que garantice el suministro en beneficio del desarrollo de los dos países. Por ello, en el marco del partenariado estratégico entre las entidades del sector eléctrico de los dos países se está trabajando en la integración de los dos mercados eléctricos y el desarrollo de infraestructuras de producción y transporte de electricidad entre el Reino de Marruecos y Mauritania que puede extenderse por África subsahariana, que sufre de grandes y graves deficiencias en el suministro eléctrico. Es un próspero mercado para un futuro próximo, tanto para África como Europa que pueden conectarse a través de España, con quien ya existe una importante colaboración hispano-marroquí plasmada en una conexión por cable submarino, además de un gaseoducto que transporta el gas argelino. En este sentido y para tener una visión global y de prospectiva sobre el espacio africano en materia de electrificación, cabe resaltar el gran déficit y las grandes oportunidades y posibilidades que se ofrecen.

África actualmente es el continente donde se consume menos electricidad en el mundo con solo un 18,5 % de la media mundial. La energía total consumida apenas supera a la consumida en Alemania. Además, está focalizada en Sudáfrica y en el Norte de África donde la electrificación alcanza el 100%, lo que demuestra la gran disparidad del reparto y la enorme carencia. Menos del 10% del territorio africano está cubierto por

redes de distribución eléctrica. Esto nos da una idea sobre el gran mercado para la producción, el transporte y la distribución de la energía eléctrica. Teniendo en cuenta que donde no hay luz, no solo reina la oscuridad, sino lo más grave aún, crece la proliferación del oscurantismo en todos sus sentidos y dimensiones.

La Zona del Estrecho de Gibraltar en prospectiva

Gracias a las infraestructuras de ferrocarriles, carreteras, zonas francas, el puerto Tánger Med y la próxima ciudad tecnológica Mohamed VI, ubicados en la zona sur del Estrecho de Gibraltar, se ofrece una excelente oportunidad para la cooperación interregional con Andalucía y la Región Tánger-Tetuán-Alhucemas, como también con Ceuta y Melilla. Una zona a ambos lados del Estrecho que constituiría un núcleo de cooperación hispano marroquí en el marco de las regiones exteriores de la UE, con MENA, CEDAO y resto de África.

DEMOGRAFÍA Y MIGRACIONES

Panorama

Otro aspecto de vital importancia a considerar es el demográfico, entre una África fértil y en gran auge de natalidad frente a Europa. Hasta finales de siglo, nacerán 40 millones de habitantes cada año. Casi el equivalente de toda la población española. Actualmente viven en África casi 1.300 millones de habitantes, el 16% de la población mundial. En los próximos ochenta años, en el 2100, serán previsiblemente 4.500 millones, el 40% de todos los habitantes del mundo. A corto plazo, en los próximos treinta años, África contará en el 2050 con 2.500 millones de habitantes. Estas cifras nos dan una idea de la dimensión de los desafíos y retos, como también, las posibilidades de una verdadera cooperación global y a gran escala.

La situación en los países de la UE y del hemisferio norte en general es totalmente diferente. Según datos recientes del 2018 Europa necesitará unos 7 millones de inmigrantes anuales hasta 2050 (200 millones en 30 años). En España, solo para salvar el sistema de la seguridad social se necesitarían 5,5 millones de inmigrantes durante los próximos treinta años. Además, según proyecciones demográficas de la OCDE y otros organismos como el Fondo Monetario Internacional (FMI), las bajas tasas de natalidad unidas al aumento de la esperanza de vida harán que España se convierta, en un futuro cercano, en el segundo país más envejecido del mundo.

El actual ministro de Seguridad Social, Inclusión y Migraciones José Luis Escrivá Belmonte durante un foro organizado por la OCDE en enero 2020 en París ofreció cifras más actualizadas; la de una media de 270 mil inmigrantes por año hasta el 2050. Dijo, basándose en estudios más recientes, que para contrarrestar el proceso de envejecimiento de la población en España y prevenir sus consecuencias, habría que atraer a España entre 8 y 9 millones de inmigrantes durante los próximos 30 años, y que lo que hace falta es una perspectiva a medio plazo y hacer pedagogía porque “las tendencias demográficas están ahí”.

La inmigración irregular

En la actualidad la inmensa mayoría de la mano de obra extranjera que se encuentra en los mercados de trabajo procede de una inmigración irregular. Pero hoy esta inmigración irregular debe cesar porque atenta contra los derechos de los trabajadores, fomenta la competencia desleal, la economía sumergida y constituye un tema que preocupa a la seguridad nacional.

Inmigración regular

Todo el mundo está a favor y reclama una inmigración regular y ordenada. Pero sorprende, y mucho, precisamente la ausencia de acuerdos de mano de obra que permitan contratar mano de obra de manera regular y ordenada en países de origen. Acuerdos como los que estaban en vigor hasta mediados de los setenta, firmados entre países de inmigración, como Alemania, Bélgica, Francia, Holanda, Gran Bretaña etc.., con otros países de emigración como los del Magreb, España y Portugal. Acuerdos de mano de obra que reglamentaban la emigración mediante la contratación en el mismo país de origen por parte de empresas solicitantes de la mano de obra.

Por lo tanto, es necesario crear un observatorio de inmigración o un centro de estudios migratorios que realice trabajos sobre las necesidades conforme a la situación económica y social, realizando estudios de prospectiva. elaborando programas de cooperación con países de la emigración en favor de contingentes de una inmigración regular, ordenada y planificada. Inmigración que incluya formación profesional según las necesidades de la demanda y una formación socio educativa en la que se imparta en el país de origen una enseñanza básica del idioma, costumbres y conductas sociales del país de acogida, que el inmigrante debe adoptar para evitar comportamientos inadecuados, como también pretextos para que otros justifiquen sus eventuales xenofobias.

Paralelamente hay que fomentar en la sociedad la cultura del respeto hacia el inmigrante y la correcta acogida, valorando su cultura y su dimensión humana y no contemplarlo solo como brazos y músculos para la producción. Porque la educación, cultura y el respeto mutuo son las mejores vacunas contra la xenofobia y permiten la buena convivencia. Faltando estas, aumentan las otras. Sobre todo, no conviene insultar el futuro ni escupir en el plato en el que juntos vamos a comer mañana.

Acuerdo de mano de obra con Marruecos

Marruecos y la UE pueden establecer una buena cooperación en materia de una migración ordenada y planificada superando el papel actual de país tampón y mero gendarme para evitar la inmigración irregular a Europa. Admitiendo sobre su suelo a subsaharianos, ello no puede sostenerse a la larga si no es acompañada con otros proyectos de refuerzo en el marco de una política común en materia de migraciones entre la UE y Marruecos. Es imprescindible evitar que con el tiempo la situación creada dentro de Marruecos, como consecuencia de la inmigración fallida a Europa por subsaharianos que quedan atrapados en Marruecos se convierta en insostenible a todos los niveles.

También, es importante alcanzar acuerdos para asegurar que la inmigración sea legal, que las personas que cruzan el Estrecho de Gibraltar puedan acceder al mercado de trabajo y tengan una residencia legal para trabajar en los países de la UE. Prever también un estatus especial para trabajadores fronterizos entre la costa africana y la UE o simplemente Marruecos en vistas de su estatus especial. Una cooperación sobre una inmigración regular y ordenada puede establecerse tanto a nivel de la UE y Marruecos, como también a nivel bilateral entre los dos países. Cooperar juntos en la gestión de una inmigración regular ordenada sería muy positivo para Europa y España, como para Marruecos y África, tanto a nivel de mano de obra como de equilibrio demográfico.

Sería aconsejable crear en Málaga un observatorio o centro de migraciones para estudiar todo lo que precede y en especial las necesidades demográficas y las de la mano de obra en Europa, a largo, medio y corto plazo contrastadas con las posibilidades demográficas que se ofrecen en África para unas migraciones planificadas. Realizar trabajos y confeccionar programas exhaustivos basados en demandas previstas, perfiles, ofertas, formación en origen y criterios de selección en función de años. Las herramientas digitales actuales permiten facilitar su gestión.

También a nivel bilateral España Marruecos, se pueden estudiar nuevas formas de cooperación sobre una inmigración regular y ordenada mediante:

- Fijación de cupos según las necesidades de mano de obra a medio plazo.

- Formación en Marruecos, según la demanda y especialidades, en favor de los candidatos a la inmigración, enseñando además un lenguaje español básico y las normas cívicas y costumbres españolas que hay que respetar como conducta de convivencia.

- Acuerdos fronterizos que consideren la costa andaluza y la zona norte de Marruecos, como zonas fronterizas, dando más facilidad y flexibilidad para el desplazamiento y trabajo entre las dos zonas.

Conclusión

Es necesario insistir en que África es una muy buena oportunidad que se brinda a Europa. Entre estos dos continentes, Marruecos y España, juntos, pueden jugar un papel esencial como enlace.

Con imaginación, prospectiva y altas miras dentro de una globalización, Marruecos y España pueden jugar un papel determinante en favor de sus dos pueblos y de los grandes espacios a los que pertenecen, ofreciéndose mutuamente soluciones y oportunidades, económicas, sociales, políticas y demográficas. Deben cooperar juntos para superar deficiencias y alcanzar logros de difícil alcance sin la contribución del uno con el otro. Las telecomunicaciones, videoconferencias, herramientas digitales, transacciones electrónicas e Internet permiten usar el Ciberespacio para acercar a ambos pueblos y sus empresas, con unas posibilidades hasta ahora inexistentes, las cuales pueden facilitar mucho las relaciones comerciales en beneficio mutuo.

Ortega y Gasset en su obra “España invertebrada”, ya hacía referencia a la importancia del “periodo formativo y ascendente”. Hoy día ese periodo formativo o proceso integrador adquiere aún más importancia en el mundo de la globalización. Sobre todo, tal y como resaltaba Gasset, que también la decadencia puede dar lugar a “una vasta desintegración”. Fenómeno que venimos observando hoy en separatismos y nacionalismos que proliferan. Es oportuno, hoy más que nunca, consolidar ese proceso integrador en favor de los grandes espacios económicos y sociales. Sería temerario dejar pasar estas oportunidades que se ofrecen sin instar a España y Marruecos a planificar juntos el futuro. A constituirse en el broche de la cooperación entre los dos continentes, y donde Málaga puede ser un puente perfecto por su apertura y nivel de excelencia.

Ricardo Nandwani

Vocal del Pleno y Presidente Comisión de Empresa y Economía Digital de la Cámara de Comercio de Málaga.

C.V.: *Empresario experto en Transformación Digital y Presidente de la Comisión Empresa y Economía Digital de la Cámara de Comercio de Málaga. Presidente de la Asociación de Jóvenes Empresarios de Málaga (AJE Málaga) y Vicepresidente de AJE Andalucía, así como miembro del Comité Ejecutivo de la Confederación Española de Asociaciones de Jóvenes Empresarios (CEAJE). Vicepresidente Comisión de Emprendimiento en Economía Digital del Cluster Andaluz OnTech.*

ARTÍCULO COLABORACIÓN : Ödön Pálla[1]

Responsable de internacionalización de la Empresa en la Dirección Provincial de Comercio de Málaga. Secretaría de Estado de Comercio.

[1] *Las opiniones vertidas en este artículo son responsabilidad del firmante y no tienen por qué coincidir con las opiniones de la Institución en la que desempeña su trabajo.*

¿ POR QUÉ ÁFRICA ?

El Foro para la Paz en el Mediterráneo aborda un buen número de campos de análisis, entre los que la Economía, la Diplomacia, el Comercio o el Medio ambiente ocupan sin duda una importancia categórica, amén de estar atento a todo el sistema integral de desarrollo de los países colindantes con el mediterráneo.

Por otra parte, su enfoque regional le confiere a su vez una dimensión geográfica de primer orden, toda vez que conecta tres continentes y los respectivos países y territorios que abrazan este hermoso mar, y que son Europa, Asia y África. Y a la vez, la concepción global de nuestra realidad mundial nos obliga a contemplar la dimensión integral mediterránea, no sólo como epicentro histórico de una buena parte de las esencias actuales de la humanidad, sino también de un sinnúmero de aspectos directamente relacionados con la paz y el desarrollo del resto del mundo.

Por ello quisiera hacer una reflexión de enorme importancia sobre el caso africano en su conjunto, pues para un país como España que, si bien ha estado tradicionalmente presente, siempre lo ha hecho desde una perspectiva limitada territorialmente. Y ello lo considero oportuno porque nuestro país está ya en condiciones de abordar un cambio en la actitud y enfoque de nuestra relación con dicho continente. África se ha convertido ya en uno de los ejes prioritarios de la atención de nuestra política exterior y de la actividad comercial. Y llegado a este punto, conviene por lo tanto recordar, aquello de que por menos conocido no resulta ser menos importante, y de que superamos ya, en nuestra relación con África, el volumen de las transacciones comerciales de España con toda Iberoamérica. El uso de las telecomunicaciones, medios informáticos, Internet o el Ciberespacio lo facilitan hoy día.

Ello es impresionante y digno de toda atención. Bien es verdad que ese volumen económico-comercial todavía se concentra de forma muy intensa en algunos países del norte africano y en muy señalados productos. Sin embargo, poco a poco, la atención de las empresas y la sociedad españolas por el resto del Subcontinente africano, el "África negra" o el continente subsahariano y su enorme potencial, después de haber recorrido el mundo europeo, americano y asiático, empieza a crecer y asentarse con firmeza y vocación de permanencia produciendo una beneficiosa diversidad. El campo de la cooperación bilateral es inmenso y altísimamente beneficioso para todas las partes involucradas, lo que exige ir preparando a nuestra sociedad y a nuestro tejido productivo y exportador para la conexión e incorporación a medio plazo al continente africano y al formato globalizado mundial, en coherencia con nuestra plena proyección de actividad internacional.

Varias son las razones que nos llevan a esta conclusión:

1. En primer lugar, África cuenta con un enorme potencial de crecimiento y desarrollo, claramente puestos de manifiesto por la evolución en los últimos años de sus tasas medias de crecimiento del PIB

regional. También es previsible que resulten en el futuro próximo – en el medio y largo plazo- mucho más relevantes tal y como acreditan las Instituciones de análisis internacionales. África se va a configurar como un gran Continente, pendiente de una explosión demográfica, económica y comercial sin parangón. ¡El Gigante se ha despertado!.

2. Desde la perspectiva española, el continente africano – tan cercano y a veces tan lejano- se ha convertido ya en uno de los ejes prioritarios de nuestra política exterior y de nuestra futura actividad comercial. La Administración española ha venido desarrollando en las últimas décadas un esfuerzo particular de adaptación de su política exterior al caso africano y a su relación armoniosa con nuestro país. El modelo desarrollado, netamente español, por haber sido el primero en su preocupación y por tener un enfoque relacional más equilibrado que el habitual, ha inspirado la más tardía reacción europea y a su vez un cambio paulatino de los enfoques tradicionales. Prueba de ello son los Planes África (I, II y III), la Casa África del Ministerio de Asuntos Exteriores y Cooperación, o la iniciativa Horizonte África de la Secretaría de Estado de Comercio, las cuales han sido puestas recientemente en marcha en nuestro país, y que constituyen el frente de la labor que en esta región se espera que la sociedad civil española habrá de continuar y, especialmente, desarrollar en profundidad. En este contexto, la próxima Cumbre UE-Unión Africana, que estaba prevista para finales del 2020 y que ha debido ser aplazada por la COVID 19, imprimirá sin duda un nuevo impulso y dinamismo a las relaciones futuras.

3. El nivel de relación comercial de nuestras empresas, especialmente las de pequeño y medio tamaño con África sigue siendo meramente testimonial. Y ello es debido no a su potencial sino, en gran medida, al aún limitado conocimiento e incertidumbre que tienen tanto las empresas como nuestros profesionales con respecto al continente. Por ello, resulta imprescindible ir preparando a nuestro tejido productivo y exportador para su incorporación a medio plazo en formato globalizado mundial, así como al entorno de su competencia exterior. Ello es particularmente importante teniendo en cuenta que el tipo de demanda actual y futura, que alcanzará elevadas dimensiones, está muy bien alineado con el tipo medio de productos y tecnología que los españoles ofertamos. A ello, hay que añadir la imagen de nuestro país y la calidad y seriedad de los productos y servicios de sus empresas, la proximidad territorial de ambos continentes, las relaciones ya consolidadas con el norte de África, el elevado desarrollo de infraestructuras, la ubicación empresarial, y el potencial de los puertos del Sur y de las Islas españoles en el desarrollo de vías futuras de transporte hacia el África subsahariana, que hacen de algunas provincias y ciudades cercanas al Continente, unos emplazamientos privilegiados.

4. A lo anterior debemos añadir que, en nuestro país, aún existen pocas instituciones especializadas que tengan una verdadera vocación africana en sus actividades generales. Como consecuencia, la información y difusión del conocimiento del Continente es todavía escaso y limitado. Además, no se dispone de una adecuada oferta de estudios africanos de elevado nivel, tanto cuantitativo como cualitativo, que permita preparar a nuestros titulados superiores, empresarios, políticos y sociedad en general, para abordar los enormes retos que la competencia futura llevará asociados.

5. En quinto lugar, la heterogeneidad de los diferentes modelos de desarrollo económico y político de los países africanos y sus claroscuros obligan a disponer de análisis, enfoques y actuaciones permanentemente actualizadas, de forma que se cree un cuerpo doctrinal útil para nuestras

empresas y sociedad, continuamente adaptada a cada caso. Ello nos permitirá a su vez priorizar entre los países motores de la estabilidad y el crecimiento continental y especializarse en ellos, dejando en un segundo plano, bien a aquellos otros países que aún no alcanzan la madurez de los primeros, o que, debido a sus deficiencias estructurales o carencias respecto a los estándares mínimos internacionales, no puedan, hoy por hoy, ser objeto de acuerdos particulares por el riesgo que llevan implícito. Para estos países inestables, o incluso fallidos, habrá que estar a expensas de lo que el efecto arrastre de los primeros ayude como referencia, para un más próspero y beneficioso futuro a medio y largo plazo para todos.

6. También debemos destacar que la atención que el continente africano ha despertado tradicionalmente en los países europeos de la UE, principales potencias ex coloniales en África, le confiere una especial importancia estratégica, económica, política y comercial nada desdeñable, si bien en paulatino descenso relativo en favor de otros países con estrategias no sólo más acordes y con enfoques más modernos y pragmáticos, sino también más coincidentes con los intereses políticos de los gobernantes africanos. En este contexto, España dispone de una imagen consolidada y diferente de la imagen histórica que todavía hoy tienen algunos países ex coloniales tradicionales, y en esa imagen se nos asocia como gentes afables, respetuosas, amigables, hospitalarias con el mundo africano, y sobre todo, con un enfoque relacional diferente y más equilibrado. Esas virtudes han de ser puestas en valor para construir el adecuado puente económico, comercial, cultural y humano entre las vertientes físicas europeas y africanas a ambos lados del Mediterráneo, y trabajar en profundidad en favor de nuestros intereses comunes. En este sentido, se impone rescatar el valor añadido de lo español.

7. Tampoco debemos dejar de mencionar la Política de Vecindad puesta en marcha en el conjunto de la UE y particularmente por España, que centra cada vez mayores esfuerzos políticos, financieros, comerciales, migratorios, militares y de cooperación con el Continente. Debemos asimismo estar atentos y aprovechar los beneficios que la Creación de la Zona de libre Cambio Comercial Africana**,** la mayor del mundo en dimensión y países, representa como oportunidad para nuestro país. La inversión española, el desarrollo de acciones productivas y deslocalización de actividades y empresas exige disponer de un cuerpo de conocimiento, de relaciones y de doctrina que debe desarrollarse y mantenerse. La red de embajadas españolas y de la UE que atienden a los asuntos diplomáticos o comerciales a través de sus agregados y consejeros comerciales, los consulados que atienden a los ciudadanos en el extranjero, los fondos FIEM (fondos de apoyo a la internacionalización de empresas), etc., son todas importantes herramientas de apoyo a las empresas.

8. España, como importante socio que somos de la UE, debemos hacer referencia a la enorme batería de actuaciones y medios centrados en la cooperación europea con África, que no podemos ni desdeñar ni dejar de lado, y en los que España, a pesar de la enorme inercia que los países europeos postcoloniales están ejerciendo, debe ejercer un papel con mayor influencia en la toma de decisiones europeas. No olvidemos que la UE es el primer socio comercial de África, tanto respecto a las exportaciones con ese destino como a las importaciones de ese origen; es el principal inversor en África con más de un 33% del total del stock, superando los 32.000 millones de euros. Adicionalmente, más de la mitad de la Ayuda Oficial al Desarrollo que recibe África procede de la UE (superior a los 22.000 millones de euros) y siendo el origen de más de un tercio de las remesas de africanos procedentes del mundo.

9. Finalmente, no podemos olvidar que el mundo empresarial y el mundo académico vienen manifestando un enorme interés en el desarrollo de mecanismos de información, transmisión de experiencias y conocimientos, de desarrollo de programas y proyectos individuales o en combinación con Instituciones multilaterales como la UE o el Banco Africano de Desarrollo, Instituciones de cooperación académica, técnica y humanitaria, y de apoyo financiero a los mismos.

El futuro es muy prometedor, y nuestra sociedad y empresas están sobradamente preparadas y a la altura de tamaño reto. Sólo falta preparar a nuestra sociedad, y dar a conocer a nuestro tejido productivo y exportador, la información necesaria y herramientas para su conexión e incorporación al continente africano con sus competitivos mercados regionales.

Las telecomunicaciones, digitalización, Internet, banca electrónica, videoconferencias o el uso del Ciberespacio, permiten hoy acercar fronteras, empresas y personas, y aunque los nuevos mercados africanos, como cualquier otra región cultural diferente a la nuestra requerirá también de medios de transporte, esfuerzo y contactos presenciales, hemos de abrir nuestras mentes a las nuevas herramientas y oportunidades que se nos presentan. ¡ Ayudemos entre todos a no perder el tren africano ¡.

TEXTOS COMPLEMENTARIOS APORTADOS POR LOS PONENTES.

2ª Mesa redonda. Panorama Utilidades cibernéticas e Inteligencia Artificial

Moderador Jornada: José María López Jiménez.

Director de Responsabilidad Social Corporativa UNICAJA Banco.

https://vimeo.com/497910937

Víctor Manuel Solla Bárcena

Director General Innovación y Digitalización Urbana Ayuntamiento de Málaga.

C.V.: *Ha sido Director general de tecnologías de la información y las comunicaciones del Principado de Asturias. Jefe de servicio de sistemas de información y atención ciudadana del ayuntamiento de Avilés. Responsable en fondo Feder Dusi 2017-2023. Responsable del proyecto europeo "urbact". Miembro técnico de la comisión de nuevas tecnologías de la federación española de municipios y provincias (FEMP) y miembro técnico de la comisión de modernización, participación ciudadana y calidad de dicha federación. Ingeniero en informática Facultad de informática, Universidad Politécnica de Madrid. Máster en dirección de sistemas y tecnologías de la información y las comunicaciones, Universidad politécnica de Madrid. Especialista en gestión pública local para directivos públicos profesionales (FEMP).*

Carlos de Palma Arrabal
Coronel Ejército del Aire (Rva.).

C.V.: *Piloto de aviación militar. Ingeniero de organización industrial. Diplomado Estado Mayor de las Fuerzas Armadas, Curso Sénior OTAN, Curso Oficiales Superiores Iberoamericanos. Experiencia en Coaching. Consejero Defensa Embajadas España en Italia, Malta y Eslovenia. Operaciones en el mediterráneo y Afganistán. Visitas de trabajo en treinta países. Ayudante honorario del Rey de España.*

AVANCES TECNOLÓGICOS

El hecho de que Málaga sea una región abierta y acoja la sede de importantes empresas relacionadas con las tecnologías de la información, la ciberseguridad y otras muchas aplicaciones de todo tipo, llevó a pensar en la celebración de unas sesiones prácticas y divulgativas sobre el Ciberespacio, encuadrándolas en el seno del Foro para la Paz en el Mediterráneo.

Así, cuando comenzamos a diseñar estas Jornadas sobre Seguridad, Defensa y Cooperación, pensamos que para el tema del Ciberespacio se usara un lenguaje lo más sencillo posible, se tocaran temas que interesasen tanto a una audiencia general como especializada, e invitar a expertos en los campos y aspectos más novedosos del tema. La motivación ha sido:

- Divulgar unos conocimientos generales sin profundizar en detalles técnicos complejos, que permitan entender todo lo que sucede a nuestro alrededor, de manera transversal y en cualquiera de nuestros ámbitos cotidianos de interés.
- Tratar esos conocimientos en conjunto y superponerlos a nuestras vidas y actividades sociales y profesionales, para ayudar a mentalizarnos de la necesidad de prestar atención al Ciberespacio, de ponernos lo más al día posible, y de protegernos frente a su mal uso.

Todos conocen en mayor o menor medida las consecuencias que los avances tecnológicos tienen en nuestras vidas en los ámbitos terrestre, aéreo, marítimo o espacial, pero pocos son conscientes de lo que ha supuesto la quinta dimensión del Ciberespacio, creada por la unión de la Electrónica y las Telecomunicaciones con la Informática, y ampliada con aplicaciones para los dispositivos digitales que hoy manejamos (teléfono móvil, tabletas, ordenadores, dispositivos digitales de todo tipo, conexiones a internet, etc.).

El Ciberespacio viene a ser el ámbito virtual, no visible pero real, por el que discurren hoy día y de forma casi instantánea enormes cantidades de información y aplicaciones beneficiosas para todos, junto a peligrosas amenazas. Además, ya no existe separación entre nuestro tradicional mundo “tangible y real”, con el nuevo entorno “virtual”. O entendemos este nuevo entorno, o nos quedaremos fuera de la nueva sociedad digital que todo lo invade. Un gran riesgo será no prestarle la suficiente atención, pues hoy día los dispositivos y posibilidades digitales están al alcance de cualquiera, para bien y para mal. De ahí la importancia de que los padres en sus hogares, los directivos en sus empresas, y las instituciones públicas para con sus servicios y ciudadanos, se tomen muy en serio las oportunidades y los riesgos que el entorno digital supone.

Estos avances tecnológicos se aplican ya ampliamente a los ámbitos de: Telemedicina, seguridad, teletrabajo, comercio electrónico, tiendas on-line, blockchain, banca on-line, criptomonedas, justicia telemática, impuestos y tasas, juegos en red, prensa digital, cursos on-line, industria 4.0, domótica, redes eléctricas inteligentes, agricultura inteligente, autómatas programables, robótica, drones, inteligencia artificial, internet inserto en las cosas, big data, inteligencia empresarial, informática computacional, robots sociales, turismo virtual, cibermascotas, cibersexo, dispositivos Smart, software, etc. y todo lo que desde

nuestro habitual mundo físico se pueda implementar en el virtual. Para transmitir datos se usan telecomunicaciones terrestres, submarinas, por satélite, fibra óptica, wifi, infrarrojos, bluetooth, GPS, 5G, etc. Y el almacenamiento de información se puede guardar en soportes de memoria, en la nube, etc. En resumen, un nuevo entorno que a veces puede producir vértigo por su enorme capacidad, velocidad de proceso y de evolución potencial, pero accesible con paciencia y cuidado.

No me detendré en aspectos técnicos, pero sí en mencionar estos importantes aspectos:

- Hay que proteger a niños y jóvenes de personas con las que compartan relación o información indebida desde sus dispositivos. La mayoría de edad es una buena referencia.

- La hiperconectividad actual agudiza las vulnerabilidades de seguridad y exige una mejor protección de las redes y sistemas, así como de la privacidad y derechos digitales del ciudadano.

- Es necesaria una actitud de permanente formación y actualización a todos los niveles: Hogar, empresa, instituciones. Y también una constante vigilancia de nuestros datos y dispositivos frente a posibles ataques malintencionados y delictivos. Es necesario reducir la brecha digital.

- Las complejas tecnologías en juego y la propiedad de diseños privativos de las empresas suministradoras nos hace enormemente dependientes. Hay que lograr un grado suficiente de autonomía y seguridad en los servicios, incluyo invirtiendo en tecnologías propietarias del sector público gubernamental, para disponer de autonomía.

- Es necesario un marco regulatorio nacional, europeo e internacional coordinado, que vaya por delante, o al menos a la par de los usos malintencionados.

En el capítulo de ANEXOS de estas jornadas, se pueden encontrar las definiciones relacionadas con el ciberespacio.

Francisco López Valverde

Departamento de Lenguajes y Ciencias de la Computación. Investigador responsable del Laboratorio de Inteligencia Artificial Aplicada, E.T.S. de Informática de la Universidad de Málaga.

C.V.: *Doctor Ingeniero por la Universidad de Málaga en 2002. Pertenece al grupo de investigación de Inteligencia Computacional y Análisis de imágenes (ICAI). Desde sus inicios en la investigación de su tesis doctoral "Detección de vasos sanguíneos en mamografías con redes neuronales" ha estado vinculado a la inteligencia artificial aplicada. Ha realizado numerosos proyectos de transferencia de tecnología en el campo de la Inteligencia Artificial. Desde 2010 lidera el laboratorio de inteligencia artificial aplicada de la UMA. Desde*
2014 hasta el presente ha sido el coordinador del programa "Google Actívate" en la Universidad de Málaga.

INTELIGENCIA ARTIFICIAL.

El mundo está cambiando con la implantación de la Inteligencia Artificial (IA) y va a ser muy diferente cuando este proceso haya madurado. Las distintas aplicaciones de la IA actúan en múltiples aspectos de la vida cotidiana del ciudadano del siglo XXI. En este artículo presentamos los campos de la sociedad donde la Inteligencia Artificial ha alcanzado un nivel suficiente como para que sea perceptible para las personas su influencia en la vida cotidiana, como por ejemplo el ámbito cultural o del bienestar. Otros campos que aún

están en un estadio inicial pero que van a tener un impacto relevante para la sociedad en el futuro próximo son el ámbito socio económico que también se incluye en este artículo.

1. Cultural:

Eliminación de barreras idiomáticas. La evolución y perfeccionamiento de los sistemas de traducción están comunicando las islas culturales de las diferentes lenguas. Que toda la literatura universal esté disponible y entendible para toda la humanidad, sin importar el idioma en que fue escrito supondrá un enriquecimiento cultural sin precedentes.

Conocimiento profundo del arte. Gracias a los sistemas de aprendizaje profundo aplicados a la pintura o la escultura podemos conocer mucho mejor los detalles de los estilos personales de los artistas. Nos permitirá determinar con más precisión la autoría de las obras en caso de que haya alguna duda. También nos permitirá conocer mucho mejor al artista a través de sus obras.

2. Medio ambiente y climático:

Agricultura de precisión. Debido al desarrollo de las últimas tecnologías en sensores en el ámbito de la agricultura es posible monitorizar los cultivos, y hacen posible lo que hoy conocemos como la agricultura de precisión. Estos sensores producen una gran cantidad de datos sobre las cosechas que permiten optimizar el rendimiento del terreno y los recursos utilizados. Las técnicas de análisis de datos basadas en aprendizaje computacional se usan para extraer conocimiento del "big data" de la agricultura. Dispositivos como drones y agentes autónomos terrestres ayudan en la inspección y actuación de precisión en el rango del metro cuadrado de la plantación agrícola. El ahorro de agua es una de las ventajas más importantes.

3. Bienestar:

Conducción autónoma. Gracias a los avances en inteligencia artificial, la conducción autónoma es ya una realidad. Las técnicas de aprendizaje profundo han demostrado ser eficaces a la hora de abordar los complejos retos que supone la conducción autónoma, consiguiendo un nivel de autonomía que resultaba impensable hasta hace poco tiempo. Los vehículos autónomos no se ven afectados por factores como el cansancio, somnolencia o distracciones, por lo que en un futuro cercano la conducción autónoma permitirá reducir de forma considerable los índices de siniestralidad, de los cuales el factor humano es el responsable hoy en día del 70% de los casos.

Medicina. La medicina es uno de los campos que más y mejor se está beneficiando del uso de la inteligencia artificial. Hoy en día ya están en marcha numerosas aplicaciones, desde agilizar el lento y costoso desarrollo de fármacos a analizar el genoma de un paciente. Sin embargo, el mayor potencial de la inteligencia artificial en el campo de la medicina es como herramienta capaz de aprender y analizar rápidamente enormes cantidades de información: historiales de pacientes, pruebas de imagen, avances científicos y otras fuentes. Ayudando de este modo a los doctores a ofrecer mejores diagnósticos y tratamientos.

Video vigilancia. La inteligencia artificial tiene importantes aplicaciones en el ámbito de la video vigilancia y la visión artificial, un ámbito en pleno auge en los últimos años debido al afán por la seguridad, que también ha causado que multitud de espacios de todo tipo dispongan de cámaras monitorizadas. Mediante el uso de la inteligencia artificial, es posible detectar los objetos en movimiento con el fin de seguirlos, analizar su comportamiento y detectar situaciones anómalas. Esto tiene importantes aplicaciones, desde el ámbito de la seguridad al seguimiento del tráfico en carretera, para detectar de forma automática en tiempo real cualquier problema que se produzca.

Procesamiento del lenguaje natural. El procesamiento del lenguaje natural es una rama de la inteligencia artificial que trata del desarrollo de sistemas automáticos que interactúen por hablado o por escrito, con los seres humanos. Tiene multitud de aplicaciones: síntesis de voz, comprensión del lenguaje hablado, contestación de preguntas, detección de correo no deseado, traducción automática y muchas otras. Estas llevan ya tiempo utilizándose en nuestra vida diaria, como ocurre en los sistemas automatizados de atención telefónica, los asistentes de voz o los traductores automáticos, entre muchos otros.

Clasificación de documentos. Hoy en día se generan ingentes cantidades de documentos y mensajes de texto tanto en la web como en las redes sociales. Mediante el uso de técnicas de inteligencia artificial, es posible extraer información, analizar el contenido u organizar en categorías esta inmensa cantidad de documentos, lo cual de otra forma resultaría prácticamente imposible. La información que se puede llegar a obtener mediante estas técnicas tiene gran cantidad de posibles aplicaciones de todo tipo, por lo que se ha convertido en una de las ramas de la inteligencia artificial con más éxito en los últimos años.

4. Socio económico:

Inclusión económica. Disminución de la brecha económica. Capacidad del empleo. De forma similar en la que una plataforma tipo Netflix puede conocer nuestras preferencias y acertar en recomendaciones de películas y series, la IA también sirve para detectar las capacidades de una persona en zona de exclusión económica y compararlo con las necesidades del mercado en el futuro próximo, y conseguir oportunidades.

Inclusión social. Disminución brecha social. Capacidad del desarrollo socio educativo. La IA puede a través de tecnologías como la Realidad Aumentada y Realidad Virtual, y usando planteamientos integrados e innovadores, la apropiación de los valores compartidos para conseguir mejorar la igualdad, la inclusión social, la diversidad y la no discriminación.

5. Conclusiones

Si analizamos las características comunes en las revoluciones tecnológicas del pasado, podemos observar que en todas ellas hubo un punto de inflexión, y la sociedad que había antes era muy diferente de la que hubo después. ¿Hemos llegado ya a ese punto de inflexión?, ¿La sociedad que hemos conocido hasta ahora será muy diferente a la que vendrá en el futuro próximo?, ¿Será beneficioso para la humanidad?. Sin lugar a duda la respuesta es afirmativa para todas ellas.

José María López Jiménez.

Responsable de la Dirección de Relaciones Institucionales y con Grupos de interés y Sociales,
Director de Responsabilidad Social Corporativa de la corporación UNICAJA Banco.

BANCOS Y CRIPTOMONEDAS.

Tras una serie de avatares históricos, el dinero en circulación tiene origen mayoritario en la actualidad, directa
o indirectamente de los bancos centrales, que se insertan en estructuras estatales o supranacionales como la Unión Europea.

La labor de intermediación de las entidades de crédito, a través de la captación de depósitos y la concesión de crédito, ha permitido su involucración en el aumento de la masa monetaria y en el sistema de pagos, y, a su vez, ha generado una estrecha relación entre los Estados y los bancos.

La transformación digital, las nuevas preferencias de los consumidores y la aparición de proveedores de servicios financieros como las entidades “Fintech” (empresas financieras con nuevos productos basados en

tecnologías de la información) y las "Bigtech" (grandes empresas proveedoras de tecnologías de la información), junto a otras circunstancias, como los tipos negativos, han erosionado la posición de preeminencia del sector bancario tradicional.

Los bancos son necesarios en nuestras sociedades, pues facilitan la eficiente asignación de recursos y la concesión de crédito a las empresas y a las familias, aunque, en casos extremos, hay quien no descarta que desaparezcan de la realidad financiera ante el empuje de las "Bigtech". Sin embargo, la situación que prevalece es la de cooperación entre el sector financiero tradicional y las "Fintech" y "Bigtech", aunque las futuras maniobras de estas últimas y su eventual acogida por el público siguen siendo una incógnita.

En el ámbito de los medios de pago, la tecnología de registros distribuidos y la cadena de bloques han permitido la aparición de nuevos instrumentos que cumplen funciones análogas a las del dinero emitido por los bancos centrales o, partiendo de este, del escriturario creado con la participación de las entidades de depósito, o del electrónico de las entidades de dinero electrónico. Se trata de las criptomonedas o monedas virtuales, que son una de las manifestaciones del fenómeno, más amplio, de los criptoactivos.

La aparición de las monedas virtuales genera una evidente tensión entre los Estados —y las entidades supranacionales con moneda propia— que monopolizan, a través de sus bancos centrales, la emisión de dinero soberano, y los promotores y los usuarios de las monedas virtuales, que, a conciencia o no, menoscaban con su actividad dicho monopolio. Indirectamente, también las entidades de crédito (en mucha menor medida, las de dinero electrónico) resultan afectadas por esta tendencia.

El mayor caso de éxito, por el momento, de estos instrumentos, es el de "Bitcoin", que concitó la atención de los supervisores y de los reguladores, como garantes de la estabilidad financiera, aunque estos consideraron, en general, que sus posibles riesgos no eran sistémicos.

El anuncio en 2019 del lanzamiento en 2020 de "Libra", un proyecto liderado por la "Bigtech" Facebook, ha alterado la situación descrita, por su potencial alcance sistémico y disruptivo.

En la medida en que "Libra" se pueda "anclar" a activos sólidos de referencia, dando carta de naturaleza a las conocidas como "monedas estables" ("stablecoins"), se podría superar uno de los mayores defectos de "Bitcoin", que ha impedido su consolidación: la fuerte oscilación de su valor.

Más allá de los aspectos técnicos, "Libra" podría beneficiarse de la geopolítica, tras el anuncio por el Banco Popular de China del posible lanzamiento de una moneda digital, y la necesidad para los Estados Unidos de disponer de un arma con la que contrarrestar el hipotético golpe.

La posible buena acogida de "Libra" por el público en general, y el riesgo real de que las monedas privadas basadas en la tecnología puedan desplazar a las monedas soberanas y a sus derivaciones (dinero escriturario y electrónico), han servido para que se acelere el interés de los bancos centrales por la emisión de monedas digitales soberanas, lo que permitiría a los particulares, por otra parte, abrir sus cuentas directamente en los bancos centrales, un privilegio hoy día reservado a los bancos y a algunas otras instituciones financieras y públicas.

Las cuestiones de orden político, jurídico, económico, monetario y financiero que resultarían de materializarse esta alternativa, serían múltiples y superarían ampliamente el objeto de este trabajo, por lo que las dejamos aquí meramente apuntadas para su ulterior tratamiento.

Belén Bahía Almansa

Profesora Titular Derecho Financiero y Tributario. Universidad de Málaga.

C.V. *Licenciada en Derecho por la Universidad de Málaga y Doctora por la Universidad de Málaga en 2005, con la calificación de Sobresaliente "cum laude" con la Tesis titulada "La Transformación de Sociedades. Aspectos Mercantiles y Fiscales". Posee igualmente el Diploma en Estudios Avanzados en "Sistemas de Calidad Total para la Innovación Industrial: Gestión Integrada de la Calidad, Medioambiente y Prevención", por la Universidad de Málaga con la calificación de Sobresaliente. También ha cursado los estudios del Máster Oficial de Posgrado "Políticas y Prácticas de Innovación Educativa para la Sociedad del Conocimiento" en la Universidad de Málaga. Profesora Titular de Universidad del Área de Derecho Financiero y Tributario. Es Profesora tutora de TFM del Máster de Abogacía en la Universidad Nacional de Educación a Distancia Cuenta con un importante número de Contribuciones a Congresos, habiendo formado parte del Comité Científico de varios de ellos.*

PROBLEMAS LEGALES QUE PLANTEA LA DIGITALIZACIÓN, LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL, CON ESPECIAL REFERENCIA A LA FISCALIDAD.

La llegada de internet, de la robótica y de diversas formas de inteligencia artificial, están planteando una serie de problemas de índole civil, penal, laboral, mercantil, y fiscal, que deben ser resueltos y regulados por normas jurídicas pertenecientes a todos los ámbitos del derecho.
En el ámbito laboral, se está produciendo una suplantación de trabajadores por robots, que va a provocar un problema importante de déficit de financiación en las arcas públicas, al reducirse las cotizaciones a la seguridad social, lo que exigirá la adopción de medidas, entre las que se encuentran las de carácter fiscal, para paliar esta situación. Se deben analizar por tanto, las medidas propuestas por la Unión Europea en diversas Comunicaciones, así como las propuestas lanzadas por la doctrina, como es la creación de un Impuesto sobre los robots, o la creación de un nuevo sujeto jurídico denominado "personalidad jurídica electrónica" que podría convertirse en sujeto pasivo de un tributo.

Aporta también su Presentación.

María Gómez Casas

Coordinadora Sección Derecho Digital, Innovación y Gestión del Colegio de Abogados de Málaga.

C.V. *Abogada en ejercicio. Especialista en Derecho digital e Innovación. Máster en seguridad de la información. Experta universitaria en propiedad intelectual en la nueva sociedad de la información. Coordinadora de la Sección de Derecho Digital, Innovación y gestión de despachos del Ilustre Colegio de Abogados de Málaga. Miembro del Comité legal de Alastria. Fundadora de www.juiciostelematicos.com y organizadora de Legal Hackers Málaga.*

JUSTICIA TELEMÁTICA.

Texto elaborado en colaboración con D. Acayro Sánchez Lázaro, Magistrado-Juez

del Juzgado de lo Contencioso Administrativo nº 2 de Santander.

1.- Los juicios telemáticos.

La pandemia ha visibilizado la vulnerabilidad de la Administración de Justicia no sólo por la sobrecarga de trabajo que ya arrastraba sino también porque era impensable que se pudiese llegar a suspender durante semanas la intensa actividad de la práctica totalidad de los Juzgados.

La realidad es que nos hemos acostumbrado a que la Administración de Justicia sea lenta, olvidándonos de que el derecho a la tutela judicial efectiva también incluye la obligación de resolver en plazos razonables. No obstante, la crisis sanitaria de la COVID 19, también ha permitido el impulso de iniciativas y un innegable avance en el empleo de medios tecnológicos.

En ese contexto, a principios de mayo 2020 se empezaron a celebrar los juicios telemáticos para lo que ya se tenía cobertura legal suficiente en la Ley Orgánica del Poder Judicial.

Luego se han ampliado las posibilidades de intervención telemática:

a.- Una es su celebración mixta. De esta manera, se favorece la opción de los intervinientes a que uno sólo de los Letrados quiera intervenir telemáticamente en estrados y el otro presencialmente o, incluso, las dos partes y que sean los testigos y peritos los que acudan bien presencialmente al Juzgado o mediante videoconferencia con conexión múltiple.

b.- Otra, que se está realizando en el Juzgado de lo Contencioso nº2 de Santander, consiste en la generación de salas de espera virtuales para testigos y peritos que intervendrían también de manera íntegramente telemática. Son casos en los que éstos no ofrecen dudas de identificación e imparcialidad para las partes.

Y toda la implementación tecnológica que se está produciendo se hace respetando las garantías procesales, lo que ha provocado que se vayan adhiriendo numerosos juzgados de toda la geografía española y de diversos órdenes jurisdiccionales.

Esto no significa que no siga siendo necesaria la inversión en medios humanos y materiales, porque son insuficientes. Y tampoco que vayan a ser la respuesta a todo. Los juicios telemáticos, para un determinado tipo de procedimientos, son una opción legal, posible y necesaria. No son un atajo en la tutela judicial ni un procedimiento de inferior calidad.

Tampoco suponen una merma de garantías durante su celebración. Al contrario, cumplen con todas las garantías procesales. De hecho, van a permitir cumplir en muchos casos el derecho fundamental a un proceso sin dilaciones indebidas.

En más de la mitad de los procedimientos contencioso administrativos, la prueba que proponen las partes es únicamente documental. Un porcentaje similar sucede en el orden social. Pero donde van a tener mayor potencial es en los Juzgados que están dirimiendo la nulidad de cláusulas abusivas, como las cláusulas suelo, gastos hipotecarios, entre otras, donde la única prueba que se pide en el 95% de los procedimientos en la audiencia previa es la documental, quedando desde ese momento vistos para sentencia. Y donde todavía se prevé la entrada de muchas demandas de idéntico tipo. Es decir, procedimientos que tienen el denominador común de una tramitación procesal sencilla.

Evidentemente, ocurrirán incidencias técnicas, harán falta protocolos y será imprescindible la formación de los operadores jurídicos. Más eficaz y más rápido será cuanto mayor sea el grado de compromiso de todos. La abogacía, sin duda, como última voz del ciudadano ante los Tribunales, y comprometidos con la defensa de los intereses de nuestros clientes, también tiene que impulsar la modernización de la Justicia.

Por todo ello, creemos que es el principio de un cambio imparable que puede colocar a la Administración de Justicia en el siglo XXI.

2.- Trabajar con flujos de datos.

Pero dentro de esta transformación digital, lo que posiblemente sea un antes y un después en la Administración de Justicia, va a ser trabajar con los flujos de datos. Para explicarlo de una manera sencilla hay que empezar por el final.

¿Qué es lo que se persigue con el empleo de flujos de datos en la Administración de Justicia?: Reducir los tiempos de respuesta en la tramitación de los procedimientos.

Si todos estamos de acuerdo en ese objetivo, también lo estaremos en que no es posible eludir la posibilidad de automatizar, en la medida de lo posible, el procedimiento judicial. El cambio social y el progreso de la tecnología dentro de la comunidad requieren de un sistema normativo apropiado y que pueda seguir el ritmo de la evolución en la sociedad.

El mundo se encuentra encauzado en una tendencia hacia la automatización. La introducción de sistemas automatizados en todas las ramas del conocer humano tiene el carácter de irreversible. El aparato de justicia debe tener acceso a esa tendencia y debe marcar el ritmo del progreso en el ámbito de su competencia. El Derecho no puede quedarse atrás, la Justicia exige celeridad en la resolución de los conflictos para ser eficaz.

Como hemos indicado, la finalidad es agilizar la tramitación procesal mediante la generación de una tramitación guiada y automatizada de los procedimientos.

La codificación existente está dispuesta de tal manera que permite que la norma sea importada a un sistema computarizado de alta tecnología mediante el cual su aplicación se pueda llevar a cabo de manera más eficaz, rápida y segura. Sobre todo, permite que algunos de los trámites que implica la codificación de la que hablamos, sean desarrollados de manera automática, sin la intervención humana a cada paso del procedimiento.

No hablamos de la sustitución del individuo o el abandono de la aplicación de la Justicia a manos de un ser mecánico. Implica dotar al individuo y al aparato judicial de una herramienta de suma utilidad.

La clave reside en que cada procedimiento responde a un esquema procesal desde su inicio hasta su archivo. Para su tramitación, el sistema de gestión actual ofrece listados de plantillas con sus correspondientes códigos, pero, para cada impulso procesal, el funcionario/a debe conocer el expediente y buscar la resolución correspondiente. Esto supone tiempo.

A esa situación tenemos que añadir la frecuencia con la que se paraliza una mesa por bajas que no son cubiertas por sustitutos/as o por traslados. Hasta que se reincorporan o se adaptan a la nueva mesa también supone tiempo. Y, lo anterior, en un contexto frecuente de importante carga de trabajo que impide dedicarle tiempo a cada expediente para conocerlo e impulsarlo.

Pues bien, mediante la tramitación guiada, lo que se puede conseguir es que sea el propio sistema de gestión el que ofrezca al funcionario/a, directamente, la resolución que tiene que dictar en cada momento sin necesidad de tener que conocer en profundidad el estado del procedimiento ni buscar la resolución porque previamente ya se ha configurado. Las ventajas serían evidentes porque puede aliviar la falta de

medios. Devolver al juez o al magistrado el tiempo que invierte en cuestiones de mero trámite, es dotarle de nuevos espacios para el estudio y la decisión. La creación de un sistema dinámico con acceso a grandes bases de datos puede incluso asistir al órgano judicial, en la toma de decisiones, mediante respuestas precisas a preguntas dadas, con base en parámetros estadísticos.

Nada de lo que se ha expuesto hasta aquí queda fuera del alcance de la mano del hombre. El desarrollo de tecnología cada día más perfecta, la evolución de los sistemas y la facilidad de accederlos, conforman una coyuntura histórica a la que resulta difícil dar la espalda. Estamos en la fase inicial.

3.- La agenda judicial electrónica.

Y otro aspecto también muy importante que se puede conseguir a través de la tecnología es hacer los Juzgados más accesibles. Debe ser una prioridad, e implementar el uso y acceso a la agenda judicial electrónica es un paso más.

Una de las situaciones más molestas para los/as, abogados/as y procuradores es que se haya acordado la suspensión de una vista oral o la práctica de una diligencia y que no se les haya avisado con suficiente antelación para, al menos, ahorrarse el tener que ir al Juzgado y no perder tiempo ni de desplazamiento ni en la preparación del mismo.

Esto sucede todos los días en muchos Juzgados de toda España y son situaciones que se pueden evitar a partir de la tecnología de la que ya se dispone en el portal del servicio al profesional (PSP) de algunas CCAA, y en el Juzgado de lo Contencioso Administrativo nº2 de Santander ya se ha logrado desde hace tiempo.

Básicamente, consiste en permitir a los profesionales personados en el procedimiento acceder a la agenda judicial electrónica para comprobar si una vista o actuación del Juzgado se mantiene o si, por el contrario, se ha cancelado. Y ese acceso puede hacerse en cualquier momento, está supervisada por la LAJ y su alcance jurídico es pleno. Es decir, cualquier consulta que se haga a partir de las 15.00 horas garantiza a los profesionales si las actuaciones del día siguiente se van a celebrar o no porque viene recogido en la agenda judicial electrónica.

Obviamente, siempre puede surgir algún imprevisto por razones personales de cualquiera de los intervinientes en la misma mañana y se tendría que suspender. Pero en los casos ordinarios de suspensión, como, por ejemplo, cuando finalmente no se ha podido citar a un testigo clave lo que obliga a suspender, pero no ha dado tiempo a notificarlo formalmente. En esos casos, al menos se consigue evitar el perjuicio que supone el desplazamiento de los/as profesionales para no celebrar la vista o el acto previsto y que no tengan que enterarse de esa nueva situación al llegar al juzgado.

Que se generalice su uso es necesario porque va a facilitar el trabajo de todos los profesionales.

En síntesis, el cambio es imparable y el futuro ilusionante.

TEXTOS COMPLEMENTARIOS APORTADOS POR LOS PONENTES.

1ª Mesa redonda. Usos y abusos en el ciberespacio. Defensa, seguridad y protección.

Moderador: F. Javier López Muñoz. Vicerrector de Empresa, Territorio y Transformación digital de la Universidad de Málaga**.**

https://vimeo.com/494049004

Mar López

Jefa de la Oficina de Ciberseguridad del Departamento de Seguridad Nacional.

C.V. *Fundadora y Vicepresidenta de la Asociación Women4Cyber Spain. Es Licenciada en Administración y Dirección de Empresas, posee diversos másteres, entre ellos: Dirección y Gestión de la Seguridad de la Información, Dirección y Planificación de Proyectos, y cursos de especialización en dirección de empresas, tecnologías aplicadas y gestión de proyectos. Es Diplomada en el curso Monográfico sobre desinformación del Centro Superior de Estudios de la Defensa Nacional y Diplomada en Altos Estudios de la Defensa Nacional.*

Carlos Seisdedos

Internet Security Auditors. Responsable de Ciberinteligencia.

C.V. *Profesor en diversos cursos de Ciberseguridad y en CIFAL-UNITAR de Málaga.*

General Raimundo Rodríguez

Mando Operaciones Especiales Ejército (MOE).

C.V. *General de Brigada del Ejército de Tierra. Actualmente desempeña el cargo de General Jefe del Mando de Operaciones Especiales y Comandante Militar de Alicante. Lleva 31 años de servicio. Doctor por la Universidad de Granada (Ciencias Políticas y de la Administración 2015) con calificación de Sobresaliente "Cum Lauden". Es Diplomado de Estado Mayor por el Ejército de Estados Unidos (2007) y Diplomado de Estado Mayor de las Fuerzas Armadas (alcanzando el primer puesto de su promoción, 2001). Ha sido General Asesor del Segundo Jefe del Estado Mayor del Ejército, Jefe del Centro Fuerza Futura 35 del Estado Mayor del Ejército, Coronel Jefe del Regimiento de Infantería «Príncipe» nº3, Teniente Coronel Jefe de Estado Mayor de la Brigada de la Legión.*

DIGITALIZACION E INTELIGENCIA ARTIFICIAL. FUERZA 35 DEL EJÉRCITO DE TIERRA.

El Ejército de Tierra aprovecha las oportunidades que presentan las tecnologías disruptivas de la cuarta revolución industrial, en la que estamos inmersos, y se transforma de forma paralela a la sociedad digital actual a la que sirve. En la actualidad se halla inmerso en un proceso de digitalización y de incorporación de

inteligencia artificial como parte de una iniciativa de cambio de las capacidades del Ejército de Tierra que denomina «Fuerza 35».

Implicaciones de la Digitalización e Inteligencia Artificial en la Fuerza 35

La «Fuerza 35» es el modelo del Ejército de Tierra necesario y de utilidad para constituir el componente esencial de la Fuerza Conjunta. Pretende ser una fuerza digitalizada, dotada de medios tecnológicamente avanzados e integrada por personal altamente preparado y motivado, que debe encontrarse consolidada en el horizonte 2035. Sin embargo, no habrá de esperarse tanto para ir incorporando progresivamente distintas generaciones de tecnologías y capacidades. A corto plazo (en el horizonte 2024) y a medio plazo (en el horizonte 2030) ya hay establecidos objetivos intermedios alcanzables.

La «Fuerza 35» surge como respuesta para afrontar los retos y oportunidades planteados por una situación que condiciona de manera importante nuestras vidas que es la cuarta revolución industrial, también denominada Revolución tecnológica 4.0.

En la actualidad, nos enfrentamos a grandes desafíos y retos para la Seguridad y Defensa como pueden ser: el terrorismo; la criminalidad; la confrontación oculta y permanente entre grandes potencias, y también entre potencias medias, que compiten por sus intereses globales, o regionales; el incremento de la temperatura del planeta, con un aumento de los niveles de los océanos y en consecuencia una mayor frecuencia e intensidad de los desastres medioambientales; sin dejar de mencionar otros eventos, como son las pandemias.

Se trata de una serie de retos a la Seguridad y Defensa de alta complejidad que no vamos a poder abordar sin aprovechar las ventajas que nos brindan la digitalización y la inteligencia artificial. No quiere decir que la inteligencia artificial vaya a ser la solución. Sino que va a ser una parte, un elemento, entre otros, que nos va a poder ayudar a prepararnos por anticipado, adelantarnos y a tomar decisiones más certeras para tener éxito.

Digitalización

El desarrollo digital de la «Fuerza 35» incluye a su vez diversos proyectos. Uno de los más destacados es un modelo de experimentación con una Brigada de combate completa. En concreto, la Brigada de la Legión, con base en Almería, que persigue integrar todos sus sistemas de armas y plataformas en una red digital eficaz, capaz de trabajar con mayor dinamismo, agilidad y precisión. De este modo, está previsto que para mejorar su maniobra se incremente el número de sensores, se integren en su estructura orgánica nuevas plataformas de vehículo de combate 8 x 8 con vehículos autónomos y robotizados y, estos a su vez, con el sistema integrado del combatiente.

Su apoyo logístico se define con sistemas de logística predictiva, seguimiento de flujos en tiempo real, anticipación de la respuesta sanitaria y fabricación aditiva (3D/4D).

Su sistema de Mando y Control permitirá llevar a cabo alguno de sus cometidos mediante infraestructuras y sistemas alejados cientos de kilómetros del campo de batalla e incluirá tecnologías Big Data y sistemas de inteligencia artificial para el apoyo a la toma de decisiones.

Los procesos de Inteligencia mejorarán fundamentalmente debido a un aumento de los sensores RPAS (drones), así como la posibilidad de llevar a cabo análisis y difundir productos desde lugares remotos y alejados del frente.

Por último, su sistema de protección mejorará por el empleo de medios de defensa antiaérea en red y un incremento de los sistemas de ciberdefensa en todos los escalones.

Campo de aplicación de la Inteligencia artificial

En relación a los campos de aplicación y en los que puede ser de utilidad la Inteligencia Artificial, hasta alcanzar el entorno 2035, se pueden destacar cuatro grandes grupos. Hay que señalar que, en todos los casos, se trata de una categoría de inteligencia denominada específica o débil. Un tipo de inteligencia artificial que es capaz de hacer muy bien una tarea, mejor que un ser humano, por ejemplo, jugar al ajedrez. No obstante, en realidad no sabe qué significa esa tarea y de hecho, si cambian las reglas del juego, por ejemplo, si se juega a algo parecido como podrían ser las damas, podría tener dificultades para adaptarse.

El primer campo de aplicación para la Fuerza 35, sería el de mando y control. En labores de apoyo a la toma de decisiones, si bien también complementará tareas de gestión de la fuerza, gestión logística y mejora en la eficiencia del personal.

Un segundo campo de utilidad, sería el de protección de la fuerza. Por ejemplo, en cometidos de seguridad física, mediante sistemas autónomos para protección perimetral. O también en cometidos de protección contra la guerra de la Información y ataques ciber-electrónicos, mediante la detección de la desinformación, la mejora en la detección de señales enemigas y, sobre todo, mejorando las capacidades de ciberdefensa.

Un tercer campo, lo constituye el de la inteligencia, con aplicación a sistemas de alerta temprana y medios de reconocimiento y vigilancia. En tres procesos principales. Hacer predicciones, mejorando la capacidad para predecir las actividades del enemigo. Para procesamiento de datos, mediante un eficaz análisis y fusión de datos. Y, en tercer lugar, para la detección y la identificación.

El cuarto campo de provecho afectaría a la maniobra en concreto a los ataques de precisión y despliegue de medios. Por un lado, para mejora de las capacidades ofensivas ciber y para mejorar su capacidad de reconocer objetivos y el control de la navegación autónoma.

En definitiva, la Fuerza 35 constituye la gran revolución digital del Ejército de Tierra para el horizonte 2035 que incorporará, entre otras, tecnologías disruptivas, sistemas avanzados de inteligencia artificial específica. Pero va a ser mucho más que eso. Va a representar una profunda transformación cultural. Los principios básicos y éticos no van a cambiar, pero sí lo van a hacer las formas de trabajo, las estructuras de organización, los talentos del personal, las actitudes que habrá que promover, la actitud positiva frente al cambio, la flexibilidad, el trabajo en equipo, y desde luego la obsesión por el combatiente, por mejorar siempre su experiencia.

Coronel Francisco Palomo

Mando Conjunto del Ciberespacio. Ministerio de Defensa.

C.V. *En sus más de 29 años de servicio ha ocupado destinos relacionados con Sistemas de Telecomunicaciones e Información, Guerra Electrónica, Seguridad de la Información y Ciberdefensa, tanto en España como en el exterior, participando en misiones en Bosnia-Herzegovina y en Líbano. En agosto de 2018 fue destinado al Mando Conjunto de Ciberdefensa, Mando que, desde septiembre de 2020, y debido a la ampliación de funciones, ha pasado a denominarse Mando Conjunto del Ciberespacio (MCCE).*

LA DEFENSA Y EL MANDO CONJUNTO DEL CIBERESPACIO.

1. El origen de la ciberdefensa en las Fuerzas Armadas.

En el año 2013 el Gobierno de España publica la primera Estrategia de Seguridad Nacional. Dentro de ella se destacan como uno de los riesgos y amenazas para la Seguridad Nacional las ciberamenazas. En cuanto a las líneas de acción estratégicas destacaba entre otras la de la ciberseguridad. En el mismo año 2013 se publica también la Estrategia de Ciberseguridad Nacional derivada de la anterior, en la que se destaca el ciberespacio como un ámbito accesible, poco regulado y de difícil control. En línea con estos dos documentos y debido a una preocupación creciente tanto interna como en el ámbito de las organizaciones internacionales (sobre todo la OTAN) en ese mismo año el Ministerio de Defensa crea el Mando Conjunto de Ciberdefensa (MCCD) con la misión del planeamiento y ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que pudieran afectar a la Defensa Nacional.

En el año 2017 el Gobierno publica una nueva Estrategia de Seguridad Nacional. Como consecuencia de la anterior, en 2019 se publica una nueva Estrategia Nacional de Ciberseguridad. En el Ministerio de Defensa en el año 2020 se crea el Mando Conjunto del Ciberespacio (MCCE) tomando como base el Mando Conjunto de Ciberdefensa (MCCD) y la Jefatura de Sistemas de Telecomunicaciones e Información de las Fuerzas Armadas (JCISFAS), es decir, se unifican el planeamiento del ciberespacio (JCISFAS) con el planeamiento y la ejecución de la protección del mismo (MCCD).

2. Misión de ciberdefensa del MCCE.

La misión del Mando Conjunto del Ciberespacio es la de planear, dirigir, coordinar, controlar y ejecutar las acciones conducentes a asegurar la libertad de acción de las Fuerzas Armadas en el ámbito ciberespacial. Esta misión incluye la realización de operaciones ofensivas, de inteligencia, reconocimiento y vigilancia y defensivas. En este documento nos centraremos en concreto en las operaciones defensivas dentro de los Sistemas de Telecomunicaciones e Información del Ministerio de Defensa (MINISDEF).

3. El ciberespionaje en los Sistemas de Telecomunicaciones e Información del MINISDEF.

En los Sistemas de Telecomunicaciones e Información del Ministerio de Defensa disponemos tanto de sistemas clasificados como sin clasificar. Los primeros son aquellos que manejan información clasificada, que se encuentran aislados (no conectados a internet), bastionados, es decir, configurados de manera segura siguiendo las guías CCN-STIC del Centro Criptológico Nacional (CCN) y que además cuentan con capacidades de ciberdefensa. Además de estos, los que tienen más probabilidad de sufrir un ataque por estar expuestos a internet son los sistemas que manejan información no clasificada. Normalmente los segundos son sistemas con un número elevado de usuarios y en los que es más complejo controlar los flujos de información tanto entrante como saliente.

Como cualquier otro sistema expuesto a internet los Sistemas del MINISDEF sin clasificar pueden sufrir ataques de ciberdelincuentes que buscan monetizar la información obtenida de manera fraudulenta de nuestras redes, que buscan obtener dinero extorsionando a la organización propietaria de la información o incluso atacando a los usuarios finales para cometer acciones de fraude o extorsión sobre los mismos.

Para evitar el éxito de estos ataques el MCCE emplea técnicas semejantes a las que se emplean tanto en el resto de las Administraciones Públicas como en las empresas civiles, elevando el nivel de protección y empleando técnicas de detección para poder mitigar los ciberincidentes con el menor impacto posible.

Pero además tenemos que luchar contra otro enemigo mucho más peligroso: el ciberespionaje. Normalmente conocido en medios técnicos como "APT" (Amenazas Persistentes Avanzadas) son equipos de personas que emplean técnicas sofisticadas, patrocinados normalmente por estados y que trabajan con sigilo, con el objetivo de obtener información de objetivos seleccionados, en este caso el Ministerio de Defensa de España.

Las vías de entrada de los ataques habitualmente no son muy diferentes a las empleadas por el resto de ciberdelincuentes, es más, en muchos de los casos intentan parecer un ciberdelicuente más para pasar desapercibidos. El método más normal es el del "Phishing" o intento de engaño a un usuario mediante el envío de un correo electrónico o similar. El atacante se hace pasar por una persona u empresa de confianza para obtener información de la víctima (datos personales, usuario y contraseña, etc.) o de su organización o, en otros casos, para conseguir mediante el envío de un enlace a una página web, que se efectúe la descarga de malware para infectar el dispositivo. Posteriormente, cuando el dispositivo está infectado, se intenta conseguir persistencia y escalar privilegios para poder acceder a los sistemas con seguridad y moverse lateralmente por los dispositivos de la organización, estableciendo nuevas vías de acceso, localizando la información objetivo de la campaña y tomando el control total, bien del dispositivo bien de la organización a la que pertenece. La gran diferencia con los ciberdelincuentes habituales es el enorme trabajo previo que hay de ingeniería social en los ataques de ciberespionaje.

A veces nos podemos encontrar lo que se denomina "spear Phishing", muy similar al anterior pero con una carga de ingeniería social mucho mayor, totalmente dirigidos hacia una persona objetivo, y que conlleva un conocimiento en profundidad de la víctima. Normalmente los objetivos de los Spear Phishings son los puestos directivos o el personal de departamentos técnicos, los primeros porque pueden tener acceso a información muy valiosa de la organización y los segundos porque pueden disponer de información de la red que permitiría el ataque a esta con mucha mayor facilidad.

Cada día más podemos ver lo que denominan ataques a través de terceros (cyberattacks through third parties), es decir, atacar a una empresa que tiene algún tipo de relación con la organización objetivo pero que tiene un nivel de protección inferior. Una vez conseguido el ataque a esta organización menos protegida, ésta se emplea como vía de entrada al organismo objetivo. En el MINISDEF en el año 2020 se ha podido observar un incremento importante de este intento de vía de entrada en el que se puede observar, además del aumento de la cantidad de ataques de este tipo que se producen, la complejidad de los mismos, lo que nos hace pensar que nos encontramos con una estructura muy organizada detrás y podemos deducir que no somos un objetivo de oportunidad sino que somos el objetivo final del ataque.

Por último, se pueden destacar los ataques más complejos y elaborados en los que se intenta explotar alguna vulnerabilidad en la parte de los sistemas expuestos a internet. Esta vulnerabilidad puede ser conocida (caso más habitual) aunque en algún caso determinado se puede hablar incluso de los conocidos como "Zero Days" que son ataques empleando vulnerabilidades no conocidas ni publicadas.

4. Cómo protegerse del ciberespionaje.

Los atacantes, bien sean ciberdelincuentes en general, bien sean ciberespías en particular, saben que el escalón más débil de la cadena normalmente es el usuario. Podemos tener a la mayor parte de los usuarios con un nivel de formación elevado, pero con que solo uno de ellos no lo esté puede provocar el compromiso

de la organización al completo. La labor de concienciación de todos los usuarios es fundamental, deben sentirse una parte muy importante y activa de la protección de la organización frente a ataques externos.

Pero además debemos tener una protección robusta, basada en capas con diferentes niveles, lo que en el entorno militar se denomina "defensa en profundidad". Es necesario conocer los activos de la organización y clasificarlos en base a su criticidad, para así poder centrarnos en un primer momento en proteger lo que pueda tener un mayor valor para la organización y posteriormente continuar con los activos de una importancia menor.

Es muy importante tener los sistemas actualizados para evitar a nuestros enemigos aprovechar vulnerabilidades conocidas para atacar nuestros sistemas. Esto en organizaciones de gran tamaño es difícil de conseguir ya que se emplean una gran cantidad de dispositivos y aplicaciones, adquiridos en momentos diferentes y que en un determinado momento dejan de estar mantenidos por las empresas suministradoras. Hay que contar con un sistema automatizado de gestión de vulnerabilidades que ayude a reducir la superficie expuesta a las amenazas.

Posteriormente debemos centrarnos en la detección y la respuesta, en un primer momento de manera reactiva, es decir, reaccionar con prontitud ante los ataques que sufra la organización para ser mitigados en el menor tiempo posible. El siguiente paso es la detección y respuesta proactiva, es decir, buscar en base a la información proporcionada por la inteligencia de ciberamenazas, que nos indica las Tácticas, Técnicas y Procedimientos (TTP,s) empleados por nuestros posibles atacantes, la obtenida por incidentes de seguridad anteriores o incluso la proporcionada por el resto de organizaciones aliadas dedicadas a la ciberdefensa/ciberseguridad con las que se colabore.

Por último, pero no por ello menos importante, debemos destacar que se debe mejorar la resiliencia de la organización, es decir, tenemos que asumir que los ataques, que los incidentes de ciberseguridad se van a producir en la organización y debemos estar preparados para cuando estos ocurran. Es necesario disponer de un sistema de copias de seguridad y fuera de línea para evitar que sea infectado en caso de un ataque.

La protección total no existe y aunque existiera seguramente tendría un precio tan elevado que no sería asumible, es mucho más realista elaborar unas políticas que permitan recuperar la normalidad en el mínimo tiempo posible y con el mínimo impacto posible, tanto económico como en la reputación.

El diseñar sistemas basados en "Zero Trust", es decir, considerar a todos los usuarios como extraños hasta que no hayan sido validados y legitimados proporciona un nivel adicional de seguridad. En estos momentos en los que el teletrabajo se ha impuesto es necesario incorporar capas adicionales de seguridad que permitan en todo momento asegurarse que los usuarios son quienes dicen ser y solo acceden a los recursos de los sistemas a los que están autorizados.

5. Conclusiones.

El Mando Conjunto del Ciberespacio es la unidad responsable de la protección y defensa de los Sistemas de Telecomunicaciones e Información del Ministerio de Defensa.

Los sistemas más susceptibles de ser atacados en el Ministerio de Defensa son los que manejan información no clasificada debido a que están expuestos a internet y tienen un mayor número de usuarios.

El Ministerio de Defensa es un objetivo tanto de ciberdelincuentes como de ciberespías teniendo estos últimos una mayor peligrosidad debido a su sofisticación, sus mayores capacidades y a estar patrocinados por estados.

Los ciberespías suelen emplear técnicas que se asemejan a las empleadas por el resto de ciberdelincuentes para enmascararse entre ellos, aunque tienen un gran trabajo previo de ingeniera social. Cuando consiguen infectar al objetivo cuentan con una persistencia que dificulta mucho su mitigación por completo, empleando como vector de entrada un amplio abanico de técnicas entre las que se encuentran los ataques a través de terceros, la explotación de vulnerabilidades conocidas y en algún caso incluso el empleo de "Zero Days".

Para defenderse del ciberespionaje es necesario montar una defensa en profundidad identificando los activos vitales de la organización y estableciendo políticas para protegerlos.

Inspector Antonio Gómez

Grupo Ciberdelincuencia de la Jefatura Provincial del Cuerpo Nacional de la Policía de Málaga.

C.V. *Experiencia en grupos operativos relacionados con Estupefacientes, Seguridad Informática, Policía Judicial y Ciberdelincuencia. Ha realizado numerosos cursos y jornadas de formación sobre Abuso sexual infantil, Cibercrimen, Delincuencia organizada y tecnológica.*

PROTECCIÓN FRENTE A LA CIBERDELINCUENCIA. CUERPO NACIONAL DE POLICÍA.

El Grupo de Ciberdelincuencia de la Comisaría Provincial de Málaga, perteneciente al Cuerpo Nacional de Policía, tiene como misión, entre otras, la investigación, como Policía Judicial específica, de aquellos hechos delictivos cometidos a través de Internet o por medio de la utilización de las Nuevas Tecnologías. Además de las investigaciones propias de policía judicial, lleva a cabo una serie de acciones de carácter técnico, en el ámbito del descubrimiento, preservación y estudio de evidencias de carácter digital.

Como grupo de investigación, se encarga de todos aquellos hechos delictivos en los que, de algún modo, se hayan utilizado técnicas delincuenciales relacionadas con las conocidas como TICs (Tecnología de la Información y la Comunicación), ya sea en cuanto a delitos que afecten directamente a personas físicas o a su patrimonio.

Los delitos más habituales investigados por este grupo, relativo a personas, son los siguientes:

- Injurias, Calumnias, Amenazas, Vejaciones, Acoso (Cyberbullying).
- Pornografía infantil. (Tenencia, Distribución, Producción).
- Child Grooming. (Acoso a menores de 16 años).
- Sexting. (Distribución de imágenes íntimas sin consentimiento).
- Descubrimiento y revelación de secretos.
- Delitos de odio.

Por otra parte, los delitos más habituales relativos al patrimonio, son los siguientes:

- Estafas en compraventas (páginas web fraudulentas).
- Transferencias Fraudulentas.
- Vulneración de sistemas informáticos (DDOS, Malware, Ransomware, etc.).
- Sextorsión.

- Phising, B.E.C., Sim Swapping (Duplicado de tarjeta Sim).

Actualmente, los delitos relativos al patrimonio más habituales siguen estando encabezados por el "phising". Esta modalidad delictiva, consiste en suplantar una entidad, habitualmente bancaria si bien no siempre tiene que ser así, indicando a la potencial víctima una serie de circunstancias que la obligan a facilitar los datos necesarios para poder acceder a su dinero. Generalmente solicitan la numeración de la tarjeta junto con la fecha de caducidad y el código CCV para poder operar. La víctima, creyendo en todo momento que se está comunicando con su entidad, facilita los datos requeridos a fin de no tener problemas. Los ciberdelincuentes se adaptan a los tiempos, habiendo crecido la suplantación de empresas de paquetería, solicitando a las víctimas datos de tarjeta a fin de realizar un reembolso o para pagar unos gastos de envío y entregar el paquete, suplantan entidades oficiales para el abono de prestaciones o incluso empresas privadas para la devolución de recibos (phising de Endesa). Nunca se han de facilitar claves por correo, las entidades siempre avisan de que jamás solicitan ese tipo de información por correo, hay que desconfiar de ese tipo de mensajes y hacer comprobaciones en caso de duda (llamada de teléfono a la entidad).

Otra modalidad delictiva que afecta tanto a particulares como a empresas, es el conocido como "Ransomware", consistente en el envío de un malware que consigue encriptar todos los archivos del ordenador o servidor de la empresa, solicitando los ciberdelincuentes un rescate a cambio de su desencriptación. El modo más habitual de infectar los equipos, es mediante el envío de un correo electrónico con algún archivo adjunto, el cual contiene el malware. En este caso, se recomienda no ejecutar archivos adjuntos de remitentes desconocidos, tener copia de seguridad del sistema, realizada de forma independiente, es decir, nunca tener conectada de forma continua la copia de seguridad, puesto que se corre el riesgo de que también sufra el ataque del malware, tener sistemas de seguridad adecuados y por supuesto, no pagar nunca a los ciberdelincuentes.

También se está notando cierto incremento en las denuncias relacionadas con la modalidad delictiva conocida como BEC (Business Email Compromise). Los ciberdelincuentes consiguen controlar el tráfico de correos de una empresa y, cuando se ha de realizar un pago, suplantan la identidad de la empresa que ha de cobrar el importe, cambiando la cuenta bancaria donde se ha de hacer el ingreso. En alguna ocasión, la víctima tarda tiempo en darse cuenta del error, llegando incluso a realizar más de un pago. ¿Qué se puede hacer para prevenir estos hechos?, lo principal es mantener informados a los trabajadores sobre esta modalidad, para que estén atentos a posibles variaciones en las cuentas bancarias, asimismo, al igual que en el caso anterior, no ejecutar archivos procedentes de fuentes desconocidas y, en el caso de la más mínima duda, realizar las comprobaciones pertinentes, en ocasiones una simple llamada telefónica de confirmación, puede ahorrar muchos quebraderos de cabeza.

Por lo que se refiere a los delitos que afectan directamente a las personas, es decir, que no hay específicamente un ánimo de lucro en los autores, destacan todos aquellos que afectan a los menores.

Uno de los más peligrosos, por el desenlace final que buscan sus autores, es conocido como "Child Grooming". Un adulto contacta con un menor de dieciséis años, con el objetivo de embaucarle para mantener un encuentro de carácter sexual con el mismo. Es muy habitual que antes de llegar a ese encuentro (el cual no siempre se llega a producir), el adulto le solicite imágenes de contenido sexual del menor, con dichas imágenes puede comenzar una secuencia de extorsiones, solicitando al mismo nuevas imágenes a cambio de no difundir las anteriores.

Otra de las modalidades delictivas que se repiten entre menores, si bien también afecta a los mayores de edad, es el conocido como "Sexting", la difusión de imágenes íntimas sin la autorización de su protagonista, que fueron obtenidas en un espacio íntimo y con el consentimiento del mismo. Suele darse en rupturas de pareja como acción de venganza. Como se apunta, se está dando en relaciones entre menores, al no

compartir domicilio y tener relaciones a distancia, suele ser habitual el envío de imágenes y vídeos de carácter sexual cuyo contenido, una vez enviado, deja de estar bajo el control de la persona. Por eso es importante concienciar a los usuarios que, todo aquello que salta a la Red, deja de ser un elemento controlable y por lo tanto es susceptible de caer en manos no deseadas, resultando prácticamente imposible su eliminación total.

En el caso de los menores y la utilización de las nuevas tecnologías, existen formas de prevenir que hagan un uso incorrecto de las mismas, como por ejemplo las aplicaciones de control parental, las cuales monitorizan el contenido visitado, limitan el tiempo de uso, etc. También conviene respetar los límites de edad establecidos para utilizar las diferentes aplicaciones, redes sociales etc. Pero lo más importante es siempre la educación en el uso de las nuevas tecnologías desde una edad temprana, acompañando al menor en cada etapa y, bajo ningún concepto, dejarle que interactúe en Internet a solas y fuera de las horas normales, lamentablemente se dan casos de menores con edades muy bajas, con su propio ordenador o tablet en su habitación, lo que conlleva el peligro de que se conecten a unas horas en las que los padres no pueden controlar lo que están haciendo.

Aporta también su Presentación.

Teniente Coronel de la Guardia Civil. José Durán.

Unidad contra el crimen organizado. Delitos telemáticos.

***C.V.** Teniente Coronel de la Guardia Civil, y en la actualidad trabaja en la Unidad de Coordinación de Ciberseguridad. Anteriormente dirigió el Grupo de Delitos Tecnológicos de la Unidad Técnica de Policía Judicial durante 4 años. Entre 2015 y 2016 representó a la Guardia Civil en el Grupo de Acción Conjunta contra la Ciberdelincuencia (JCAT) de Europol.*
Cuenta con más de 20 años de experiencia profesional, desarrollada siempre en los ámbitos de la investigación policial, análisis de inteligencia, y en el campo de la colaboración policial internacional. Ha realizado distintos cursos de carácter profesional como el Curso Superior de Información, Curso de Liderazgo de Equipos Conjuntos de investigación, Curso de Inteligencia Prospectiva contra el Crimen Organizado, etc. Además, cuenta con diversos estudios de postgrado relacionados con el ámbito de la seguridad incluyendo un Máster en Seguridad Informática y un Máster en Evidencias Digitales y lucha contra el cibercrimen.

DELITOS TELEMÁTICOS Y TECNOLÓGICOS. GUARDIA CIVIL.

La Guardia Civil, junto al resto de fuerzas y cuerpos de seguridad, tiene la misión de proteger el libre ejercicio de nuestros derechos y garantizar la seguridad ciudadana. Y, aunque con distintas formulaciones, los guardias civiles hemos estado llevando a cabo esta misión desde los tiempos de nuestra fundación en 1844, y recientemente hemos celebrado el 175 Aniversario.

Al principio únicamente por tierra, pero a medida que la Institución fue creciendo en entidad, funciones y competencias, se vio avocada a hacer uso también del medio aéreo y marítimo. Y como no podía ser de otra manera, a mediados de la década de los 90 la Guardia Civil creó el entonces llamado Grupo de Delitos Informáticos para atender a la todavía incipiente demanda de los ciudadanos. Mucho ha llovido en estos casi 25 años. Internet ha sufrido una transformación tremenda y ha cambiado las comunicaciones, los negocios, las relaciones personales, el ocio, en definitiva, ha transformado el mundo. Y lo ha hecho hasta el punto de que podemos afirmar que se ha creado una nueva dimensión de la realidad, una dimensión en la que vivimos gran parte de nuestras vidas y que denominamos ciberespacio. La Guardia Civil también ha evolucionado, creciendo y adaptándose a las nuevas circunstancias, lo que le ha llevado a dotarse con Unidades muy especializadas dedicadas a amenazas como el Hacktivismo o Ciberterrorismo.

Además, en el ámbito de la lucha contra la ciberdelincuencia, que es en el que más recursos se dedican, la pequeña unidad creada en 1996 se ha convertido en una de las unidades más reconocibles y mediáticas de la Guardia Civil, el Departamento de Delitos Telemáticos de la Unidad Central Operativa. Además, contamos con un Grupo de Delitos Tecnológicos dentro de la Unidad Técnica de Policía Judicial, nuestra unidad de inteligencia criminal, y con un importante y avanzado Laboratorio de Informática forense encuadrado en el Servicio de Criminalística de la Guardia Civil. Adicionalmente, contamos con especialistas en investigación Tecnológica desplegados por todo el territorio nacional, los denominados EDITEs, que suponen un primer escalón de proximidad para el ciudadano.

Al margen de estas capacidades, todas dedicadas a la lucha contra el cibercrimen, la Guardia Civil también se ha visto en la necesidad de proteger sus sistemas e infraestructuras informáticas. Somos una institución con unos 80.000 efectivos y más de 2.000 instalaciones desplegadas por todo el territorio nacional. La información que se gestiona, sobre terrorismo, crimen organizado, sobre nuestros ciudadanos… es ciertamente muy sensible y por lo tanto hacer seguros los sistemas que utilizamos es de vital importancia. En este aspecto, la unidad competente es la Jefatura de Servicios Técnicos. El último actor en incorporarse a todo este abanico de recursos dedicados de una manera u otra a la ciberseguridad ha sido la Unidad de Coordinación de Ciberseguridad. Creada formalmente en 2019 y puesta en marcha a principios del año 2020, tiene entre sus funciones las de servir de Punto de Contacto institucional de la Guardia Civil para la interlocución en materia de ciberseguridad, así como la definición de criterios de coordinación y optimización del potencial disponible para hacer frente a las ciberamenazas, impulsando la actuación coordinada de las distintas unidades con competencias en ciberseguridad.

Obviamente existe una demanda creciente en la ciudadanía, empresas e Instituciones que han empujado a la Guardia Civil a crecer en capacidades. Sin embargo, es preciso señalar también la existencia de referencias a nivel estratégico, como la Estrategia de Seguridad Nacional (2017) y, sobre todo, la Estrategia Nacional de Ciberseguridad de 2019 que viene a establecer una serie de objetivos, con los que la Guardia Civil obviamente ha de alinearse. Esto impulsa a la Institución a luchar contra todas las formas de criminalidad en internet manteniendo actualizadas sus capacidades y adaptándose a la evolución de las distintas amenazas.

También supone que la Guardia Civil contribuya a la difusión de la Cultura de ciberseguridad, cuestión que sin duda se lleva haciendo muchos años y en diversos frentes, pero que ahora se pretende relanzar desde la Unidad de Coordinación de Ciberseguridad mediante el establecimiento de un plan concreto a tal efecto.

Otros aspectos fundamentales para el papel que la Guardia Civil desempeña en el mundo de la ciberseguridad y que se impulsan desde la Estrategia Nacional de Ciberseguridad son el fomento de la colaboración con el sector privado y la protección de los sistemas propios y de la información que gestiona la Institución. Adicionalmente, todas estas actividades han de impulsarse y llevarse a cabo tanto a nivel nacional como internacional.

En cuanto a Ciberamenazas, veamos a continuación las amenazas procedentes del ciberespacio que más preocupan, y ocupan, en la actualidad a las agencias policiales de todo el mundo. En primer lugar, tenemos el fenómeno del “Ransomware”, que hace años que se mantiene como la amenaza más prevalente y dañina desde el punto de vista económico. Como aspecto novedoso se puede indicar que se observa cómo los ataques ya no son totalmente indiscriminados, sino que se realizan de manera cada vez más dirigida a empresas y entidades, tanto del sector público como privado. Otro de los ciberataques que más pérdidas está produciendo a las empresas es el denominado BEC (Business Email Compromise) que, aunque puede tomar muy diversas formas, básicamente consiste en engañar a un empleado para que realice un pago de una factura falsa a una cuenta bancaria controlada por los cibercriminales. En ocasiones se trata de simples engaños, “ingeniería social” sencilla que, por un motivo u otro, llega a funcionar. Pero también podemos encontrar ataques muy sofisticados desde el punto de vista técnico y que implican intrusiones en los

sistemas de la empresa atacada o sus proveedores. Las Fugas de información son otro de los incidentes de ciberseguridad más frecuentes.

Aquí la casuística es también muy variada y encontramos desde ataques relativamente sencillos hasta otros llevados a cabo por grupos vinculados a actores estatales. Lo que sí podemos afirmar es que cualquier tipo de información puede ser de interés. No pensemos que los cibercriminales únicamente buscan credenciales de acceso a banca online, o datos de medios de pago. Muy al contrario, los criminales tratan de sacar partido a todo tipo de información, y otros datos personales, que pueden no ser directamente "monetizables", pero pueden llegar a tener un valor potencial incluso mayor al permitirles extorsionar a empresas, o realizar, gracias a esa información, ataques más complejos como los BEC antes mencionados. Además, otro aspecto a valorar con respecto a este tipo de ataques, son las consecuencias legales e importantes multas que pueden imponerse en determinadas circunstancias.

Otro aspecto que lleva años cobrando relevancia creciente son los ataques a la cadena de suministro que, precisamente son el origen de muchas de las fugas de información de las que acabamos de hablar. Y es que se observa una tendencia creciente en el uso de clientes, proveedores y partners como una forma de atacar un objetivo que, a priori, puede estar mejor protegido. Todos los negocios forman parte de una cadena y, aunque resulte obvia la afirmación, ésta es tan fuerte como el más débil de sus eslabones. Por último, y aunque no se trata de un ciberataque propiamente dicho, los ataques de desinformación o "fake news" sí que pueden llegar a ser una amenaza para nuestras empresas y, obviamente, se trata de una amenaza que se propaga por el ciberespacio. La solución en estos casos pasa por la concienciación, prevención, y gestión de la comunicación, más que por medidas de ciberseguridad propiamente dichas. Retos para las investigaciones policiales ¿Qué podemos hacer al respecto de todas estas amenazas? Pues desde el punto de vista policial la respuesta es obvia: investigar, como con cualquier otro delito.

Sin embargo, las investigaciones tecnológicas, tienen una serie de dificultades añadidas o peculiaridades que precisamente derivan de la propia naturaleza de las conductas que se investigan. Aunque el objetivo de una investigación policial es siempre el mismo (identificar al autor de un delito y obtener pruebas de la comisión de este), las investigaciones tecnológicas normalmente van a afectar a procesos de comunicación, que están especialmente protegidos en la mayoría de los ordenamientos jurídicos y, desde luego, en el nuestro. Además, las técnicas de investigación tradicionales resultan insuficientes, siendo necesario utilizar y aprovechar la potencialidad de las herramientas tecnológicas que, además, van a tener que ser utilizadas por personal altamente especializado. Estos factores van a condicionar las investigaciones y, en cierto sentido, a dificultarlas.

Pero ¿qué dificultades concretas nos encontramos a la hora de llevar a cabo investigaciones tecnológicas? A efectos didácticos y sin ánimo de ser exhaustivo, hemos clasificado aquí las dificultades/retos en tres grandes grupos:

- Por un lado, dificultades relacionadas con la imposibilidad por parte de los investigadores de acceder a información necesaria para la investigación.
- También la incapacidad para determinar una ubicación ya sea de autor, infraestructura, pruebas e incluso de las víctimas.
- Finalmente, por supuesto, existen toda una serie de problemas relacionados con aspectos legales que dificultan el éxito de las investigaciones policiales.

Con respecto a la pérdida de información necesaria para la investigación o incapacidad de acceso a la misma, existen varios factores que contribuyen negativamente: En primer lugar, tenemos los proveedores de servicios

OTP (Over the Top) que ofrecen comunicaciones vía IP y que actúan con independencia de la red de telecomunicaciones que les da soporte. Servicios como Whatsapp, Telegram, etc. son usados para mensajería, llamadas de voz, video llamadas, etc.

Estos servicios, no están normalmente sujetos a la normativa de interceptación legal de comunicaciones, ni tampoco a la de Conservación de Datos, con lo que el acceso a dichas comunicaciones resulta muy complejo para los investigadores. Precisamente las diferencias entre los distintos regímenes de Conservación de datos, y en ocasiones la inexistencia de estos también supone un gran reto para los investigadores. Sin embargo, este tipo de información que, recordemos, no incluye el contenido de la comunicación sino sólo datos asociados a la misma, ha demostrado ser útil en casos tan complejos como el caso de Diana Quer.

La creciente implementación de tecnologías de cifrado por defecto en todo tipo de dispositivos y comunicaciones supone también un hándicap. Aunque el cifrado tiene un evidente efecto positivo en el ámbito de la ciberseguridad, es también innegable que dificulta extremadamente algunas técnicas de investigación como la interceptación de comunicaciones o el análisis forense de dispositivos electrónicos, fundamentales para la investigación criminal.

También el uso de criptomonedas y otros servicios asociados que incrementan el anonimato y actúan a modo de cortafuegos, impiden a los investigadores seguir el flujo del dinero, y complican significativamente la recuperación de activos y las actividades de prevención de blanqueo de capitales y de transacciones fraudulentas.

Por último, también en este grupo de dificultadas relacionadas con la incapacidad de los investigadores de tener acceso a información relevante para sus investigaciones, quiero mencionar la elevada “cifra negra” existente. Es decir, delitos que no son denunciados y que, por tanto, no existen a efectos de investigación policial. Es necesario realizar, y lo estamos haciendo, una labor de concienciación en este sentido ya que cuanta más información tengamos, mayores serán las posibilidades de éxito de la investigación.

Hablemos ahora de los problemas relacionados con la determinación de una ubicación de interés para la investigación. Existen tecnologías como el uso de criptomonedas basadas en sistemas distribuidos, y que carecen de autoridad central a la que dirigirnos (para bloquear y/o solicitar información); las tecnologías de anonimización como VPNs, y Darknets como Tor, I2P, etc. que además de ofrecer anonimato, albergan mercados y servicios criminales de muy difícil localización; e incluso el hoy generalizado uso de servicios y almacenamiento en la nube, que hace que la información pueda encontrarse simultáneamente o de forma fragmentada en diferentes jurisdicciones. Pues bien, todos estos factores hacen que las agencias policiales tengan problemas para establecer la ubicación física del ciberdelincuente, de la infraestructura usada en la actividad criminal, de las pruebas electrónicas, e incluso en ocasiones, como en el caso de algunos delitos sexuales contra menores, de las víctimas. En estas situaciones normalmente no está claro qué país tiene jurisdicción para investigar, obtener evidencias ni perseguir judicialmente a los cibercriminales, lo cual puede suponer un grave perjuicio para la investigación.

Con respecto al marco legal, es necesario recordar que la práctica totalidad de investigaciones tecnológicas cruzan las fronteras de un país y hacen necesario la utilización de mecanismos de cooperación internacional que se ven dificultados por las diferencias entre los distintos marcos normativos nacionales. Estas diferencias, que suelen responder a una transposición incompleta de instrumentos de cooperación internacional, se dan principalmente en cuanto a: conductas criminalizadas (Código Penal) y/o medidas de investigación previstas (Ley procesal). Tampoco existe en la actualidad un marco que permita el intercambio o remisión rápida de evidencias digitales, como sí ocurre con la preservación rápida (arts. 16 y 17 Convenio Budapest). En la práctica, los tiempos de los procedimientos de Cooperación Jurídica Mutua pueden llegar a poner en peligro la eficacia de las investigaciones.

Resulta igualmente necesario reconocer que nos resulta imposible legislar al ritmo que marcan los avances en tecnología y el uso criminal de éstos. La justicia siempre ha corrido detrás de los delincuentes, pero en la actualidad se podría afirmar que la distancia entre unos y otros va en aumento y resulta difícil de reducir.

Finalmente, otra deficiencia comúnmente observada en muchos países es la falta de regulación específica sobre las investigaciones online que, sin duda, dificulta la colaboración policial internacional y pone en peligro el buen fin de las investigaciones. Por fortuna podemos decir que, desde 2015, España cuenta con una moderna regulación, que, al menos en parte, nos ofrece los instrumentos jurídicos necesarios para enfrentarnos a muchos de los retos y problemas que hemos mencionado. Así, la Ley orgánica 13/2015 viene a regular aspectos tales como la figura del agente encubierto online, el registro de dispositivos electrónicos y su posible extensión a terceros sistemas legalmente accesibles desde el dispositivo registrado, el registro remoto de dispositivos… y muchas otras medidas de investigación tecnológica que, ofreciendo los máximos estándares en cuanto a garantías para los ciudadanos, ofrecen soluciones legales para que los investigadores puedan hacer su trabajo y proteger a los ciudadanos.

Aporta también su Presentación.

José Miguel Ruiz Padilla

Director Servicios Gestionados y Ciberseguridad. INGENIA. Málaga TechPark-Parque Tecnológico Andalucía.

C.V. *Ingeniero de Telecomunicación por la Universidad de Málaga y MBA Executive por la EOI, con más de 23 años experiencia en sector TIC. Inició etapa profesional como Ingeniero de Diseño de Servicios en Telefónica Móviles en Madrid, en Ericsson Eurolab en Alemania y en Belgacom Mobile en Bélgica. Posteriormente regresa a España para cofundar Libera Networks, compañía especializada en tecnologías inalámbricas. Ha sido Decano del Colegio Oficial de Ingenieros de Telecomunicación en Andalucía Oriental y Melilla, y miembro de la junta directiva de ETICOM. Es ponente habitual en foros de tecnologías móviles, tecnologías inalámbricas y ciberseguridad, así como de emprendimiento y estrategias de negocio.*

SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS.

No hace tanto no se manejaba el concepto de Oficial de Seguridad de la Información (CISO – Chief Information Security Officer) como Responsable de Seguridad en una organización, el CIO (Responsable de Tecnologías de la Información - TI) no estaba presente en los Comités de Dirección, y se hacían planes estratégicos de negocio sin que hubiera mención relevante a las TI, mucho menos a la ciberseguridad. Por supuesto en los Consejos de Administración tampoco se hablaba de estos asuntos.

Esto ha cambiado en los últimos años y va a seguir así, exponencialmente acelerado por eventos tan disruptivos como la actual pandemia del COVID-19. Vivimos en un mundo hiperconectado, casi 8.000 millones de personas y más de 25.000 millones de dispositivos conectados, y están llegando tecnologías emergentes que actuarán como aceleradores: 5G, inteligencia artificial, biotecnología y computación cuántica. La continua digitalización en todos los aspectos de la vida cotidiana y de los negocios, el abaratamiento del acceso a las brutales capacidades de proceso, memoria y comunicación que poseen hoy día miles de millones de dispositivos móviles conectados – que con 5G se podrán comunicar no sólo con alta velocidad sino también en tiempo real con muy baja latencia – está transformando el mundo como no se veía desde el telégrafo, o incluso puede llegar a tener el impacto que tuvo la máquina de vapor. Toda organización, pequeña, mediana o grande que quiera seguir sobreviviendo en el ecosistema futuro de negocios tiene que ser digital y segura, o no será.

Desde el punto de vista de Ingenia, por lo que nuestros especialistas ven en el día a día, y por las estadísticas, hay muchísimo camino por recorrer. En 2018 se estimaron unos 30 millones de ciberataques (¡80.000 por

día!) en el mundo. Aproximadamente un 64% de compañías de un muestreo a nivel mundial se estima que sufrieron ataques de "phishing" o ingeniería social en 2019. Y este volumen de ataques es creciente.

Simplemente, hoy es muy sencillo para cualquier ciberdelincuente actuar desde cualquier parte del mundo, y es a su vez tremendamente complicado encontrarlos y detenerles como ya se ha comentado por los distintos ponentes de las Fuerzas y Cuerpos de Seguridad del Estado. Las grandes corporaciones y muchas administraciones públicas (AAPP) han avanzado mucho en los últimos años (en las AAPP, que no son objeto de esta charla, es especialmente destacable la labor realizada por el Centro Criptológico Nacional y su capacidad de respuesta a incidentes (CCN-CERT), pero en las Pymes y en el hogar el panorama es muy complicado.

En España recordemos que aproximadamente había (y utilizo el pasado por el impacto que va a tener la pandemia) unos 3,4 millones de empresas activas en 2019, de las que el 97% eran Pymes. Por tanto, millones de empresas, con millones de trabajadores y millones de dispositivos conectados, en un porcentaje muy alto micropymes, en las que ni siquiera hay Responsable de Tecnologías de la Información. Simplemente porque el volumen de negocio no lo permite en la mayoría de los casos. Estas compañías suelen emplear los servicios de un operador de telecomunicaciones para conectividad a Internet, telefonía fija y centralita, móvil, etc., y en su propio conocimiento o el de "amigos y familia". No se pueden permitir mucho más. Pero claro, los "malos", los ciberdelincuentes, no son precisamente comprensivos, si bien es lógico que, sobre todo los organizados, prefieran atacar objetivos más grandes, y no sólo por dinero, sino también por relevancia en el "mundillo", también es cierto que en muchos casos prefieren obtener menores ganancias en un mayor número de objetivos, y las empresas pequeñas son un objetivo más fácil y numeroso. Por tanto, en las Pymes hay mucho por hacer, y no es sencillo abordarlo, aún con ayuda desde el sector público, donde organismos como el Instituto Nacional de Ciberseguridad (INCIBE) han hecho una labor de formación y concienciación necesaria e importante en los últimos años. En mi opinión los operadores de telecomunicaciones y el sector público, trabajando colaborativamente, pueden jugar un papel determinante al respecto.

En las grandes empresas, e infraestructuras críticas especialmente, es otra cuestión. En este caso las estadísticas, y nuestra propia experiencia, nos indican que se ha dado un salto muy importante en los últimos tiempos. Las pruebas realizadas indican que en las principales empresas se está al nivel de nuestro entorno. Parece que la importancia de la ciberseguridad está llegando a los Directores Ejecutivos (CEOs – Chief Executive Officer) e incluso a los Consejos de Administración, que están pidiendo más información, y aprobando planes, inversión, seguros y quieren estar mejor preparados. Estas compañías pueden y en los últimos años están poniendo el foco en ello. Y no ha sido sólo por la concienciación, ni por los profesionales que llevamos en esto 20 años desde los primeros antivirus y firewalls, sino también por el impacto de las continuas noticias y ejemplos de grandes corporaciones que, aún con toda su inversión en seguridad, con mucho presupuesto y personal especializado, han sufrido ataques importantes con un gran coste de negocio y de reputación. Sólo en 2020 están los ejemplos de Tesla (frustrado in extremis), Bolsa de Nueva Zelanda, Mapfre, ADIF, Honda, ENEL, Easyjet, Fresenius (Quirón), EPD, Banco de Chile, o más recientemente Segurcaixa Adeslas, e incluso Garmin, etc. A ello hay que añadir vulnerabilidades críticas continuas publicadas y solucionadas, unas más tarde que pronto, por los grandes fabricantes de IT, Microsoft, Cisco, Fortinet, F5, etc.

La Ciberseguridad se debe abordar en diferentes planos. No puede ser sólo una cuestión de equipos informáticos, hay que tener en cuenta el negocio, la componente estratégica, los procesos, el plano de las personas, su formación y concienciación; y el plano técnico por supuesto, desde el diseño, el software y los datos, los equipos informáticos, pero también los equipos industriales, que ya no pueden confiar simplemente en no estar conectados; y el perímetro, cada día más amplio y difícil de defender pasivamente. Sin olvidar a los proveedores y clientes, porque también pueden ser una brecha de entrada de ataques importante. Se necesita un análisis de riesgos, un análisis de impacto en el negocio y un plan de respuesta

ante incidentes, con un comité de riesgos organizado y donde al frente de una crisis se sitúe el propio CEO. Ahora mismo, en el futuro cercano, las empresas se están enfocando en reforzar principalmente tres áreas: proteger los ingresos, proteger al empleado y proteger los entornos híbridos, porque la pandemia ha supuesto la aceleración de entornos en la nube y el teletrabajo.

Pero aún en muchas organizaciones, la ciberseguridad sigue siendo percibida más como un problema que como otro componente importante e incluso diferencial en el negocio. Como un gasto más que una inversión. Y los CISOs, como "stoppers", si me permiten la expresión. En muchas compañías el CISO y el CIO son la misma persona – nada recomendable - y viven saturados. La ciberseguridad es algo en lo que no se repara cuando frena ataques, porque nada sucede, pero basta un mal día, un agujero en un equipo no parcheado, un descuido de cualquiera de los miles de empleados al pinchar en un adjunto de un correo electrónico, para que se produzca un grave incidente. Especialmente notorios han sido en los últimos tiempos los casos de "ransonware". Cuando no hay un plan de mejora de la seguridad basado en un análisis de riesgos exhaustivo, ni un análisis de impacto en el negocio, se va a ciegas y en muchos casos se tiene la percepción de una seguridad en nuestra organización que no es tal.

Aún persisten como "mitos": Cuanto más se invierta en ciberseguridad, más seguro se estará. Ni existe la seguridad 100%, ni únicamente depende de la inversión. Si bien es cierto que cuantas más medidas disuasorias se implementen en cada plano mayor nivel de seguridad se consigue, es mucho más efectivo conocer los riesgos y trabajar sobre ellos. Muchas organizaciones, sobre todo las más grandes, se siguen midiendo en base a cuánto presupuesto invierten en ciberseguridad, e instalan equipos y equipos de unos y otros fabricantes, más o menos de moda ("la sopa de letras": FW, NGFW, WAF, NAC, SIEM, etc.), en ocasiones buscan únicamente obtener/mantener una certificación, o hay tendencia a "auto-medicarse". Sin un diagnóstico previo, sin saber realmente donde se debe apuntalar, se despliegan controles y medidas que no son necesariamente las que mayor beneficio van a reportar en términos de protección. No son las que más ayudan a mitigar los riesgos o no todos los planos están analizados y asegurados de una manera compensada. Por eso es fundamental ese abordaje previo global, desde el negocio, e implicando a todos los niveles de la organización. Así se obtendrá el máximo provecho de la inversión, que además debe ser adecuada al valor de lo que se está protegiendo. Todos los activos de una organización deben protegerse de la misma forma.

Es esencial priorizar el negocio y proteger de manera eficaz los activos principales, aceptando que habrá intrusiones y que deben tener el mínimo impacto posible. Tarde o temprano algo puede fallar o simplemente un ciberdelincuente va a ser más hábil. La superficie es demasiado extensa para defenderla toda por igual. Antes había un perímetro abordable y los antivirus y firewalls bastaban. Ahora hay "ciudades modernas y complejas" que no se pueden defender como las antiguas ciudades amuralladas medievales, si me permiten el símil. Nuestro equipo rojo (equipo de hackers o de ataque, en contraposición al equipo azul, de defensa) suele tardar poco más de un día en encontrar vulnerabilidades importantes en bastantes clientes sin que sea necesario utilizar ingeniería social o técnicas de suplantación.

Por tanto y para concluir, la ciberseguridad es y va a ser tan esencial en todas las organizaciones en los próximos años como la transformación digital. El futuro es digital y conectado y sólo será sostenible siendo lo más ciberseguro posible, y para ello, las empresas, todas, deben trabajar este aspecto crítico desde su plan estratégico, desde el negocio, con la colaboración de todas las direcciones, y con el CEO y el Consejo de Administración al frente, abordándola desde un punto de vista global, invirtiendo de manera proporcional al valor de lo que se deba proteger, y siendo conscientes de que hay que estar preparados para intrusiones, teniendo en cuenta todos los planos y todos los actores internos y externos, donde se debe perseguir la máxima concienciación posible y la mejora continua, anticipándose y no adoptando una actitud pasiva en la que se actúe cuando ocurra el incidente.

TEXTOS COMPLEMENTARIOS APORTADOS POR LOS PONENTES.

2ª Mesa redonda. Identidad Digital, Comunicación y Manipulación

Moderador: F. Javier López Muñoz. Vicerrector de Empresa, Territorio y Transformación digital de la Universidad de Málaga**.**

https://vimeo.com/498313436

Vicente Díaz

Ingeniero de Seguridad de Google

C.V. *Especialista en Threat Intelligence e ingeniero de seguridad en Google. Se unió al equipo de VirusTotal en 2020. Es Ingeniero Superior en Informática y MsC en Inteligencia Artificial por la UPC. Anteriormente, trabajó como E-crime manager en S21sec durante 5 años, y fue miembro del GReAT (Global Research and Analysis Team) en Kaspersky durante 10 años, siendo responsable del servicio de APT Intelligence Reporting y subdirector del equipo en Europa.*

Aporta también su Presentación.

AMENAZAS PERSISTENTES AVANZADAS.

Esta ponencia se centra en el análisis de la evolución de los ataques conocidos como Amenazas Persistentes Avanzadas (APTs por sus siglas en inglés, correspondientes a Advanced Persistent Threats).

Se puede considerar Stuxnet como el ataque APT por antonomasia. Este ciberataque saltó a la luz pública en 2010, cuando se descubrió un código malicioso que afectaba a las centrifugadoras de uranio utilizadas para el programa nuclear Iraní, destruyendo más de 1000. Evidentemente, era un código destructivo muy específico y creado a medida. Para su creación era necesario disponer de información técnica muy precisa acerca de las instalaciones a atacar. También su despliegue se debía realizar mediante ayuda de operativos externos. Todo esto limitaba el tipo de organizaciones que podían tener interés y capacidad para realizar operaciones de este estilo.

A partir de entonces se adoptó el término APT para ciberataques que implementasen exitosamente una notable complejidad técnica, o cuya fuente u objetivo tuvieran cierta relevancia (por ejemplo, entidades gubernamentales o empresas estratégicas). Inicialmente, no existían gran cantidad de organizaciones con la capacidad de realizar ataques APT, y en general, únicamente un selecto grupo de agencias disponían de este tipo de programas.

En el origen de las primeras campañas APT, cada agencia desarrollaba herramientas muy específicas y personalizadas, lo cual además de tener un coste elevado también proporciona una atribución clara. El descubrimiento y publicación de la campaña Stuxnet tuvo un gran eco en todos los medios, con sus correspondientes repercusiones a todos los niveles. Aunque esto depende en gran medida de las doctrinas que sigan los distintos grupos atacantes, está claro que en la mayoría de casos el hecho de que se publiquen detalles de una operación supone la desarticulación de la misma. No sólo eso, también hace inútiles las herramientas utilizadas, ya que su descubrimiento proporciona la información necesaria para crear una detección. Este mismo eco mediático hizo que la comunidad que trabaja en seguridad se dedicase a

investigar y publicar detalles de todo tipo de campañas categorizadas como amenazas APT, desarticulando muchas de ellas. Todos estos hechos marcaron un cambio de paradigma.

A esta necesidad de herramientas que proporcionasen la capacidad de realizar campañas de ciberespionaje sin la necesidad de desarrollar largos y costosos programas reaccionó el mercado con multitud de empresas que cubrían esta demanda. Todo esto no estuvo exento de polémica, pero la falta de un marco legal junto con el interés de los compradores abonó el terreno para este tipo de soluciones, que, además, hacían más difícil la atribución dado que podían ser usadas por cualquiera que contratase el servicio. Aun así, existían clientes que dadas sus doctrinas o la naturaleza de sus operaciones, no contemplaban el uso de soluciones de terceros. Pero el mercado les proporcionaba la opción de decidir en función de la naturaleza de la operación a realizar.

En paralelo a todo esto, se preparaban una serie de actores que ansiaban disponer de la capacidad de realizar ataques APT, pero que no tenían el músculo económico para desarrollar costosos programas o para comprar soluciones a terceros. Esta nueva generación de atacantes aprovecha la gran cantidad de recursos fácilmente accesibles gracias a Internet o de herramientas creadas para analistas de seguridad. Armados con este conocimiento y código, es posible realizar operaciones con ciertas garantías mientras se evoluciona hacia un modelo propio. El uso de este tipo de herramientas genéricas y disponibles para cualquiera tiene la ventaja adicional de evitar que se pueda atribuir el ataque. Evidentemente, todos estos recursos no serán suficientes para operaciones sofisticadas, pero sí para un gran número de casos en los que lo único que se necesita es estar un paso por delante de la víctima.

Los objetivos de las campañas que persiguen los ataques APT también han evolucionado con el tiempo. Aunque Stuxnet tenía como fin sabotear una infraestructura crítica, en general el principal fin siempre ha sido el ciberespionaje. No obstante, durante los últimos años hemos sido testigos de una evolución de los ataques hacia campañas de desinformación. Algunos ejemplos incluyen el ataque contra el Comité Demócrata de Estados Unidos (DNC por sus siglas en inglés) antes de las elecciones del 2016, o la publicación de información referente a la campaña de Macron en las elecciones francesas del 2017. No sólo eso, también han aparecido grupos anónimos proporcionando todo tipo de detalles acerca de operaciones y herramientas utilizadas por distintos actores, lo que por una parte expone información sensible de sus operaciones pasadas y presentes, y por otra desactiva el uso de dichas herramientas de cara a futuras campañas. No hay que olvidar que la exposición de código malicioso habilita su uso por parte de terceros, en otras palabras, hace a los oponentes más fuertes a costa de la investigación y desarrollo propios. Se puede entender el uso de datos robados en campañas de desinformación como una consecuencia, hasta cierto punto lógica, de la obtención de gran cantidad de datos robados anteriormente. También se puede leer en clave de la facilidad que tienen ciertos actores para obtener datos que puedan usar en este tipo de operaciones.

Un objetivo, hasta cierto punto sorprendente y que ha pasado a formar parte de las operaciones APT es el del lucro de los atacantes. Esto se observó con cierta sorpresa al poderse atribuir de forma técnica ataques contra instituciones financieras por parte de grupos que se cree pertenecen a agencias gubernamentales. Para dar una idea de la escala, en alguno de los casos se intentó el robo de cerca de 1000 millones de dólares. Esto no tardó en replicarse en el tejido cibercriminal, surgiendo grupos altamente especializados en ataques contra entidades financieras aplicando técnicas observadas anteriormente en ataques APT. En la actualidad estos grupos son operativamente difícilmente distinguibles de actores especializados en ataques APT con finalidades de espionaje, suponiendo una amenaza mayúscula para el sector financiero.

No es sencillo entender las capacidades técnicas de las que disponen todos estos grupos y actores. En realidad, sólo podemos hacernos una idea a partir de las operaciones que se hacen públicas o provenientes de filtraciones. Hay que recordar el alto coste para un atacante cada vez que una operación se hace pública, lo que supuso en su día un cambio de paradigma, especialmente de los grupos más avanzados y con mayor

cantidad de recursos. Todo esto aumentó la opacidad de futuras operaciones, lo que hace aún menos visible su capacidad operativa. No obstante, en ocasiones sí podemos hacernos a la idea de en qué punto de desarrollo se encuentran algunos grupos.

Las vulnerabilidades de día 0 (en inglés, 0-day o Zero-day) reciben este nombre dado que son vulnerabilidades existentes en algún programa informático (y que pueden ser usadas por parte de un atacante) para las cuales no existe un "parche" de seguridad que evite su explotación. Estas vulnerabilidades son desconocidas para todo el mundo, excepto para el atacante que las descubre y utiliza. El valor táctico es evidente; en algunos casos alcanzan un precio de mercado de hasta 2 millones de dólares. En la actualidad, las vulnerabilidades que tienen un valor más alto son las que afectan a dispositivos móviles. Sólo como ejemplo, una campaña descubierta en 2019 usaba hasta 14 vulnerabilidades de día 0 contra dispositivos con IOS (como los iPhone, por ejemplo). La conclusión es clara: las capacidades técnicas y la inversión detrás de muchos de estos grupos está por encima de cualquier estimación.

En definitiva, la evolución en los últimos 10 años de este tipo de ataques ha sido meteórica y se ha desarrollado en distintas direcciones, ya sea por cambios de doctrina, por la evolución del mercado o por los nuevos objetivos operacionales. Como conclusión, podemos asegurar que la barrera de entrada para realizar operaciones APT ha bajado considerablemente y todo tipo de actores disponen de estas capacidades a distintos niveles. Quizá lo más preocupante es el desconocimiento que tenemos de los actores más avanzados que apostaron por un cambio de paradigma para ocultar sus operaciones hace ya casi 10 años, y de cuyas capacidades operativas sólo podemos especular que se han hecho prácticamente invisibles para sus víctimas.

Alex Borrás Pardo

Director de Comunicación. Agencia comunicación Digital Site 360.

C.V. *Consultor de Comunicación Digital. Comenzó hace 35 años en la multinacional de informática Ibermática, donde trabajó 13 años. Empezó como programador junior hasta llegar a responsable de productos en Cataluña. En 1.998 se establece por cuenta propia para centrarse en el desarrollo de software empresarial, especializándose finalmente en los sectores de Medicina Privada y Fútbol. Progresivamente trabajó en desarrollo de páginas Web, y en 2010 empezó a trabajar en comunicación política hasta junio de 2016. A partir de ese momento volvió a desarrollar su actividad profesional para empresas y profesionales hasta la fecha. Se ha especializado en la Identidad Digital y la influencia del posicionamiento en buscadores en la toma de decisiones.*

Carlos de Palma Arrabal

Coronel Ejército del Aire (Rva.).

C.V.: *Piloto de aviación militar. Ingeniero de organización industrial. Diplomado Estado Mayor de las Fuerzas Armadas, Curso Sénior OTAN, Curso Oficiales Superiores Iberoamericanos. Experiencia en Coaching. Consejero Defensa Embajadas España en Italia, Malta y Eslovenia. Operaciones en el mediterráneo y Afganistán. Visitas de trabajo en treinta países. Ayudante honorario del Rey de España.*

MANIPULACIÓN MENTAL.

La capacidad, potencia, velocidad y variedad de posibles usos de las tecnologías y dispositivos digitales permite facilitar mucho nuestras vidas, siempre que se usen de acuerdo a Ley y respetando los principios y valores humanos básicos. Esta Ley y valores son los cimientos sobre los que se asienta el verdadero progreso.

En el caso de España, esos cimientos se han formado en el transcurso de la historia, y a través de la Filosofía Griega, el Derecho Romano, la Religión Cristiana, el mestizaje con pueblos de Europa, África y América, el Derecho Internacional, la Declaración Universal de Derechos Humanos, el cuidado del medio ambiente, la atención a la familia, infancia, mujer, mayores, desfavorecidos, etc. Una trayectoria que se condensa y queda reflejada en nuestra Constitución española de 1978.

Las tecnologías, dispositivos digitales y redes sociales que usan el Ciberespacio, unidos a los tradicionales medios de comunicación social, han ampliado las capacidades humanas hasta límites inimaginables hace unos años, y han "empoderado" desde individuos solitarios, a grupos y sociedades enteras que anteriormente no podían ejercer su influencia en la sociedad. Este "empoderamiento" se usa a veces para facilitar la solidaridad, la justicia y el progreso, pero en otras se emplea para manipular nuestras mentes o para delinquir.

Para enfrentarse a las intenciones de manipulación tan sofisticadas que se dan hoy día, es necesaria la reflexión y el juicio crítico, que son capacidades que debe proporcionar una adecuada educación e información previas. Y en redes sociales es necesario, además, tener criterio propio, leer la prensa consultando todas las fuentes de uno y otro signo para salir de nuestras burbujas informativas, oir y hablar con personas de distinta opinión sin caer en la trampa de formar bandos, elegir bien los modelos o líderes a seguir, detectar la mentira y la demagogia, y escapar del rebaño manipulado en que a veces se quiere convertir a determinados grupos sociales. Periódicamente hay que preguntarse ¿estoy manipulado, y en qué grado y aspectos?

Si ya prestamos enorme atención a proteger nuestros dispositivos digitales frente a miles de ataques informáticos y virus, más importante aún es proteger nuestra mente de los cientos de miles de eventos, planes y acciones de manipulación que nos lanzan. No seamos orgullosos. Frente a la manipulación, somos más frágiles de lo que pensamos, pues se manipula siempre por fases, progresivamente, hasta lograr que nos encontremos más cómodos asintiendo que cuestionando, y nos convirtamos en dóciles miembros del rebaño frente a una pantalla.

Y concluyo con una frase atribuida a George Orwell: "*Más importante que mantenerse vivo es mantenerse humano"*. Y esta idea es válida tanto para el mundo físico como para el virtual. Los ordenadores, internet, redes sociales, etc., no deben despojarnos de nuestra humanidad. Caso contrario, la vida única y singular de la que disponemos, podría discurrir y agotarse sin darnos cuenta, separados de los seres queridos y más cercanos que nos rodean, imitando a otros seres lejanos sin propósito alguno, y rodeados de una enorme indiferencia y aburrimiento frente a una pantalla, ya sea de móvil, tableta u ordenador. Hemos de tener mucho ánimo e inteligencia para encontrar nuestro particular lugar en el Ciberespacio.

ARTÍCULO COLABORACIÓN: Luis R. Macua Sánchez

Responsable de proyectos del Centro Internacional de Formación de Autoridades y Líderes (CIFAL) de Málaga.
Doctorando del Programa de Seguridad Humana y Derecho Global, Universidad Autónoma de Barcelona.

DESINFORMACIÓN, RADICALIZACIÓN Y NACIONES UNIDAS: UN PROBLEMA GLOBAL.

Ni la desinformación ni el anglicismo "fake news" son fenómenos recientes, aun cuando el dotar a términos tan antiguos como "bulo", "infundio", o "filfa", de una voz extranjera y disfrazarla como un neologismo nos

incite, por sí mismo, al desconcierto. Los escolares de Estudios Estratégicos se sabrán conocedores de las operaciones psicológicas, un elemento de desestabilización significativo en la guerra de la información.

Prueba de la antigüedad del término data del siglo IV, cuando el *strategos* Sun Tzu indicó que "el arte de la guerra se basa en el engaño" (1), añadiendo, además, que "no se dirige sólo a los enemigos, sino que empieza por las propias tropas, para hacer que le sigan a uno sin saber adónde van (2). Podría observarse en esta apreciación que, para la consecución de los objetivos políticos de según qué actores, tan importante es el manipular a la población propia como a la ajena.

Para ejemplificar esto último podríamos destacar hitos que cambiaron el rumbo de nuestra historia reciente, como la utilización de la desinformación a modo de elemento manipulativo de la población estadounidense en el periodo previo a la invasión de Iraq. La superpotencia norteamericana acusó al país asiático de poseer armas de destrucción masiva, y la campaña mediática hacia el pueblo estadounidense condujo a la decisión unilateral del envío de sus tropas. Esta decisión soslayó la autoridad del Consejo de Seguridad de Naciones Unidas con un apoyo de más de un 70% de su población a favor de la invasión (3) .

Aún más reciente es la utilización de la consultora política Cambridge Analítica dedicada a la ingeniería social en masa gracias a la transferencia de datos personales de millones de usuarios (4) cedidos por Facebook, y que ayudaron a influenciar a la población en acontecimientos clave como las elecciones presidenciales de EE.UU. en 2016, para finalmente desequilibrar la balanza en favor del candidato Donald Trump (5). Otros ejemplos más geográficamente cercanos los encontramos en el Brexit (6) o la utilización del discurso inflamatorio a través de cuentas falsas en los últimos años en el asunto enquistado de Cataluña (7).

La particularidad de nuestro tiempo, a diferencia de la época del general Tzu, reside en encontrarnos inmersos en la cuarta revolución industrial que, a diferencia de las previas, concentra una estructura altamente tecnológica que avanza a tal velocidad que se escapa, en gran medida, a la cognición humana. Esta rapidez e incertidumbre la hace particularmente peligrosa. Nuestra era está marcada por nuestra exposición a constantes cambios que se producen a gran velocidad, donde internet y las redes sociales juegan un importante rol en el posicionamiento político de los ciudadanos y ciudadanas. La ejecución de operaciones psicológicas ha centrado los ataques en la población (8) y la utilización de las noticias falsas se ha probado como un arma infalible para la desestabilización de la cohesión social y el acuciamiento del extremismo violento, dejando en manos de la responsabilidad moral e intelectual de cada uno de los usuarios el poder reproducir y difundirlas. Según Villota, la utilización de noticias falsas se encuadraría en el marco de la Guerra de Nueva Generación: "Estrategia de influencia que excluye la fuerza bruta y se ajusta al entorno virtual redistribuido desde agentes involuntarios, enigmáticos entusiastas acosadores, falsas identidades virtuales, bots automatizados que igualmente aprovechan los conflictos internos de una sociedad polarizada por la crisis de legitimidad y de credibilidad" (9).

Cabría destacar aquí la investigación de Vosoughi y Roy que analizaron la difusión de 126.000 rumores por, aproximadamente, 3 millones de personas en el periodo comprendido entre 2006 y 2017. Los investigadores llegaron a la conclusión de que las noticias falsas, al incluir un componente más novedoso y despertar sentimientos de miedo, asco, y sorpresa, se difunden más ampliamente y a una velocidad mayor que las reales (10). Ante el peligro y la incertidumbre que este fenómeno supone para la paz del planeta, las Naciones Unidas deben jugar un papel fundamental en la lucha contra este incentivador de la violencia y la ruptura social, especialmente durante tiempos de pandemia. Para ello, la organización lanzó una campaña de comunicación basada en tres ejes: Ciencia, Solidaridad y Soluciones. El proyecto, liderado por la Secretaria General Adjunta de Comunicaciones Globales, Melissa Fleming, tiene como objetivo evitar que el "miedo, la incertidumbre y la proliferación de las noticias falsas tengan el potencial de debilitar las respuestas nacionales contra el virus" y así evitar "reforzar narrativas nativistas y la creación de

oportunidades para aquellos que quieren explotar este periodo para ahondar la división social" (11). Es así como nace la iniciativa Verified (12).

NOTAS Y CITAS (x):

(1) Tzu, S. (2003). El arte de la guerra. Biblioteca virtual Universal. https://biblioteca.org.ar/libros/656228.pdf.

(2) Ibid, p.34.

(3) Newport, F. (24 de marzo de 2003). Seventy-Two Percent of Americans Support War Against Iraq. Gallup News Service. https://news.gallup.com/poll/8038/seventytwo-percent-americans-support-war-against-iraq.aspx.

(4) Kang, C. y Frenkel, S. (4 de abril de 2018) Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. The New York TImes. https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.

(5) Kozlowska, I. (30 de abril de 2018). Facebook and Data Privacy in the Age of Cambridge Analytica. The Henry M. Jackson School of International Studies, Universidad de Washington. https://jsis.washington.edu/news/facebook- data-privacy-age-cambridge-analytica/.

(6) Cadwalladr, C. y Graham-Harrison, E. (17 de marzo de 2017). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

(7) Hernández-Santaolalla, V. y Sola-Morales, S. (2019). Postverdad y discurso intimidatorio en Twitter durante el referéndum catalán del 1-O. Observatorio, 13 (1), 102-121.

(8) Prats i Amorós, J. y Guillaume-Barry, A. (19 de setiembre de 2019). No solo sangre. La necesidad de integrar las operaciones psicológicas en la cultura militar occidental. Instituto de Estudios Estratégicos. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO81_2019JOAPRA_Psyops.pdf.

(9) Villota, O. (2020) La guerra de des-información de Rusia en Estados Unidos. Revista Conjeturas Sociológicas, 21 (8) 37 - 64. https://revistas.ues.edu.sv/index.php/conjsociologicas/article/view/1526.

(10) Vosoughi, S. y Roy, D. (9 de marzo de 2018). The spread of true and false news online. American Association for the Advancement of Science. https://science.sciencemag.org/content/sci/359/6380/1146.full.pdf.

(11) UN Department of Global Communications (30 de abril de 2020). 5 ways the UN is fighting 'infodemic' of

misinformation. https://www.un.org/en/un-coronavirus-communications-team/five-ways-united-nations-fighting- %E2%80%98infodemic%E2%80%99-misinformation. (www.shareverified.com), una herramienta de verificación de noticias lanzada en mayo de 2020 cuyo peso reside en la participación de "voluntarios de la información" y en las alianzas con importantes empresas comprometidas del sector privado. Otro elemento interesante es la creación del Convenio de los Medios de Comunicación por los Objetivos de Desarrollo Sostenible (ODS), al que más de 100 medios de comunicación internacionales se han adherido, comprometiéndose a cumplir con los principios de solidaridad, respeto y dignidad de la Agenda 2030 y los 17 ODS bajo el lema de "No Dejar a Nadie atrás". La utilización de esta herramienta podría ser un elemento clave en la lucha contra la desinformación, puesto que puede servir para crear narrativas conducentes a la reducción de la polarización política a través de noticias que reduzcan los índices de frustración y tiendan puentes que acerquen más a los miembros de las comunidades locales.

El principio clave de la Agenda 2030 reside en que el cambio hacia un futuro más sostenible debe comenzar desde lo individual y lo local, para proyectarse así hacia lo social, y a niveles superiores del plano regional, nacional, e internacional. Es por esto que la colaboración de los medios de comunicación y otros representantes de los sectores privados y público, junto con la acción individual de cada uno de nosotros, puede conducir finalmente a la creación de políticas inclusivas y holísticas que hagan frente al fenómeno de la desinformación que afecta gravemente a nuestra sociedad actual.

(12) UN Department of Global Communications (28 de mayo de 2020) 'Verified' initiative aims to flood digital space with facts amid COVID-19 crisis. https://www.un.org/en/coronavirus/%E2%80%98verified%E2%80%99-initiative-aims-flood-digital-space-facts-amid-covid-19-crisis.

TEXTOS COMPLEMENTARIOS APORTADOS POR LOS PONENTES.

1ª Mesa redonda. Mundos físicos y virtuales. Málaga como Ciudad-Región

Moderador: Carlos de Palma Arrabal.

Director Comisión XIV Jornadas sobre el Ciberespacio

https://vimeo.com/498182383

Salvador Moreno Peralta

Arquitecto y Urbanista.

C.V. *Arquitecto Urbanista, Escuela Técnica Superior de Arquitectura de Madrid (1972). Premio Nacional de Urbanismo 1985 por el Plan General de Ordenación Urbana de Málaga. Premio Europa Nostra 1999 por la Rehabilitación de los Cuatro Recintos Fortificados de Melilla. Coordinador de la Cooperación Internacional entre la Junta de Andalucía y las municipalidades de Buenos Aires y Córdoba (Argentina) (1991- 2000). Autor de la ampliación del PTA de Málaga, de los edificios de Opplus del BBVA, Oracle y Ericsson. Ha sido Académico de Bellas Artes de San Telmo y presidente del Consejo Social de la Universidad de Málaga. Medalla de Oro del Ateneo, ha escrito más de 500 artículos en la prensa diaria y especializada.*

MUNDOS FÍSICOS Y VIRTUALES. LAS CIUDADES-REGIÓN.

Como todas las pandemias, la de la Covid19 se ha gestado en las ciudades, y no es difícil establecer el vínculo entre la extensión del contagio y la fragilidad de una sociedad conceptualmente urbanizada en su totalidad, concentrada en unas megalópolis cuya saturación nos sitúa ante la primera gran crisis de lo urbano, después de que la ciudad haya paseado su triunfo a lo largo de la historia. La ciudad, el primer y gran invento del hombre junto al lenguaje y el derecho, afronta hoy una triple embestida: la desmesura del proceso de metropolización, la insostenibilidad del modelo económico planetario sobre el que se sustenta, y la necesidad de encontrar el punto de coexistencia con esa otra ciudad, la del espacio de los flujos, la de las redes e Internet.

Esta ciudad “virtual” parece estar creando hoy una realidad distinta y paralela en la que no sabemos qué sentido adquieren todos los valores que tradicionalmente habían estado ligados a la ciudad tradicional y, consecuentemente, el sentido del mismo concepto de ciudadanía. Nuestra hipótesis es que, si abordamos resueltamente estas cuestiones, podremos transformar esta crisis en la oportunidad de que vuelva a surgir de ella otra ciudad, pero renovada y otra vez triunfante.

La metropolización intensiva y extensiva del planeta, con aglomeraciones urbanas que por sí solas tienen el tamaño de países, había llegado a un punto de bloqueo en el que la ciudad ya no podía dar las respuestas que ha estado dando a lo largo de sus más de 5.000 años de historia: Protección, seguridad, fecundidad entre diversidades, oportunidades, conocimiento, plasmación de ideales democráticos, etc. Por un lado:

a) La inmensidad de la huella urbana supera la capacidad de comprensión de la ciudad por sus habitantes, incluso su misma gobernabilidad.

b) El consumo de energía de esos hervideros humanos que son las más de treinta ciudades conurbadas que alojan el 65% de la población mundial, no puede abordarse con los recursos disponibles.

c) Esas aglomeraciones desbordantes anulan las sinergias ventajosas de las tradicionales economías de aglomeración que siempre han ofrecido las ciudades, ahondando esa brecha social entre ricos y pobres que parece ya ser algo natural en la condición urbana. La competitividad inserta en la matriz de lo urbano llevaba mucho tiempo generando guetos, diferencias, inseguridad, comunidades cerradas, miedo a la inmigración, etc., y todo ello traducido en una segregación social de los espacios que no nos permite ya exhibir "El triunfo de la ciudad", sino "La ciudad de los triunfadores… y los perdedores".

No parece haber dudas de que la contaminación por el gigantesco consumo de energía obtenida de la combustión de recursos fósiles, es el principal causante del calentamiento global. Hay que celebrar a este respecto los adelantos mundiales en la generalización del "pensamiento verde". Una de sus consecuencias es el desarrollo de una floreciente industria basada en la aplicación de avances tecnocientíficos al funcionamiento de las infraestructuras urbanas y domésticas, las llamadas "smart cities" o "ciudades inteligentes", con el objetivo de lograr la máxima eficiencia funcional con el máximo ahorro energético. Esto estaría muy bien si no fuera porque las tecnologías "smart" son las terminales de grandes empresas transnacionales que las detentan en régimen de monopolio, casi todas de origen norteamericano, que han logrado introducirla con carácter normativo en las legislaciones medioambientales del mundo occidental. En cualquier caso, si para limpiar nuestra atmósfera de CO2 y NO2, si para ver delfines en nuestros puertos y patos en nuestras calles, hizo falta nada menos que un confinamiento global y una paralización universal de las ciudades, es ingenuo, si no falaz, intentar combatir la metástasis del modelo urbano con "aspirinas" de eficiencia energética.

Porque el reto hoy es de mayor calado y exige atacar el problema en su raíz, que es la insostenibilidad de las aglomeraciones y las formas de vida que en ellas se dan. Y esto es algo que nos afecta de una manera muy próxima. Recordemos que días antes de que la pandemia reclamara la atención mundial, el problema que teníamos encima de la mesa era el de una España interior despoblada por la atracción de las aglomeraciones metropolitanas. Las reflexiones que la Covid19 ha suscitado sobre el incierto futuro trae de nuevo el problema al primer plano. Si la Revolución Industrial a principios del siglo XIX indujo un proceso de abandono del campo y concentración en las grandes ciudades, ahora con el temor general a un contagio incontrolado y con la Revolución digital puede producirse una corriente inversa. Intentemos explicarlo más claramente con el caso concreto de Málaga.

Málaga capital, sin dejar de ser lo que es, podría "esponjarse" hacia los hermosos pueblos de sus comarcas, la Axarquía, la Sierra de las Nieves, el Guadalhorce…, siempre que estuvieran plenamente interconectados entre sí física pero, sobre todo, digitalmente, como una saludable alternativa residencial y laboral absolutamente integrada en la dinámica de la vida cotidiana: Estos lugares podrían aportar unos nuevos "caladeros de productividad" si, mediante la innovación tecnológica, " se reinventaran alternativas propias para la revitalización de las economías locales, proporcionando con ello más autosuficiencia, cohesión social, democracia y protección ambiental que las que les puede ofrecer el reino de las multinacionales", como escribe David Hammerstein.

Con ser todo esto importante, lo fundamental de este enfoque es la repercusión que esta decisión de política económica tiene sobre una nueva concepción del territorio. Estamos ante el alumbramiento de un nuevo modelo territorial de "ciudad-región" que imbricara estrechamente a la capital con su área: hablamos de un concepto geográfico y económico, moderno y abierto, que englobara en una misma lógica, como un

manantial de riqueza con distintos veneros, a la conjunción de la realidad estrictamente metropolitana y las "descompresiones" de sus pueblos y ciudades medias. Aquí la ciudad es ya el territorio y viceversa, extrayendo de esa simbiosis toda su potencialidad. De esta forma:

a) La digitalización contribuiría a la democratización del territorio, equilibrado en su distribución de rentas mediante la interacción de sinergias productivas.

b) Así planteada, esta concepción geográfico-digital, en la que todos los núcleos estarían trabajando en red, reforzaría el protagonismo de los Ayuntamientos en el reparto del gasto público en concordancia con las responsabilidades que afrontan, hoy muy por debajo del porcentaje de otros países de nuestra órbita europea.

Podemos extraer de lo dicho conclusiones de validez general. Sabemos que un país sólo está en la senda de la riqueza y el progreso si está vertebrado, y la vertebración, antes confiada a las comunicaciones físicas, ahora se encomienda fundamentalmente a las comunicaciones digitales. Pero más allá del reequilibrio demográfico, el reequilibrio social pasa por eliminar otro tipo de brecha anímica muy profunda y consolidada, que sigue subsistiendo ligada al contraste entre los conceptos de Centro y Periferia. Por mucha conexión que exista, por mucho que se generalice el teletrabajo, y por mucha simultaneidad en el flujo interactivo de la información, las grandes urbes seguirán generando la irresistible atracción de la aglomeración física, movida por la inercia de la cultura de masas, significante del consumo, que es uno de los motores de la economía capitalista; y si antes había una brecha entre modernos digitales y catetos analógicos, ahora podrá seguir existiendo otra brecha, pero entre modernos digitales y catetos… igualmente digitales, pues la cobertura generalizada del 5G en el territorio no determina por sí sola la superación social entre lo capitalino y lo periférico. De ahí que, para su materialización, la idea de Ciudad-Región implique interiorizar políticamente la conciencia de una comunidad integrada, lo cual no es fácil en un país tan proclive a su fragmentación cantonalista.

Pero esta valorización de la España agraria, periférica y olvidada no es sólo importante en sí misma por las razones aducidas, sino porque el ejemplo de sus formas de vida nos ilustra de cómo interpretarlo en las ciudades, cómo compaginar el ejercicio de la ciudadanía en la presunta contradicción entre los mundos paralelos de la ciudad analógica y la ciudad digital.

Aun viviendo en una metrópoli inabarcable el ciudadano no debe sentirse extraño dentro de ella porque la ciudad está obligada a procurarle espacios con los que pueda restablecer los valores tradicionales de lo urbano, de forma que el plano, digamos, anímico, de la ciudad digital tenga su correlato en el plano tangible de la ciudad física. Más claramente: que tras dejar el ordenador que minutos antes nos ha conectado con el universo, podamos volver a la estimulante aleatoriedad de la calle, hacia esos lugares comunales en los que nos juntamos con nuestros semejantes para compartir con ellos nuestras alegrías y nuestras inquietudes, restableciendo la comunicabilidad física sobre la obsesiva comunicabilidad digital. No es nada nuevo: es la vida de los barrios tradicionales (que ahora la cursilería rampante llama la ciudad de los 14 minutos), y que no es otra cosa que un trasunto de esa vida de los pueblos y núcleos tradicionales a los que nos hemos referido.

La tradición no es una ideología reaccionaria: es un islote de presente situado entre el pasado de nuestra vida y el futuro de nuestros anhelos, en el cual no debemos sentirnos como náufragos. Nuestra vida, hoy, se desarrolla simultáneamente tanto entre el pasado y el futuro como entre la ciudad digital y la ciudad tradicional, sin caer en la esquizofrenia y sin que podamos prescindir de ninguna de las dos. Pero para que la ciudad tradicional siga siendo la ciudad de siempre y sus habitantes quieran seguir disfrutando de la plenitud de los derechos de ciudadanía no pueden ser analfabetos en el lenguaje de hoy, porque el analfabetismo siempre produce ciudadanos de segunda categoría.

Por otro lado, para que en la ciudad de siempre sigan subsistiendo los elementos que la caracterizan, es decir, las librerías, las tiendas de alimentación, las ferreterías, los bares y todo ese mundo de Pymes y de proximidad física que indefectiblemente nos siguen enraizando a la vida, es necesario que se digitalice, porque de lo contrario está condenada a morir, y muy rápidamente. Afortunadamente es un hecho creciente la extensión global de la digitalización, que permite aplicar innovación a toda la cadena de valor del sector del retail, del comercio minorista, con plataformas que le ayudan a utilizar las mismas armas con las que, de una manera hasta ahora desigual, juegan los grandes monopolios a los que antes me refería, con el uso del Big Data y el marketing digital. Se produciría así un efecto paradójico: que la digitalización fuera fundamental para que no desaparecieran las tiendas y, con ellas la vida de esos barrios. Dicho de otro modo, digitalizar lo cotidiano para salvar la tradición.

Y por último una consideración final sobre el modelo de producción global y sus consecuencias urbanas.

El sistema capitalista, que es como una atmósfera que se respira, se mueve con tres motores hoy dañados seriamente por haberse pasado de revoluciones: la competitividad, el consumo y el crecimiento.

Con Internet, el principio de la competitividad ha desembocado de hecho en una práctica monopolista global y transnacional, que antes sólo era imaginable en un escenario de totalitarismo político. No deja de ser desolador ver cómo Internet, que posibilita la máxima extensión y democratización del conocimiento, esté siendo utilizado para crear un sistema cerrado de monopolios a partir de la extracción masiva de información a los ciudadanos (Google, Amazon, Facebook, Intel, Apple, etc.). Y que nuestra pobre democracia, como una barquilla desarbolada, esté navegando hoy entre las tormentosas aguas de un nuevo totalitarismo político- neofascismo, neocomunismo y populismo- que no es más que el trasunto de los totalitarismos económicos que ejercen los gigantes tecnológicos; y convengamos con Karl Popper, que tan detestables son los unos como los otros.

Por su parte el uso planetario de los dispositivos móviles, como prótesis tecnológicas, permite la obtención de unos beneficios incalculables al favorecer el consumo adictivo de bienes en un mercado infinitamente fragmentado de productos, cuya fabricación está esquilmando materias primas no renovables.

Y en cuanto al crecimiento, hoy un capitalismo hiperliberal sin contrapesos keynesianos está montado sobre ese caballo desbocado que encomienda la generación de riqueza sólo al crecimiento expansivo. Pretender cambiar el modelo de producción capitalista nos llevaría a una actitud estéril para la galería. Pero lo que sí parece urgente es atajar la hipertrofia de sus excesos. En este sentido parece lógico propugnar, a partir de las posibilidades de la digitalización, una especie de “parada biológica” que convierta en modelos de negocio fórmulas de desarrollo que no impliquen necesariamente un crecimiento expansivo, sino “implosivo”, como una vuelta de la mirada hacia lo existente, abordando todo aquello que lleve el prefijo “re”: reurbanizar lo mal urbanizado, reconstruir lo mal construido, reciclar lo usado, reconsiderar los tipos de vivienda, reutilizar polígonos industriales de nuestras ciudades con una mayor compatibilidad de usos, repoblar lo desertizado, repensar nuestros hábitos, reprogramar nuestras mentes en torno a ideas más sostenibles…

En definitiva, se trata de incorporar a la lógica empresarial la idea de una especie de “regeneración universal” en la cadena de beneficio con unos objetivos y unos resultados que en principio están orientados hacia una mejora de nuestros entornos, en una acepción verosímil- y no sólo “buenista”- de la sostenibilidad. Dicho de otra manera: generar riqueza mejorando lo existente. La clave de la economía ha estado siempre en la ecuación virtuosa de una oferta bien adaptada a la demanda, y hoy la demanda va a ir forzosamente por ahí; luego bueno será que, con la técnica del judoca y la ayuda de la digitalización, el sistema convierta en beneficiosas las fuerzas incontenibles de una sociedad que después de la pandemia universal ya no volverá a ser la misma.

TEXTOS COMPLEMENTARIOS APORTADOS POR LOS PONENTES.

2ª Mesa redonda. Perspectivas y estrategias para el mundo virtual

Moderador: Carlos de Palma Arrabal.

Director Comisión XIV Jornadas sobre el Ciberespacio

https://vimeo.com/498183143

Susana Carillo Aparicio.

Primer Teniente Alcalde y Concejala Innovación y Digitalización Urbana Ayuntamiento de Málaga.

C.V. *Doctora Ingeniero Industrial, especialidad en Smart Grids por la Universidad de Málaga. Profesora Asociada durante 5 años al Departamento de Mecánica de Medios Continuos, colaborando y publicando en universidades y revistas internacionales. Desde 1998 trabajó en Endesa Distribución. Ha sido Responsable de Planificación de Andalucía Centro, trabajando con redes de alta, media y baja tensión. Desde el principio del proyecto Smartcity Málaga coordinó el Centro de Control, trabajando en telegestión, automatización, comunicaciones, generación renovable, sistemas de almacenamiento, eficiencia energética, gestión de la demanda y vehículo eléctrico. Posteriormente fue la Responsable del Smartcity Málaga Living Lab del Grupo Enel coordinando distintos proyectos de Innovación financiados por CE y CDTI como son Flexiciency, Coordinet, PALOMA, MONICA y PASTORA, en los cuales se utilizan técnicas de Inteligencia Artificial, con modelos de Machine Learning y Deep Learning, y Big Data Analytics. Actualmente es la primera Teniente Alcalde del Ayto. de Málaga, Delegada de innovación y Digitalización Urbana.*

Felipe Romera Lubia.

Director General Parque Tecnológico de Andalucía y Málaga Tech Park.

C.V. *Ingeniero de Telecomunicación por la Escuela Técnica Superior de Ingenieros de Telecomunicación de Madrid, graduado en 1976. Tras terminar sus estudios trabajó en INTELSA (Ericsson), Secoinsa y Fujitsu España realizando labores en diseño de productos de telecomunicaciones y entre 1982 y 1993 fue Director del Laboratorio de I+D de Fujitsu España en Málaga. Desde 1990 dirige el Parque Tecnológico de Andalucía (PTA), hoy Málaga TechPark y desde 1998 es Presidente de la Asociación de Parques Científicos y Tecnológicos de España (APTE). Además, fue miembro del Consejo Asesor para la Ciencia y la Tecnología del Ministerio de Ciencia y Tecnología en representación de la APTE (2001-2004). Y fue presidente de la Red de Espacios Tecnológicos de Andalucía (RETA) desde su constitución en abril de 2005 hasta 2015.*

Carmen García Peña.

Directora Gerente Fundación CIEDES
(Centro Investigaciones Estratégicas y Desarrollo Económico y Social de Málaga).

C.V. *Licenciada en Ciencias Económicas y Empresariales, especialidad Economía Regional y Urbana por la Universidad de Málaga. Máster en Dirección y Administración de Empresas (MBA Plus Executive), por el Instituto de Práctica Empresarial (IPE) y Curso de Experto en Urbanismo y Desarrollos Inmobiliarios, por el mismo Instituto. Directora del Centro de Transferencia de Conocimientos del Mediterráneo en Metodologías y Buenas Prácticas de Planificación Estratégica para el Desarrollo Sostenible, de la Asociación MEDCITIES. Profesora en varios*

centros superiores. Miembro del Comité Científico del Centro de Formación de Autoridades y Líderes (CIFAL) de la Agencia UNITAR de Naciones Unidas en Málaga. Ha participado en el diseño, gestión y evaluación de múltiples proyectos europeos (Ecos Ouverture, INTERREG, SUDOE, MED, ENPI, 7º Programa Marco y H2020). Es miembro, asesora y colaboradora de numerosas redes de ciudades y grupos de expertos en materia de desarrollo urbano, planificación estratégica territorial y sostenibilidad en Europa, Mediterráneo y América Latina; como el Centro Iberoamericano de Desarrollo Estratégico Urbano (CIDEU), la Red Andaluza de Desarrollo Urbano y Territorial (RADEUT), la Asociación América Europa de Regiones y Ciudades (AERYC), la Unión Iberoamericana de Municipalistas (UIM) y la red de ciudades mediterráneas por la planificación estratégica urbana (MedCities).

Aporta también la Presentación 3.2.4

Francisco Salas Márquez.

Director Gerente de Promálaga.

***C.V.** Ingeniero de Telecomunicación por la Universidad de Málaga, MBA Executive por la Escuela Superior de Estudios de Empresa (ESESA) y Diplomado Alta Dirección de Empresas por el Instituto Internacional San Telmo (AD1 Málaga). Concejal de Nuevas Tecnologías en el período 2007-2011 y de Parques Empresariales de 2009 a 2011 y Presidente del Distrito Este. En 2011 fue Director del Área de Parques Empresariales del Ayuntamiento de Málaga. Actual miembro de los consejos de Administración de Bic-Euronova, Esesa e Ingenia. Ha sido también Decano, Vicedecano, Secretario y Vocal del Colegio Oficial de Ingenieros de Telecomunicación en Andalucía Oriental y fue Secretario y Vocal de la Asociación Andaluza de Ingenieros de Telecomunicación.*

Yolanda De Aguilar Rosell.

Directora General del Palacio de Ferias y Congresos de Málaga (FYCMA).

***C.V.** Directora General de FYCMA (Palacio de Ferias y Congresos de Málaga) desde el año 2002. Su vinculación al mundo de las ferias y los eventos se inició en 1990 a través de su incorporación a IFEMA, como directora comercial y más tarde como directora de FITUR. Su extensa trayectoria la ha llevado a formar parte de la Mesa del Turismo Español, actualmente como Vocal Asesora MICE del Consejo Directivo, y también ostenta las vicepresidencias de AFCAN (Asociación de Palacios de Congresos y Ferias de Andalucía) y de AFE (Asociación de Ferias Españolas).*

DATOS Y APORTACIONES DE LA INDUSTRIA FERIAL.

<u>INDUSTRIA FERIAL</u>

- Impacto económico ferias: 13.000 mill. €
- Impacto económico industrial congresual: 6.000 mill. €
- Aportación PIB actividad ferial: 6.500 mill. €
- Empleos generados por industria ferial y congresual: + 150.000

1. “Las ferias forman un centro neurálgico de dinamización de la actividad empresarial”.

2. “Son indiscutibles termómetros sectoriales que analizan la evolución de una determinada actividad, reflejo cada una de su tiempo y circunstancias”.

3. “Mención al tejido empresarial que dinamizan”.

4. “Las ferias serán clave en la recuperación económica, poniendo en escena”: Talento, Negocio y Conocimiento.

➢ Los eventos profesionales como motor para el avance de los sectores y las industrias

✓ Innovación	✓ Captación del talento
✓ Competitividad	✓ Generación de conocimiento
✓ Negocio	✓ Redes
✓ Inversión	✓ Internacionalización

➢ Actores

➢ Cadena de valor

FYCMA

➢ La misión

"La misión de FYCMA es convertir a Málaga en referente entre las principales capitales de negocio ferial y congresual para abrir oportunidades, dinamizar la economía, crear riqueza y generar empleo." "Lo haremos con nuestro compromiso para que cada evento alcance sus objetivos con los máximos estándares de calidad y excelencia".

➢ La evolución

➢ Áreas de negocio

TRANSFORMACIÓN DIGITAL EN FYCMA

FYCMA es un recinto que desde sus inicios ha evolucionado muy rápidamente, haciendo una fuerte apuesta por la organización de eventos propios, muchos de ellos de ámbito profesional y con el foco puesto en la innovación en diferentes áreas. Entendimos que teníamos que dar un paso más y apostar por la innovación y la tecnología en la propia organización si queríamos que nuestros eventos reflejaran la innovación que estábamos predicando.

• La automatización es la única vía para una experiencia de usuario personalizada.

• Necesaria digitalización para contribuir a la estrategia de ciudad y a los objetivos de desarrollo sostenible.

• Transformación de los procesos y las áreas de negocio: En 2018 empezamos a realizar análisis de los procesos, con el foco en el cliente y sus necesidades. El Sistema de trabajo interno es muy intenso, con una planificación exhaustiva de reuniones interdepartamentales, medidas de mejora coordinadas e innovadoras.

• Objetivos basados en ejes estratégicos:
    • Incrementar los ingresos.
    • Mejorar la experiencia de cliente.
    • Digitalizar los procesos de negocio.
    • Reforzar la arquitectura de datos y sistemas.
    • Apostar por la innovación y cultura digital.
    • Participar en ecosistemas.

• ¿Qué estamos mejorando?
    • Sistema de gestión de datos.
    • Procesos de venta.
    • Campañas de marketing digital.

- Renovación de webs y APPs.
- Proceso feedback cliente.
- Business Intelligence.
- Comunicación interna.
- Inscripción, acreditación y networking.
- Espacios y oficinas.
- Mejora del customer journey.

• La clave de la transformación digital no es la tecnología, son los procesos y el equipo:
- Tomar conciencia de la necesidad de cambio.
- Analizar las necesidades de cambios y la potencialidad de retorno.
- Flexibilizar nuestras formas de trabajar y estar abiertos al cambio.
- Entender los objetivos. Por qué estamos haciéndolo.
- Crear los nuevos procesos de trabajo. Evaluar herramientas digitales.
- Implementar los nuevos procesos de trabajo con ayuda de la tecnología.
- Evaluar resultados.

FYCMA ANTE EL COVID

• La actividad profesional responsable contribuye en el proceso de reactivación económica.
• Compaginar la protección de la salud con la actividad económica.
• Cumplimos con la normativa de manera rigurosa para crear un marco puramente profesional.
• Desde el primer momento, FYCMA ha estado en contacto permanente con el tejido sectorial y ha participado en el proceso de interlocución y toma de decisiones para la elaboración de protocolos específicos.

RECUPERACIÓN DE LA ACTIVIDAD FERIAL CON FORMATOS PRESENCIALES ADAPTADOS Y DIGITALIZADOS

• La actividad de FYCMA quedó pausada, el recinto malagueño enfocó todas sus energías en la reubicación de los eventos y ferias previstos para ese periodo.
• El Palacio ha estado organizando convocatorias profesionales hasta el mes de noviembre 2020.
• Las próximas convocatorias para la última parte del año serán online.
• Se mantiene el impulso a la red de proveedores.

• FYCMA ha conseguido reinventarse y adaptarse:
- Implementación de las medidas de seguridad.
- Startup Europe Smart Agrifood Summit - 1.450, y Greencities y S-Moving - 1.560; adaptar los formatos de las ferias a las normas de aforo.
- Estos encuentros han sido escenario de la primera prueba piloto del Ayuntamiento de Málaga de test de antígenos.
- Simed, Salón Inmobiliario del Mediterráneo, ha sido el único de los salones inmobiliarios más importantes de España en celebrarse de manera presencial.

• FYCMA actividad presencial con la parte virtual.

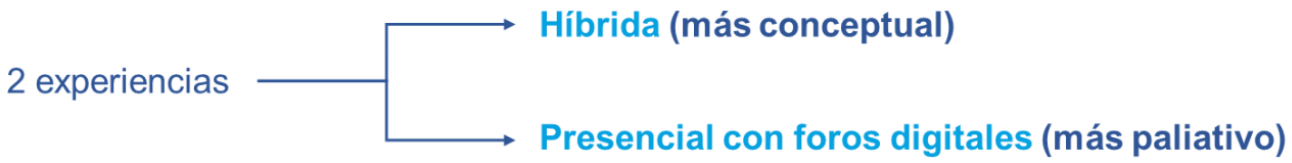
• Nació FYCMA ON, un proyecto que engloba e impulsa todo el contenido e iniciativas virtuales de las ferias de organización propia: webinars y programas online.

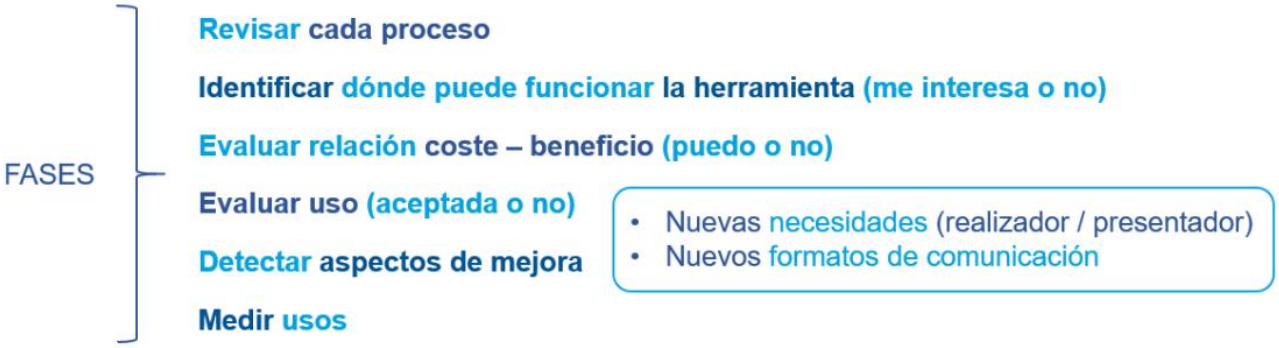
TECNOLOGÍA: HERRAMIENTA ESTRATÉGICA

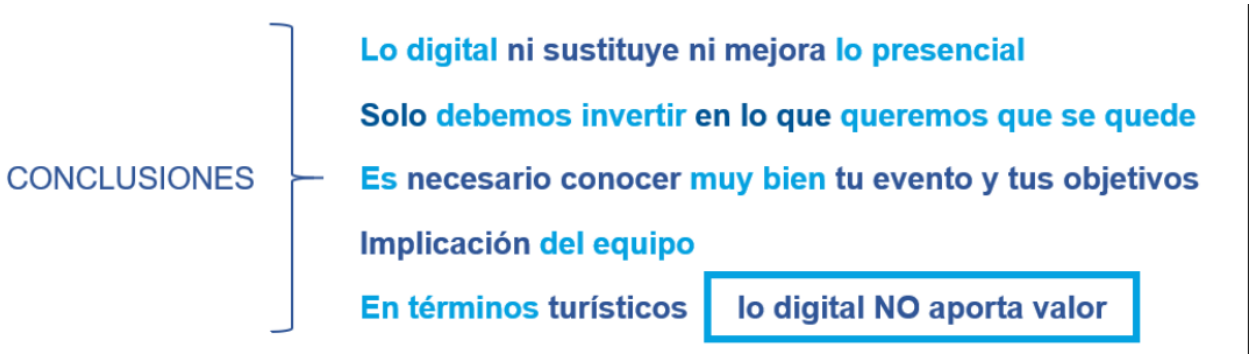
• La tecnología no es un fin sino una herramienta que nos permita innovar para mejorar la experiencia de los usuarios, abrir nuevas oportunidades, alcanzar un mayor impacto:

- Realizar un análisis más amplio del estado de situación, temática o sector.
- Ayuda en la realización y producción.
- Extensión del evento físico: más oportunidades y posibilidades para generar networking.

• Necesaria para el cumplimiento de los protocolos COVID-19.







MEDIDAS Y PROTOCOLOS COVID-19

• FYCMA ha elaborado un plan de contingencia. Entre ellas, podemos enumerar:
- Uso obligatorio de mascarillas.
- Adecuación de los espacios.

- Establecimiento de flujos de entrada y salida.
- Aforos limitados.
- Intensificación de la limpieza y desinfección.
- Puntos de dispensación de gel desinfectante.
- Digitalización para evitar elementos de necesaria manipulación.
- Toma de temperatura.
- Atención segura por parte de todo el equipo de FYCMA.

• 'Safe Tourism Certified'.

VER DOCUMENTOS ANEXOS EN LA WEB.

XIV JORNADAS DE SEGURIDAD, DEFENSA Y COOPERACIÓN. FORO PARA LA PAZ EN EL MEDITERRÁNEO.

EL CIBERESPACIO: RETOS Y OPORTUNIDADES EN EL MUNDO VIRTUAL.

Patrocinado por:

Organizadores:

Colaboradores: