

Grado en Relaciones Internacionales

Tercer Curso

Asignatura: Derecho Internacional de los Espacios

Dr. Juan Aurelio Bernal Ruiz

Dr. Alberto Gallego Gordón

Tema 6: El ciberespacio, donde quiera que esté



Bibliografía principal



- **Gutiérrez Espada, C. (2020). “La responsabilidad internacional por el uso de la fuerza en el ciberespacio”. Estudios Aranzadi.**
- **Álvarez Rodríguez, I. (2019). “*Constitución y Derecho del Ciberespacio*”. Universidad Complutense de Madrid. Recuperado de <https://www.acoes.es/congreso-xvii/wp-content/uploads/sites/3/2019/03/Constituci%C3%B3n-y-Derecho-del-Ciberespacio-.pdf>**
- **“Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional”. Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad. BOE 103. 30 de abril 2019**
- **Plan estratégico INCIBE 2021-25 (14:53). Disponible en <https://www.incibe.es/que-es-incibe/que-hacemos>**
- **The United States International Cyberspace & Digital Policy Strategy, de 6 de mayo 2024. https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf**
- **Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican diversos Reglamentos. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689**

Artículos de interés

- **Álvarez Rodríguez, I. (2019), "El Derecho del ciberespacio. Una aproximación". *Revista de internet, Derecho y Política*. IDP. 12 noviembre 2019. Recuperado de https://www.researchgate.net/publication/339640455_El_Derecho_del_ciberespacio_Una_aproximacion**
- **Robles Carrillo, M. (2019). "El régimen jurídico de las operaciones en el ciberespacio: estado del debate". *Documento de opinión 101/2019*. IEEE.12 noviembre 2019. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO101_2019MARROB_legalciber.pdf**
- **Teruel Lozano, G. (2019). "Fundamental Rights in the Digital Society: Towards a Constitution for the Cyberspace?" *Revista Chilena de Derecho*, vol. 46 N° 1, pp. 301 – 31. Recuperado de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-34372019000100301&lng=en&nrm=iso&tlng=en**
- **Daniel T. Kuehl, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. Disponible en <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210>**
- **Crilly, Martin; Mears, Alan. *Multi Dimensional and Domain Operations (MDDO)*. Disponible en <https://wavelroom.com/2022/01/26/mddo/>**



Índice



- 1. Introducción y definiciones.**
- 2. Algunos ejemplos de actos en el ciberespacio.**
- 3. Estrategia de Seguridad Nacional 2017: *Global commons*.**
- 4. Informe sobre las amenazas en la red y sus efectos.**
- 5. Operaciones en el ciberespacio. La amenaza “híbrida”.**
- 6. La UE y la OTAN.**
- 7. La posición de España. La Estrategia Nacional de Ciberseguridad.**
- 8. Estudio sobre cibercriminalidad en España.**
- 9. El dominio “cognitivo”.**
- 10. Conclusiones.**



OFERTA REYES

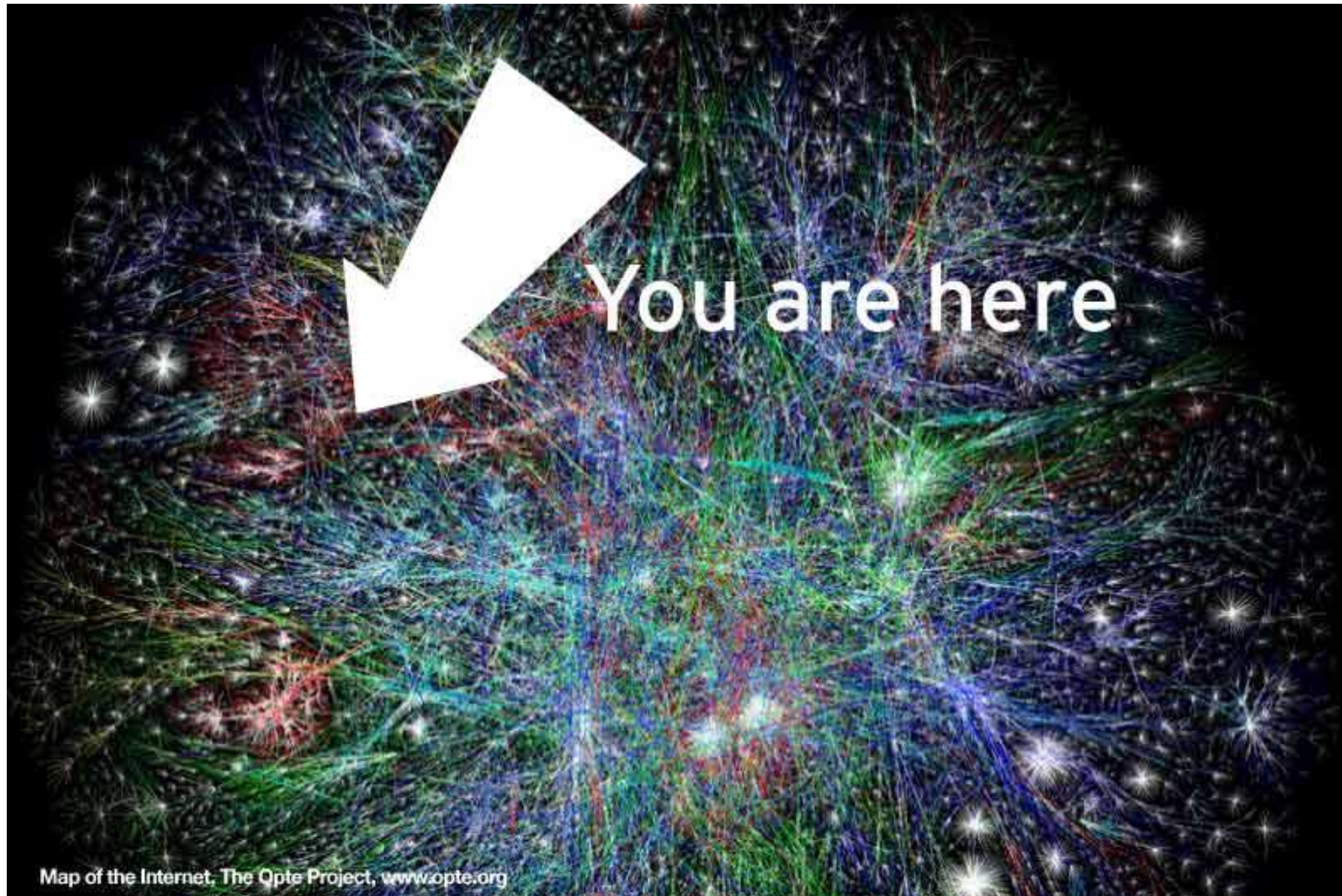
ESTE PORTÁTIL ¿TIENE QUINTO CONVO
DISTANCIAL BLUE KSI' PARA INTERNET?

ESO YA ES ANTIGUO, CABALLERO

¿ANTIGUO? PERO
SI AYER LEI' QUE...

AYER, CABALLERO, AYER





¿Definiciones de ciberespacio?



Departamento de Defensa EE.UU.

“A global domain within the information environment consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” (“until further notice”)

J-5 Cyber Directorate (DepSecDef memo of 12 May 2008)

Daniel T. Kuehl

“Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communications technologies (ICT)”

Dan Kuehl, “Cyberspace & Cyberpower: Defining the Problem”, *Cyberpower & National Security*, 2009



Amenazas en y desde el Ciberespacio

- **Adware**
- **Botnet**
- **Cyberbullying**
- **Cracker**
- **Fake news**
- **Defacement**
- **Gusano**
- **Hacker**
- **Hoax**
- **Infector de archivos**
- **Pharming**

- **Phishing**
- **Ransomware**
- **Rootkit**
- **Scareware**
- **Smishing**
- **Spam**
- **Spoofing**
- **Spyware**
- **Troyano**
- **Virus**
- **Vishing**
- **Web bug**
- **Zombie**



- **Infodemia**
- **Misinformation**
- **Disinformation**
- **Malinformation**



Efectos de usos no deseados del ciberespacio (1)



CSO UNITED STATES ▾ DIGITAL MAGAZINE EVENTS NEWSLETTERS RESOURCE LIBRARY IDG TECH(TALK) COMMUNITY INSIDER 🔍 ☰

Home > Security

CYBERSECURITY BUSINESS REPORT
By [Steve Morgan, CSO](#) | MAY 15, 2017 8:45 AM PDT

HOW-TO

Wanna stop WannaCrypt? Don't pay ransoms, backup data, and train employees

Top 3 things for CISOs and IT security teams to do in response to the WannaCry ransomware outbreak

[f](#) [t](#) [in](#) [r](#) [e](#) [m](#)

CSO UNITED STATES ▾ DIGITAL MAGAZINE EVENTS NEWSLETTERS RESOURCE LIBRARY IDG TECH(TALK) COMMUNITY INSIDER 🔍 ☰

Home > Security

CYBERSECURITY BUSINESS REPORT
By [Steve Morgan, CSO](#) | JUN 06, 2017 7:58 AM PDT

NEWS ANALYSIS

Petya: Is it ransomware or cyberwarfare?

It turns out Petya is a cyber weapon being used to carry out cyberwarfare activities

[f](#) [t](#) [in](#) [r](#) [e](#) [m](#)

Why Your Cloud Needs
A Data Strategy [Learn More](#)
splunk>

6 Cloud Pitfalls

Expert Roundtable: Protecting your personal security in the new normal.

REGISTER NOW!

TECHNOLOGY The New York Times

All 3 Billion Yahoo Accounts Were Affected by 2013 Attack

Access more for free.

Create a free account or log in to access more of The Times.



EL MUNDO España Opinión Economía Internacional Deportes Cultura Tv Papel Más -

Internacional EEUU

SEGURO DE COCHE
ESTE VERANO TU COCHE NO PUEDE FALLAR
MAPFRE

#SoyFanDeCruzRoja Alex Márquez

EEUU - Información revelada por 'The Washington Post'

La CIA concluye que Rusia ayudó a ganar las elecciones a Donald Trump

10% Descuento Panda Security

33 Comentarios

La CIA concluye que Rusia ayudó a ganar las elecciones a Donald Trump

Personas conectadas con el Kremlin filtraron a Wikileaks los correos pirateados del Partido Demócrata y de la campaña de Hillary Clinton

Mundo España África Asia Europa Medio Oriente

Coronavirus

Hackers rusos «atacan a organizaciones involucradas en el desarrollo de la vacuna contra el coronavirus», dicen funcionarios de seguridad del Reino Unido

Por Luis Michel
19/09/2020 14:07 (UTC+02:00)

Denuncian a Rusia por intento de sustracción de vacunas

Los hackers rusos están atacando a organizaciones involucradas en el desarrollo de la vacuna contra el coronavirus, según funcionarios de seguridad del Reino Unido.

Los datos del Centro Nacional de Seguridad de la Información (CNSI) revelan la actividad de hackers rusos en la red.

VIDEOS RECOMENDADOS

<https://cybermap.kaspersky.com/>

BBC NEWS | MUNDO

Noticias América Latina Internacional EE.UU. 2020 ¿Hablas español? Hay Festival Economía

Centroamérica Cuenta BBC Extra

Anuncios Google
Dejar de ver anuncios ¿Por qué este anuncio? B-

Trump vs Biden: Microsoft denuncia ataques de hackers rusos a las campañas de los dos candidatos

Redacción
BBC News Mundo
10 septiembre 2020

GETTY IMAGES

Microsoft asegura que hackers de Rusia, China e Irán han apuntado a las campañas demócrata y republicana.

ESTRATEGIA DE SEGURIDAD NACIONAL

2017



UN PROYECTO COMPARTIDO
DE TODOS Y PARA TODOS



GOBIERNO
DE ESPAÑA

PRESIDENCIA
DEL GOBIERNO



UNIVERSIDAD
DE MURCIA



Facultad de
Turismo y Relaciones
Internacionales



ESTRATEGIA DE **SEGURIDAD NACIONAL** **2021**

UN PROYECTO COMPARTIDO

Cap. 1. Seguridad global y vectores de transformación



Figura 1.1. Seguridad global y vectores de transformación

Transformación digital



Otros riesgos, pero también múltiples oportunidades, derivan de los avances tecnológicos en campos como la biotecnología, que han facilitado el rápido desarrollo de vacunas eficaces contra la COVID-19, pero plantean interrogantes éticos ante actividades como determinados empleos de la ingeniería genética.

Por otro lado, la vulnerabilidad ante posibles injerencias de terceros es extensible al dominio de infraestructuras digitales, como los centros de procesamiento de datos o los cables submarinos, y a los activos que sustentan la propiedad intelectual e industrial del sector empresarial. También habrá que considerar el mapa mundial de conectividad y la aparición de nuevos operadores satelitales, especialmente aquellos vinculados a las grandes empresas tecnológicas.

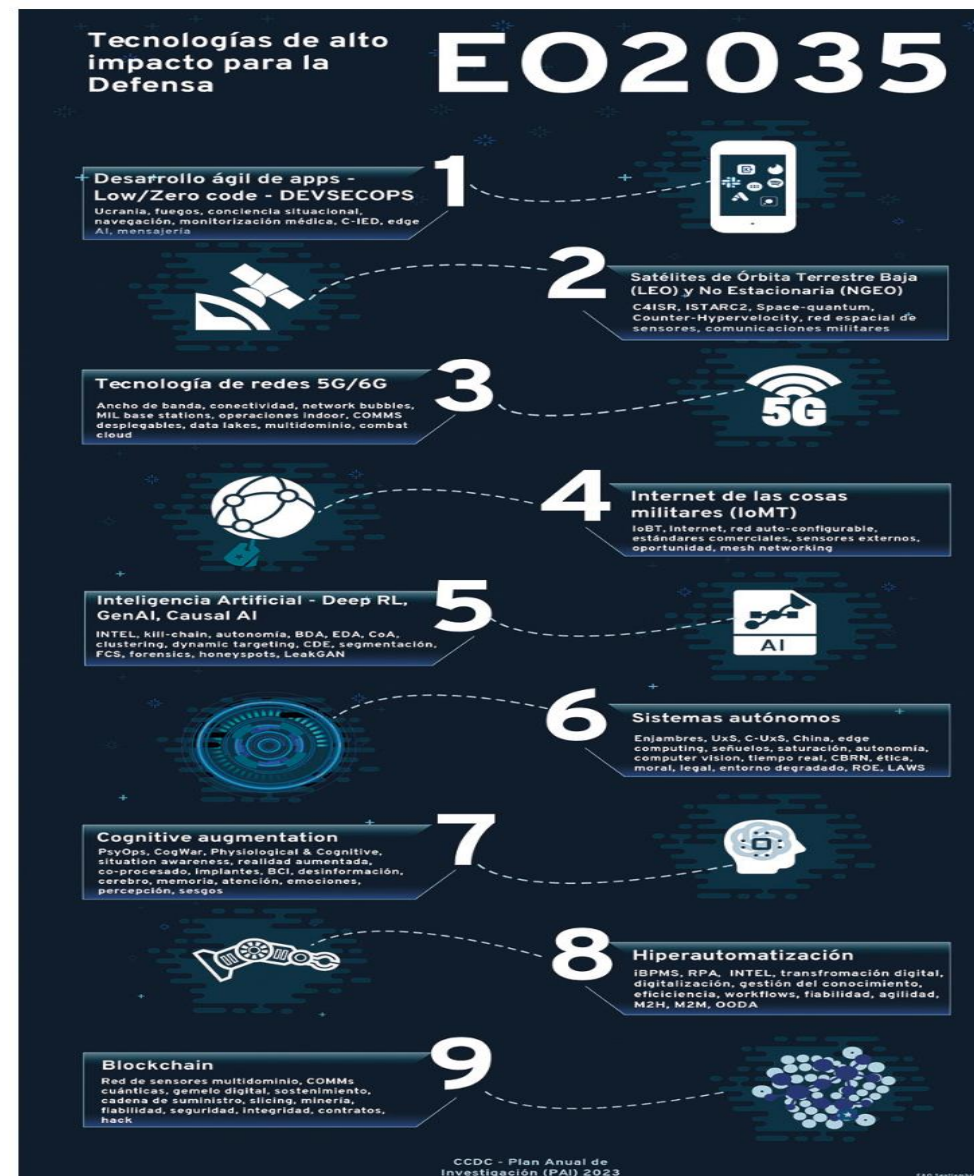
Con el dato convertido ya en un recurso estratégico de primer orden, se ha intensificado el debate sobre la ética y la defensa de derechos digitales, condicionado especialmente por la concentración de la información en las grandes compañías tecnológicas y por su uso abusivo por parte de algunos actores políticos. En este debate, el derecho a la privacidad de los usuarios de servicios digitales ocupa un lugar central y ha dado lugar a pronunciamientos judiciales que podrían condicionar el desarrollo tecnológico.

El acceso seguro a los servicios públicos y privados, en particular a los servicios esenciales en línea, supone que la ciudadanía pueda proteger su identidad y controlar los datos que comparte y cómo se utilizan, de manera que se garantice la privacidad y la protección de datos personales. Disponer de una identidad digital segura es una pieza clave para la ciberseguridad.

Plan Anual de Investigación. Tecnologías de alto impacto para la defensa en el entorno operativo 2035. 2023



Secretaría General Técnica.
MINISDEF



Amenazas y desafíos a la seguridad de España. “*Global Commons*”

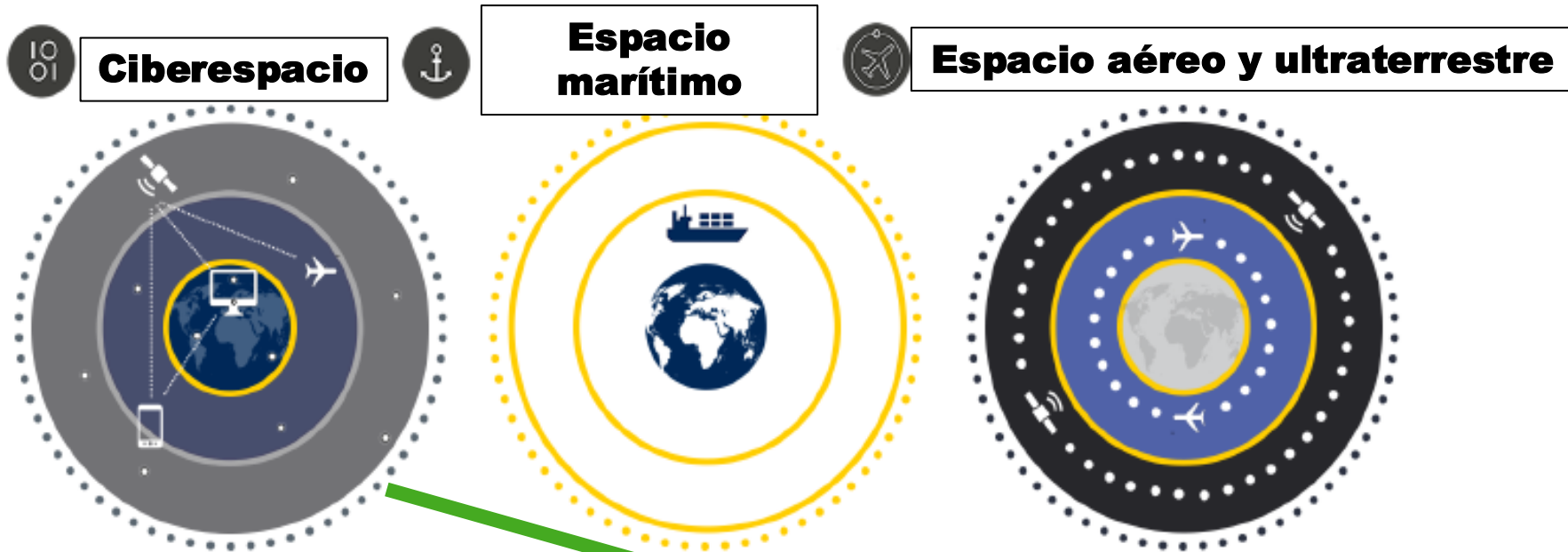


Amenazas y desafíos a la seguridad de España. “*Global Commons*”



Espacios comunes globales (ESN 2017).

Global common spaces



PRINCIPALES CARACTERÍSTICAS

Apertura geográfica y funcional

Ausencia de soberanía y jurisdicción por parte de los Estados

Facilidad de acceso

Dificultad de “atribución” del origen de la actividad.
Asimetría

Cap. 3. Riesgos y amenazas a la seguridad nacional



Figura 3.1. Riesgos y Amenazas a la Seguridad Nacional



Amenazas a infraestructuras críticas. Protección



Informe Anual de Seguridad Nacional

2023

.....

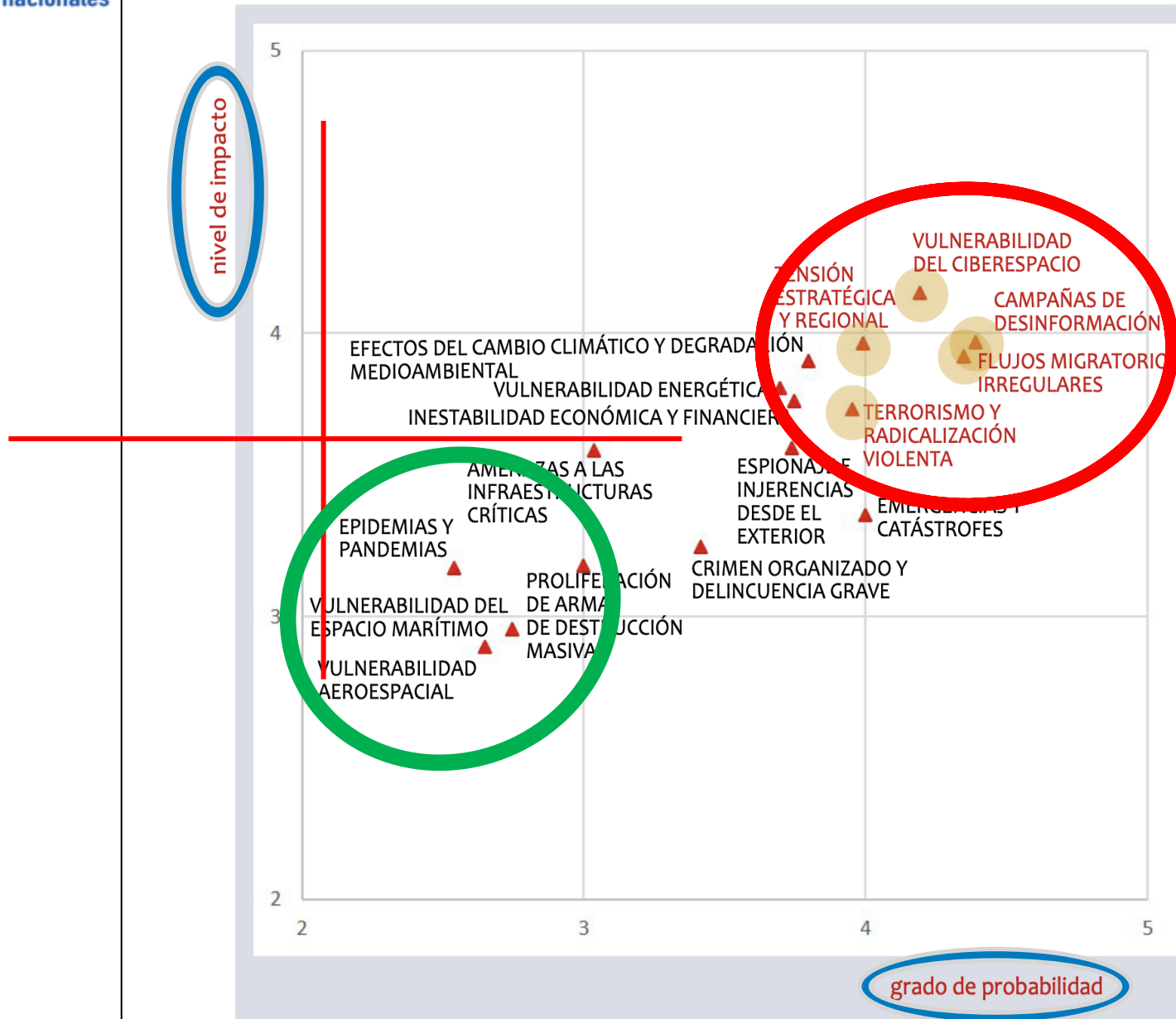


UNIVERSIDAD
DE MURCIA



Facultad de
Turismo y Relaciones
Internacionales

Figura A-2
Mapa de Riesgos para la Seguridad Nacional 2023



	IMPACTO	PROBABILIDAD	INTENSIDAD DEL RIESGO
Campañas de desinformación	3,97	4,39	17,43
Vulnerabilidad del ciberespacio	4,14	4,19	17,35
Flujos migratorios irregulares	3,91	4,34	17,02
Tensión estratégica y regional	3,96	4	15,82
Terrorismo y radicalización violenta	3,90	3,79	14,81
Efectos del cambio climático y de la degradación del medio natural	3,7	3,95	14,74
Inestabilidad económica y financiera	3,76	3,74	14,08
Vulnerabilidad energética	3,80	3,69	14,06
Espionaje e injerencias desde el exterior	3,59	3,73	13,43
Emergencias y catástrofes	3,35	4	13,42
Crimen organizado y delincuencia grave	3,24	3,41	11,07
Amenazas a las infraestructuras críticas	3,58	3,03	10,87
Proliferación de armas de destrucción masiva	3,18	3	9,54
Vulnerabilidad del espacio marítimo	2,95	2,74	8,11
Epidemias y pandemias	3,17	2,54	8,05
Vulnerabilidad aeroespacial	2,89	2,64	7,66

Figura A-3
 Intensidad del riesgo

Cuantificación del riesgo

Percepción de riesgos a 5 años



Figura A-6

Resultados de la encuesta de percepción de riesgos para la Seguridad Nacional (a cinco años)

Informe Anual de Seguridad Nacional

2024



GOBIERNO
DE ESPAÑA

PRESIDENCIA
DEL GOBIERNO

SUMARIO

INTRODUCCIÓN	7
RIESGOS Y AMENAZAS A LA SEGURIDAD NACIONAL	13
Tensión estratégica y regional	14
Terrorismo y radicalización violenta.....	44
Epidemias y pandemias	60
Amenazas a las infraestructuras críticas	68
Emergencias y catástrofes	76
Espionaje e injerencias desde el exterior.....	92
Campañas de desinformación	98
Vulnerabilidad del ciberespacio	110
Vulnerabilidad del espacio marítimo.....	140
Vulnerabilidad aeroespacial.....	162
Inestabilidad económica y financiera	178
Crimen organizado y delincuencia grave	194
Flujos migratorios irregulares.....	212
Vulnerabilidad energética.....	224
Proliferación de armas de destrucción masiva	242
Efectos del cambio climático y de la degradación del medio natural.....	252
ANÁLISIS DE RIESGOS 2024/25	275
CULTURA DE SEGURIDAD NACIONAL	290
GLOSARIO	299



Los cinco riesgos y amenazas de mayor impacto 2024

2021/22

Epidemias e pandemias

Vulnerabilidad del ciberespacio
Inestabilidad económica y financiera
Vulnerabilidad energética
Flujos migratorios irregulares

2022/23

Vulnerabilidad energética

Vulnerabilidad del ciberespacio
Inestabilidad económica y financiera
Campañas de desinformación
Tensión estratégica y regional

2023/24

Campañas de desinformación

Vulnerabilidad del ciberespacio
Flujos migratorios irregulares
Tensión estratégica y regional
Terrorismo y radicalización violenta

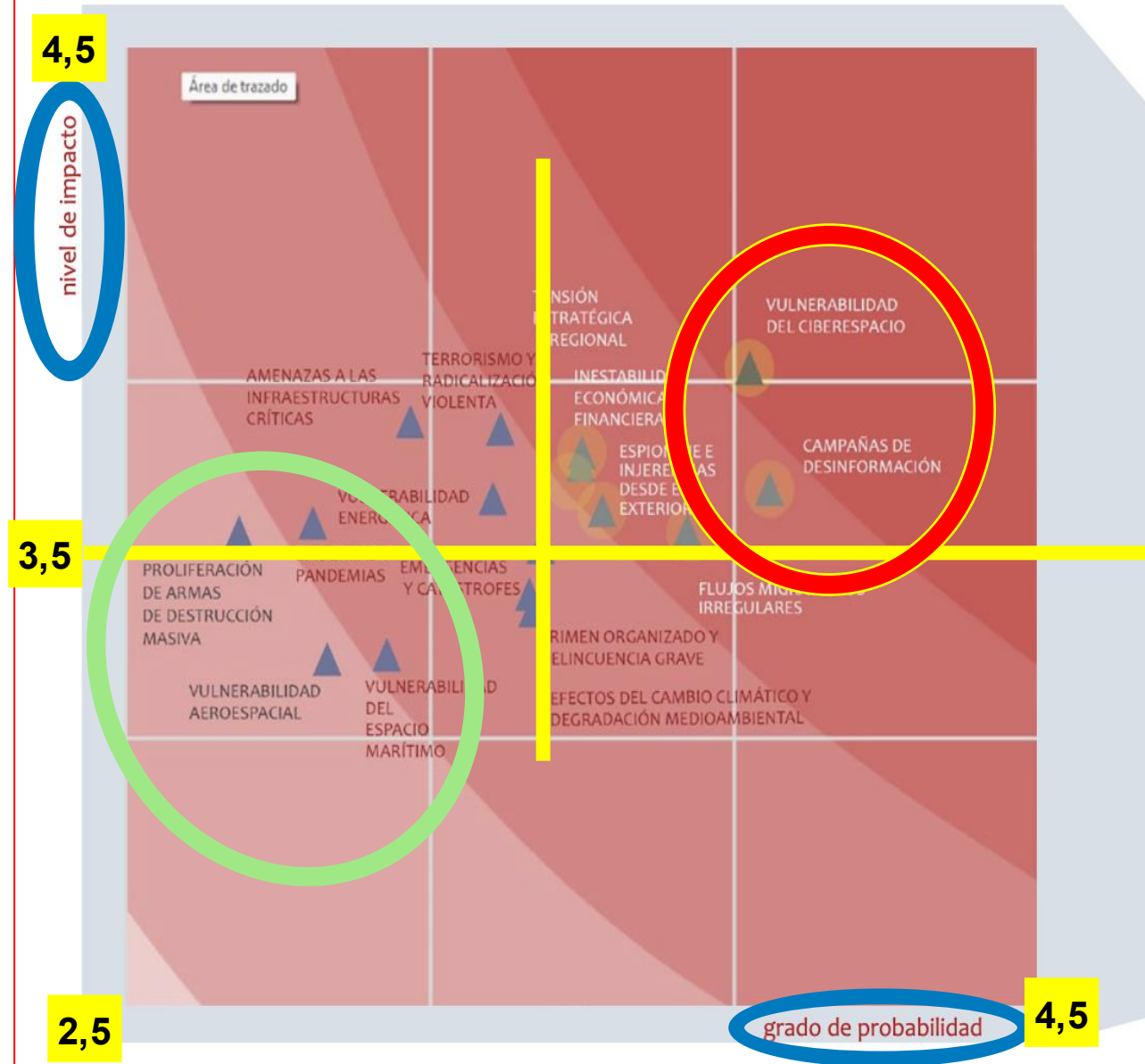
2024/25

Vulnerabilidad del ciberespacio

Campañas de desinformación
Flujos migratorios irregulares
Tensión estratégica y regional
Inestabilidad económica y financiera

Figura A-2

Mapa de Riesgos para la Seguridad Nacional 2024



	IMPACTO	PROBABILIDAD	INTENSIDAD DEL RIESGO
Vulnerabilidad del ciberespacio	4,044117647	4,053921569	16,39453576
Campañas de desinformación	698529412	4,117647059	15,22923875
Flujos migratorios irregulares	571078431	3,850490196	13,75040249
Tensión estratégica y regional	3,796568627	3,49754902	13,27868488
Inestabilidad económica y financiera	3,764705882	3,495098039	13,15801615
Espionaje e injerencias desde el exterior	3,639705882	3,566176471	12,97983348
Terrorismo y radicalización violenta	3,867647059	3,227941176	12,4845372
Emergencias y catástrofes	3,534313725	3,365196078	11,89365869
Vulnerabilidad energética	3,666666667	3,208333333	11,76388889
Amenazas a las infraestructuras críticas	3,887254902	2,93872549	11,42357507
Crimen organizado y delincuencia grave	3,406862745	3,325980392	11,33115869
Efectos del cambio climático y de la degradación del medio natural	3,360294118	3,338235294	11,21745242
Epidemias y pandemias	3,600490196	2,617647059	9,424812572
Vulnerabilidad del espacio marítimo	3,225490196	2,850490196	9,194228181
Vulnerabilidad aeroespacial	3,213235294	2,666666667	8,568627451
Proliferación de armas de destrucción masiva	3,575980392	2,367647059	8,466659458

Producto del impacto y de la probabilidad de cada evento

Figura A-3
Intensidad del riesgo

Algunos datos (1)



- **La World Wide Web (WWW) se inventó en 1989.**
- **El primer “sitio” empezó a funcionar en 1991.**
- **Hoy día hay más de 1.900 millones de páginas.**
- **En 2015: 2.000 millones de usuarios de internet.**
- **En 2018: 4.700 millones de usuarios.**
- **En 2025 se estiman unos 6.000 (70% población) millones de una población de casi 8.100.**
- **Y subiendo.**



Algunos datos (2)



- Se calcula que en 2017, se producía un ciberataque a una empresa cada 14 segundos.
- En 2021 sería cada 11 segundos.
- Los gastos previstos en ciber seguridad entre 2017-2021. 1 billón (España) de USD (1 trillón americano), con un incremento anual entre un 12-15%.
- Los costes originados por el *ransomware* se calculan en unos 10.500 millones USD.



Efectos en las empresas



Incorporación de las TICs:

- **La mayor dependencia de las nuevas tecnologías.**
- **La mayor interconexión entre diferentes sistemas.**
- **La gran cantidad de datos (*big data*) que deben asegurarse.**

Grave impacto económico en las empresas por los delitos informáticos:

- **Pérdida de propiedad intelectual.**
- **Ciberdelito por fraudes económicos.**
- **Pérdida de información empresarial confidencial, incluyendo la posible manipulación del mercado bursátil.**
- **Costes de oportunidad, incluyendo interrupción de servicio y descenso de la confianza para actividades en la red.**
- **Coste adicional de garantizar la seguridad de las redes, seguros y recuperación a partir de ciberataques.**
- **Daño a la reputación de la empresa atacada.**



¿Qué venden?



designed by freepik



¿Qué venden?

**A nosotros: nuestros datos, nuestra información,
nuestros gustos, nuestros amigos y un largo etc.**



- El “*big data bang*” será en el Internet de las cosas” (IoT).
- En 2006 había unos 2.000 millones de objetos.
- Actualmente, unos 20.000 millones.



¿Quién dijo desempleo? (1)

- Por muchas tecnologías de protección que tengamos, antivirus más actualizados o todas las medidas que queramos, el punto más débil del sistema ha sido y sigue siendo: **XXXXXX**
- Casi un 90% de todos los casos de hackeos y obtención ilegal de datos se originaron a través de un simple correo electrónico con una de esas palabras tan novedosas que ya hemos visto.
- La mejor solución: formación de los empleados y de uno mismo.
- Previsiones de gasto en formación de personal en ciberseguridad: 10.000 Millones USD hasta 2027. (1.000 millones en 2014).
- Profesionales de ciberseguridad necesarios en 2019: Unos 6 millones .
- Cada vez más necesidades de expertos en ciberseguridad e IA.
- Desempleo en el ámbito de la ciberseguridad: 0% !



¿Quién dijo desempleo? (2)



ABOUT RESEARCH LISTS VIDEOS RADIO CONTACT

Cybercrime Costs. PHOTO: Cybercrime Magazine.

Cybercrime To Cost The World \$10.5 Trillion Annually By 2025

Special Report: Cyberwarfare In The C-Suite.

- [Steve Morgan](#), Editor-in-Chief

Sausalito, Calif. - Nov. 13, 2020

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling \$6 trillion USD globally in 2021 — would be the world's third-largest economy after the [U.S. and China](#).

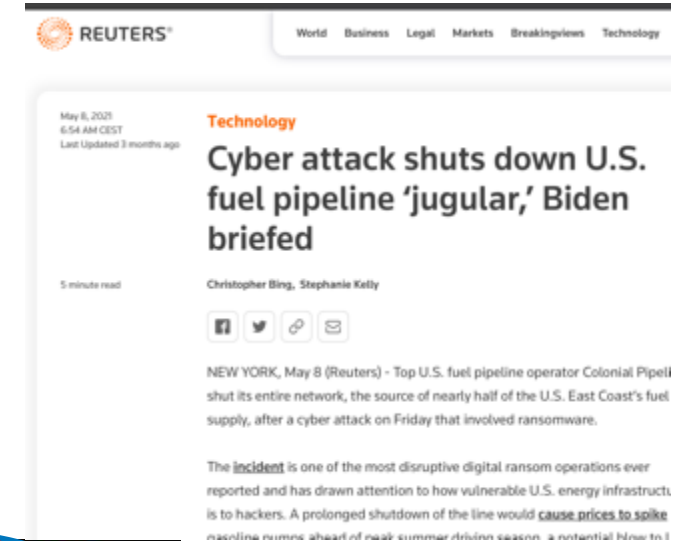
Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching \$10.5 trillion USD annually by 2025, up from [\\$3 trillion USD in 2015](#). This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the [damage inflicted from natural disasters](#) in a year, and will be [more profitable](#) than the global trade of all major illegal drugs combined.

Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021

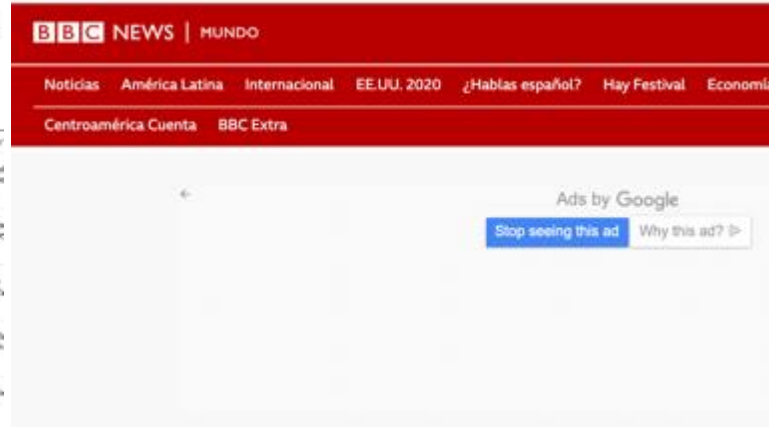
Tweets by @CybersecuritySF

Global #Ransomware Damages Costs To Hit \$20 billion USD in 2021 — which is 57X more than it was in 2015, according to Cybersecurity Ventures @CybersecuritySF [cybersecurityventures.com/global-ransome...](#) via Cybercrime Magazine

Global Ransomware Damage Costs Pr... Fastest growing type of cybercrime is exp... [cybersecurityventures.com](#)



¿Quién dijo “gran hermano”?



Buen ciudadano, a la fuerza: China acelera su plan de control social para 2020

Antes de que Black Mirror fantaseara con cómo la tecnología podría modificar nuestras vidas, el Gobierno chino ya barajaba medidas para controlar a su ciudadanía



Una prueba del sistema de reconocimiento facial en China. (Reuters)

La polémica en China por la imposición del reconocimiento facial a todos los compradores de teléfonos

Redacción
BBC News Mundo

1 diciembre 2019



Estamos [asociados con los socios](#) y podemos ganar una comisión si compra a través de un enlace de la web.

Pagos mediante smartphone en China: la guía de Wechat y Alipay

10/11/2019 POR MANUEL RECOMA

[DEJAR UN COMENTARIO](#)



Pago mediante smartphone en China – Índice

- 1 WeChat Pay y Alipay: ¿qué son?
- 2 Configuración inicial
- 3 Cómo realizar pagos con Wechat





Criptomonedas y criminales



“Deep / Dark Web” (1)



UNIVERSIDAD
DE MURCIA



Facultad de
Turismo y Relaciones
Internacionales



“Deep / Dark Web” (2)



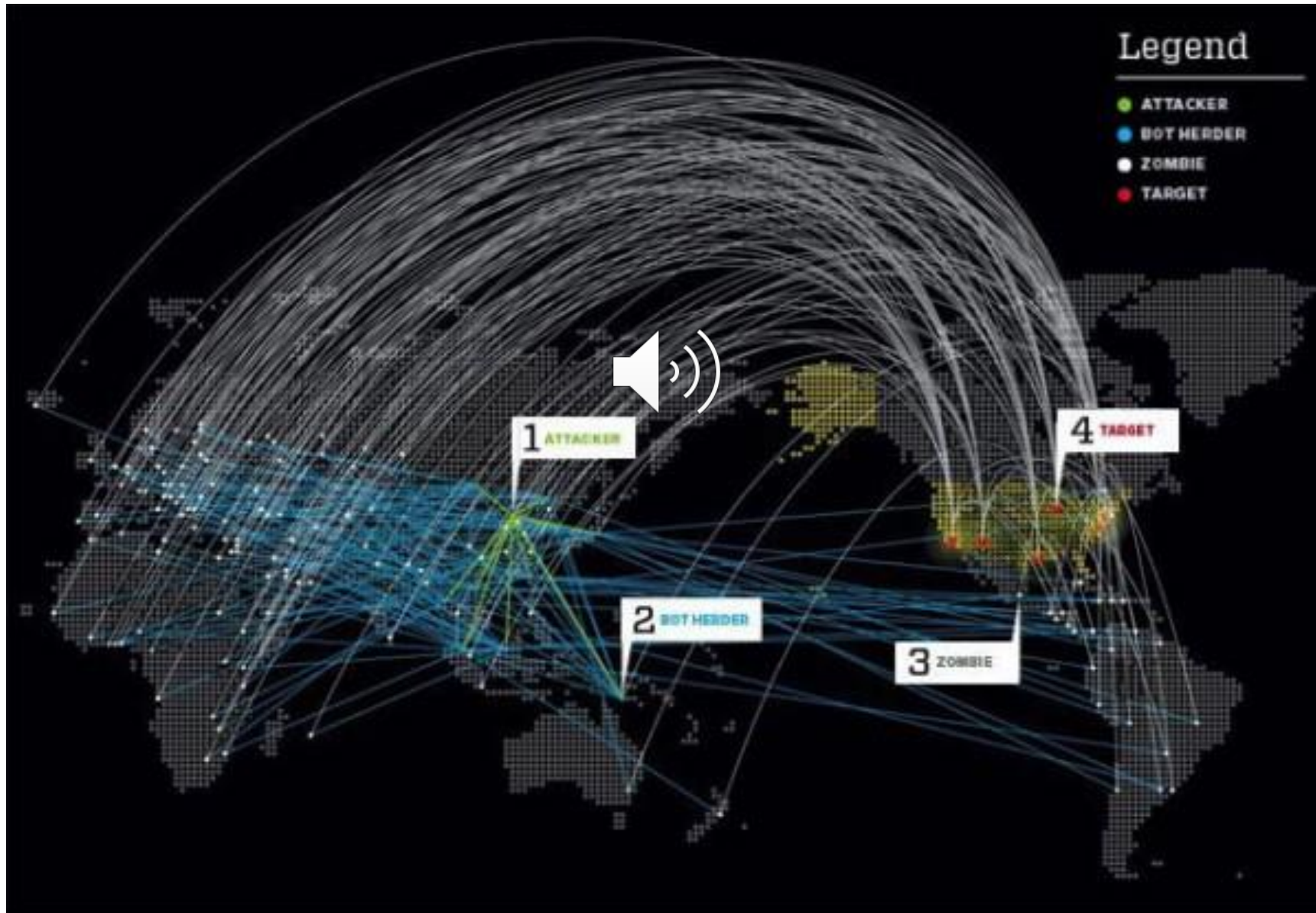
El marco estratégico y el entorno de la información



LOS NUEVOS “MARES”:
El entorno cibernético es una extensión global del campo de batalla



Operaciones en el Ciberespacio



Ciberdefiniciones

**"Lo que estamos viendo no es ciberguerra, sino un aumento en el uso de tácticas similares a las de la guerra y eso nos confunde. No tenemos buenas definiciones acerca de lo que constituye la ciberguerra y cómo debe pelearse".
(Bruce Schneier, 2011).**



Ataque a instalación nuclearar de Irán. 2010



SEGURIDAD INTEGRAL MUNDO JURÍDICO INTERNACIONAL FORMACIÓN EMPLEO PERSONAL DE SEGURPRI IFCCSS ORGANIZACIONES NOVEDADES

STUXNET: La primera ciberarma de la historia

16 mayo, 2018 Gustavo Romero Sánchez Ciberseguridad



Facebook Twitter LinkedIn Email WhatsApp Telegram

Stuxnet es considerado la primera arma digital de la historia. Su irrupción en el tablero geopolítico sentó las bases que han inaugurado un tipo de guerra diferente. Batallas que no se libran en teatros operacionales convencionales sino en el ciberespacio, un escenario que hace imposible discernir el bien del mal y en el que, cada paso que se inicia, supone asumir un riesgo de consecuencias imprevisibles... acaso apocalípticas.

ENTRADAS RECIENTES



Clanes familiares en España y tráfico de drogas. Una aproximación criminológica (1ª Parte)

4 OCTUBRE, 2020

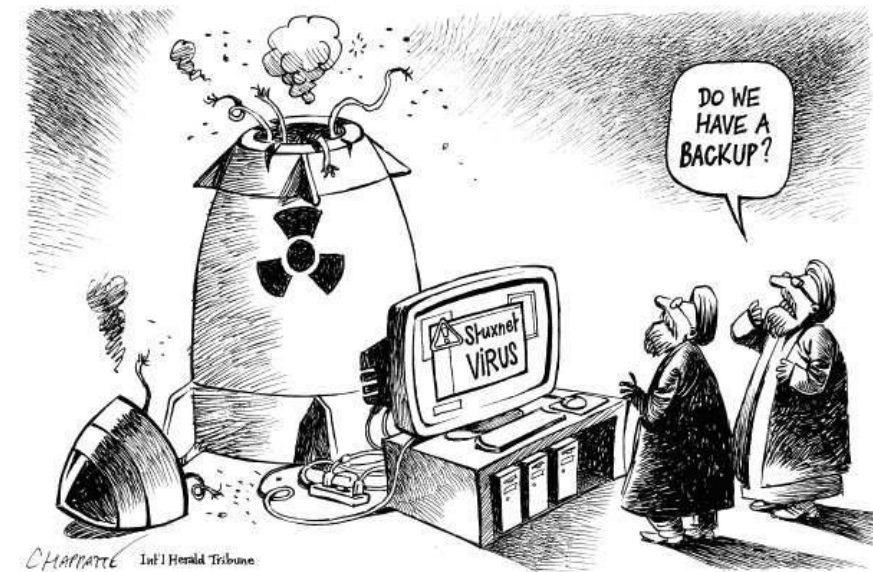


Granjas de trolls rusas

30 SEPTIEMBRE, 2020



El Ministerio del Interior dota a las Fuerzas de Seguridad del Estado de un



Rusia-Ucrania

La guerra en el ámbito cibernético



BBC NEWS MUNDO

Noticias América Latina Internacional Hay Festival Economía Ciencia Salud Cu

Centroamérica Cuenta BBC Extra

La otra guerra inclemente que libran Ucrania y Rusia

Joe Tidy
Corresponsal de asuntos cibernéticos

15 abril 2023



Oleksandr es uno de los hackers más prominentes en Ucrania.

Cuando Rusia invadió Ucrania, arrancó una segunda y menos visible batalla en el ciberespacio. Joe Tidy, corresponsal de asuntos cibernéticos de la BBC, viajó a Ucrania para hablar con quienes pelean la guerra cibernética.

Descubrió que el conflicto ha difuminado las líneas entre cibernéticos y actividades 'hacktivistas'. Este es su reportaje en primera persona.

LA VERDAD

(ESPECIAL SEGURIDAD)

EN LAS TRINCHERAS DE LA CIBERSEGURIDAD NACIONAL



La guerra en Ucrania se ha convertido en la primera ciberguerra mundial. El conflicto tiene en tensión a los centros españoles de respuesta, públicos y privados, que llevan meses combatiendo con éxito una oleada de ciberataques contra nuestro país. Es una lucha en la que nos jugamos mucho y, aunque no seamos conscientes, todos estamos implicados. Se lo contamos.

POR FERNANDO GARCÍA FOTO: CARLOS CARRIÓN



Amenazas híbridas: ¿A qué nos enfrentamos?

¿Nuevo concepto para las
prácticas de siempre?

La ambigüedad como
amenaza

Lucha contra lo difuso

La sociedad como objetivo

FAKE NEWS? o...





Amenazas híbridas: ¿A qué nos enfrentamos?

¿Nuevo concepto para las
prácticas de siempre?

La ambigüedad como
amenaza

Lucha contra lo difuso

La sociedad como objetivo

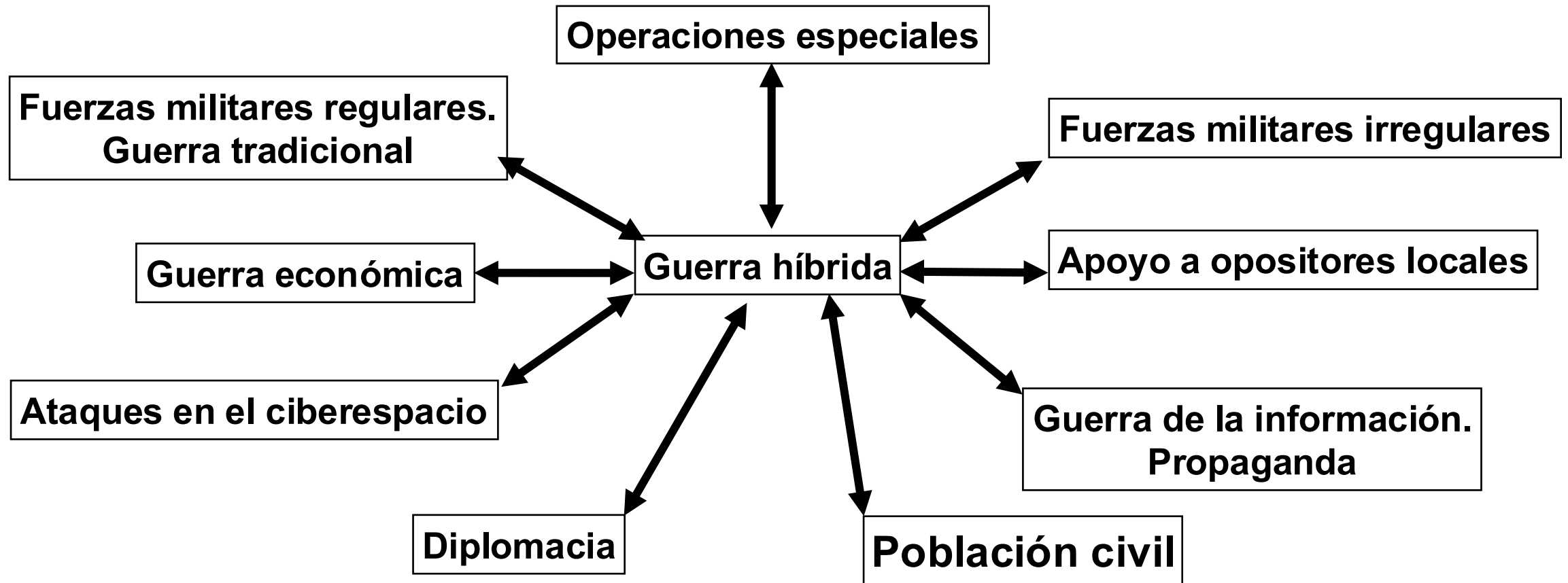
FAKE NEWS? o...

¿O NEWS FAKE?

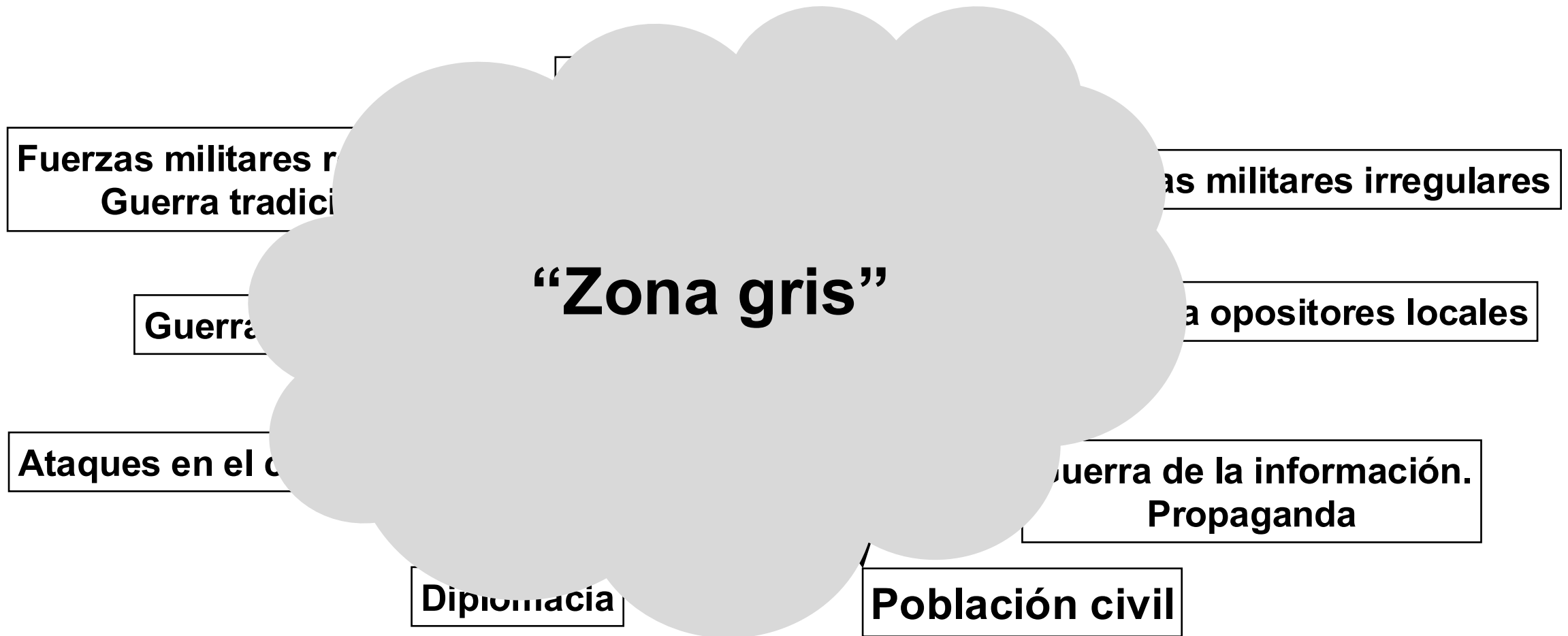


Amenaza / Guerra Híbrida

Medios empleados



Amenaza / Guerra Híbrida Medios empleados



GUERRA HÍBRIDA

LA AMENAZA EN LA ZONA GRIS

No siempre comienza con disparos.
Puede empezar mucho antes.



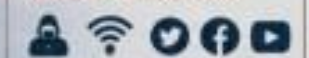
CEUTA



INSTRUMENTOS DE PODER

- DESINFORMACIÓN Y MANIPULACIÓN INFORMATIVA
- CIBERATAQUES
- PRESIÓN MIGRATORIA INSTRUMENTALIZADA
- COERCIÓN ECONÓMICA
- PRESIÓN DIPLOMÁTICA
- ESPIONAJE
- SABOTAJE Y ATAQUES A INFRAESTRUCTURAS CRÍTICAS

OTROS ACTORES PUEDEN EXPLOTAR LA CRISIS EN EL ÁMBITO INFORMATIVO



LA PREGUNTA ESTRATÉGICA

¿Quién creó o permitió las condiciones para que se produjera la crisis?

LA MEJOR DEFENSA

- COMPRENDER
- ANTICIPAR
- DISUADIR
- RESPONDER

ZONA GRIS

Entre la paz y la guerra. El adversario actúa sin cruzar el umbral que desencadenaría una respuesta militar convencional.

UNA RESPUESTA INTEGRAL DEL ESTADO

INTELIGENCIA Y ALERTA TEMPRANA Detectar indicios antes de que la amenaza se convierta en crisis.	COORDINACIÓN INSTITUCIONAL Acción unida de todos los instrumentos del Estado.	MARCO LEGAL Y REGLAS CLARAS Soldados con misión, medios adecuados y seguridad jurídica. Legalidad no puede significar indefensión.	FUERZAS ARMADAS PREPARADAS Capacidad, medios y determinación para proteger los intereses de España.	DISUASIÓN Y DETERMINACIÓN El adversario debe saber que cualquier agresión tendrá un coste.
--	---	--	---	--

ESPAÑA TIENE LAS CAPACIDADES. LA CUESTIÓN ES TENER LA VOLUNTAD, LA UNIDAD Y LA CLARIDAD PARA EMPLEARLAS.

Índice



1. Introducción y definiciones.
2. Algunos ejemplos de actos en el ciberespacio.
3. Estrategia de Seguridad Nacional 2017: *Global commons*.
4. Informe sobre las amenazas en la red y sus efectos.
5. Operaciones en el ciberespacio. La amenaza “híbrida”.
- 6. La UE y la OTAN.**
- 7. La posición de España. La Estrategia Nacional de Ciberseguridad.**
- 8. Estudio sobre cibercriminalidad en España.**
- 9. El dominio “cognitivo.**
- 10. Conclusiones.**



¿Qué ha hecho la Unión Europea?

(1)



- 2004, Agencia de Seguridad de las Redes y de la Información de la Unión Europea, ENISA (*European Union Agency for Cybersecurity*).
- 2013, Estrategia de ciberseguridad de la Unión Europea.
- 2016, Organización Europea de Ciberseguridad, ECSO (European Cyber Security Organization) para reforzar la investigación y el desarrollo conjunto de medidas de prevención y protección cibernética entre Estados, empresas e instituciones europeas.
- 2017, Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU. European Union Agency for Network and Information Security (ENISA).
- 2019, Reglamento del Consejo sobre Ciberseguridad.
- 2019, Decisión por la que se regula un sistema de medidas restrictivas contra los ciberataques a las instituciones europeas y a los Estados miembros.



¿Qué ha hecho la Unión Europea? (2)



2021, REGLAMENTO (UE) 2021/784 DEL PE y del CUE (29 de abril de 2021), sobre la lucha contra la difusión de contenidos terroristas en línea.

¿Qué se entiende por contenidos terroristas en línea?: Texto, imágenes, archivos de audio o vídeos utilizados para:

- **Incitar a cometer actos terroristas.**
- **Dar instrucciones sobre cómo cometer delitos.**
- **Solicitar la participación en grupos terroristas.**

¿Qué ha hecho la Unión Europea?

(3)



Acta de servicios digitales. Octubre 2022:

- **Proceso hasta principios de febrero 2024.**
- **Asociada al Acta de mercado digital.**
- **Objetivos:**
 - **Proteger a los consumidores online: derechos fundamentales, contenidos ilegales, infancia, desinformación.**
 - **Promover la innovación y la competitividad de proveedores de servicios digitales.**
 - **Fomentar el emprendimiento, PYMEs.**
 - **Todo ello, acorde con los principios y valores de la UE.**

¿Qué ha hecho la Unión Europea?

(4)



Ley de la inteligencia artificial UE. Febrero 2024

- **Clasificación de la IA en función del riesgo:**
 - **Alto riesgo**, p.e., de puntuación social o manipuladora.
 - **Menor riesgo**, juegos "normales" autorizados en la UE.
- **Las obligaciones recaen en los desarrolladores de IA:**
 - Incluso los que tengan su sede en un tercer país.
- **Usuarios son personas físicas o jurídicas con fines profesionales:**
 - **Obligaciones de usuarios (implantadores) de sistemas de IA de alto riesgo**, aunque menos que los proveedores (desarrolladores).
- **IA de propósito general (GPAI) para proveedores:**
 - **Proporcionar documentación técnica.**
 - **Respetar derechos de autor.**
 - **Realizar seguimiento y notificar incidentes graves.**

¿Qué ha hecho la Unión Europea? (5)



Ley de Mercados Digitales (DMA) UE

- **Objetivo:**
 - **Establecer reglas justas para los mercados digitales, limitando el poder de las grandes plataformas en línea.**
- **Funcionamiento:**
 - **Impedir que las plataformas dominantes abusen de su posición, por ejemplo, obligándolas a permitir la interoperabilidad con otras aplicaciones o a no favorecer sus propios servicios frente a los de la competencia.**
- **Beneficios:**
 - **Dar más opciones a los consumidores, fomentar la competencia y ayudar a las pequeñas y medianas empresas (pymes) a digitalizarse.**

¿Qué ha hecho la Unión Europea? (6)



Ley de Servicios Digitales (DSA) UE

- **Objetivo:**
 - **Crear un espacio digital más seguro y transparente para los ciudadanos, obligando a las plataformas a ser más responsables.**
- **Funcionamiento:**
 - **Establece un marco para detectar y eliminar rápidamente el contenido ilícito (como el discurso de odio, la desinformación o el material terrorista) y obliga a las plataformas a ser más transparentes sobre la publicidad que muestran.**
- **Beneficios:**
 - **Protege a los usuarios contra contenidos dañinos y malos actores, aumenta el control sobre lo que se ve en línea y proporciona un mecanismo para denunciar contenido ilegal.**

Declaración Europea sobre Derechos y Principios Digitales (2023)

Entregar resumen de una página a mano para el próximo día

<https://digital-strategy.ec.europa.eu/es/library/european-declaration-digital-rights-and-principles>

¿Qué ha hecho la OTAN?



Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE

Los responsables comunitarios quieren plantear hoy el conflicto en su cumbre con Putin



RICARDO MARTÍNEZ DE RITUERTO
Bruselas - 18 MAY 2007 - 00:00 CEST

La Unión Europea y la OTAN ven con alarma los *ciberataques* sufridos en las últimas semanas por Estonia en represalia por el traslado en Tallin del monumento a los soldados soviéticos caídos durante la II Guerra Mundial. El asunto será planteado en la cumbre que hoy celebran los Veintisiete con Rusia en Samara, después de que un representante comunitario calificara de "inaceptables" las agresiones. Especialistas de la Alianza Atlántica han visitado Tallin para analizar sobre el terreno lo sucedido, un fenómeno nuevo para el que de momento no hay doctrina de respuesta.

SUSCRIPCIÓN
DIGITAL
ILIMITADA



About us f

2008

The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub

We do research, training and exercises in four core areas: technology, strategy, operations and law



Made for minds.

TOP STORIES MEDIA CENTER TV RADIO LEARN GERMAN

CORONAVIRUS WORLD GERMANY BUSINESS SCIENCE ENVIRONMENT CULTURE SPORTS

TOP STORIES / WORLD / EUROPE



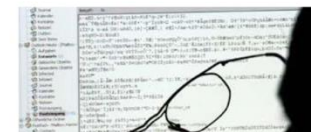
MLA Thin film optics

PIR Fresnel Lens For SmartThings Motion Detector
Fresnel Factory Inc.

EUROPE

NATO Sees Recent Cyber Attacks on Estonia as Security Issue

The massive wave of cyber attacks which have hit Estonia's websites this month are a security issue which concern NATO, the Alliance's Secretary General Jaap de Hoop Scheffer said Friday.



"These cyber attacks have a security dimension without any doubt and that is the reason that NATO expertise was sent to Estonia to see what can and should be done," he told a meeting of lawmakers from NATO member states held in Funchal on the Portuguese

NATO AJP-3-20 Doctrine for Cyberspace OPS

Sección 3. Consideraciones legales:

- **A pesar del cierto consenso internacional sobre el asunto, hay muchas variaciones de interpretación e implementación.**
- **Al no haber normas acordadas, cada país, grupo o individuo debe decidir para sí si el acto, incidente o ataque son constitutivos de delito y como responder.**
- **Consecuentemente, no existen “líneas rojas” que determinen umbrales de actuación.**
- **Por tanto, es imperativo que el comandante militar reciba asesoramiento legal claro para cómo actuar en operaciones en el ciberespacio.**



Respuesta de la OTAN ante la desinformación

- **Comprender.**
- **Prevenir.**
- **Contener y mitigar.**
- **Recuperar.**

¿Y qué hace hace España?



Convenio de Budapest sobre la Ciberdelincuencia, 23.11.2001. Consejo de Europa

Objetivo:

- **Que los países tengan leyes compatibles, puedan investigar estos delitos de forma eficaz y cooperen entre sí, incluso cuando las pruebas o los autores se encuentren en otro país.**

Aspectos fundamentales:

- 1. Tipifica los delitos informáticos.**
- 2. Persigue el fraude y la falsificación informáticos.**
- 3. Combate los delitos contra menores y la propiedad intelectual.**
- 4. Facilita la obtención de pruebas electrónicas.**
- 5. Establece cooperación judicial internacional.**
- 6. Crea una red de contacto permanente 24/7.**
- 7. Exige garantías para proteger los derechos fundamentales.**

Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC). 2007:

- Oficina de Coordinación Cibernética (OCC).
- Depende de Secretaría de Estado de Seguridad (SES) del MININT.
- Coordina los Equipos de Respuesta ante Incidentes de Seguridad Informática de Referencia (CSIRT) con la SES.
- Coordina con equipos equivalentes de la UE.

Instituto Nacional de Ciberseguridad de España (INCIBE): <https://www.incibe.es/incibe-cert/tags/administraci%C3%B3n%20p%C3%BAblica>

- Dependiente del INCIBE, está el INCIBE-CERT, Equipo de respuesta contra emergencias informáticas (*Computer emergency response team*).
- Este CERT se considera el CSIRT de referencia para delitos cibernéticos, contra empresas, ciudadanos e infraestructuras críticas.
- Coordina con el CNPIC.
- Sectores más atacados: tributario y financiero, transportes y energía.

La Estrategia Nacional de Ciberseguridad 2019. <https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf>

INCIBE CONFERENCIA SEGURIDAD



YouTube ^{ES}

Buscar



25 Abril / 11:00h

JORNADA SOBRE CIBERSEGURIDAD Y FRAUDE ONLINE

En breve comenzamos

JORNADA DE CIBERSEGURIDAD Y FRAUDE ONLINE



ocutv
42,7 K suscriptores

Suscribirse

47



Compartir

Descargar

Recortar



Métodos más usados **(Centro Criptológico Nacional, CCN-CERT)**

- **Propagación de código dañino por Email.**
- **Uso de malware de criptojacking/cryptomining.**
- **Refinamiento del phishing para persuadir a los usuarios de la autenticidad de las estafas.**
- **Innovación en las plataformas del Ciberdelito como Servicio (Crime as a Service).**

Constantes mejoras en los servicios ofertados, mayor facilidad de uso, lo que contribuye a extender su popularidad y propiciar ataques más eficientes.



La Estrategia Nacional de Ciberseguridad 2019

- **Aprobada por el Consejo de Seguridad Nacional**
- **Cap.1. El ciberespacio como espacio común global.**
- **Cap. 2. Amenazas y desafíos en el ciberespacio.**
- **Cap. 3. Propósito, principios y objetivos para la ciberseguridad.**
- **Cap. 4. Líneas de acción y medidas.**
- **Cap. 5. La ciberseguridad y el Sistema de Seguridad Nacional.**



Nuevo Sistema de Seguridad Nacional



LEYENDA

- Comités de apoyo **existentes**
- Comités de apoyo **de nueva creación**

DSN

Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno
Secretaría Técnica y Órgano de Trabajo Permanente del Consejo de Seguridad Nacional



Consejo Nacional de Ciberseguridad



Mando Conjunto del Ciberespacio (1)



- **Órgano responsable de la dirección, la coordinación, el control y la ejecución de las acciones conducentes a asegurar la libertad de acción de las Fuerzas Armadas en el ámbito ciberespacial.**
- **Planea, dirige, coordina, controla y ejecuta las operaciones militares en el ciberespacio y, en este ámbito, las acciones necesarias para garantizar la supervivencia de los elementos físicos, lógicos y virtuales críticos para la Defensa y las Fuerzas Armadas.**



Mando Conjunto del Ciberespacio (2)



UNIVERSIDAD DE MURCIA



Facultad de Turismo y Relaciones Internacionales



Selección: ESPAÑA

HAZTE PREMIUM

ALBERTO GALLEGO

EL PAÍS

España

ANDALUCÍA · CATALUÑA · COMUNIDAD VALENCIANA · GALICIA · MADRID · PAÍS VASCO · ÚLTIMAS NOTICIAS

DEFENSA >

El centro donde los soldados se entrenan para luchar en el ciberespacio

La base de Retamares acoge la primera Escuela Militar de Ciberoperaciones conjunta del mundo



Los alumnos Lucia, suboficial del Ejército del Aire, y Roberto, suboficial del Ejército de Tierra, en la entrada del Mando Conjunto del Ciberespacio, donde por ahora se encuentra la Escuela Militar de Ciberoperaciones (EMCO), en la Base de Retamares, Madrid. INÉS ARCONES



BELÉN DOMÍNGUEZ CEBRIÁN

Madrid · 06 ENE 2025 · 05:40 CET

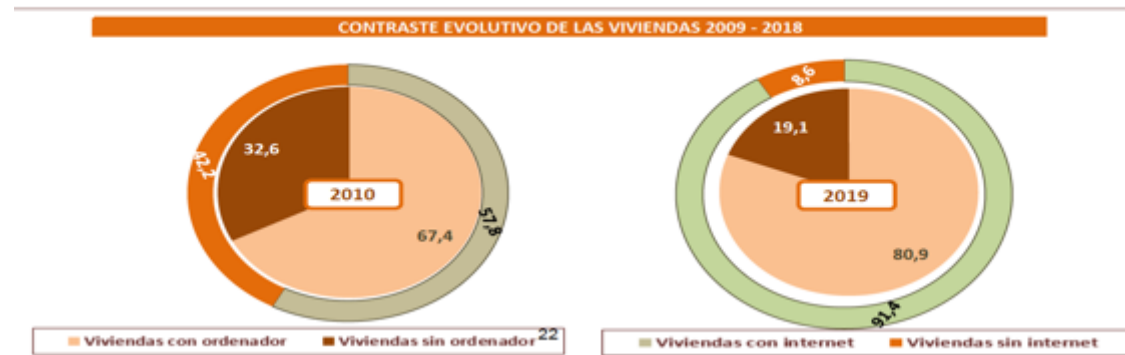
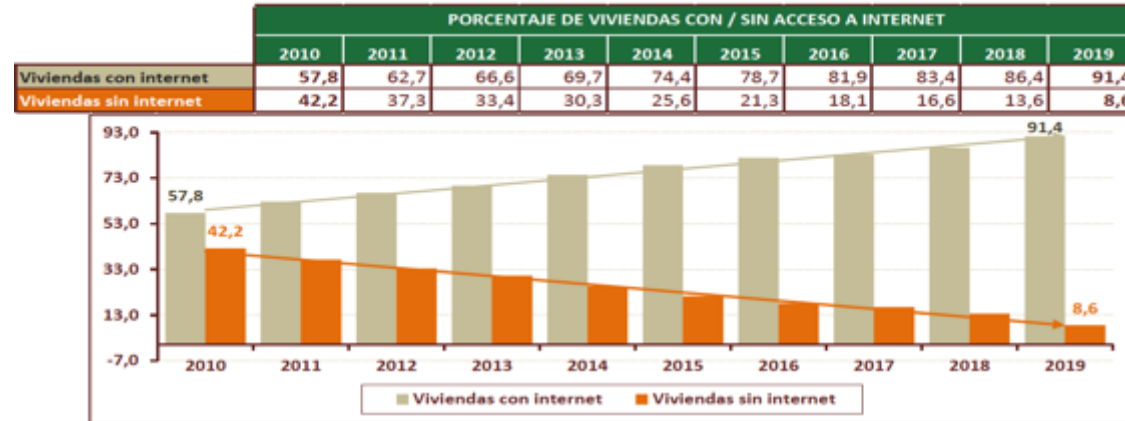
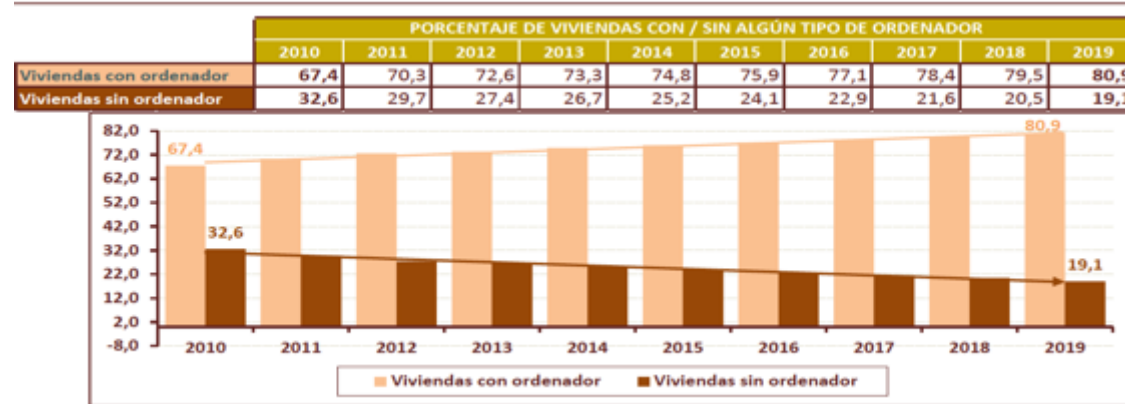


<https://elpais.com/espana/2025-01-06/el-centro-donde-los-soldados-se-entrenan-para-luchar-en-el-ciberespacio.html#https://imagenes.elpais.com/resizer/v2/QBYAHCC5BFG63EP3YLXCYYWAYY.jpg?auth=d676aee38a2bd6efc9537dce16c08e590d1de9a2df16390642885d565b629649&width=828>

El avance de Internet



Ordenadores nuevos vs. accesos a Internet



Perfil del usuario de Internet

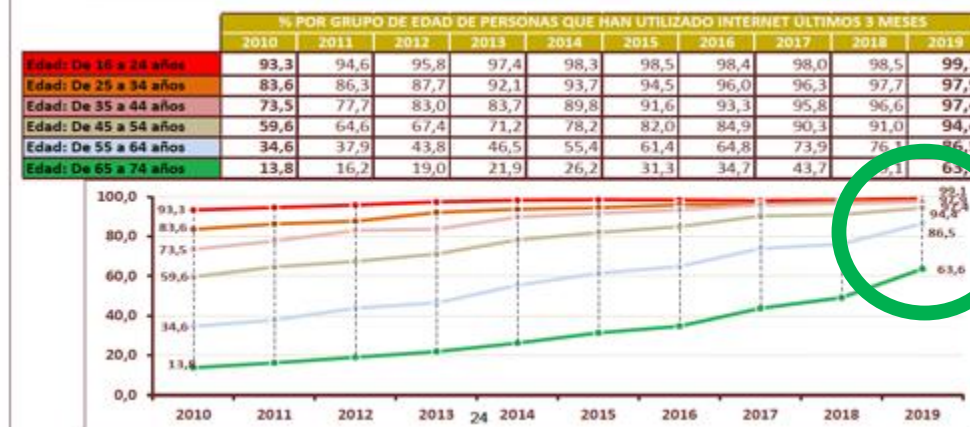


2

RADIOGRAFIA DE LA SOCIEDAD DE LA INFORMACION

(Fuente de datos: INE)

>> 2.2.PERFIL DEL CIUDADANO ANTE LA SOCIEDAD DE LA INFORMACION. USO DE INTERNET



Confianza en compras por Internet



2 RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN (Fuente de datos: ONTSI)

>> 2.7. INDICADORES DE LA SOCIEDAD DE LA INFORMACIÓN (Publicación: Indicadores destacados de la sociedad de la información)

Hogares con telefonía fija y móvil (% sobre el total de hogares)



Empresas que utilizan medios sociales por tipo (% sobre las empresas que usan Medios Sociales)



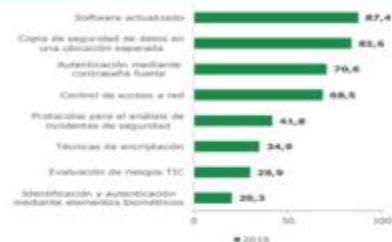
Grado de confianza en Internet (% sobre la población total)



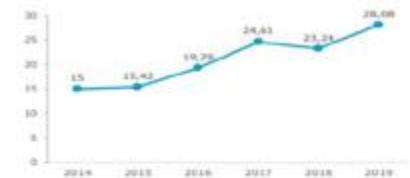
Particulares que usan Internet con fines específicos (% sobre la población total)



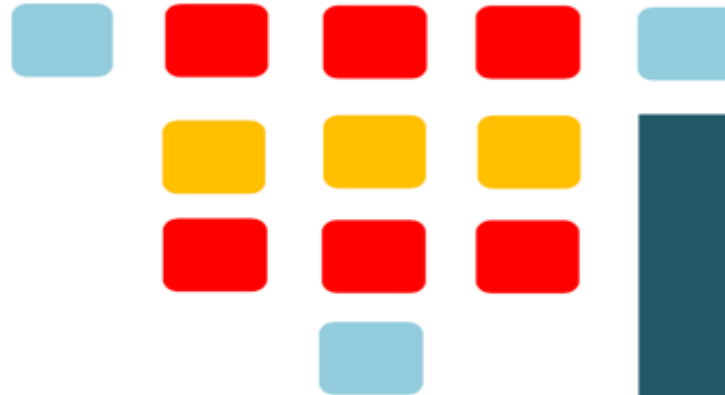
Empresas que utilizan sistemas internos de seguridad por tipo (% sobre el total de empresas que utilizan sistemas internos de seguridad)



Evolución de las empresas que compraron algún servicio de cloud computing usado a través de Internet en España (% sobre el total de empresas)



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



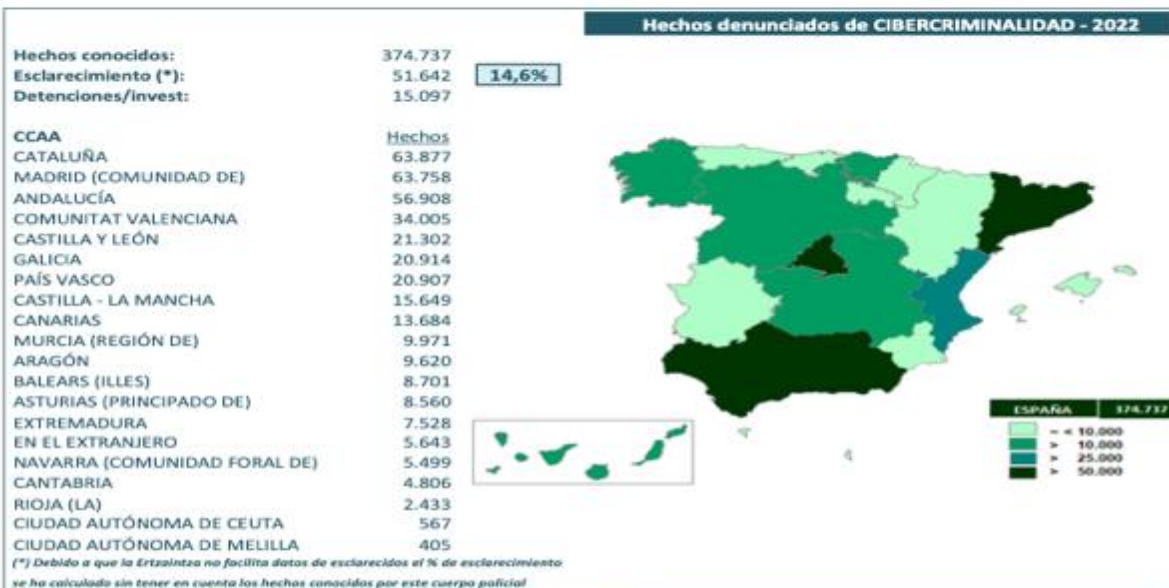
INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.5. Representación territorial de hechos denunciados de cibercriminalidad. Año 2022



Informe Anual de Seguridad Nacional

2024

.....

Posición de España en el índice internacional de ciberseguridad de la UIT

Según la quinta edición del “Global Cybersecurity Index (GCI)” de la Unión Internacional de Telecomunicaciones (UIT) publicada en septiembre de 2024, España figura en el nivel 1, de un total de 5, en cuanto a compromiso con la ciberseguridad. El GCI es un índice compuesto para medir el compromiso con la ciberseguridad de los 194 Estados Miembros de la UIT, a partir de datos recogidos en 2023-2024, en los cinco pilares siguientes: marco legal, medidas técnicas, medidas organizativas, desarrollo de capacidades y medidas de cooperación. España obtiene la máxima puntuación en 4 de los 5 pilares medidos por el GCI y se posiciona en todos por encima de la media de la Unión Europea. (Figura 8.17)

España



Puntuación País
de un máximo de 20 puntos por colmena

Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de capacidades	Medidas de cooperación
20	20	20	19,74	20

*Los Países se clasifican de acuerdo con www.itu.int

Fuente: Unión Internacional de Telecomunicaciones (UIT)

GCI 5ª Edición Perfil del País

Áreas de Fortaleza Relativa

Medidas legales
 Medidas técnicas
 Medidas organizativas
 Medidas de cooperación

Área de Crecimiento Potencial

Medidas de desarrollo de capacidades

Nivel de Rendimiento

T1 Modelo de conducta



Figura 8.17: Datos de España del Índice de Ciberseguridad Global 2024

Informe Anual de Seguridad Nacional

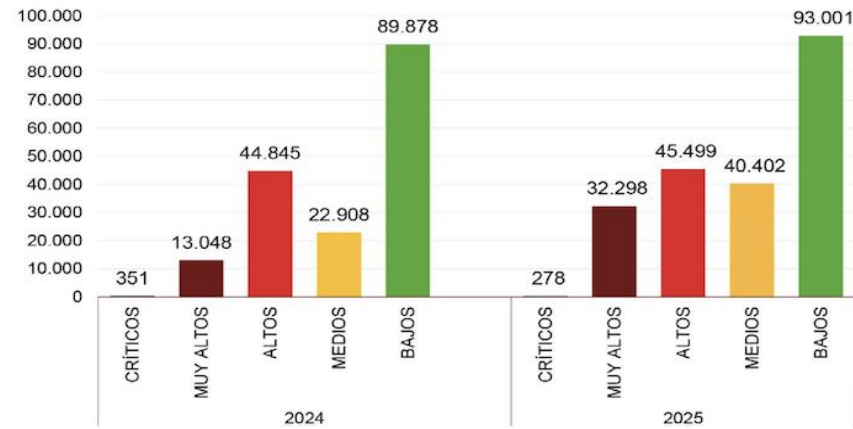
2025

.....



Fuente: Centro Criptológico Nacional

Figura 8.1: Incidentes gestionados por el CCN-CERT



Fuente: Centro Criptológico Nacional

Figura 8.2: Comparativa del número total de incidentes por peligrosidad 2024-2025



Fuente: Centro Criptológico Nacional

Figura 8.3: Clasificación de los incidentes gestionados por el CCN-CERT

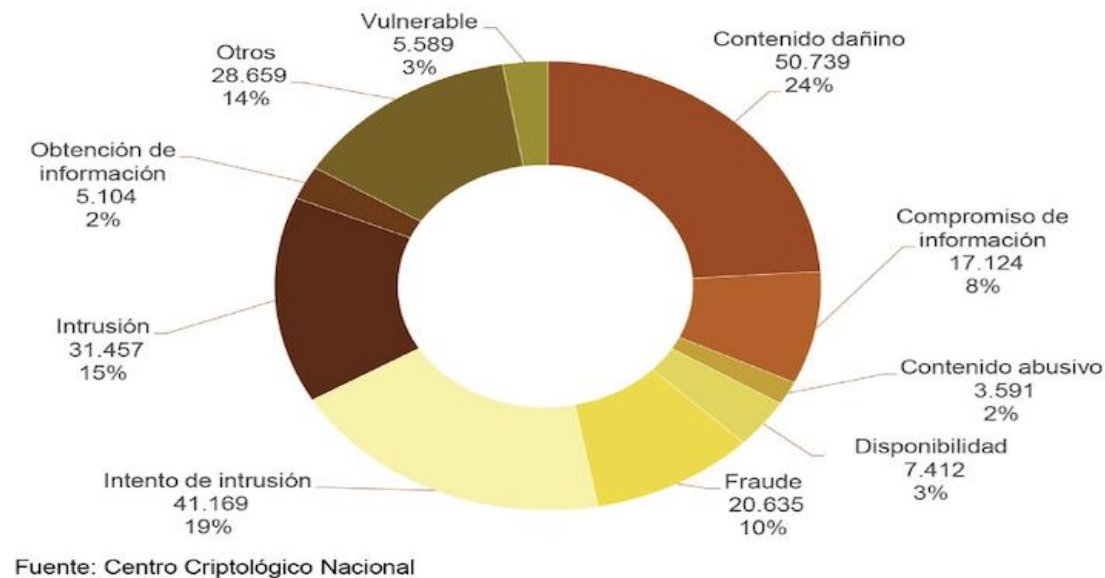


Figura 8.4: Tipología de incidentes gestionados en 2025

Incidentes gestionados por INCIBE en ciudadanos, sector privado y red académica

(Figuras 8.5 a 8.7)

Figura 8.5: Número de ciberincidentes por público objetivo gestionado por INCIBE en 2025

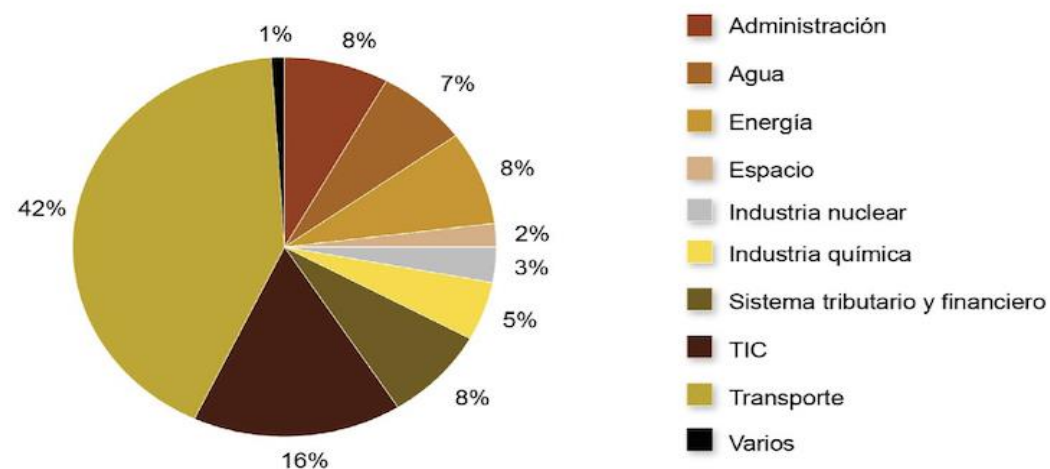
Público objetivo	TOTAL
Ciudadanos y empresas (C&E)	121.348
Red Académica (RedIRIS)	474
Operadores esenciales e importantes (OOEE/OOII)	401
TOTAL	122.223

Fuente: INCIBE

Incidentes en Operadores de Servicios Esenciales de riesgo alto, muy alto o crítico, notificados a la Oficina de Coordinación de Ciberseguridad (OCC) del Ministerio del Interior (Figuras 8.10 a 8.13)



SECTOR ESTRATÉGICO	2021	2022	2023	2024	2025
ADMINISTRACIÓN	7	4	2	2	7
AGUA	4	3	2	12	6
ALIMENTACIÓN	0	0	0	0	0
ENERGÍA	5	11	7	23	7
ESPACIO	0	0	2	0	2
INDUSTRIA NUCLEAR	5	1	3	3	3
INDUSTRIA QUÍMICA	7	8	3	10	5
INSTALACIONES DE INVESTIGACIÓN	0	0	0	0	0
SALUD	0	2	2	2	0
SISTEMA TRIBUTARIO Y FINANCIERO	23	12	18	28	7
TECNOLOGÍAS INFORMACIÓN Y COMUNICACIONES (TIC)	20	11	17	19	14
TRANSPORTE	17	11	23	60	38
VARIOS	3	4	2	1	1
	91	67	81	160	90



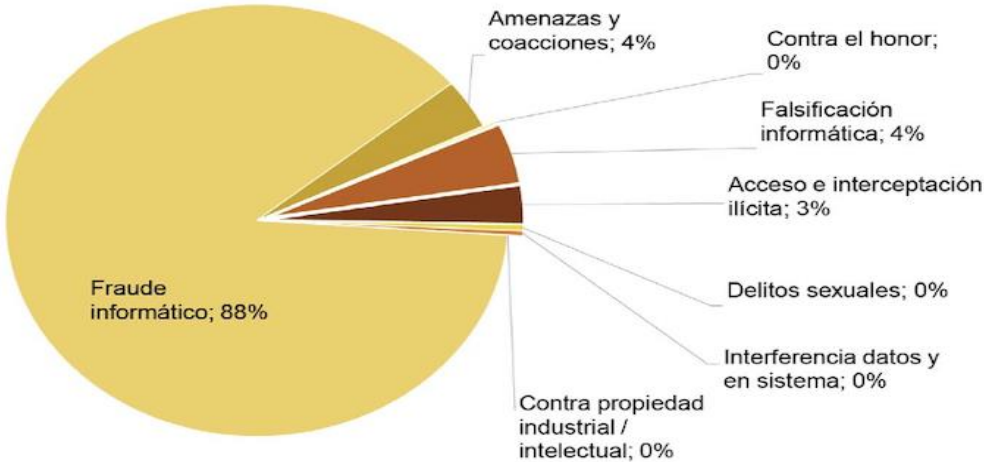
Fuente: Ministerio del Interior

Figura 8.10: Número de incidentes por Sector estratégico que presentan niveles de riesgo alto, muy alto o crítico, de obligada notificación a la OCC

Hechos conocidos de infracciones penales relacionadas con la criminalidad

(Figura 8.14)

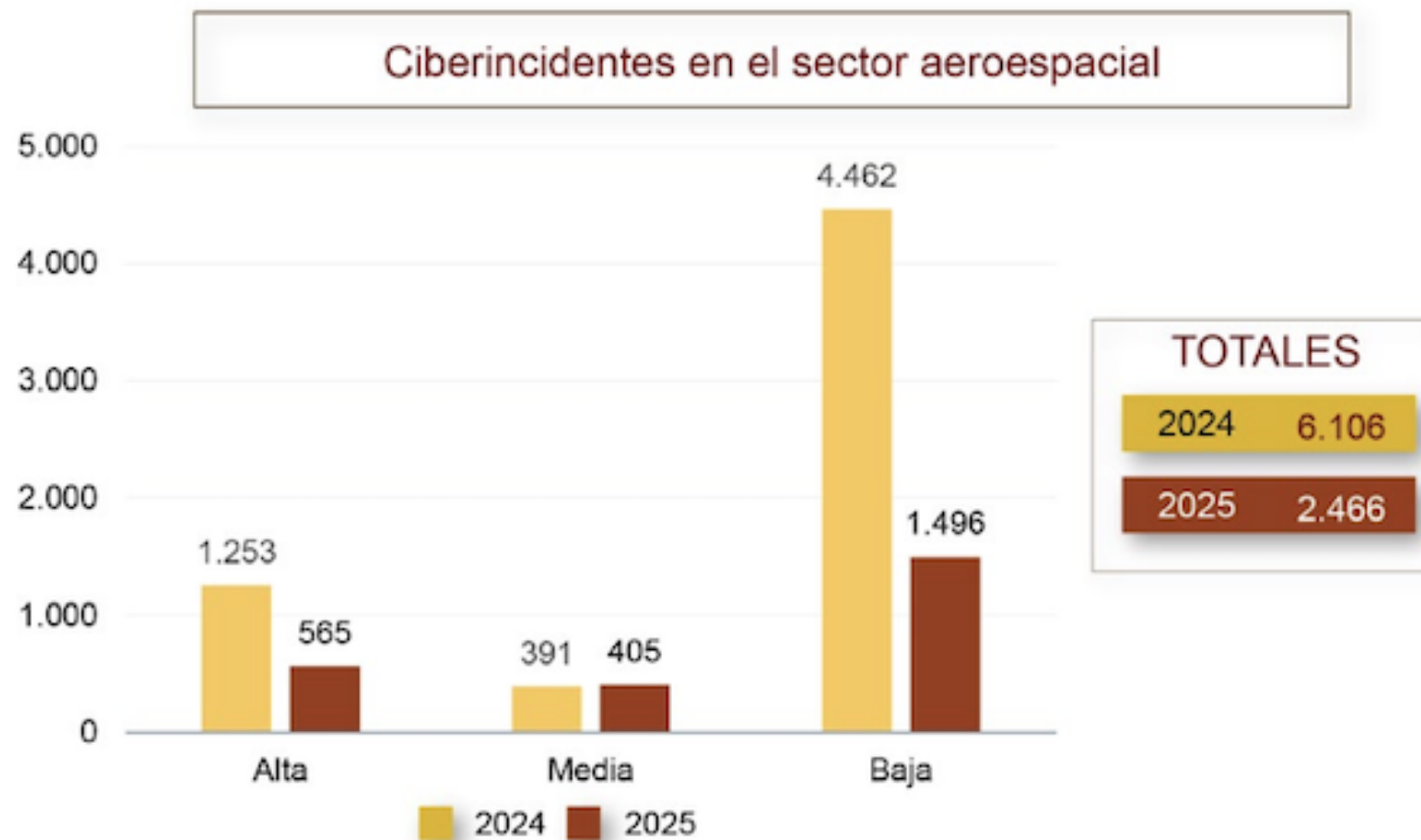
HECHOS CONOCIDOS	2019	2020	2021	2022	2023	2024	2025
ACCESO E INTERCEPTACIÓN ILÍCITA	4.004	4.653	5.342	5.578	7.367	9.773	13.753
AMENAZAS Y COACCIONES	12.782	14.066	17.319	15.982	17.472	17.738	18.194
CONTRA EL HONOR	1.422	1.550	1.426	1.191	1.174	1.128	1.173
CONTRA LA PROPIEDAD INDUSTRIAL/INTELLECTUAL	197	125	137	114	117	227	145
DELITOS SEXUALES	1.774	1.783	1.628	1.646	1.804	1.676	2.031
FALSIFICACIÓN INFORMÁTICA	4.275	6.289	10.476	12.569	15.137	19.492	21.690
FRAUDE INFORMÁTICO	192.375	257.907	267.011	335.995	427.448	412.850	429.681
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	1.437	1.590	2.138	1.662	1.741	1.917	1.763
TOTAL HECHOS CONOCIDOS	218.302	287.963	305.477	374.737	472.260	464.801	488.430



Fuente: Sistema Estadístico de Criminalidad

Figura 8.14: Evolución de hechos conocidos por categorías delictivas





Fuente: Agencia Espacial Española

Figura 10.5: Ciberincidentes en el sector aeroespacial

Cibercriminalidad



UNIVERSIDAD DE MURCIA



Facultad de Turismo y Relaciones Internacionales

redseguridad

Las estafas informáticas lideran la cibercriminalidad en España

Las estafas informáticas lideran la cibercriminalidad en España. En 2022 las estafas informáticas representaron la mitad anual de los delitos informáticos, mientras que en 2021 lo hizo con el 35,7%. Se han registrado un total de 10.500 delitos de estafa, con un importe de 10,5 millones de euros. Los delitos de estafa informática han crecido un 75% en 2022, se han producido un incremento del 13,8 por ciento.

Estafas informáticas

En 2022 las estafas informáticas representaron la mitad anual de los delitos informáticos, mientras que en 2021 lo hizo con el 35,7%. Se han registrado un total de 10.500 delitos de estafa, con un importe de 10,5 millones de euros. Los delitos de estafa informática han crecido un 75% en 2022, se han producido un incremento del 13,8 por ciento.

Región | Murcia | Cartagena | Lorca | Molina | Alcantarilla | Mazarrón | Águilas | Yecla | Totana

Las denuncias por 'ciberestafas' se disparan un 75% con la pandemia

Casi 6.000 murcianos se vieron afectados el pasado año por delitos cometidos a través de la Red y la cifra se cuadruplica en un lustro

Los agentes Eloy Sevilla e Iñaki Sánchez, en la sede del equipo Andia en Murcia. / NACHO GARCÍA / AGF

ALICIA NEGRE

Selección: **ESPAÑA** | **SUSCRIBIRSE** | INICIAR SESIÓN

EL PAÍS

Tecnología | TECNOLOGÍA | CIBERSEGURIDAD | PRIVACIDAD | INTELIGENCIA ARTIFICIAL | INTERNET | GRANDES TECNOLOGÍAS | ÚLTIMAS NOTICIAS

SEGURIDAD EN INTERNET

El cibercrimen alcanza niveles inéditos: 90 millones de ataques anuales que cuestan 10,5 billones de euros

Uno de cada cinco delitos en España se comete en la red, que generará 150.000 denuncias en 2025

RÚCER LINÓN
20 JUN 2023 - 09:20 CEST

Cada ordenador, móvil, router, vehículo o electrodoméstico conectado es un ciberdelincuente. "Todos tenemos algo que le interesa a un ciberdelincuente", afirma Luis Hidalgo, del Instituto Nacional de Ciberseguridad (Incipe). Esta mina individual, empresarial e institucional de dimensiones gigantescas es el objetivo del piratería informática, que han alcanzado niveles inéditos no solo por cantidad, sino también por sofisticación. "Cada día se registran 90 millones de ciberataques en el mundo [más de un millón por segundo] que suponen un coste de 10,5 billones de euros (10 billones en el sistema contable de EE.UU.)".

Tu dinero en libertad:

- ✓ Sin comisiones de ningún tipo.
- ✓ Abono trimestral de intereses.
- ✓ Para todos los niveles de inversión.
- ✓ Rendimiento anual de hasta 10,50%.
- ✓ Rendimiento anual de hasta 10,50%.
- ✓ Rendimiento anual de hasta 10,50%.

EL MUNDO | ESPAÑA | OPINIÓN | ECONOMÍA | INTERNACIONAL | DEPORTES | CULTURA | LOG | TELEVISIÓN | MENÚ

España | Madrid | Andalucía | Baleares | Castilla y León | Cataluña | Comunidad Valenciana

CATALUÑA

El Parlamento Europeo constata que Rusia interfirió en Cataluña

Un informe de la comisión creada para analizar la injerencia extranjera en la Unión Europea pide que se investiguen estas conexiones con Moscú

Josep Lluís Alay y Carlos Puigdemont, en una rueda de prensa en Berlín en 2019. Felipe Traveira (7)

Cataluña (E) amigo ruso del círculo de Puigdemont confirma que Alay fue a Moscú a "traerle su mensaje"

Procede la investigación de la injerencia rusa en el proceso independentista catalán ha entrado en la agenda del Parlamento Europeo como una preocupante evidencia, en paralelo a las nuevas revelaciones periodísticas y las investigaciones de los servicios secretos occidentales sobre la estrategia de «guerras híbridas» impulsada por Moscú para desestabilizar las democracias.

ABC Tecnología

NUEVO E-2008
100% ELÉCTRICO

Guerra Israelí llamas Los rebeldes yemeníes anuncian el secuestro de un buque de carga israelí en

→ ABC → Tecnología

Félix Barrio, director del Incibe: «Las mafias ofrecen dinero a trabajadores descontentos para que faciliten ciberataques»

La IA, la conectividad 5G y el cibercrimen organizado van a dar muchos problemas en 2024, según el jefe del Instituto Nacional de Ciberseguridad

Los auditores internos alertan: «Las empresas tenemos ciberataques todos los días»

La UE prohíbe a Facebook e Instagram utilizar los datos de los usuarios para mostrarles anuncios

Pues no hemos acabado aquí

El nuevo reto de la inteligencia artificial. (1)



El nuevo reto de la inteligencia artificial. (2)



Acronis Cyberthreats Report 2022. Available at <https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Threats-Report-2022-EN-US.pdf>

El Confidencial

Últimas noticias

España Cotizalia Opinión Salud Internacional Cultura Teknautas Deportes ACyV Televisión Vanitatis

VER MÁS

Tecnología

¿HACIA DÓNDE VA TODO ESTO?

Tres años tras su boom, los 'padres' de la IA siguen diciendo que la humanidad está en peligro

Los investigadores que dieron vida a los primeros sistemas de inteligencia artificial discrepan sobre el uso que se les está dando por parte de las tecnológicas. Dos de ellos tienen una visión muy pesimista de lo que viene

Los tres investigadores galardonados con el premio Turing: Yoshua Bengio, Geoffrey Hinton y Yann LeCun. (Archivo)

Por Albert Sanchis
12/10/2025 - 05:00

EC EXCLUSIVO

Geoffrey Hinton se levanta cada mañana con una sensación extraña. Hace una década, su nombre aparecía en titulares por haber dado

Elige Self Bank para tus ETFs
0€ comisión de custodia
si operas desde la Cuenta

https://www.elconfidencial.com/tecnologia/2025-10-12/hinton-bengio-lecun-padres-ia-humanidad-peligro-seguridad_4225416/

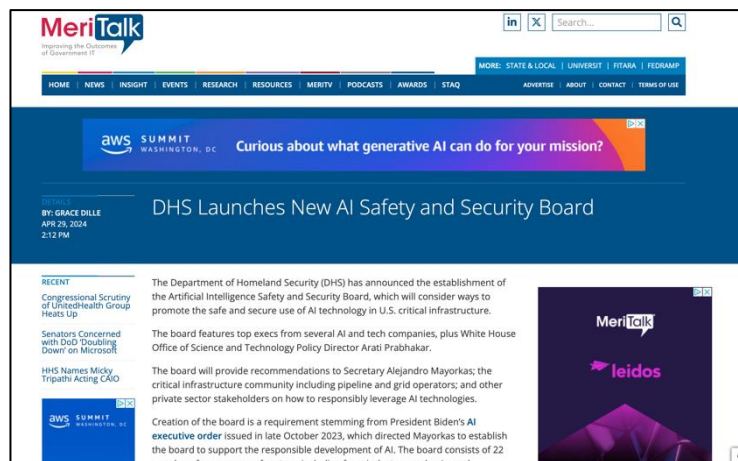
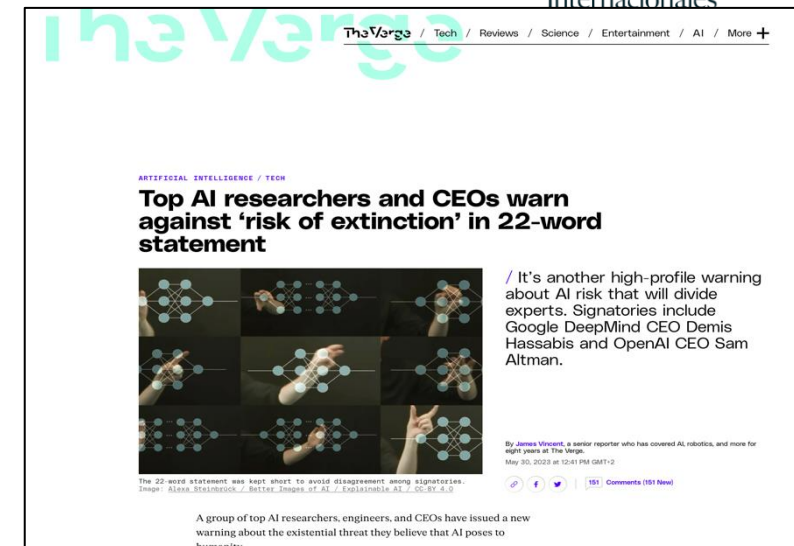
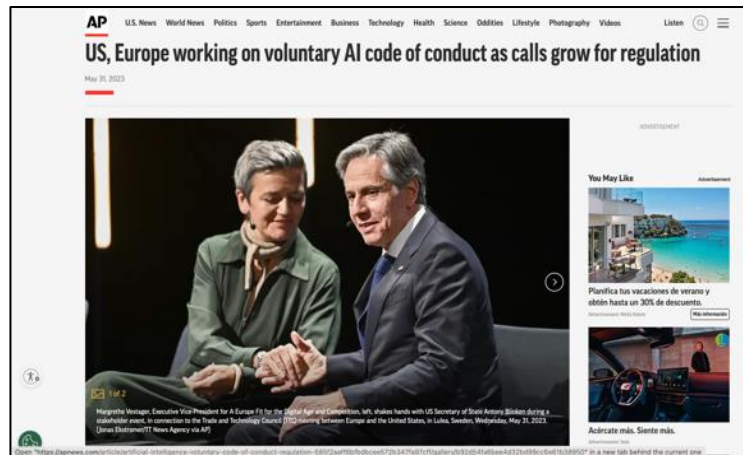
El nuevo reto de la inteligencia artificial. (3)



UNIVERSIDAD DE MURCIA



Facultad de Turismo y Relaciones Internacionales



<https://apnews.com/article/artificial-intelligence-voluntary-code-of-conduct-regulation-585f2aaf6bfbdbcee572b347fa97cfff>



<https://www.commerce.gov/news/press-releases/2024/02/biden-harris-administration-announces-first-ever-consortium-dedicated>

<https://elpais.com/tecnologia/2023-10-30/biden-recurre-a-una-ley-de-tiempos-de-guerra-para-regular-la-inteligencia-artificial-la-tecnologia-debe-ser-gobernada.html>



<https://www.lavanguardia.com/ciencia/20241008/10004294/nobel-fisica.html>

LA VANGUARDIA

Sociedad

ANG / TECNOLOGÍA / SALUD / QUÉ ESTUDIAR / UNIVERSO JR / FORMACIÓN / VIVO SEGURO / TODOS SOLIDARIOS / VIVO / CATALUNYA RELIGIÓ

UNA NORMA PIONERA

La ley de IA europea abre una era

V+

- El Parlamento ha aprobado un texto de plena aplicación en el 2026



El comisario de mercado interior de la Unión Europea, Thierry Breton, se felicitó ayer por la previsible aprobación hoy de la pionera ley de inteligencia artificial (RONALD WITTEK / EFE)

 **Francesc Bracero**
Barcelona

13/03/2024 06:00 | Actualizado a
14/03/2024 17:00

f b t p c

success@uvm



Hong Kong's public broadcaster, RTHK, [reported that the employee was a clerk working for an unnamed multinational firm](#). It quoted acting senior superintendent Baron Chan as speculating that the fraudster used artificial intelligence to dupe the worker.

"[The fraudster] invited the informant [clerk] to a video conference that would have many participants. Because the people in the video conference looked like the real people, the informant ... made 15 transactions as instructed to five local bank accounts, which came to a total of HK\$200m," he said.

Support the Guardian

Fund independent journalism with €12 per month

Support us →

Print subscriptions

Search jobs

Sign in

Eur ▾

News

Opinion

Sport

Culture

Lifestyle



The Guardian

World Europe US news Americas Asia Australia Middle East Africa Inequality Global development

Hong Kong

This article is more than 1 year old

Company worker in Hong Kong pays out £20m in deepfake video call scam

Police investigate after employee says she was tricked into sending money to fraudsters posing as senior officers at her firm

Dan Milmo

Mon 5 Feb 2024 17:46 CET

Share



Police said the woman made 15 transactions to banks accounts totalling HK\$200m. Photograph: Blend Images/Alamy

Hong Kong police have launched an investigation after an employee at an

Advertisement

STANLEY
Engineered Fastening

Built-To-Last
Fastening System
for
Torque Tube Assembly



AVBOLT® 8M
BLC40PB-3

Xanthorox: IA criminal



SCI
AM

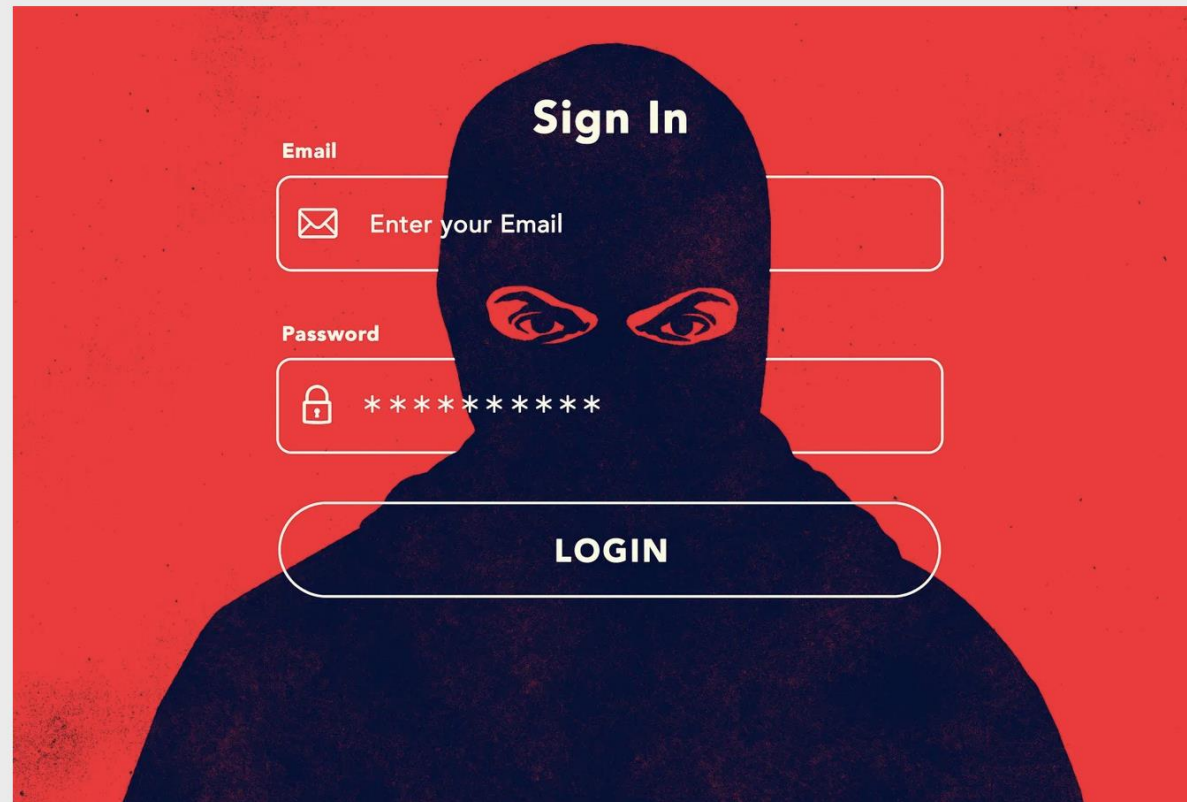
Special Offer: \$1 for 90 days

MAY 7, 2025 | 9 MIN READ

Criminal AI is Here—And Anyone Can Subscribe

A new AI platform called Xanthorox markets itself as a tool for cybercrime, but its real danger may lie in how easily such systems can be built—and sold—by anyone

BY DENI ELLIS BÉCHARD EDITED BY DEAN VISSER



● **GUERRA ARANCELARIA** ▶ Trump confirma los aranceles del 50% a Europa a partir del 1 de junio

● **ORIGEN DEL APAGÓN** ▶ 'The Telegraph' asegura que el apagón eléctrico fue por un "experimento" del Gobierno con las renovables y Moncloa lo desmiente

Economía Vivienda Empleo

Estafas/

Instagram, Whatsapp y Facebook se convierten en la principal puerta de estafas: el 70% de los nuevos anunciantes engañan

Meta ha afirmado que está desbordada y no logra detener la "epidemia de estafas", según 'The Wall Street Journal'.



Imagen de archivo de Meta AI y de WhatsApp. | Europa Press

Cultura ■



Por Israel Merino

Ahora, también nos geolocalizamos: Instagram apuesta por controlarnos y nosotros estamos de acuerdo

Las aplicaciones de rastreo de la ubicación triunfan entre los jóvenes por lo mismo que la ultraderecha: la sensación de control



Fotograma de un episodio de Blackmirror. (HBO)

Por Israel Merino

12/10/2025 - 05:00



EC EXCLUSIVO

Es curioso: hace cuatro meses, en una cena con algunos amigos más mayores, empezamos a hablar de la función de geolocalización del iPhone, un extra del terminal de Apple que permite compartir con quien quieras tu ubicación en tiempo real, como si llevaras un **transmisor GPS** postsoviético pegado en los bajos del coche – existen funcionalidades parecidas para el resto de móviles de otras marcas, **aunque no igual de efectivas y precisas** –.

Comentando sobre el tema, varios amigos mayores se escandalizaron por el uso que los más jóvenes hacíamos del invento; para nosotros, lo veo casi a diario en otros amigos de mi edad, es relativamente normal compartir nuestra ubicación; es parte de **nuestra identidad digital**, nunca lo apagamos, lo tenemos siempre encendido para que otros amigos lo vean y nosotros mismos nos metamos en la de otros amigos por puro cotilleo: en



[https://urldefense.com/v3/https://www.elconfidencial.com/cultura/2025-10-12/ahora-tambien-nos-geolocalizamos-instagram-apuesta-por-controlarnos-y-nosotros-estamos-de-acuerdo_4225903/__;!!D9dNQwwGXtA!R4uidjOMITcV08zJAMsFxMFFUedu71pa6440NwOj0kNVEig76LajkrYUuSntW43FD9igQY78YmYspHbgM37H5pY\\$](https://urldefense.com/v3/https://www.elconfidencial.com/cultura/2025-10-12/ahora-tambien-nos-geolocalizamos-instagram-apuesta-por-controlarnos-y-nosotros-estamos-de-acuerdo_4225903/__;!!D9dNQwwGXtA!R4uidjOMITcV08zJAMsFxMFFUedu71pa6440NwOj0kNVEig76LajkrYUuSntW43FD9igQY78YmYspHbgM37H5pY$)



UNIVERSIDAD DE MURCIA



Facultad de Turismo y Relaciones Internacionales

Inteligencia artificial y ‘seudonimato’: el Gobierno presenta la primera versión de la Carta de Derechos Digitales



La Secretaría de Estado abre el documento a consulta pública para que los ciudadanos pueda realizar aportaciones que se tendrán en cuenta en la redacción final del texto:

- **Derecho al *seudonimato*.**
- **Derecho a no ser localizado y *perfilado*.**
- **Derecho a la herencia digital.**
- **Protección de menores en el entorno digital.**
- **Derecho a la neutralidad de Internet.**
- **Libertad de expresión y libertad de información.**
- **Derechos en el ámbito laboral.**
- **Derechos ante la Inteligencia artificial.**
- **Derechos en el empleo de las neurotecnologías.**



El nuevo reto del “ámbito/dominio cognitivo”. 1



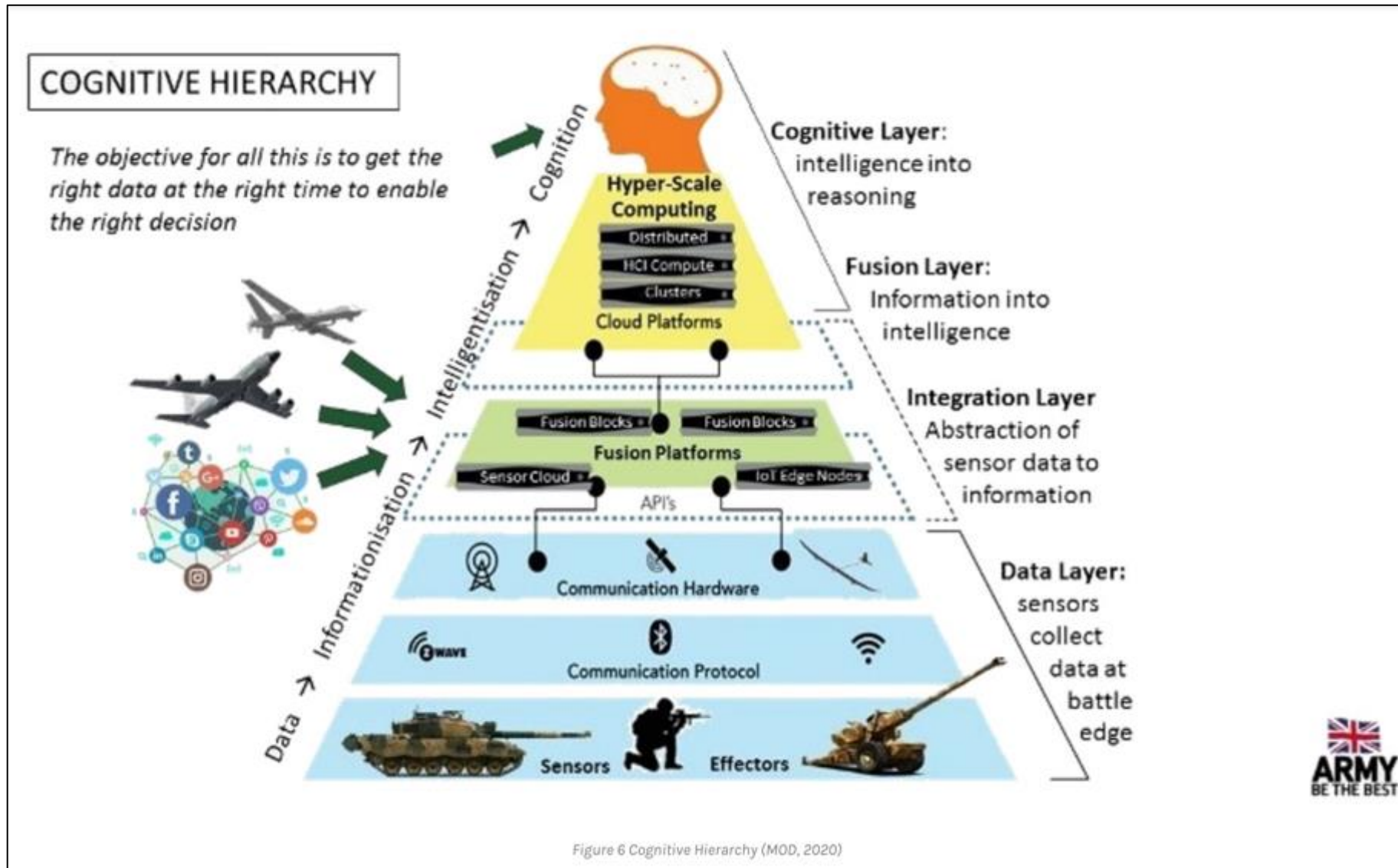
- **La in/desinformación siempre ha jugado un papel esencial en los conflictos: la verdad, "primera víctima" de un conflicto.**
- **Operaciones de Información: Guerra psicológica *Psyops*.**
- **El advenimiento de los avances tecnológicos ha potenciado su uso.**
- **“Dominio” (“*Domain*”): permite a las FAS operar en él y lograr objetivos estratégicos.**
- **5 Dominios “tradicionales” de las FAS: Terrestre, Marítimo, Aéreo, Ciberespacio (Varsovia, julio 2016), Espacio Exterior (OTAN, 2019).**

El nuevo reto del “ámbito/dominio cognitivo”. 2

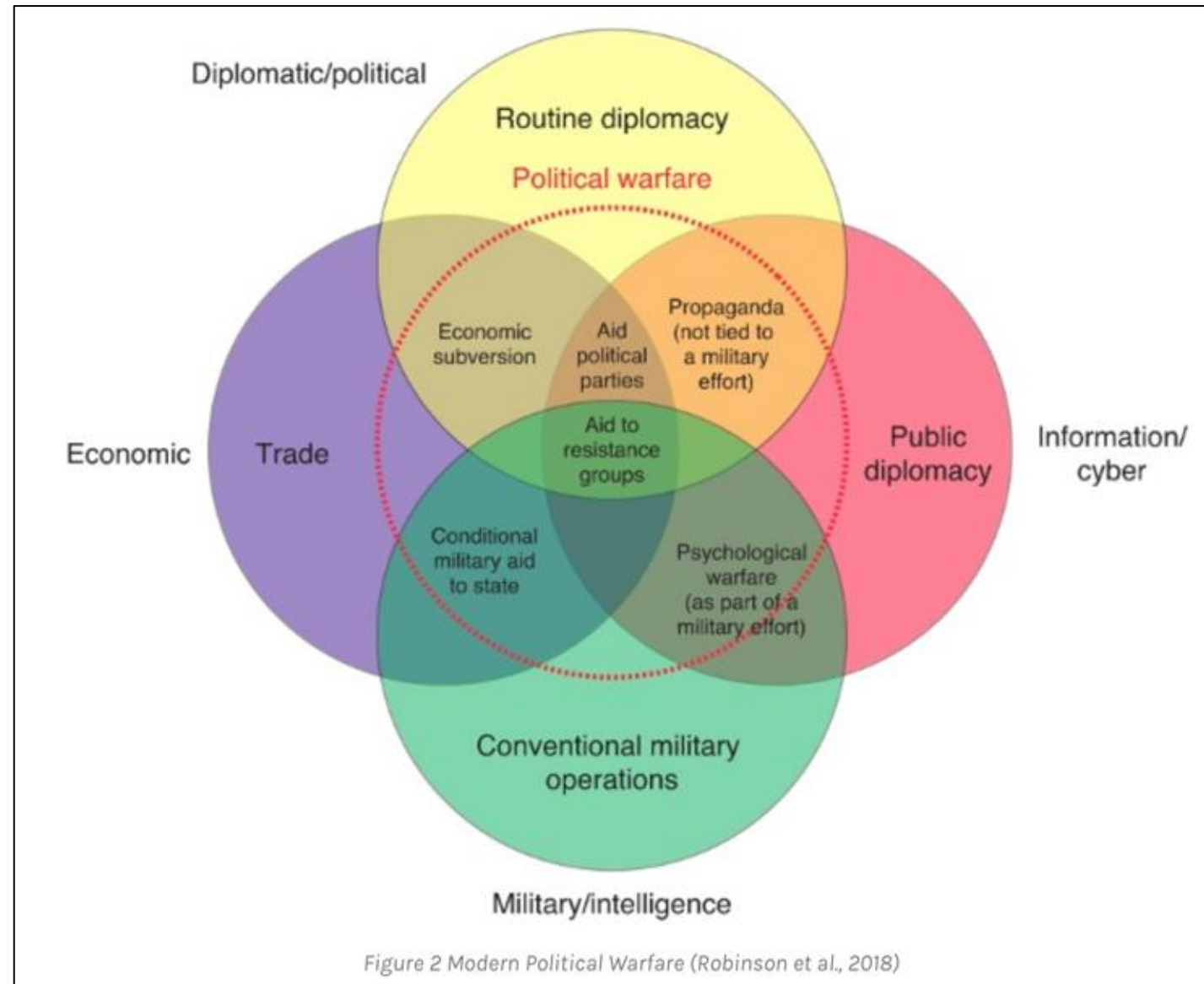


- **El sexto, Dominio Cognitivo:**
- **“Aquel que incluye las percepciones, creencias, comportamientos y toma de decisiones de los seres humanos, y la influencia externa que se puede ejercer sobre estos aspectos para modificarlos”.**
- **Gestionar la información para INFLUIR en la población, como individuos y como sociedad, indispensables para el apoyo moral y logístico.**
- **Características del ciberespacio:**
 - **Dificultad de atribución.**
 - **Asimetría.**
- **La batalla de las “narrativas”: ganar las mentes y los corazones.**
- **Diferencia entre Estados democráticos y “autocráticos”.**
- **Credibilidad y superioridad ética de los países democráticos (?): Informar correctamente.**
- **Operaciones “multidominio”: interacción entre todos ellos, NO aisladamente.**

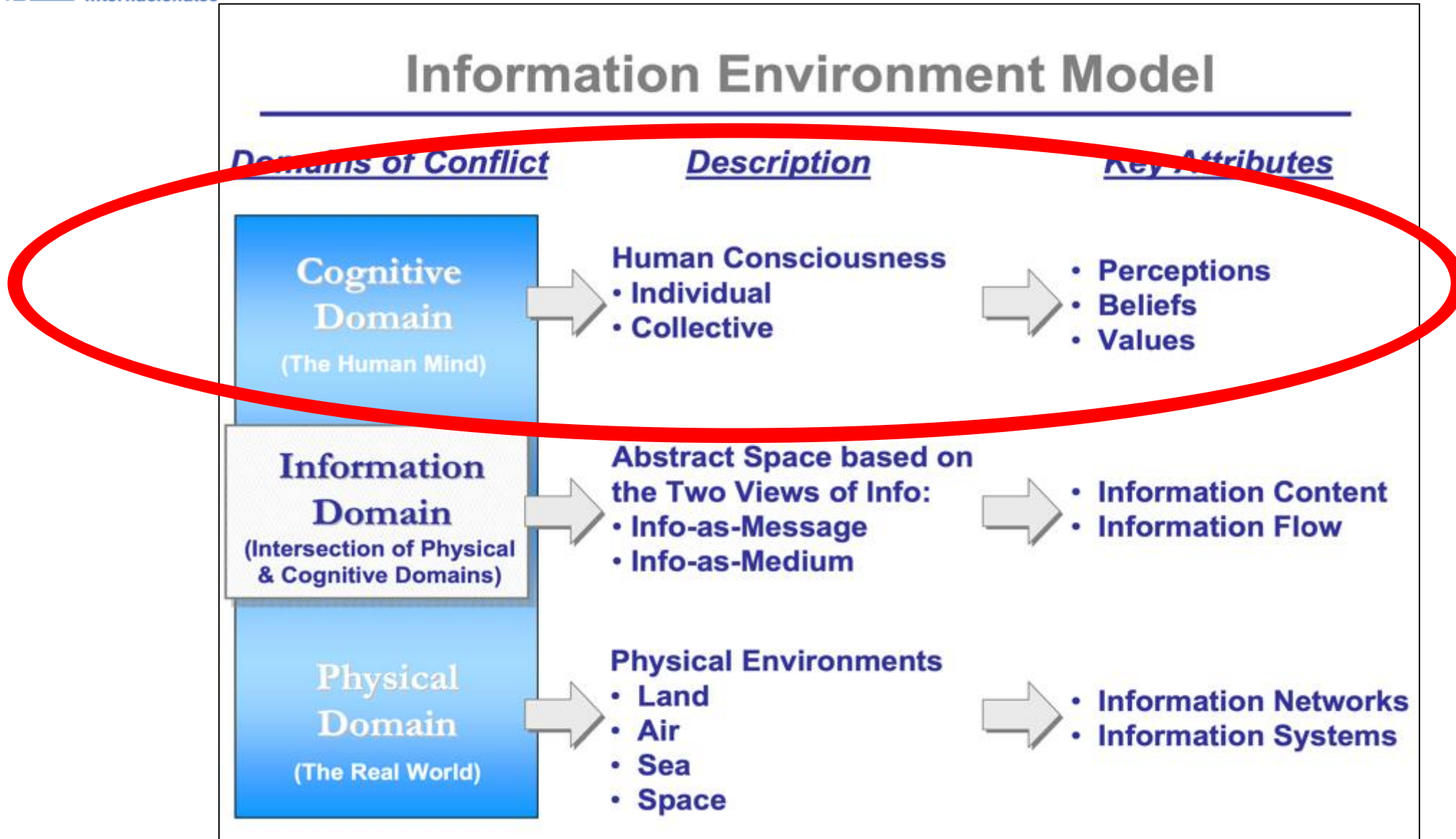
El nuevo reto del “ámbito/dominio cognitivo”. 3



El nuevo reto del “ámbito/dominio cognitivo”. 4



El nuevo reto del “ámbito/dominio cognitivo”. 5



El nuevo reto del “ámbito/dominio cognitivo”. 6

<u>Layers of Warfare</u>	<u>Domains of Warfare (Trans-domain regions)</u>	<u>Multi-Domain Operation Constructs</u>
Physical	Land	Special Operations
Electromagnetic	Maritime (Littorals)	Cyber Operations
Information	Air (Close Air)	Intelligence Operations
Cognitive	Space (Orbital Space)	Global Logistics and Mobility Operations

Figure 5 Proposed Typology of Warfare (Kreuzer, 2021)

El nuevo reto del “ámbito/dominio cognitivo”. 7



Evolución y respuestas*



*Dionisio Urteaga Todó (2024). “La respuesta a la guerra cognitiva” (pp. 158). En *Desinformación y Defensa*. Dykinson S. L. Madrid.

Estrategia de Inteligencia Artificial 14.05.2024

Está estructurada en 3 ejes que activarán 8 palancas de acción:

- 1. Eje 1: Refuerzo de las capacidades para el desarrollo de la IA.**
- 2. Eje 2: Facilitar la aplicación de la IA en el sector público y privado.**
- 3. Eje 3: Fomentar una IA transparente, ética y humanística.**

Seguimiento y modelo de gobernanza: Esta Estrategia y sus iniciativas serán coordinadas por la Secretaría de Estado de Digitalización e Inteligencia Artificial.

¿Cuál es el eslabón débil de la cadena?



¿Cuál es el eslabón débil de la cadena?



Ángel Gómez de Ágreda

MUNDO ORWELL



MANUAL DE
SUPERVIVENCIA
PARA UN MUNDO
HIPERCONECTADO

Ariel



Índice



- 1. Introducción y definiciones.**
- 2. Algunos ejemplos de actos en el ciberespacio.**
- 3. Estrategia de Seguridad Nacional 2017: *Global commons*.**
- 4. Informe sobre las amenazas en la red y sus efectos.**
- 5. Operaciones en el ciberespacio. La amenaza “híbrida”.**
- 6. La UE y la OTAN.**
- 7. La posición de España. La Estrategia Nacional de Ciberseguridad.**
- 8. Estudio sobre cibercriminalidad en España.**
- 9. El dominio “cognitivo.**
- 10. Conclusiones.**



**“Disfrutamos de inmediatez, gratuidad y
comodidad, pero comprometiendo nuestra
Libertad, seguridad y dignidad”**

Conclusiones



Vuestra tarea para el próximo día

Fin del Tema 5, el Ciberespacio

