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 Nº 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://wavellroom.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 QUINTOCONIO DISTANCIAL BLUE KSÍ PARA INTERNET?
ESO YA ES ANTIGUO, CABALLERO
¿ANTIGUO? PERO SI AYER LEÍ QUE...
AYER, CABALLERO, AYER


You are here
Map of the Internet. The Opte Project, www.opte.org

¿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

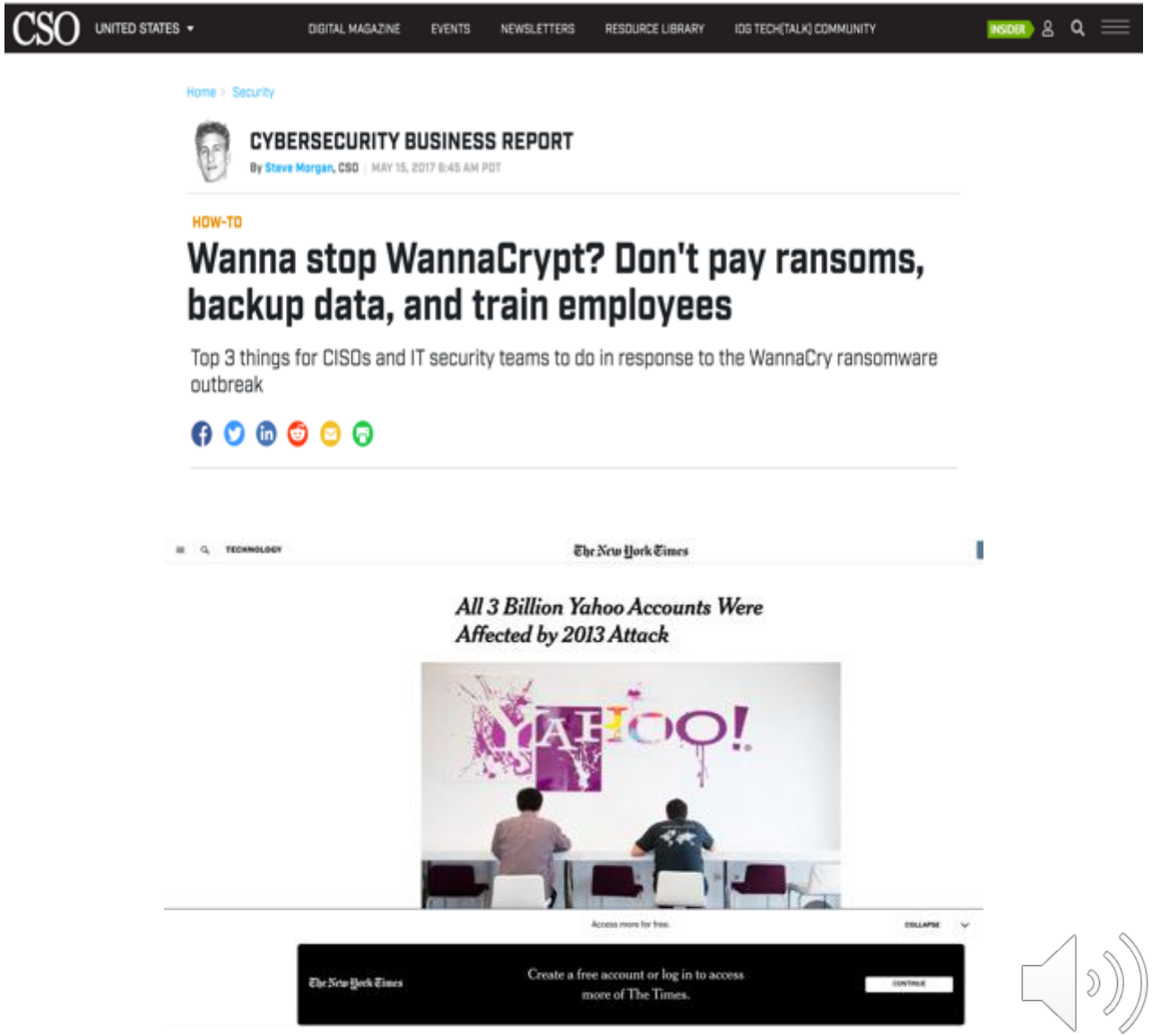
Amenazas en y desde el Ciberespacio

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

- Phishing
- Ramsomware
- Rootkit
- Scareware
- Smishing
- Spam
- Spoofing
- Spyware
- Troyano
- Virus
- Web bug
- Zombie

- Infodemia
- Misinformation
- Disinformation
- Malinformation

Efectos de usos no deseados del ciberespacio (1)



Efectos de usos no deseados del ciberespacio (2)

https://cybermap.kaspersky.com/

Centro Universitario THE OPEN FACULTY Turismo y Relaciones Internacionales

UNIVERSIDAD DE MURCIA

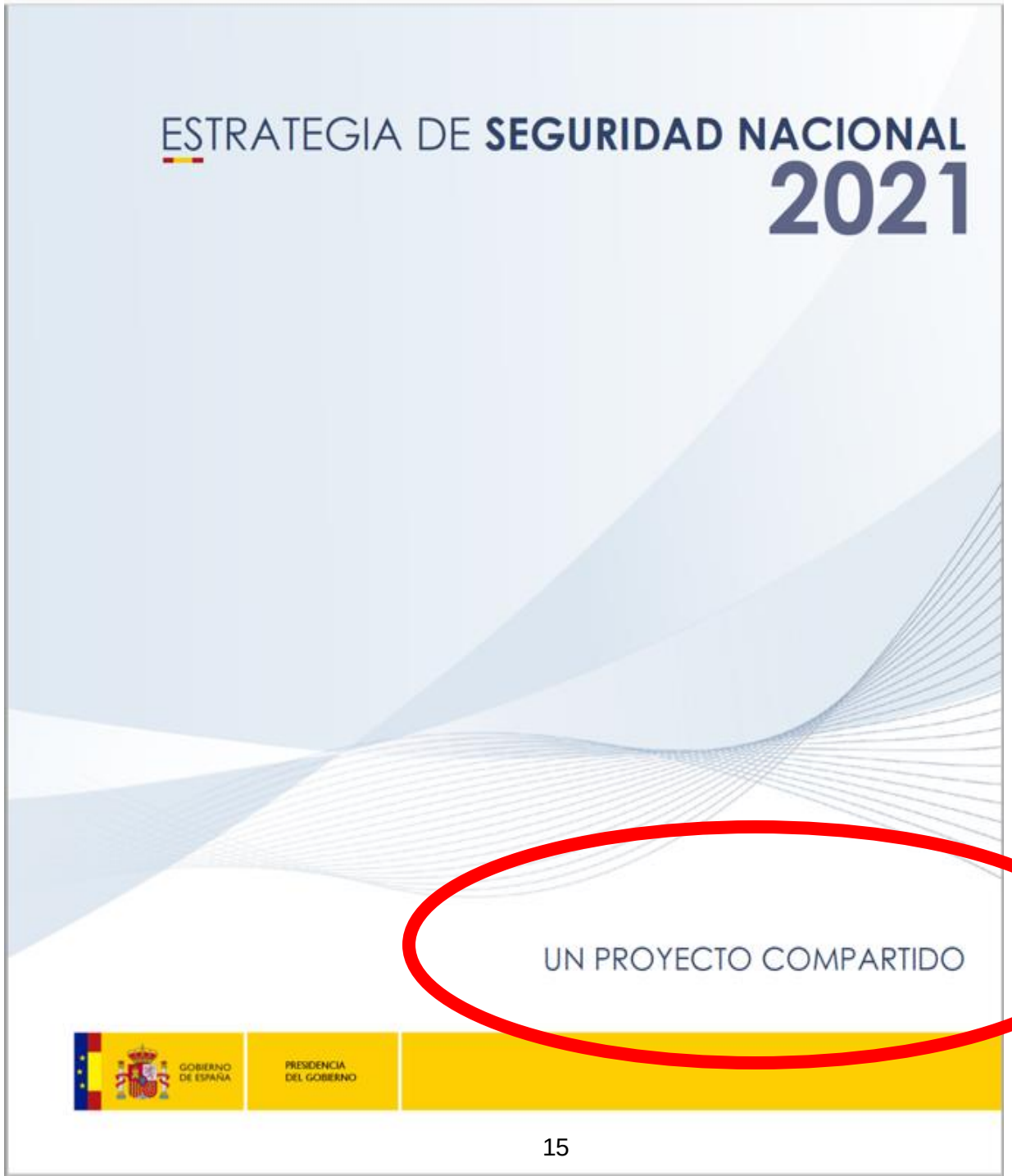
Facultad de Turismo y Relaciones Internacionales

ESTRATEGIA DE **SEGURIDAD NACIONAL**

2017

UN PROYECTO COMPARTIDO
DE TODOS Y PARA TODOS

GOBIERNO DE ESPAÑA
PRESIDENCIA DEL GOBIERNO


ESTRATEGIA DE SEGURIDAD NACIONAL
2021
UN PROYECTO COMPARTIDO
GOBIERNO DE ESPAÑA
PRESIDENCIA DEL GOBIERNO

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.

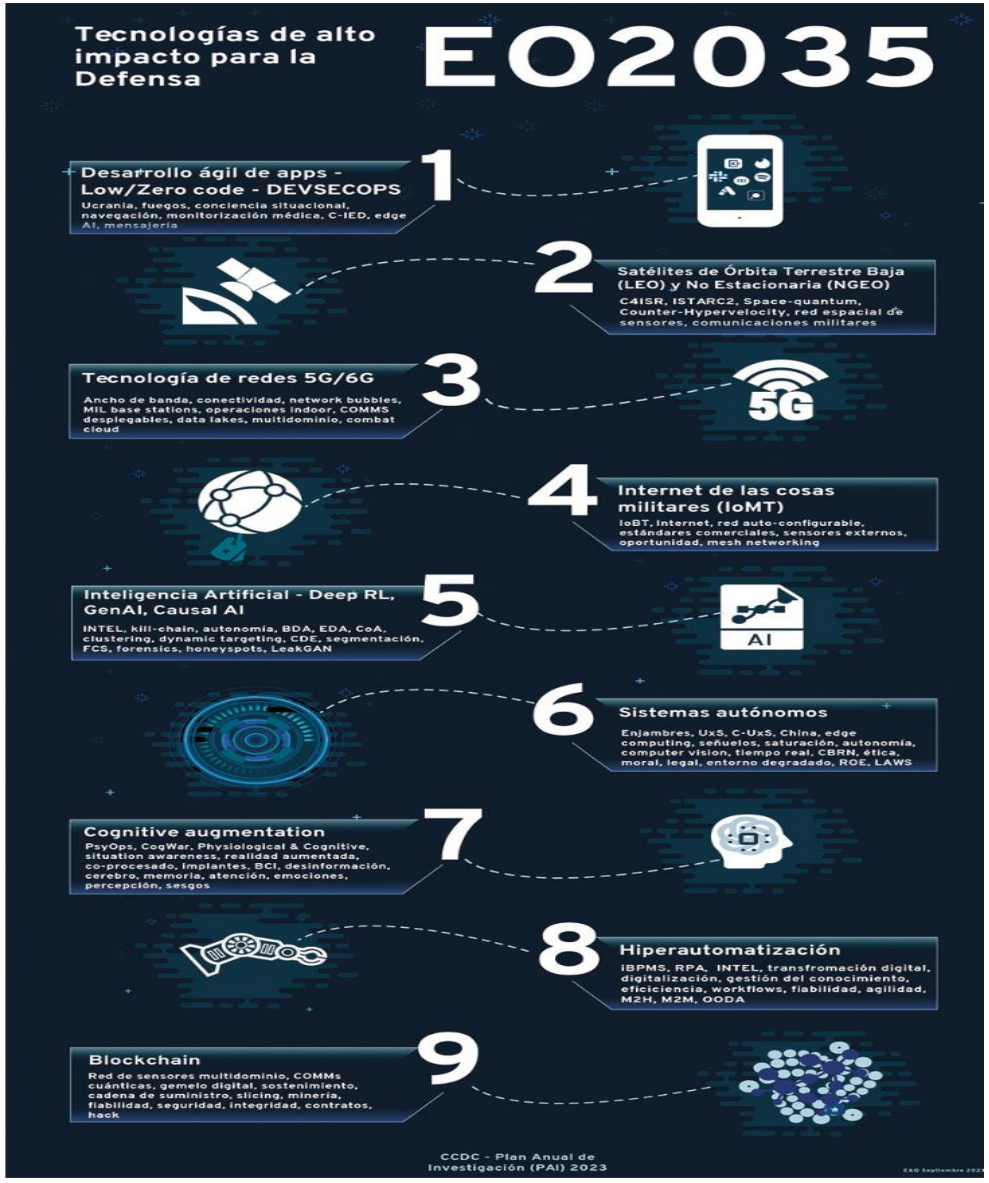
Por otro lado, la vulnerabilidad ante posibles injerencias de terceros es extensible al dominio de infraestructuras digitales, como los centros de procesamiento de datos o los cables submarinos, y a los activos que sustentan la propiedad intelectual e industrial del sector empresarial. También habrá 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 Annual de Investigación. Tecnologías de alto impacto para la defensa en el entorno operativo 2035. 2023

Secretaría General Técnica.
MINISDEF



https://publicaciones.defensa.gob.es/media/downloadable/files/links/t/e/tecnolog_as_de_alto_impacto_.pdf

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

Ciberespacio

Espacio marítimo

Espacio aéreo y ultraterrestre

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

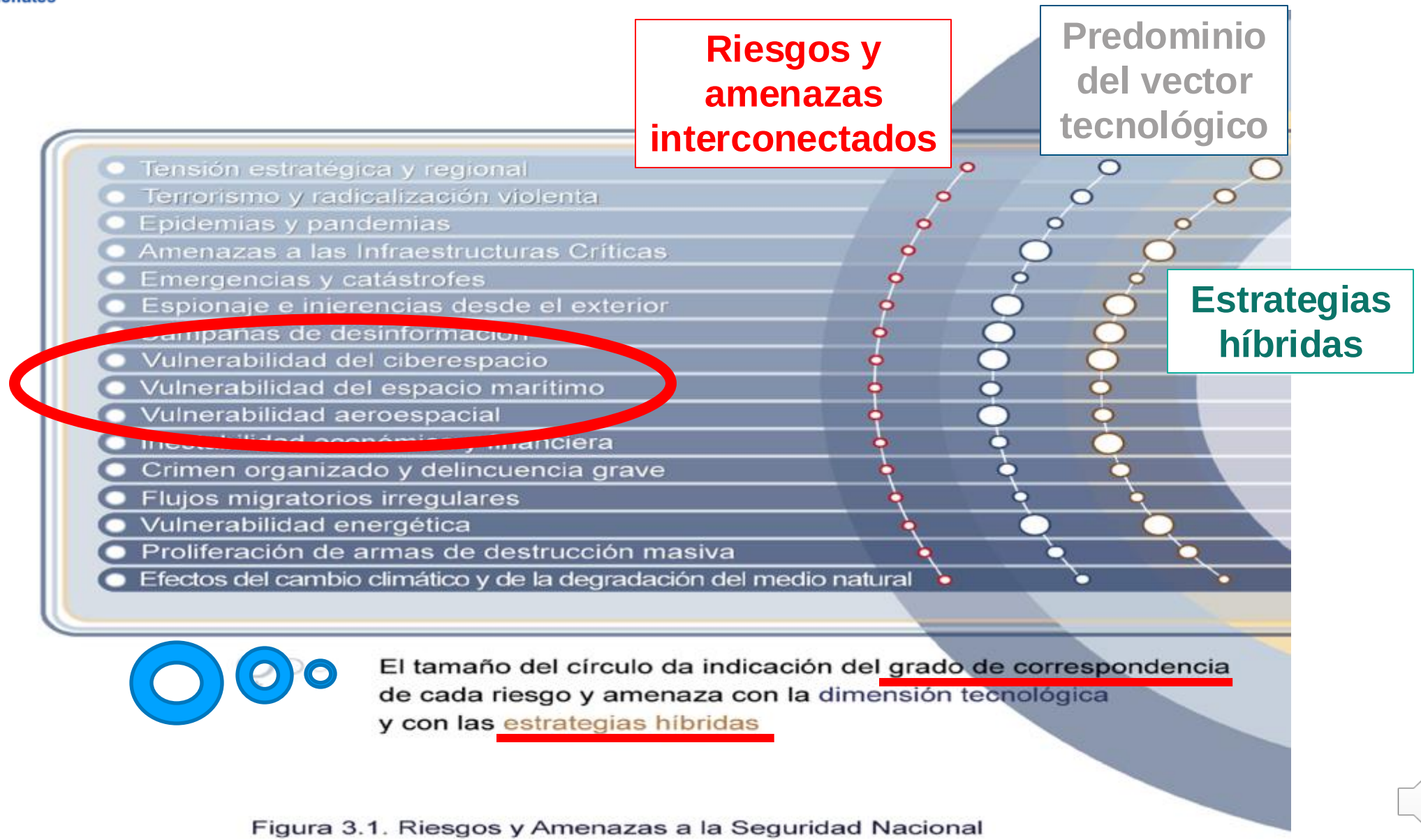


Figura 3.1. Riesgos y Amenazas a la Seguridad Nacional

Amenazas a infraestructuras críticas. Protección

Centro Universitario THE OPEN FACULTY Turismo y Relaciones Internacionales

UNIVERSIDAD DE MURCIA

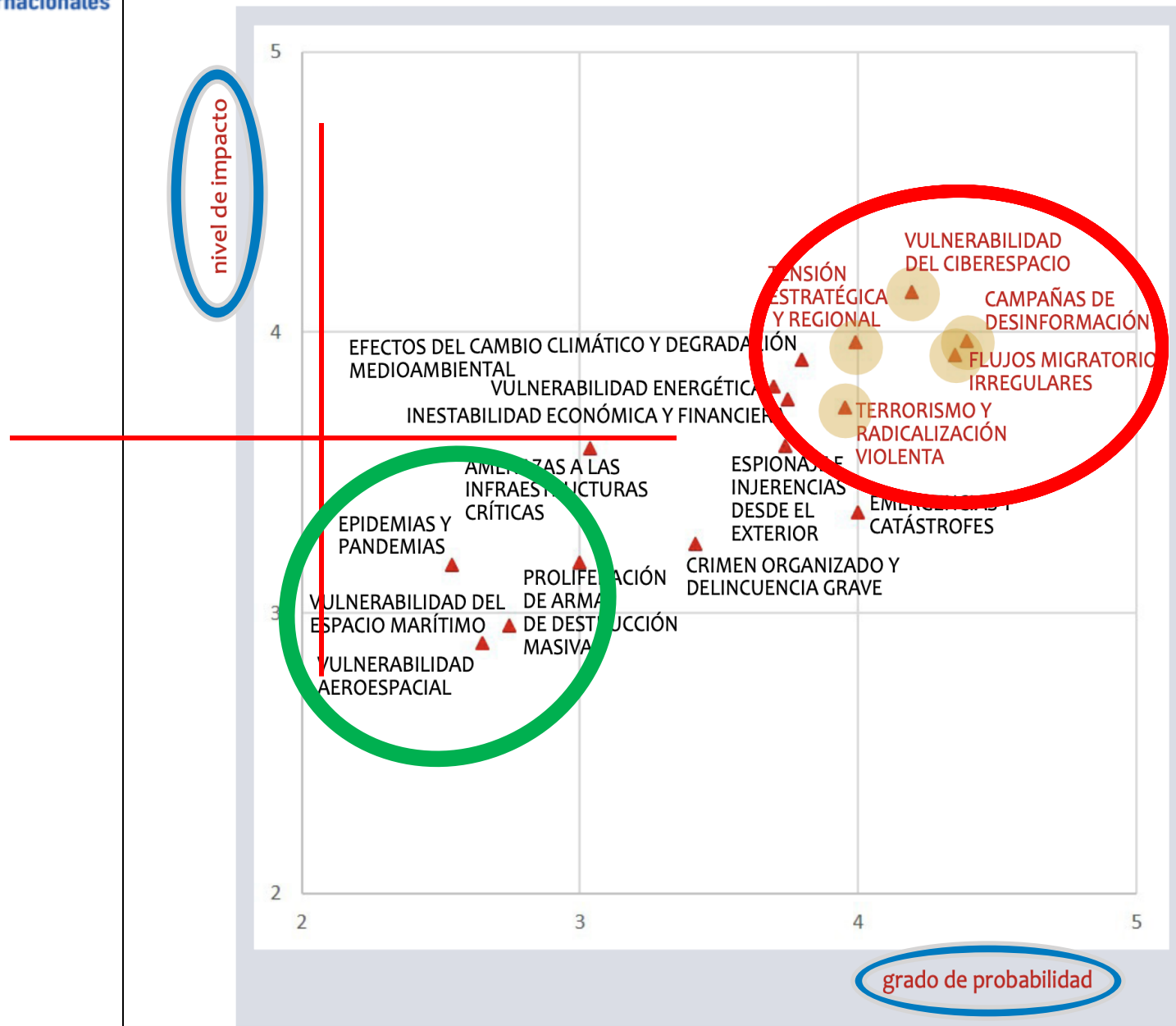
Facultad de Turismo y Relaciones Internacionales

Informe Anual de Seguridad Nacional

2023

GOBIERNO DE ESPAÑA PRESIDENCIA DEL GOBIERNO

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



Cuantificación del riesgo

	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

Percepción de riesgos a 5 años

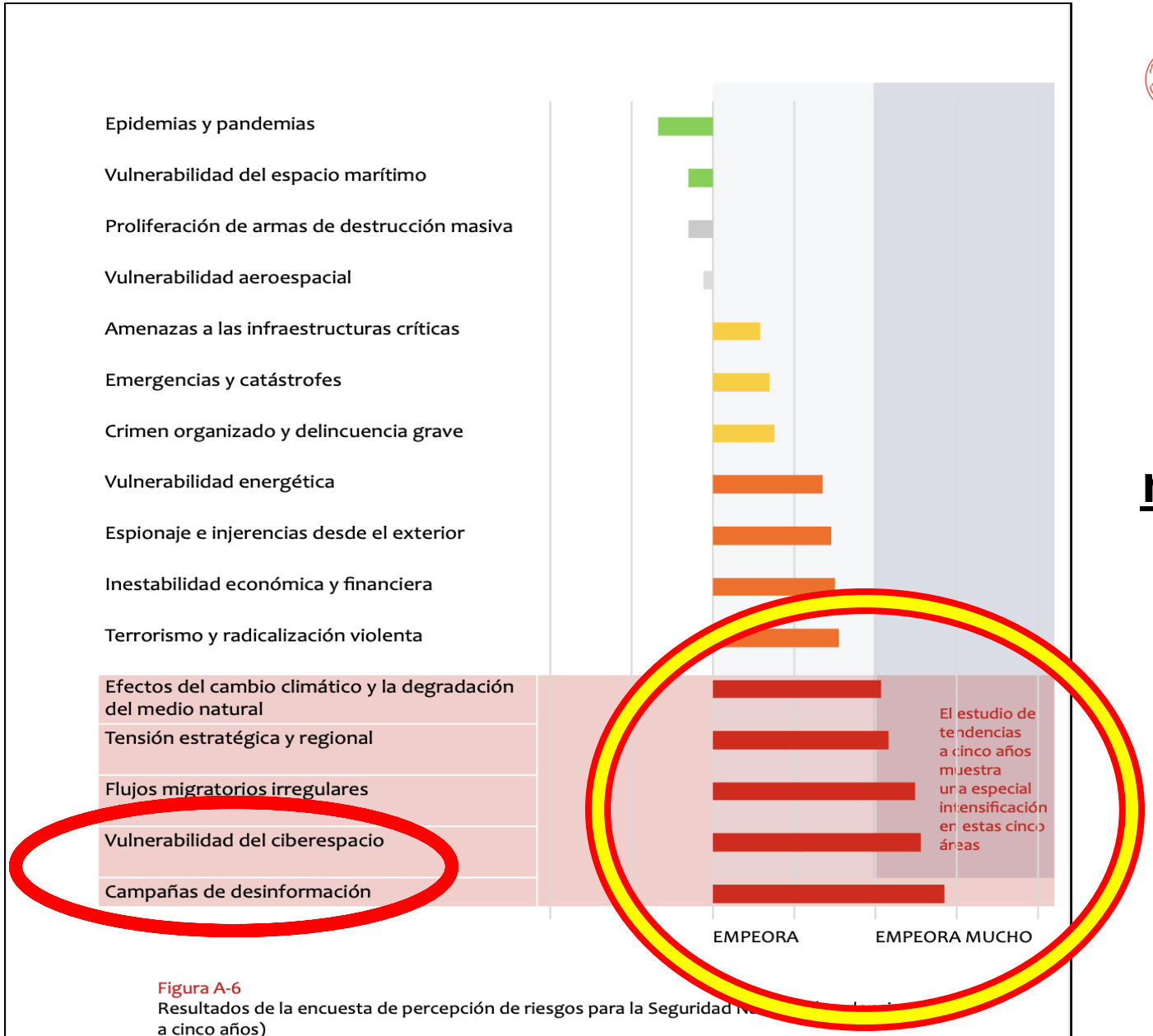


Figura A-6
Resultados de la encuesta de percepción de riesgos para la Seguridad N
a cinco años)

Percepción de la evolución de riesgos

Mayor percepción de "inseguridad"

Figura A-8
Elementos de mayor preocupación como resultado de la encuesta de percepción de riesgos para la Seguridad Nacional (Mapa de riesgos, tendencias a 5 años y escenarios 2033)

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.
- En 2018: 4.700 millones de usuarios.
- En 2022 se estiman 6.000 (75%) población) millones de una población de más de 8.000.
- 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 *ramsoware* se calculan en unos 5.000 millones USD. En 2021 ya eran de unos 20.000 millones.**

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.**
- **Cibercrimen 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?

¿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.
- En 2020, unos 200.000 millones (Intel).

¿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: XXXXX**
- **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 .**
- **Para 2021 se necesitarían unos 3,5 millones de nuevos puestos.**
- **Desempleo en el ámbito de la ciberseguridad: 0% !**

Centro Universitario THE OPEN FACULTY Turismo y Relaciones Internacionales

UNIVERSIDAD DE MURCIA

Facultad de Turismo y Relaciones Internacionales

¿Quién dijo desempleo? (2)


The Washington Post Podcasts

The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds


REUTERS

World Business Legal Markets Breakingviews Technology

May 8, 2021
6:54 AM CEST
Last Updated 3 months ago

Technology

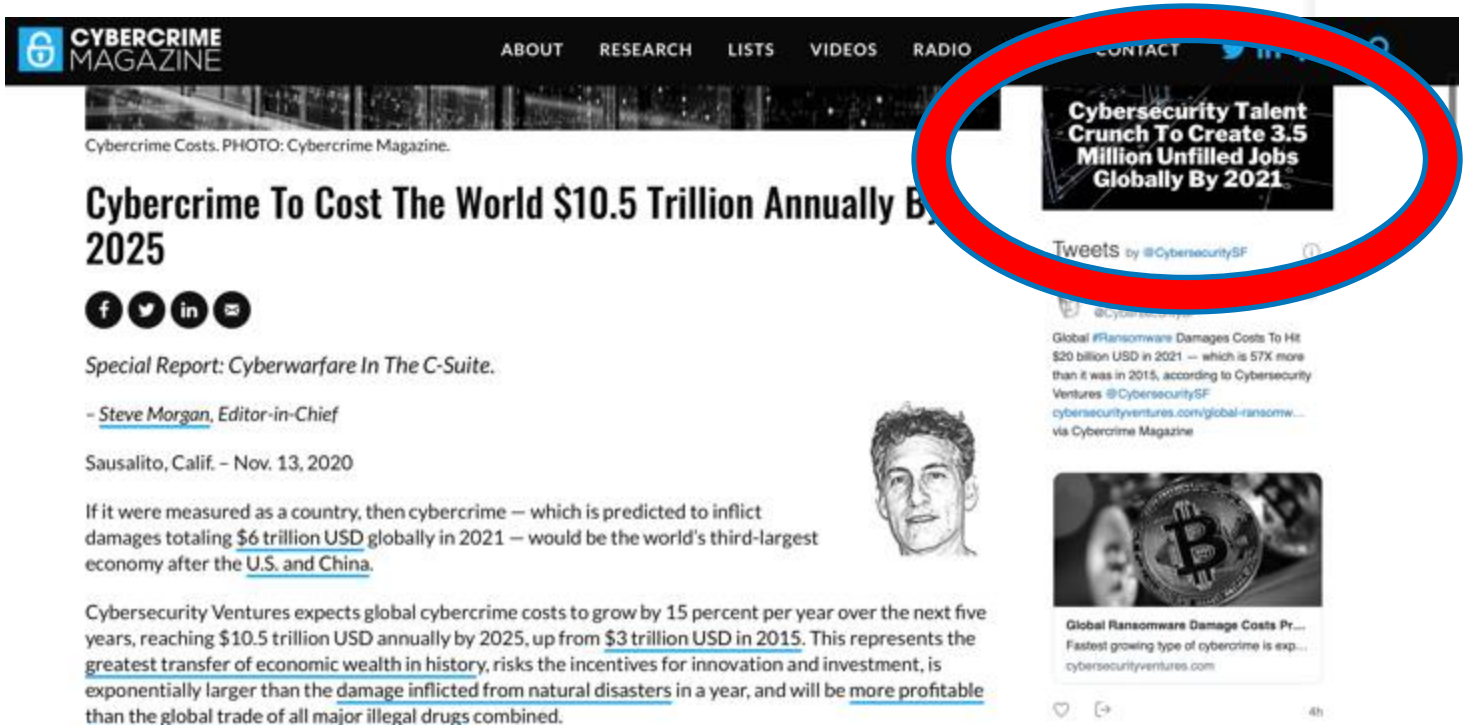
Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed

5 minute read

Christopher Bing, Stephanie Kelly

NEW YORK, May 8 (Reuters) - Top U.S. fuel pipeline operator Colonial Pipeli shut its entire network, the source of nearly half of the U.S. East Coast's fuel supply, after a cyber attack on Friday that involved ransomware.

The incident is one of the most disruptive digital ransom operations ever reported and has drawn attention to how vulnerable U.S. energy infrastructu is to hackers. A prolonged shutdown of the line would cause prices to spike


CYBERCRIME MAGAZINE

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-ransomw...
via Cybercrime Magazine

Global Ransomware Damage Costs Pr...
Fastest growing type of cybercrime is exp...
cybersecurityventures.com

4h

¿Quién dijo “gran hermano”?

Los Angeles Times

Cómo China dominó el mercado de vigilancia de reconocimiento facial

BBC NEWS | MUNDO

Noticias América Latina Internacional EE.UU. 2020 ¿Hablas español? Hay Festival Economía Centroamérica Cuenta BBC Extra

Ads by Google

Stop seeing this ad Why this ad?

El Confidencial

MUNDO

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

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

Redacción
BBC News Mundo

1 diciembre 2019

VIAJAR A CHINA TOURS EN CHINA VISADO PARA CHINA VIVIR EN CHINA APRENDER CHINO

Estamos 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

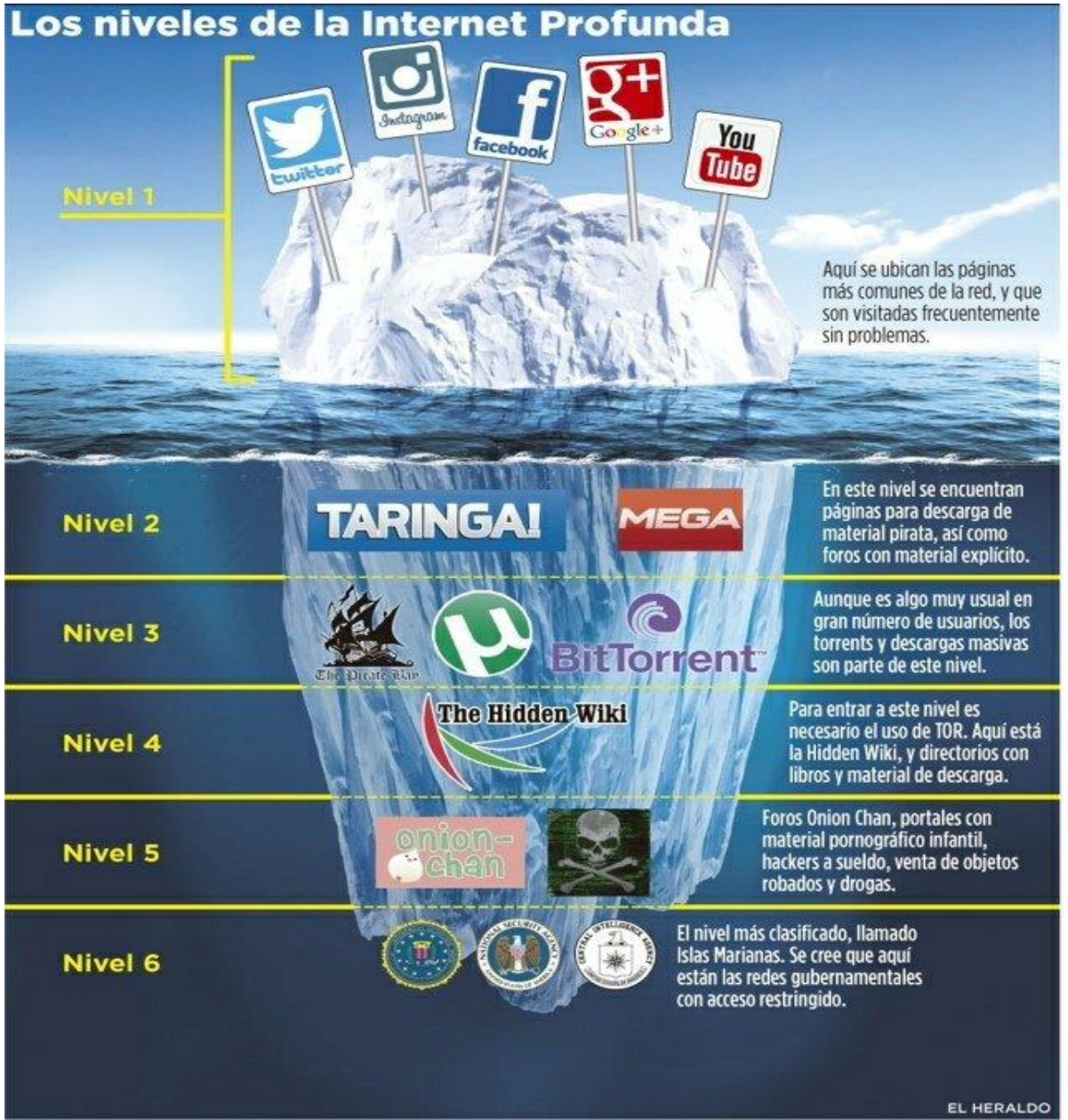
DEJAR UN COMENTARIO

Pago mediante smartphone en China – Índice

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

“Deep / Dark Web” (1)

Criptomonedas
y
criminales

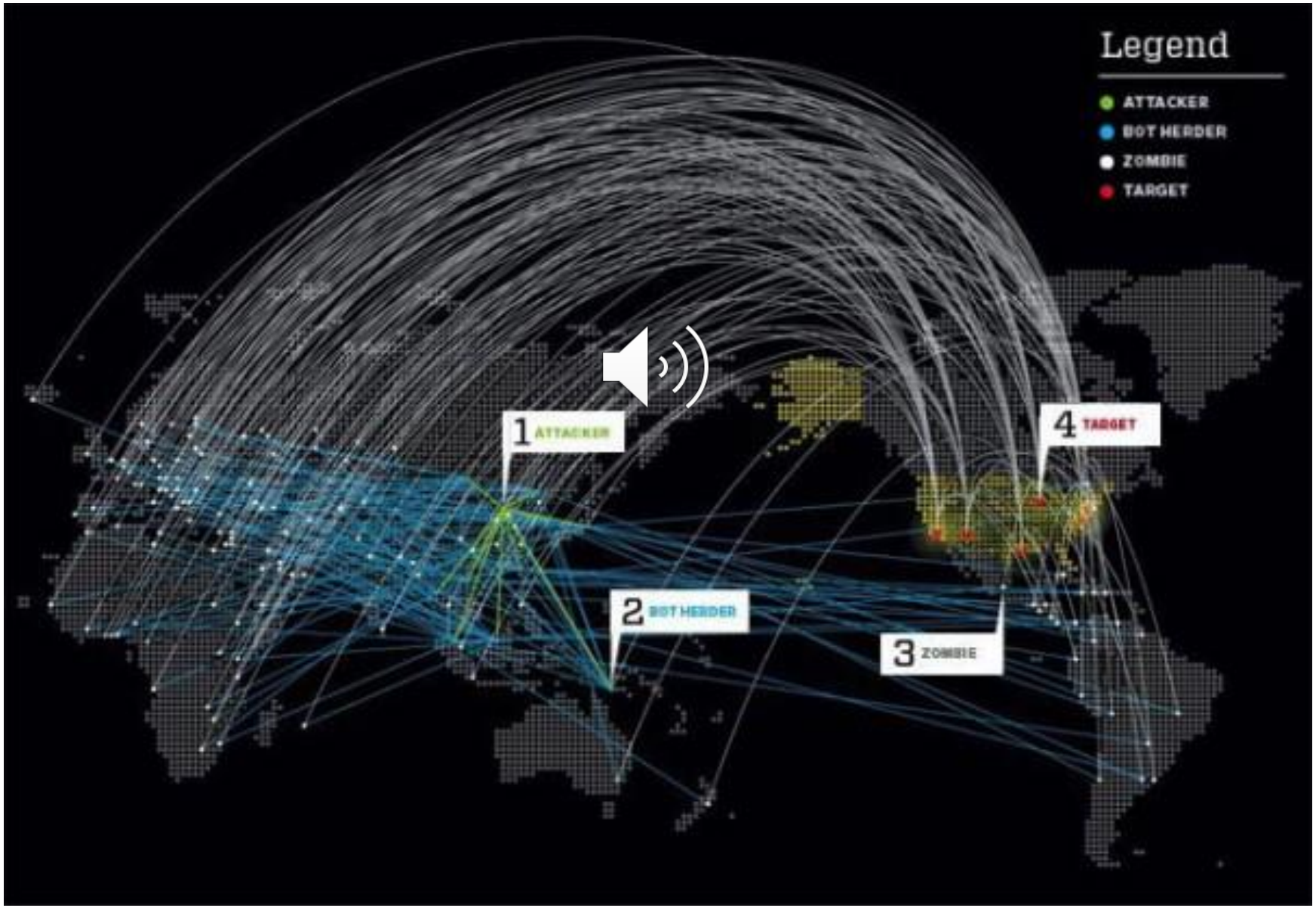


“Deep / Dark Web” (2)

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 nuclerar de Irán. 2010

cronicaseguridad.com

SEGURIDAD INTEGRAL MUNDO JURÍDICO INTERNACIONAL FORMACIÓN EMPLEO PERSONAL DE SEGURPRI FFCCSS 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.

BUSCAR …

ENTRADAS RECIENTES

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.

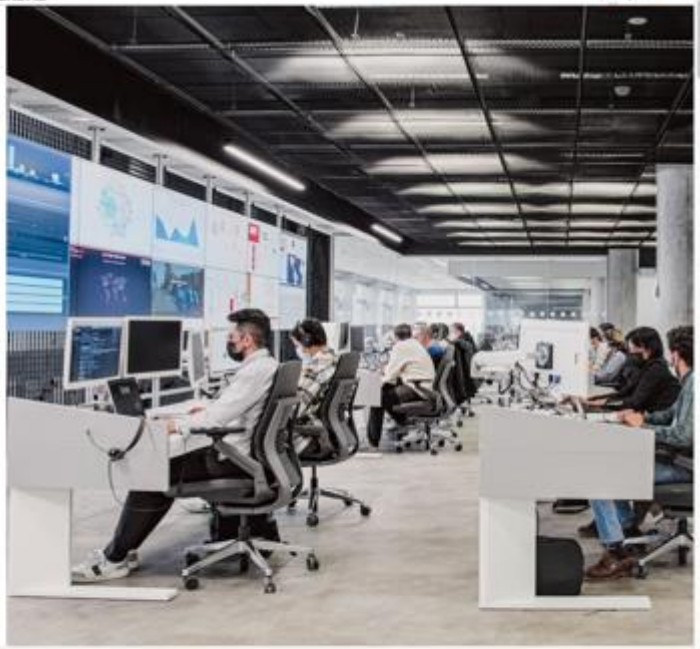
Cuando Rusia invadió Ucrania, arrancó una segunda y menos visible batalla en el ciberespacio. Joe Tidy, corresponsal de asuntos cibernéticos de la BBC, viajó a Ucrania para hablar con quienes pelean la guerra cibernética.

Descubrió que el conflicto ha difuminado las líneas entre cibermilitares 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 GRITTA / 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

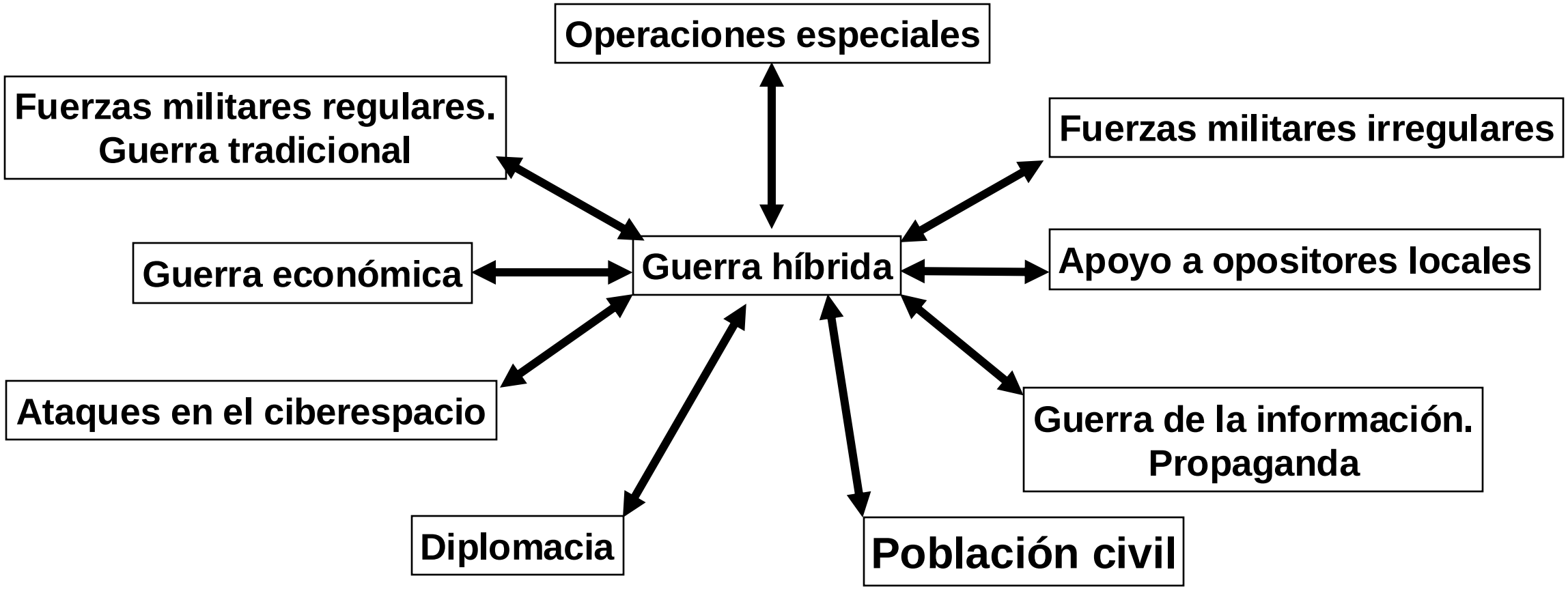
Amenazas híbridas: ¿A qué nos enfrentamos?

FAKE NEWS? o...

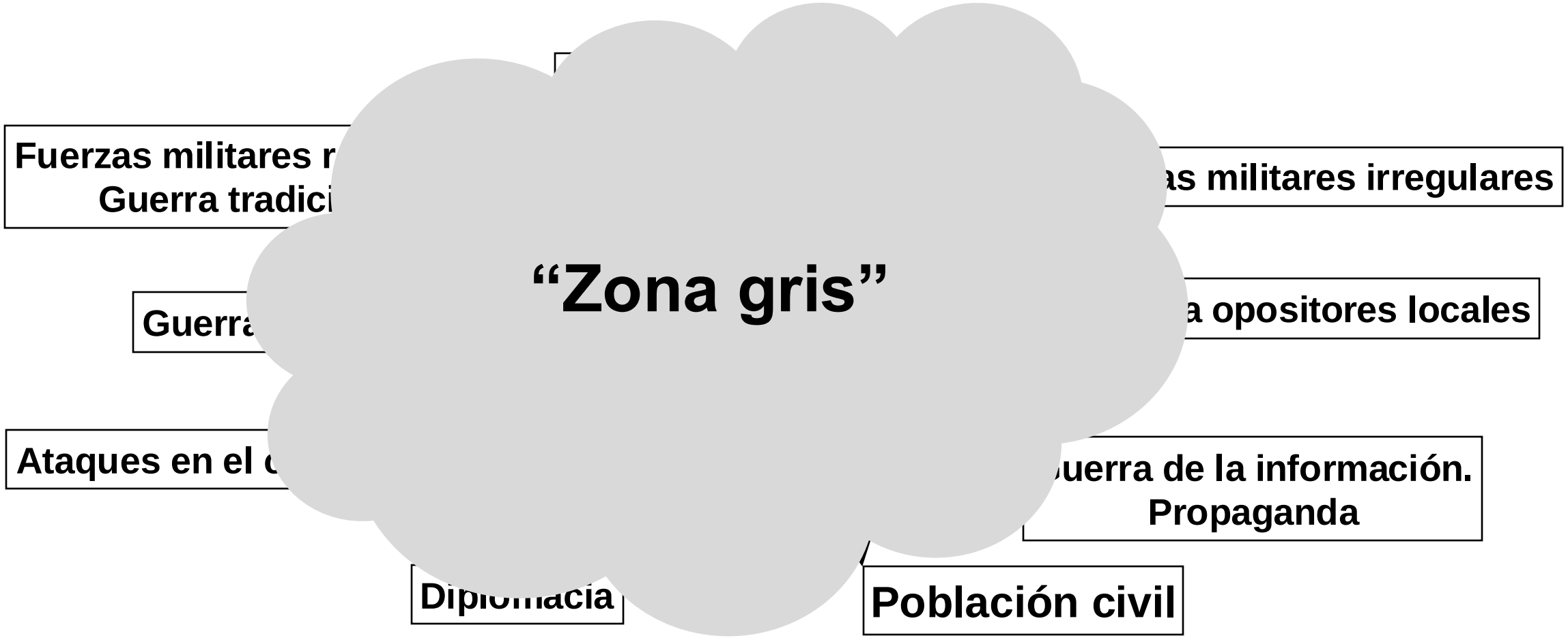
¿ O NEWS FAKE ?

- ¿Nuevo concepto para las prácticas de siempre?
- La ambigüedad como ame...
- ...ucha contra lo difuso
- La sociedad como objetivo

Amenaza / Guerra Híbrida
Medios empleados



Amenaza / Guerra Híbrida
Medios empleados



Índice

¿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.**

https://www.consilium.europa.eu/es/infographics/terrorist-content-online/

https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX%3A32021R0784

¿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.

Proyecto de ley de la inteligencia artificial:

- 14 de junio de 2023 el Parlamento Europeo.

¿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.

DW Made for minds.

TOP STORIES MEDIA CENTER TV RADIO LEARN GERMAN

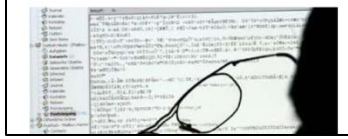
CORONAVIRUS WORLD GERMANY BUSINESS SCIENCE ENVIRONMENT CULTURE SPO

TOP STORIES / WORLD / EUROPE

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

2008. Creación en Tallin del Centro de Excelencia de Ciberdefensa de la OTAN (CCDCOE): Formación y capacitación.

¿Y qué hace hace España?

Ámbito institucional

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 repuesta 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

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

Consejo Nacional de Ciberseguridad

https://www.dsn.gob.es/es/actualidad/sala-prensa/reuni%C3%B3n-del-consejo-nacional-ciberseguridad-6

Mando Conjunto del Ciberespacio

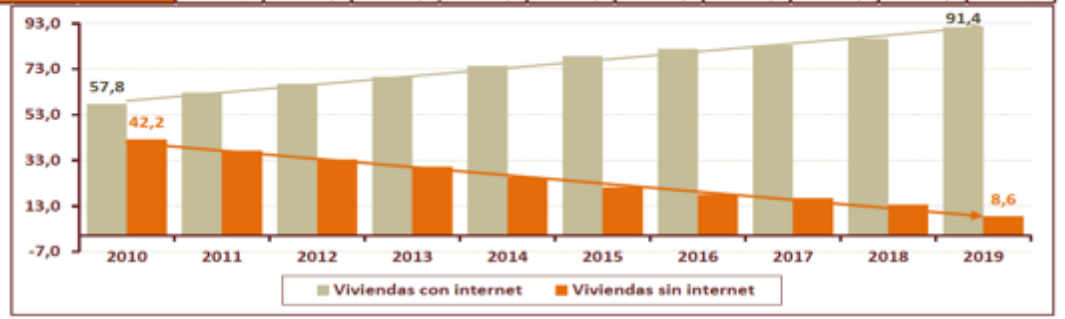
- **Órgano responsable de la dirección, la coordinación, el control y la ejecución de las acciones conducentes a asegurar la libertad de acción de las Fuerzas Armadas en el ámbito ciberespacial.**

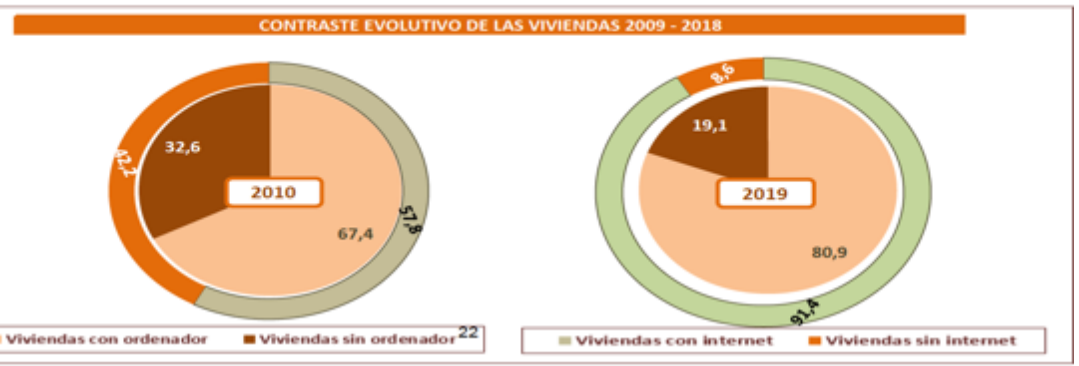
- **Planea, dirige, coordina, controla y ejecuta las operaciones militares en el ciberespacio y, en este ámbito, las acciones necesarias para garantizar la supervivencia de los elementos físicos, lógicos y virtuales críticos para la Defensa y las Fuerzas Armadas.**

Ordenadores nuevos vs. accesos a Internet

PORCENTAJE DE VIVIENDAS CON / SIN ALGÚN TIPO DE ORDENADOR	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Viviendas con ordenador	67,4	70,3	72,6	73,3	74,8	75,9	77,1	78,4	79,5	80,9
Viviendas sin ordenador	32,6	29,7	27,4	26,7	25,2	24,1	22,9	21,6	20,5	19,1

PORCENTAJE DE VIVIENDAS CON / SIN ACCESO A INTERNET	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Viviendas con internet	57,8	62,7	66,6	69,7	74,4	78,7	81,9	83,4	86,4	91,4
Viviendas sin internet	42,2	37,3	33,4	30,3	25,6	21,3	18,1	16,6	13,6	8,6





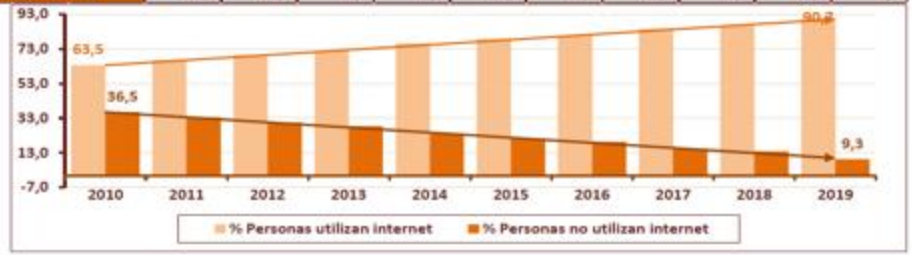
Perfil del usuario de Internet

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

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

% DE PERSONAS QUE HAN UTILIZADO O NO INTERNET ÚLTIMOS 3 MESES

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Utilizado internet	63,5	66,5	69,5	71,6	76,2	78,7	80,6	84,6	86,1	90,7
No utilizado internet	36,5	33,5	30,5	28,4	23,8	21,3	19,4	15,4	13,9	9,3

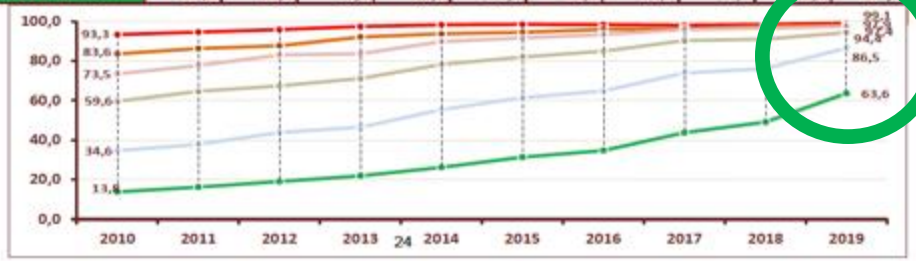


% POR SEXO DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES

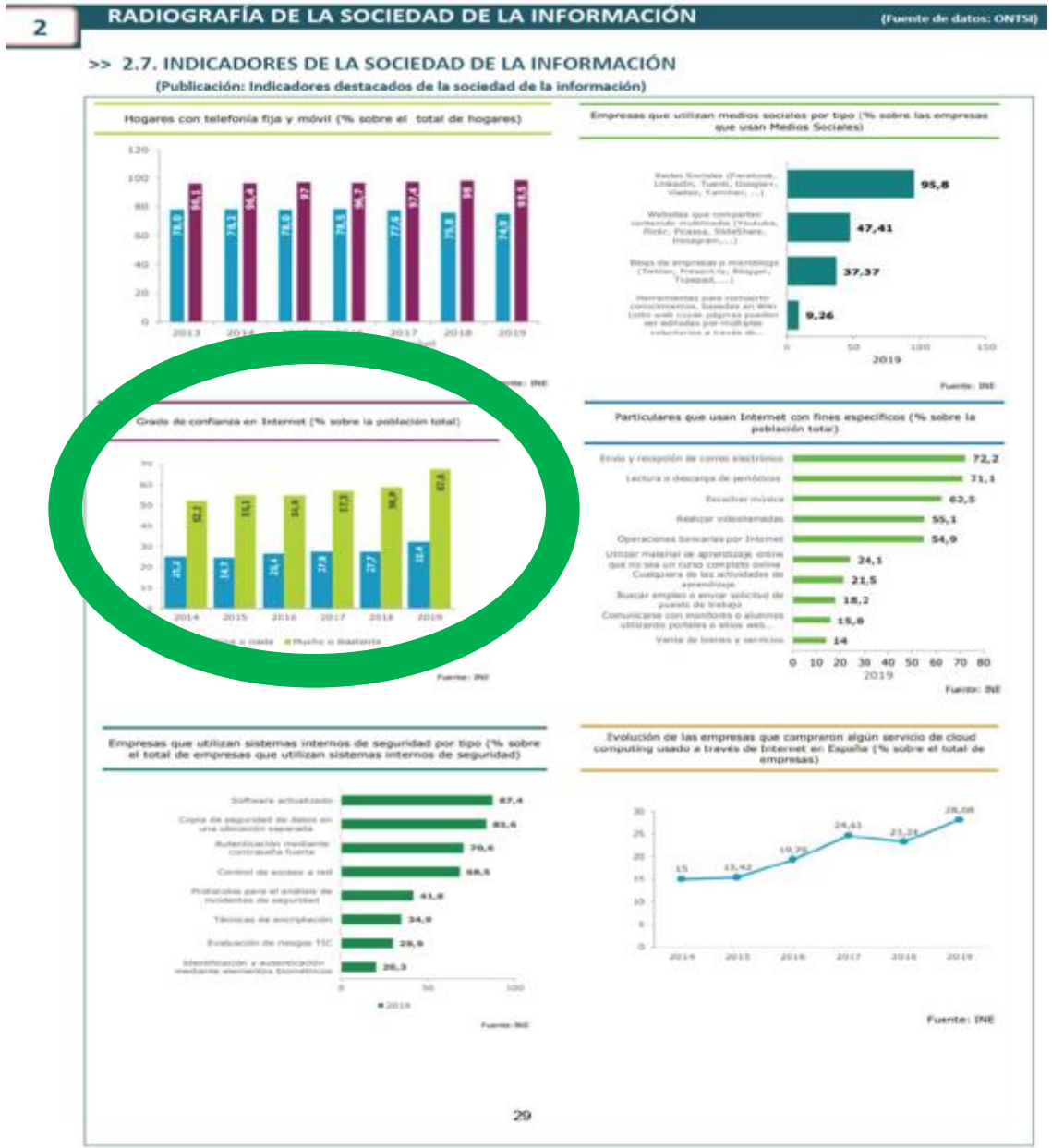
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Hombre	66,3	69,2	72,1	73,7	77,9	80,3	82,5	85,5	85,6	90,7
Mujer	60,8	63,8	66,8	69,6	74,5	77,1	78,6	83,7		

% POR GRUPO DE EDAD DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Edad: De 16 a 24 años	93,3	94,6	95,8	97,4	98,3	98,5	98,4	98,0	98,5	99,1
Edad: De 25 a 34 años	83,6	86,3	87,7	92,1	93,7	94,5	96,0	96,3	97,7	97,9
Edad: De 35 a 44 años	73,5	77,7	83,0	83,7	89,8	91,6	93,3	95,8	96,6	97,4
Edad: De 45 a 54 años	59,6	64,6	67,4	71,2	78,2	82,0	84,9	90,3	91,0	94,4
Edad: De 55 a 64 años	34,6	37,9	43,8	46,5	55,4	61,4	64,8	73,9	76,1	86,5
Edad: De 65 a 74 años	13,8	16,2	19,0	21,9	26,2	31,3	34,7	43,7	51,1	63,6



Confianza en compras por Internet



Cibercriminalidad

Centro Universitario THE OPEN FACULTY Turismo y Relaciones Internacionales

UNIVERSIDAD DE MURCIA

Facultad de Turismo y Relaciones Internacionales

https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2022/Informe-Cibercriminalidad-2022.pdf

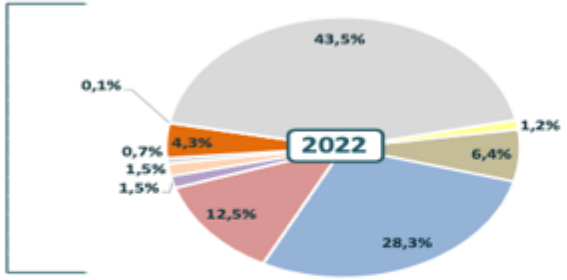
INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 2.1. Incidentes gestionados por el INCIBE-CERT

Tipo de incidente	INCIDENTES GESTIONADOS						
	2016	2017	2018	2019	2020	2021	2022
Intrusión	14.373	19.275	8.541	6.479	9.557	7.039	7.649
Fraude	11.843	11.959	55.932	31.938	42.641	31.213	33.576
Malware	76.811	81.090	27.016	27.358	46.893	32.605	14.855
SPAM	10.279	7.957	0	0	0	0	0
Disponibilidad	495	514	100	58	1.971	7.177	1.768
Intento de intrusión	381	1.435	396	1.518	1.289	1.753	1.839
Robos de información	37	47	63	77	161	920	823
Contenido Abusivo			9.353	4.064	2.986	5.253	5.110
Recolección de información			5.605	84	87	106	73
Sistema Vulnerable			3.731	31.414	23.161	20.609	51.711
Otros	1.038	787	782	4.407	4.409	2.451	1.416

Porcentaje del total de incidentes gestionados

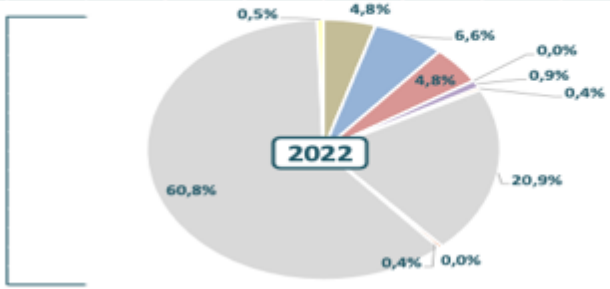


*Véase metadatos explicativos

>> 2.2. Incidentes gestionados en relación con las infraestructuras críticas

Tipo de incidente	INCIDENTES GESTIONADOS						
	2016	2017	2018	2019	2020	2021	2022
Intrusión	39	97	26	14	13	11	26
Fraude	13	66	41	78	37	16	36
Malware	311	387	200	166	348	177	26
SPAM	8	21	0	0	0	0	0
Disponibilidad	28	55	54	12	52	10	5
Intento de intrusión	24	159	9	7	3	2	2
Robos de información	1	1	7	8	0	117	114
Contenido Abusivo			11	6	6	3	2
Recolección de información			111	1	45	2	0
Sistema Vulnerable			224	514	351	339	332
Otros	55	99	39	12	6	3	3

Porcentaje del total de incidentes gestionados



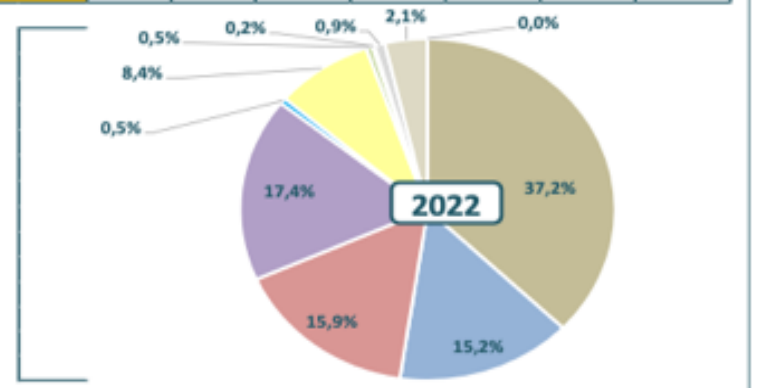
*Véase metadatos explicativos

2.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 2.3. Incidentes gestionados por sector estratégico

Sector estratégico	INCIDENTES GESTIONADOS						
	2016	2017	2018	2019	2020	2021	2022
Energía	126	213	149	151	121	207	203
Transporte	90	152	192	197	176	92	83
Tecnologías Informac. y Comunicac. (TIC)	17	40	46	50	29	47	87
Sistema tributario y financiero	152	250	214	266	452	172	95
Alimentación	47	42	40	57	1	3	3
Agua	40	134	57	64	31	117	46
Industria nuclear	4	12	5	18	22	9	3
Administración	2	10	1	0	4	1	1
Espacio	0	1	3	4	3	7	5
Industria química	0	0	15	11	18	23	20
Instalaciones de Investigación	0	0	0	0	0	0	0
Salud	0	1	0	0	0	0	0
Todos los sectores afectados	1	0	0	0	4	2	0

Porcentaje del total de incidentes gestionados



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

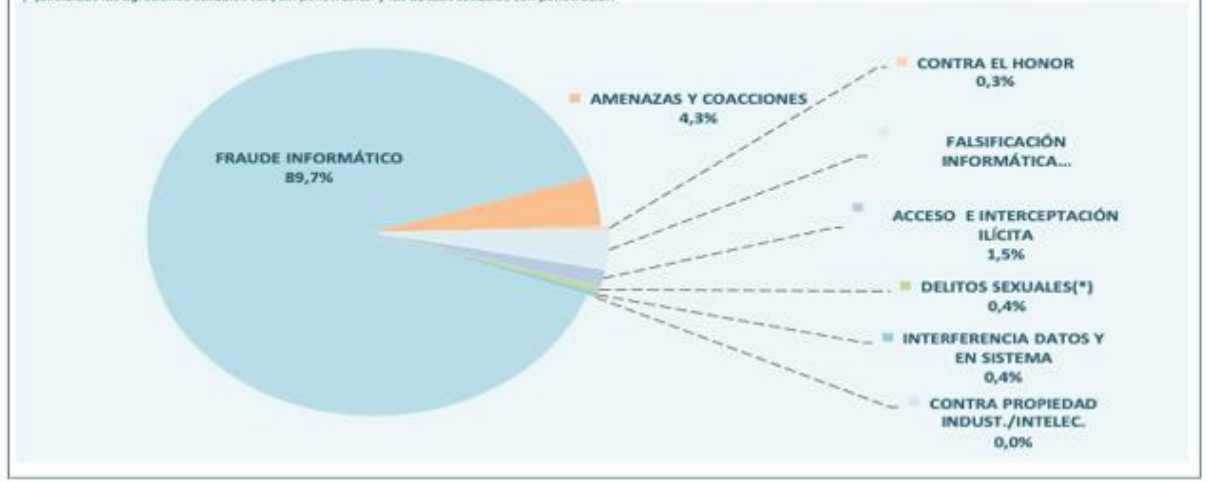
3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 3.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2018	2019	2020	2021	2022
ACCESO E INTERCEPTACIÓN ILÍCITA	3.384	4.004	4.653	5.342	5.578
AMENAZAS Y COACCIONES	12.800	12.782	14.066	17.319	15.982
CONTRA EL HONOR	1.448	1.422	1.550	1.426	1.191
CONTRA PROPIEDAD INDUST./INTELEC.	232	197	125	137	114
DELITOS SEXUALES(*)	1.581	1.774	1.783	1.628	1.646
FALSIFICACIÓN INFORMÁTICA	3.436	4.275	6.289	10.476	12.569
FRAUDE INFORMÁTICO	136.656	192.375	257.907	267.011	335.995
INTERFERENCIA DATOS Y EN SISTEMA	1.192	1.473	1.590	2.138	1.662
Total HECHOS CONOCIDOS	**160.729**	**218.302**	**287.963**	**305.477**	**374.737**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



>> 3.2. Evolución global de hechos conocidos. esclarecidos y detenciones / investigados

3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

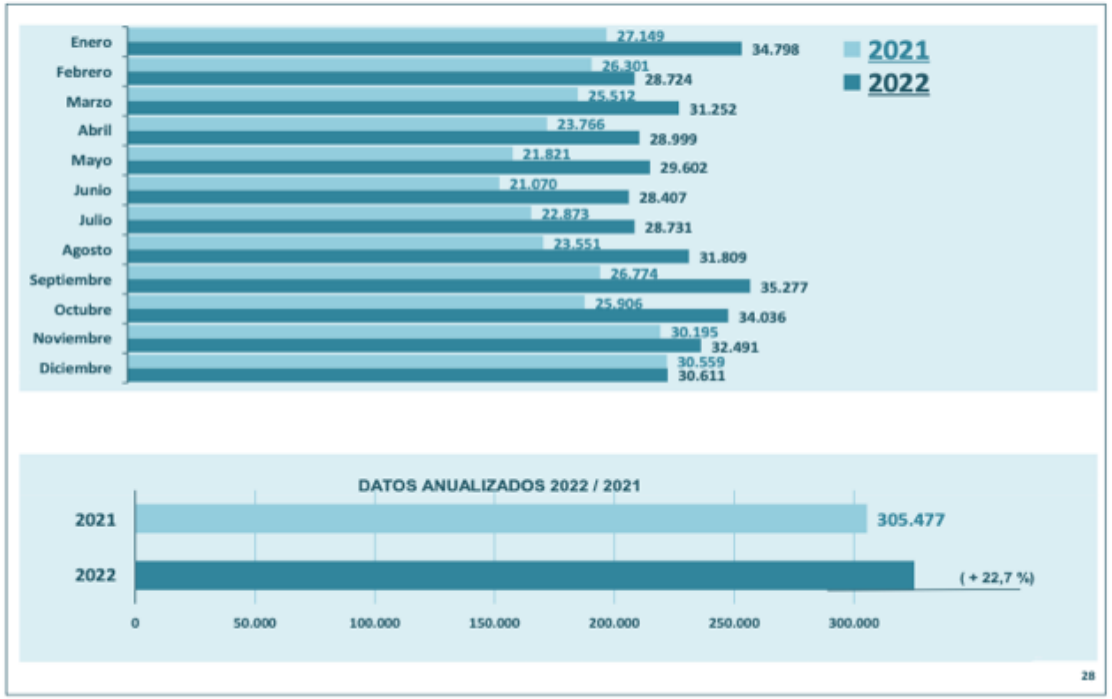
(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 3.3. Distribución mensual de hechos conocidos. Año 2022

HECHOS CONOCIDOS	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic	TOTAL
ACCESO E INTERCEPTACIÓN ILÍCITA	307	367	426	420	538	502	529	466	575	457	570	421	5.578
AMENAZAS Y COACCIONES	1.326	1.434	1.570	1.282	1.319	1.403	1.322	1.340	1.288	1.295	1.255	1.148	15.982
CONTRA EL HONOR	78	104	127	91	91	107	107	101	114	103	90	78	1.191
CONTRA PROPIEDAD INDUST./INTELEC.	9	12	16	9	1	13	5	13	12	10	6	8	114
DELITOS SEXUALES(*)	168	135	195	119	159	145	90	128	138	139	137	93	1.646
FALSIFICACIÓN INFORMÁTICA	910	1.075	1.239	1.045	1.200	1.074	962	925	1.045	1.014	1.143	937	12.569
FRAUDE INFORMÁTICO	31.873	25.471	27.545	25.878	26.147	25.026	25.582	28.681	31.973	30.890	29.166	27.763	335.995
INTERFERENCIA DATOS Y EN SISTEMA	127	126	134	155	147	137	134	155	132	128	124	163	1.662
Total HECHOS CONOCIDOS	**34.798**	**28.724**	**31.252**	**28.999**	**29.602**	**28.407**	**28.731**	**31.809**	**35.277**	**34.036**	**32.491**	**30.611**	**374.737**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

>> 3.4. Comparativa de la distribución mensual de hechos conocidos 2022 / 2021



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

Hechos denunciados de CIBERCRIMINALIDAD - 2022

Hechos conocidos:	374.737	
Esclarecimiento (*):	51.642	14,6%
Detenciones/invest:	15.097	

CCAA	Hechos
CATALUÑA	63.877
MADRID (COMUNIDAD DE)	63.758
ANDALUCÍA	56.908
COMUNITAT VALENCIANA	34.005
CASTILLA Y LEÓN	21.302
GALICIA	20.914
PAÍS VASCO	20.907
CASTILLA - LA MANCHA	15.649
CANARIAS	13.684
MURCIA (REGIÓN DE)	9.971
ARAGÓN	9.620
BALEARS (ILLES)	8.701
ASTURIAS (PRINCIPADO DE)	8.560
EXTREMADURA	7.528
EN EL EXTRANJERO	5.643
NAVARRA (COMUNIDAD FORAL DE)	5.499
CANTABRIA	4.806
RIOJA (LA)	2.433
CIUDAD AUTÓNOMA DE CEUTA	567
CIUDAD AUTÓNOMA DE MELILLA	405

(*) Debido a que la Ertzaintza no facilita datos de esclarecidos el % de esclarecimiento se ha calculado sin tener en cuenta los hechos conocidos por este cuerpo policial

Hechos denunciados de CIBERCRIMINALIDAD - 2022

Provincias más afectadas:	Hechos
Madrid	63.758
Barcelona	46.513
Valencia/València	18.354
Sevilla	14.590
Alicante/Alacant	13.075
Málaga	11.863
Bizkaia	11.277
Cádiz	10.306
Murcia	9.971
Balears (Illes)	8.701
Asturias	8.560
Coruña (A)	8.437
Palmas (Las)	8.054
Pontevedra	8.035
Zaragoza	7.227
Girona	7.118
Tarragona	6.175
Gipuzkoa	6.069
Toledo	5.717
EN EL EXTRANJERO	5.643

Pues no hemos acabado aquí

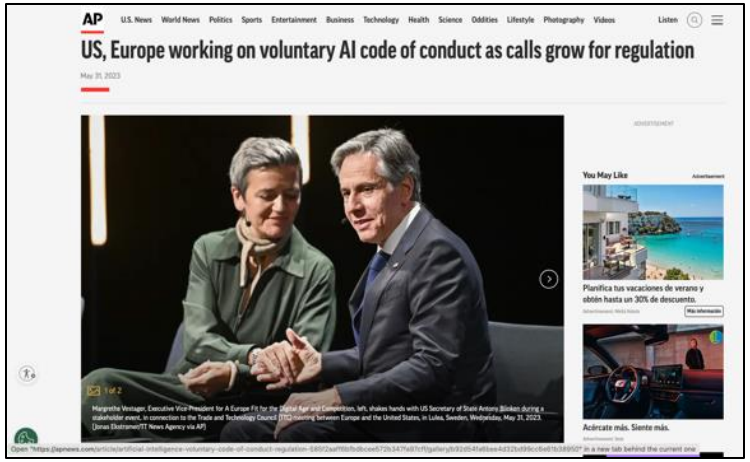
El nuevo reto de la inteligencia artificial. (1)

https://www.fingent.com/wp-content/uploads/fingent-5-1024x555.jpg

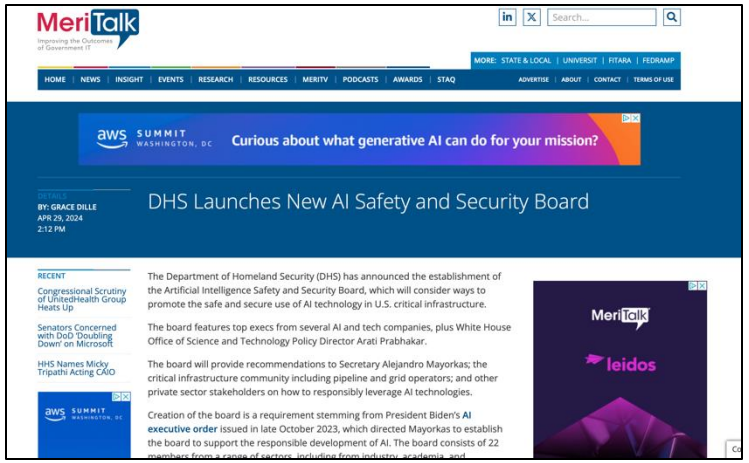
El nuevo reto de la inteligencia artificial. (2)

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

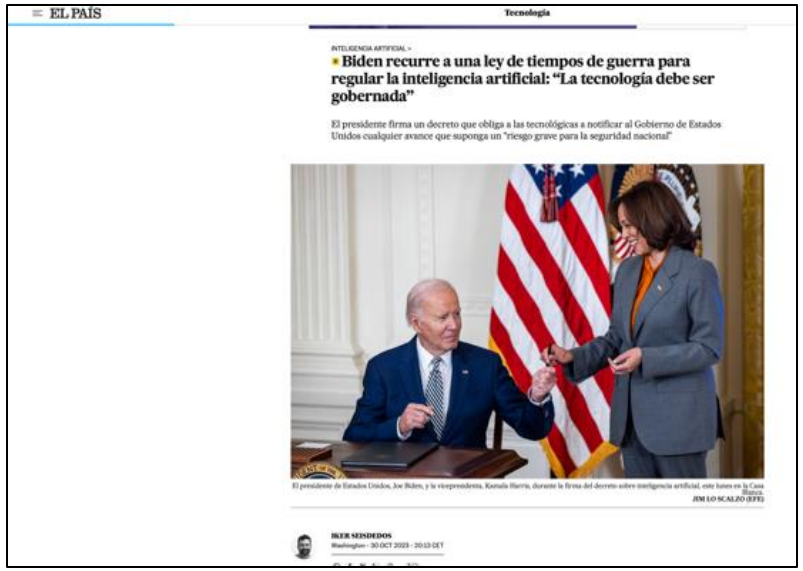
El nuevo reto de la inteligencia artificial. (3)

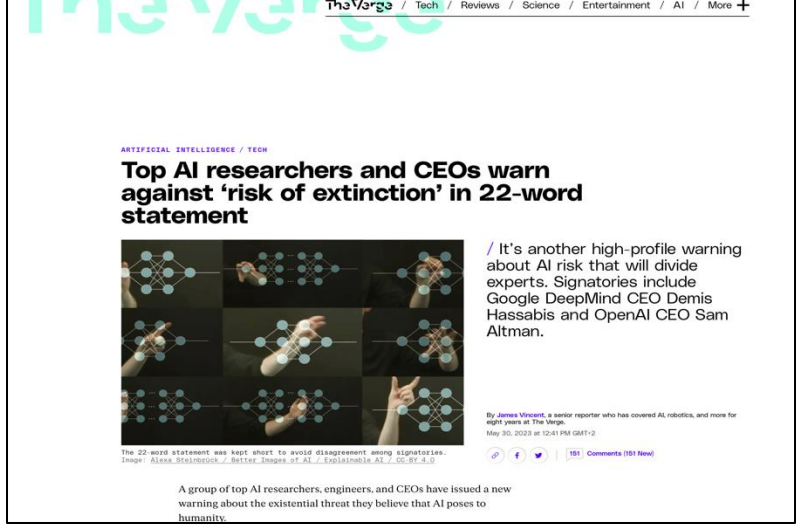


https://apnews.com/article/artificial-intelligence-voluntary-code-of-conduct-regulation-585f2aaff6bfbdbcee572b347fa97cff

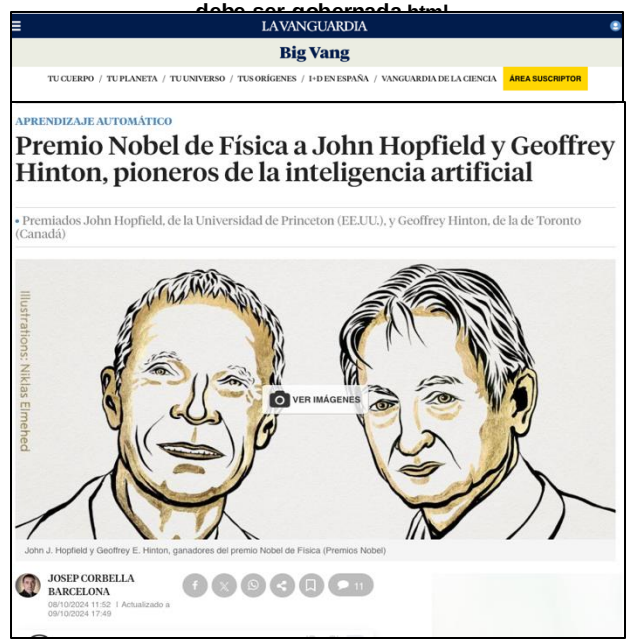


https://www.commerce.gov/news/press-releases/2024/02/biden-harris-administration-announces-first-ever-consortium-dedicated





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

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.**

https://elpais.com/tecnologia/2020-11-17/inteligencia-artificial-y-pseudoanonimato-el-gobierno-presenta-la-primera-version-de-la-carta-de-derechos-digitales.html?rel=mas

El nuevo reto de la inteligencia artificial. (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 de la inteligencia artificial. (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 de la inteligencia artificial. (4)

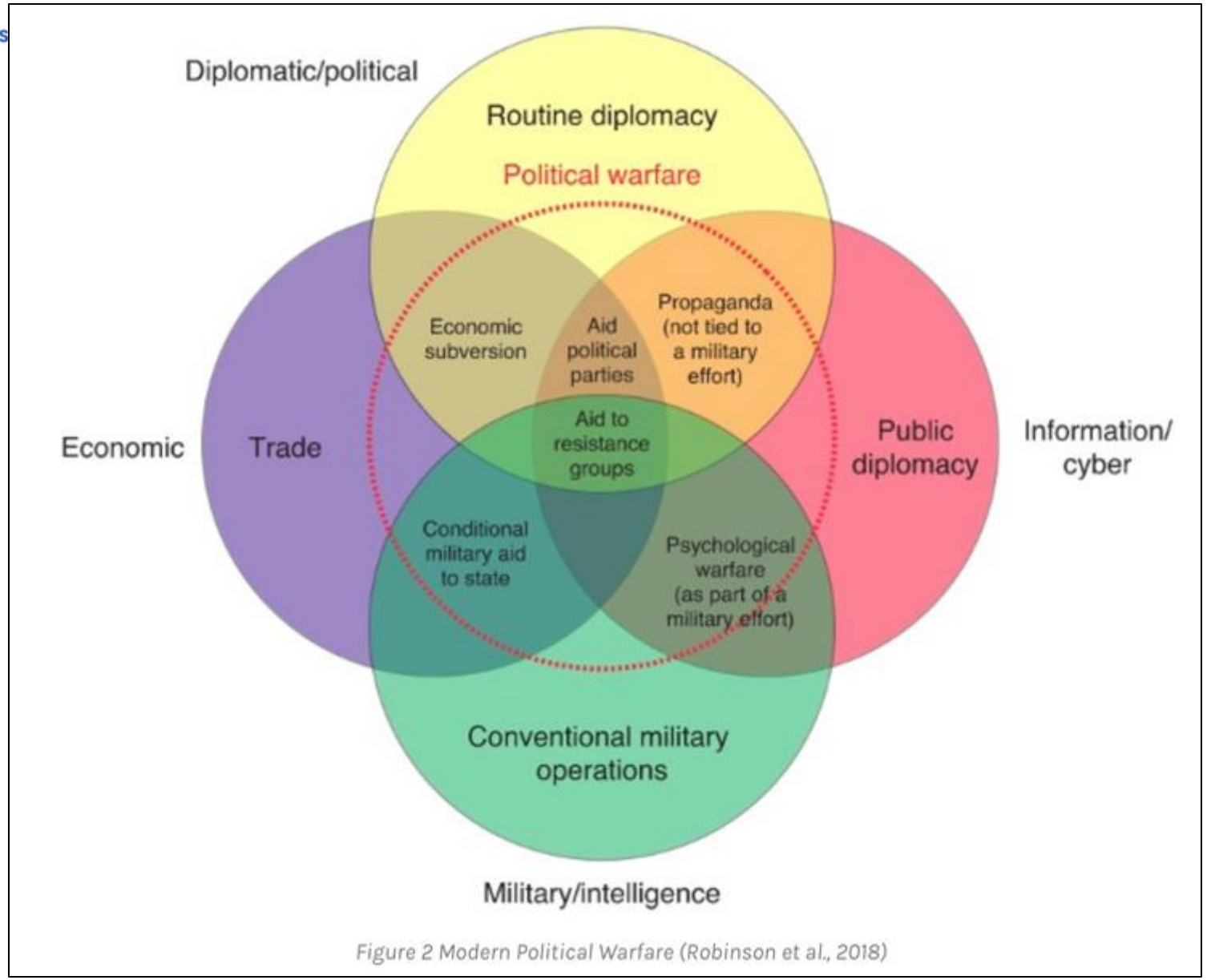


Figure 2 Modern Political Warfare (Robinson et al., 2018)

https://wavellroom.com/2022/01/26/mddo/

El nuevo reto de la inteligencia artificial. (3)

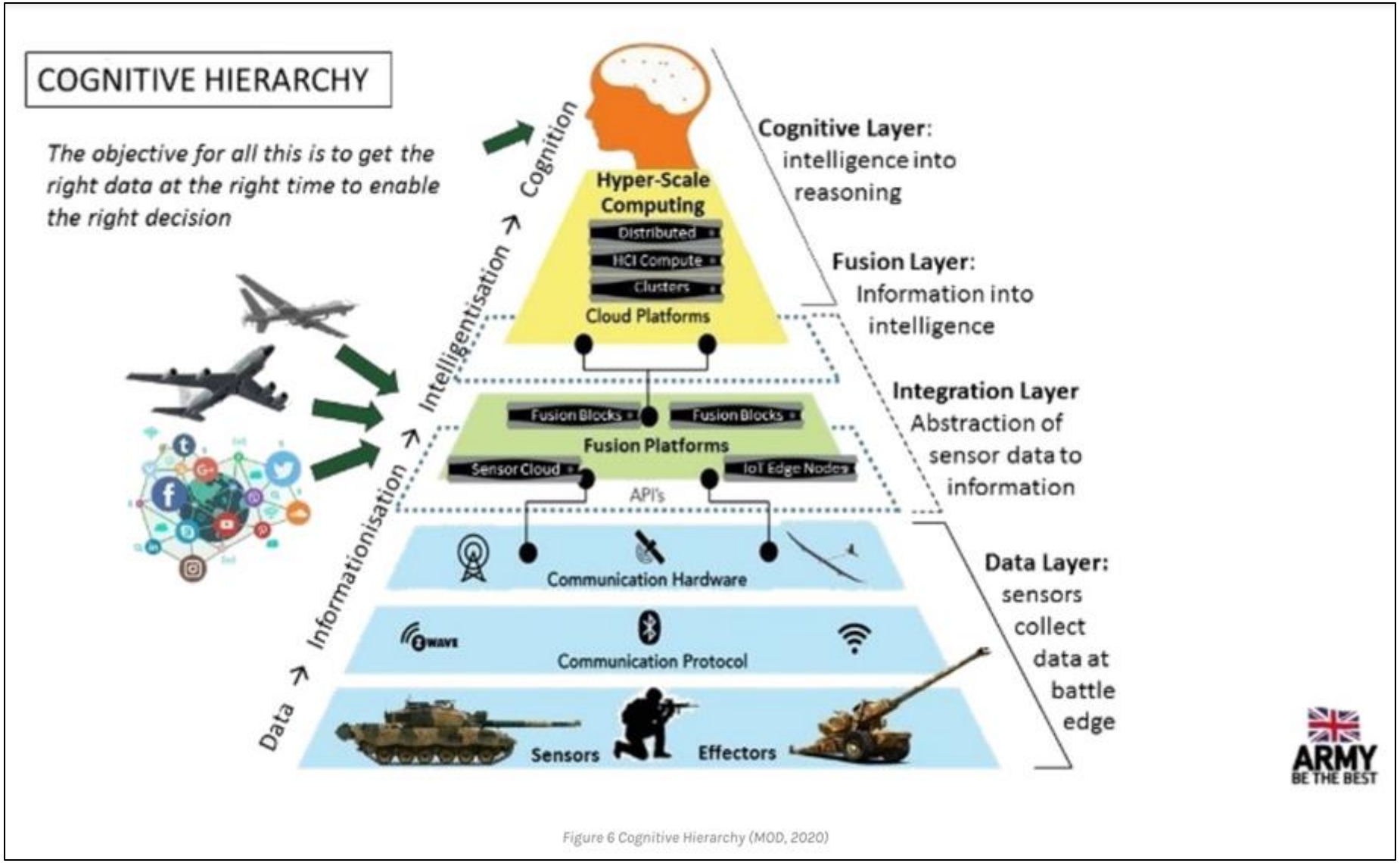
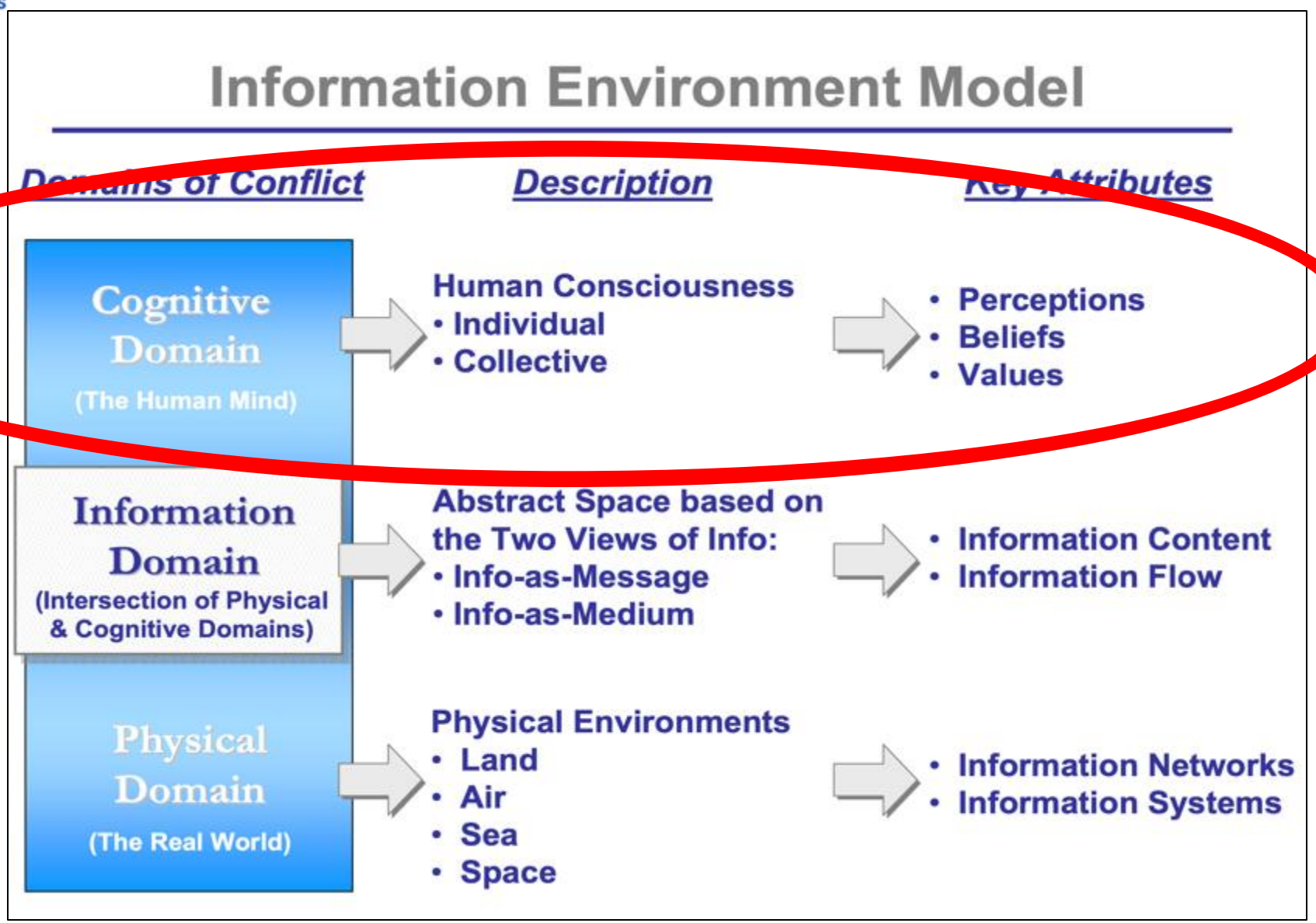


Figure 6 Cognitive Hierarchy (MOD, 2020)

https://wavellroom.com/2022/01/26/mddo/

El nuevo reto de la inteligencia artificial. (3)



http://www.dodccrp.org/events/10th_ICCRTS/CD/presentations/036.pdf

El nuevo reto de la inteligencia artificial. (5)

Layers of Warfare	Domains of Warfare (Trans-domain regions)	Multi-Domain Operation Constructs
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)

https://wavellroom.com/2022/01/26/mddo/

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.

https://planderecuperacion.gob.es/noticias/gobierno-aprueba-estrategia-inteligencia-artificial-2024-prtr

https://portal.mineco.gob.es/es-es/digitalizacionIA/Documents/Estrategia_IA_2024.p

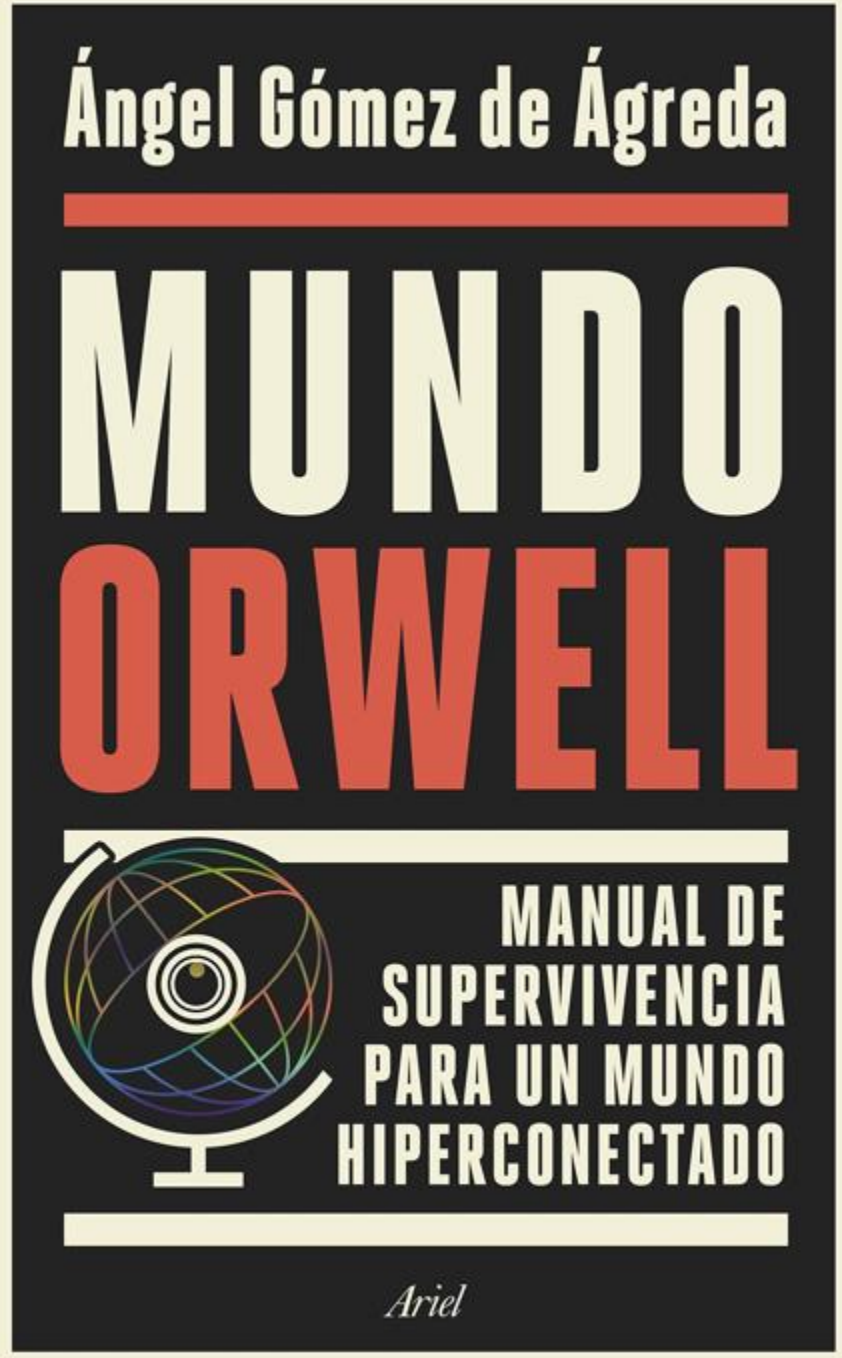
¿Cuál es el eslabón débil de la cadena?

¿Cuál es el eslabón débil de la cadena?

Centro Universitario THE OPEN FACULTY Turismo y Relaciones Internacionales

UNIVERSIDAD DE MURCIA

Facultad de Turismo y Relaciones Internacionales



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

Centro Universitario THE OPEN FACULTY Turismo y Relaciones Internacionales

UNIVERSIDAD DE MURCIA Facultad de Turismo y Relaciones Internacionales

Fin del Tema 6, el Ciberespacio, y de la asignatura, Derecho Internacional de los Espacios.