

**XIII
JORNADAS
STIC
CCN-CERT**

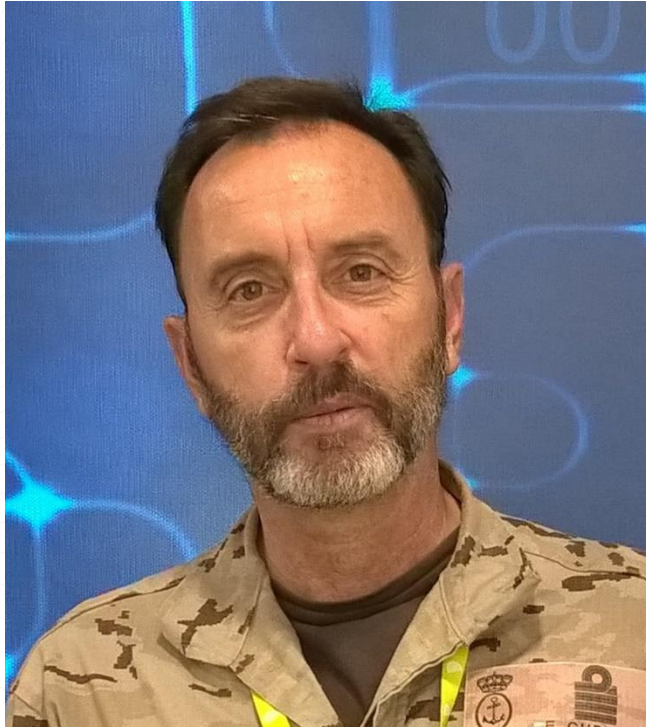


Peculiaridades del combate en el ciberspacio



**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



CN Enrique Cubeiro Cabello

Jefe del Estado Mayor del Mando Conjunto de Ciberdefensa

MCCD / Ministerio de Defensa

Índice

- 1. Ciberguerra**
- 2. Ciberespacio, nuevo campo de batalla**
- 3. La dimensión ciberespacial de los conflictos**
- 4. Ciberejércitos**
- 5. Conclusiones**



Ciberguerra

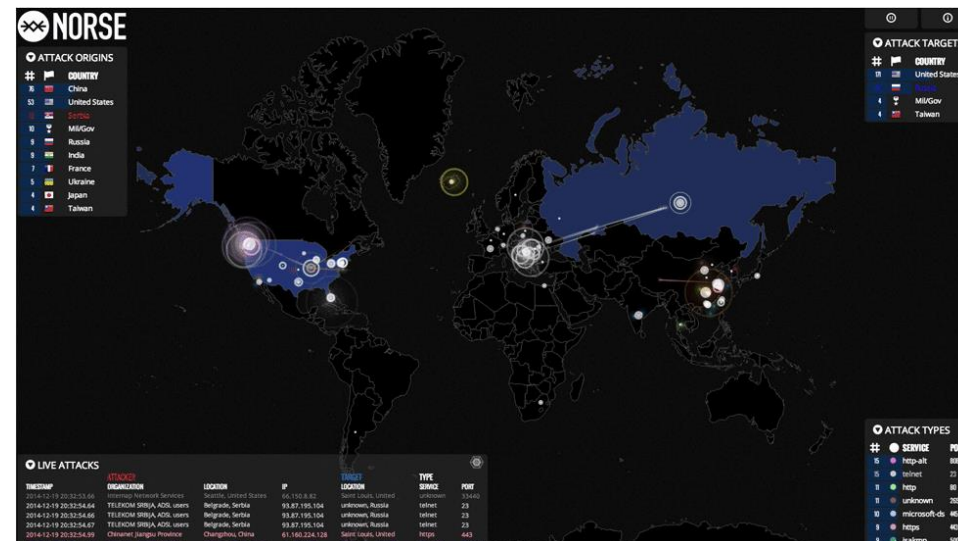
Guerra Naval

Conflicto armado que se desarrolla fundamentalmente en los espacios marítimos.



Ciberguerra / Guerra Ciberespacial

Conflicto ¿armado? que se desarrolla principalmente en o a través del ciberespacio



Ciberespacio, nuevo campo de batalla



El ser humano, en cada momento de la Historia, ha combatido con las armas y en los ámbitos en los que la tecnología disponible se lo ha permitido.



Ciberespacio, nuevo campo de batalla

Ciberespacio, 5º ámbito de las operaciones militares

- Features that identify an Operational domain (NATO doctrine):
 1. Differentiated capabilities are required to operate on it.
 2. Not completely included in other domain.
 3. Presence of own and adversary forces.
 4. Allows to exercise control over the opponent.
 5. Allows synergy with other domains.
 6. Provides opportunity for asymmetry between domains.

NATO Warsaw Summit (8 – 9 July 2016) recognised Ciberespace as a 'domain of Operations'.



Ciberespacio, nuevo campo de batalla

Objetivo:

Asegurar la libertad de acción de las fuerzas propias en el ciberespacio y negárselo/dificutárselo al adversario.



Ciberspacio, nuevo campo de batalla

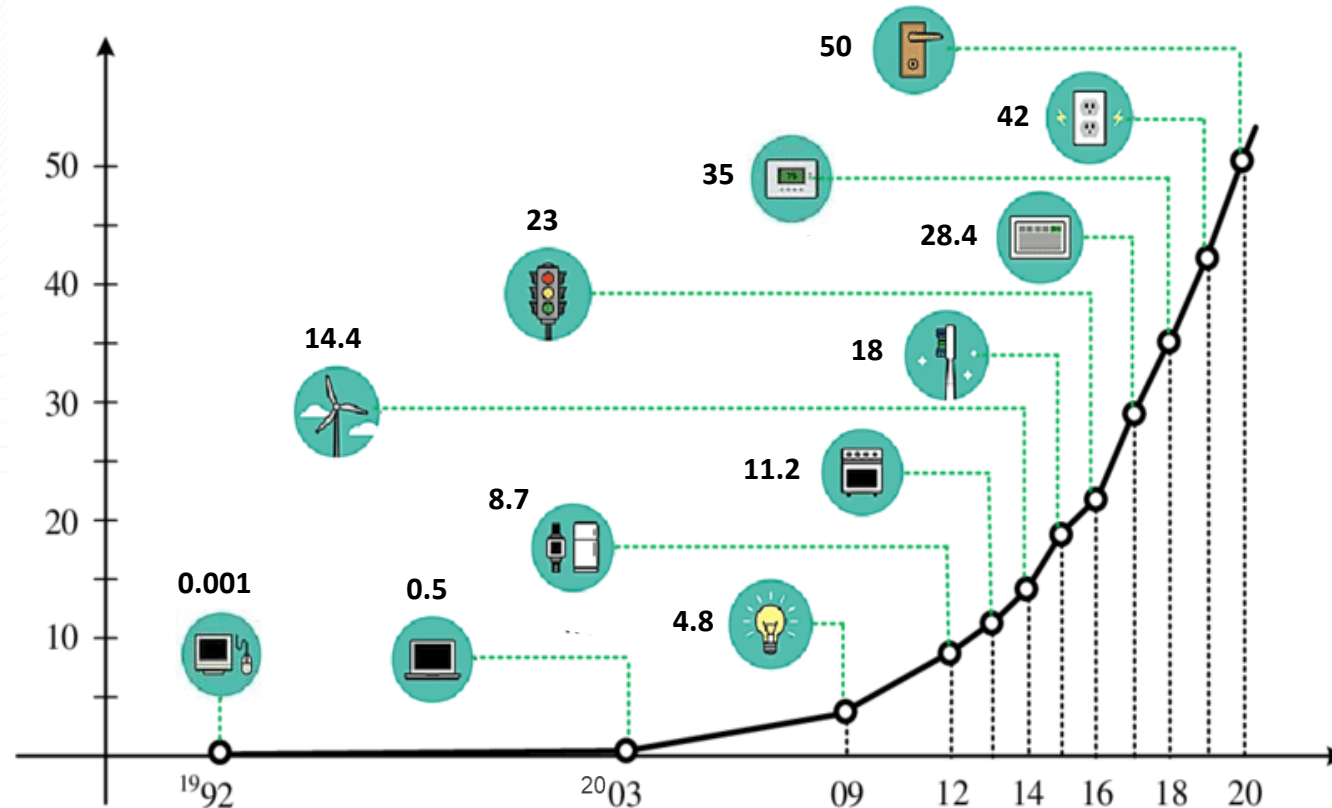


Ciberspacio, nuevo campo de batalla

Ámbito en continua expansión

Evolución nº dispositivos conectados a Internet

Miles de millones



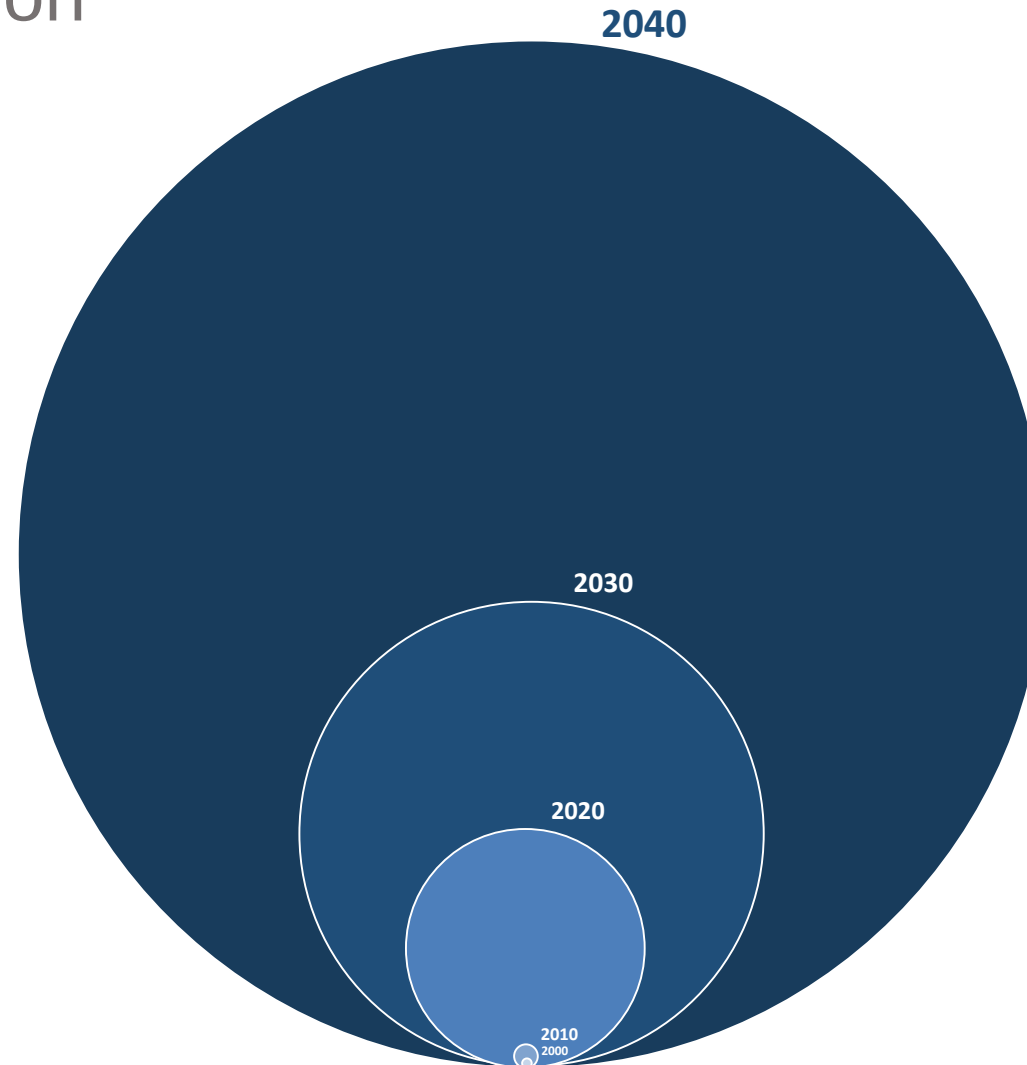
x3 cada 5 años

2040
¿5 billones?

Ciberespacio, nuevo campo de batalla

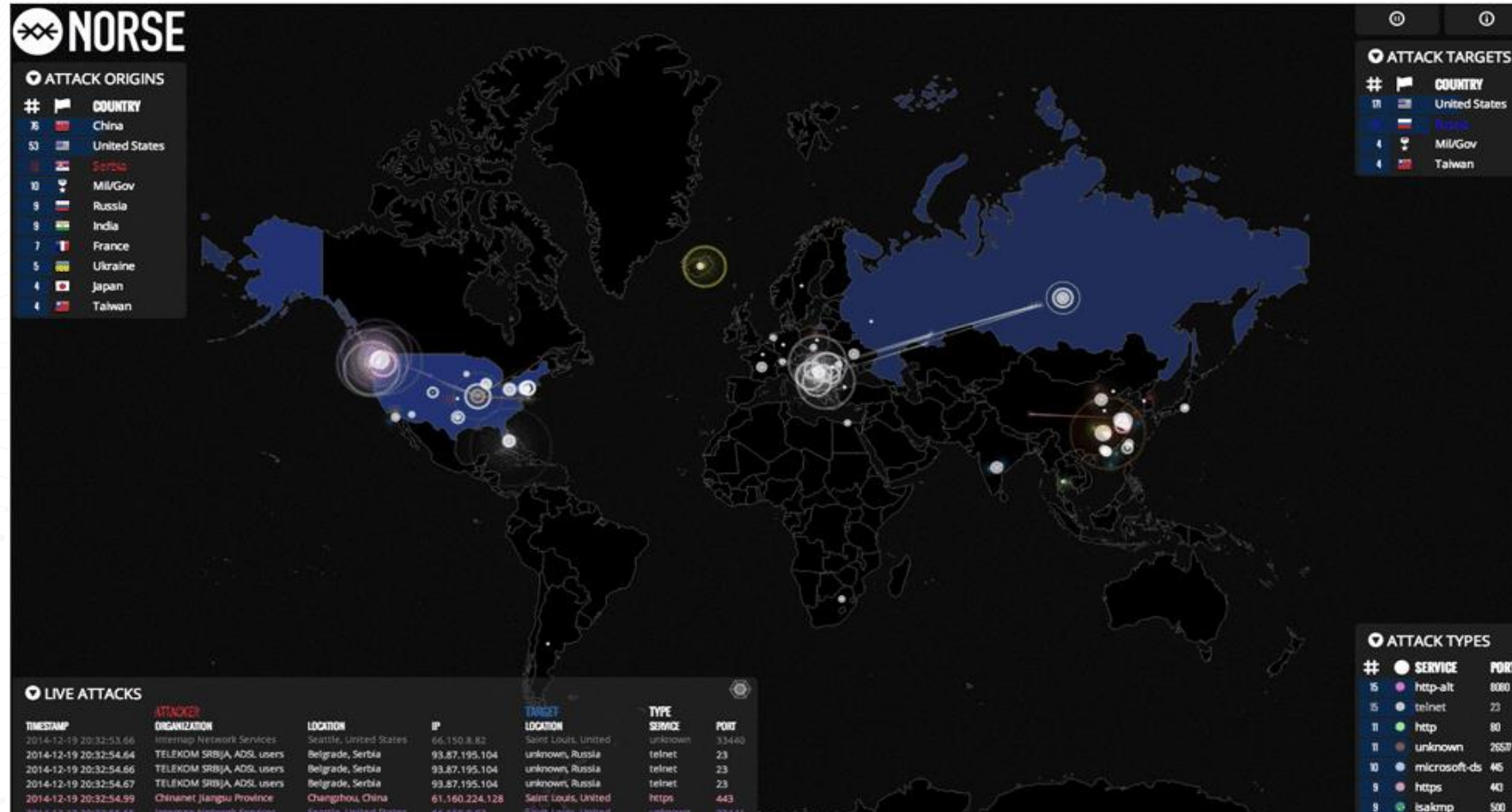
Ámbito en continua expansión

Evolución del tamaño del
ciberespacio



Ciberspacio, nuevo campo de batalla

Permanente e intensa actividad hostil



Ciberspacio, nuevo campo de batalla

Infinidad de vulnerabilidades explotables

Físicas

- Fallos de fabricación
- Limitaciones estructurales
- Resistencia de materiales
- Diseño
- Emanaciones
- Equipos informáticos
- Equipos de comunicaciones
- Electrónica de red
- Programación

Lógicas

- Sistemas operativos
- Protocolos
- Aplicaciones
- Configuración
- Incumplimiento

Humanas

- Desconocimiento
- Falta de concienciación
- Desentendimiento
- Ingenuidad
- Sabotaje / traición

- Error de diseño
- Tampering
- Error de configuración
- Error de validación de entrada
- Salto de directorio
- Seguimiento de enlaces
- Inyección de comandos en el sistema operativo
- Secuencias de comandos en sitios cruzados (XSS)
- Inyección SQL
- Inyección de código
- Desbordamiento de búfer
- Agotamiento de búfer
- Formato de cadena
- Errores numéricos
- Gestión de credenciales
- Permisos, privilegios y/o control de acceso
- Políticas inadecuadas
- Fallo de autenticación
- Carácter criptográfico
- Falsificación de petición en sitios cruzados (CSRF)
- Condición de carrera
- Revelación de contraseña
- Error en la gestión de recursos
- Revelación/Filtrado de información

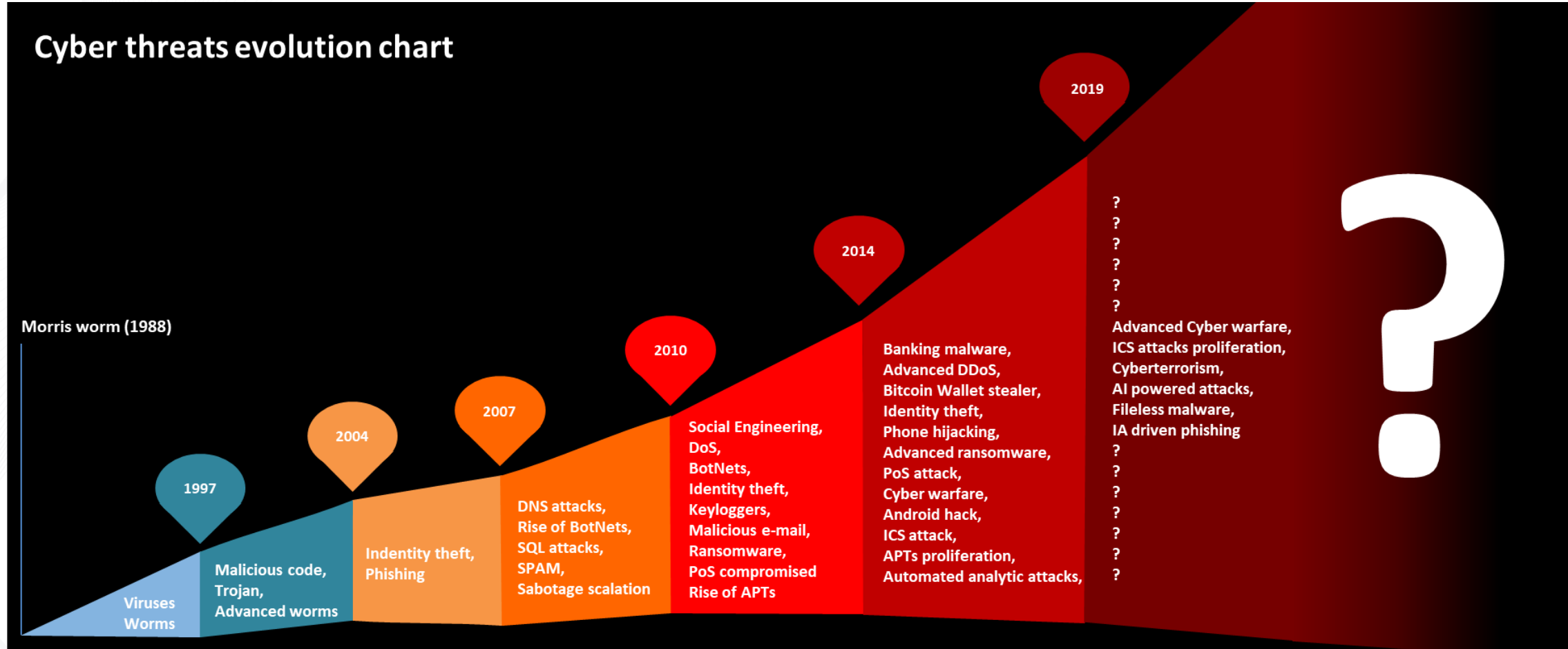
Ciberspacio, nuevo campo de batalla

Amenaza muy heterogénea



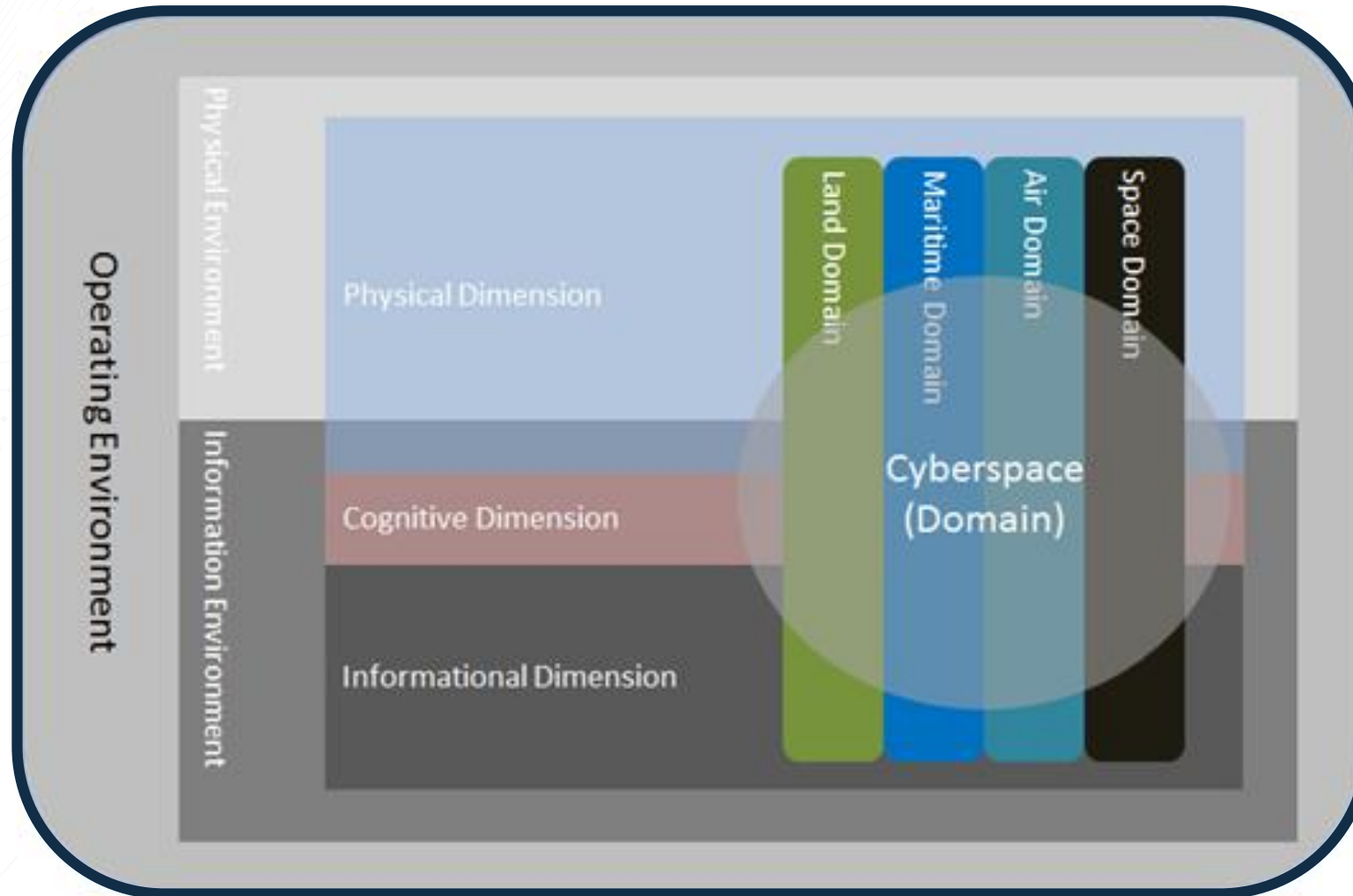
Ciberspacio, nuevo campo de batalla

Amenaza en continua y muy rápida evolución



Ciberspacio, nuevo campo de batalla

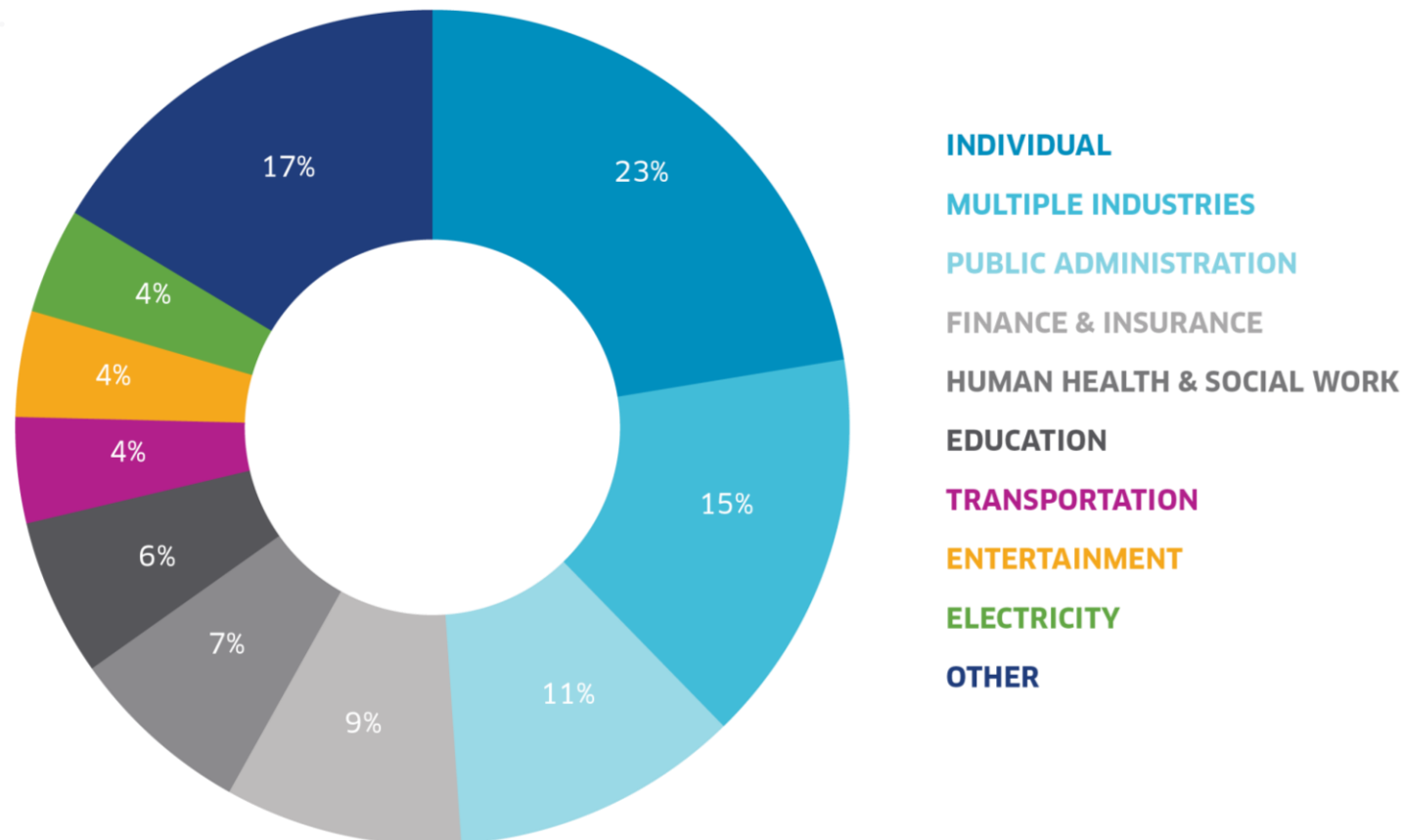
Transversalidad



Ciberspacio, nuevo campo de batalla

Afecta a todos los sectores de actividad

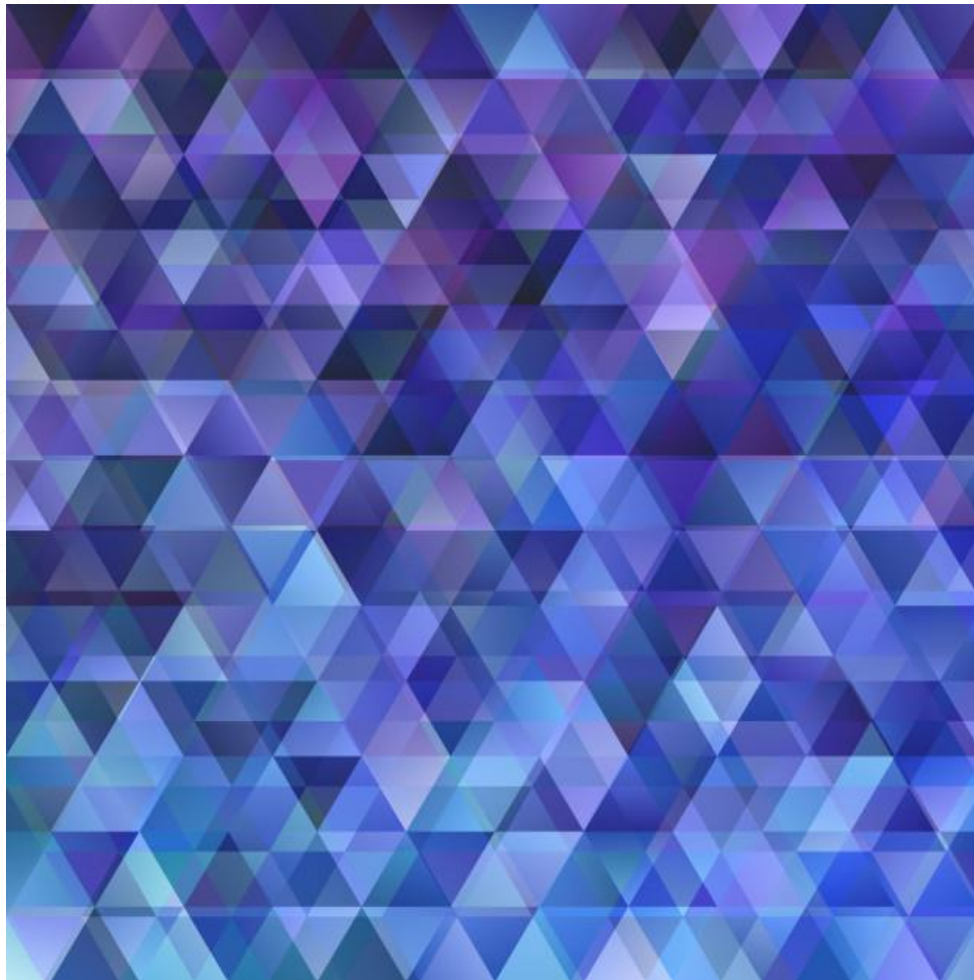
Distribution of Targets: March 2018



Fuente: <https://www.hackmageddon.com/2018/04/19/march-2018-cyber-attacks-statistics/>

Ciberspacio, nuevo campo de batalla

Opacidad



- Desconocimiento del adversario:
 - Capacidades.
 - Intenciones.
- Carencia de alerta previa.
 - No cambios de alistamiento.
 - No movimientos de tropas.
 - No actividades logísticas.
- Bandera falsa, anonimización.
- Difícil comprensión situacional.
- Compleja gestión de las crisis.

Ciberespacio, nuevo campo de batalla

Diferente marco espacio-tiempo



Ciberspacio, nuevo campo de batalla

Armamento muy peculiar



- Efectividad incierta.
- Utilidad efímera.
- Un solo uso (?).
- Efectos colaterales impredecibles.

Ciberspacio, nuevo campo de batalla

Bajo coste / Elevada eficacia



Ciberspacio, nuevo campo de batalla

Asimetría



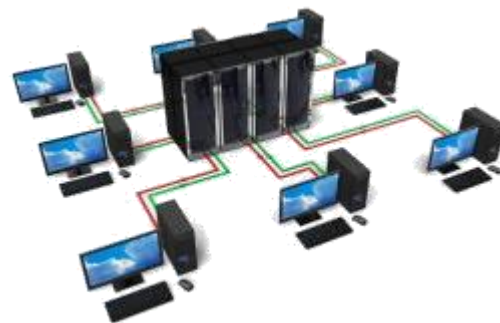
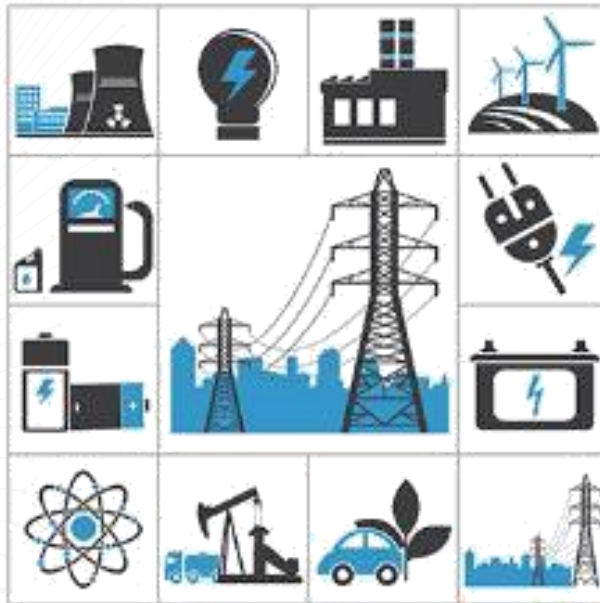
Ciberspacio, nuevo campo de batalla

Tecnología vs Elemento humano



Ciberspacio, nuevo campo de batalla

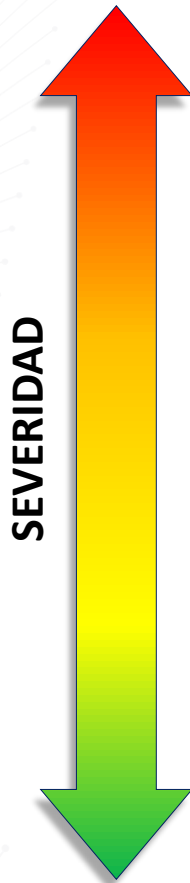
Muy amplio espectro de objetivos



Ciberspacio, nuevo campo de batalla

Muy variadas formas de actuación

Posibles acciones contra el adversario



Ataque contra la integridad de los datos que produce daños físicos o víctimas.

Ataque contra la integridad de los datos (sin daños físicos / víctimas).

Denegación de Servicios (DoS / DDoS)

Exfiltración (robo de datos / ciberespionaje)

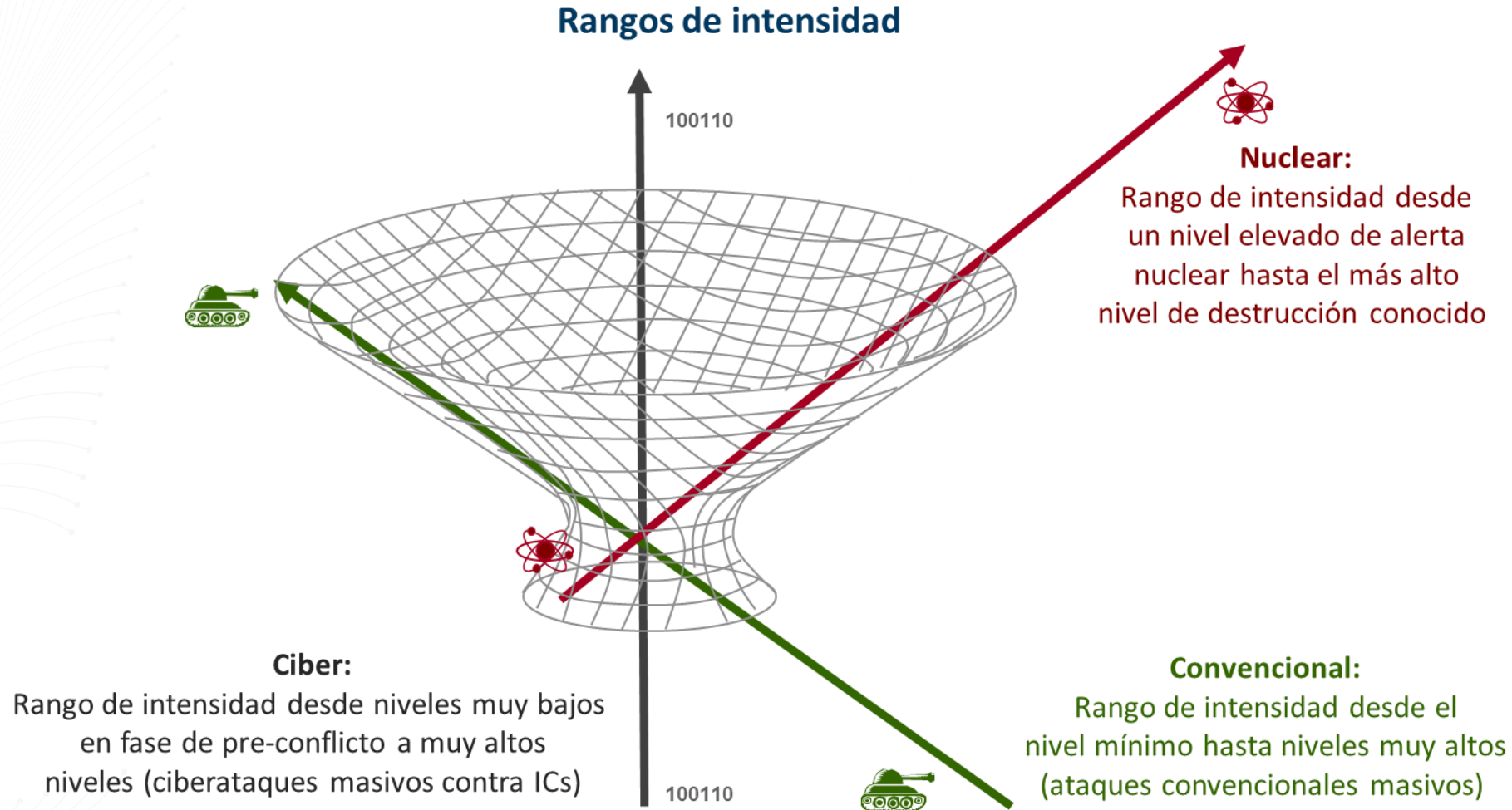
Infección

Reconocimiento intrusivo

Reconocimiento no intrusivo

Ciberespacio, nuevo campo de batalla

Muy amplio rango de efectos



Ciberspacio, nuevo campo de batalla

Compleja integración de lo ciber en la COP

Ámbito ciber vs Ámbitos físicos

Attribute	Physical Environment	Cyber Environment
Location	Latitude, Longitude	IP-Address
Speed	Air and ground in mph	Mbps or Gbps through communications links
Path	Roads, Rails, Flight Path, Sea-lanes	Links, Connections
Terrain	Hills, Valleys, Urban Canyons	Operating Systems, Disk Drives, Routers, Switches, Memory Devices, "thumb-drives"
Environment	Rain, Snow, Thunderstorms, Hurricanes	Condition of the links/nodes, protocols ¹² , speeds of the internet "highways", threats to existence



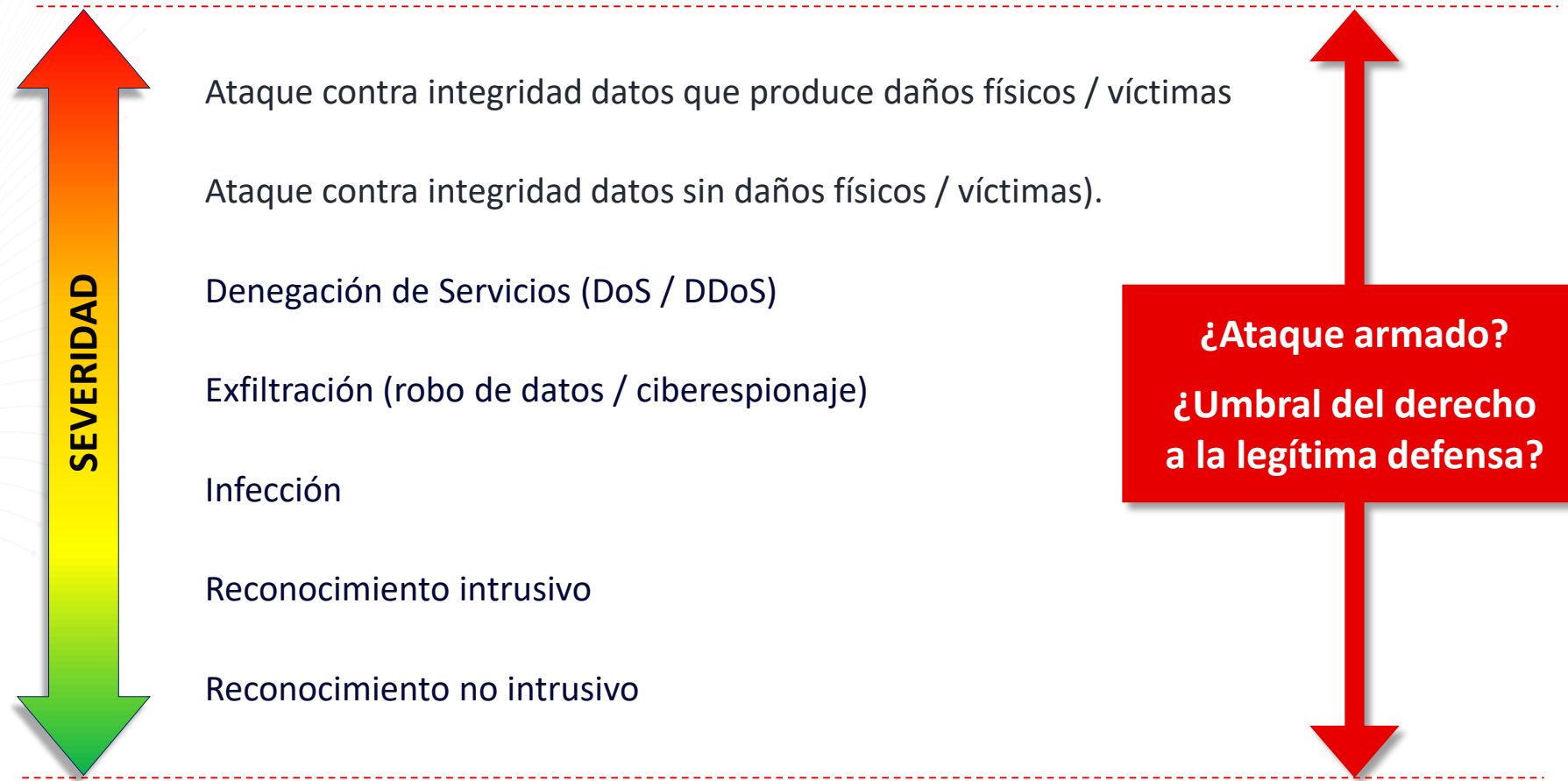
Ciberspacio, nuevo campo de batalla

Muy complejo marco legal



Ciberspacio, nuevo campo de batalla

Complejidad de la respuesta



Ciberspacio, nuevo campo de batalla

Complejidad de la respuesta

Efectos colaterales sobre terceros actores

Interconexión creciente



90% infraestructuras en poder de compañías privadas

Ciberspacio, nuevo campo de batalla

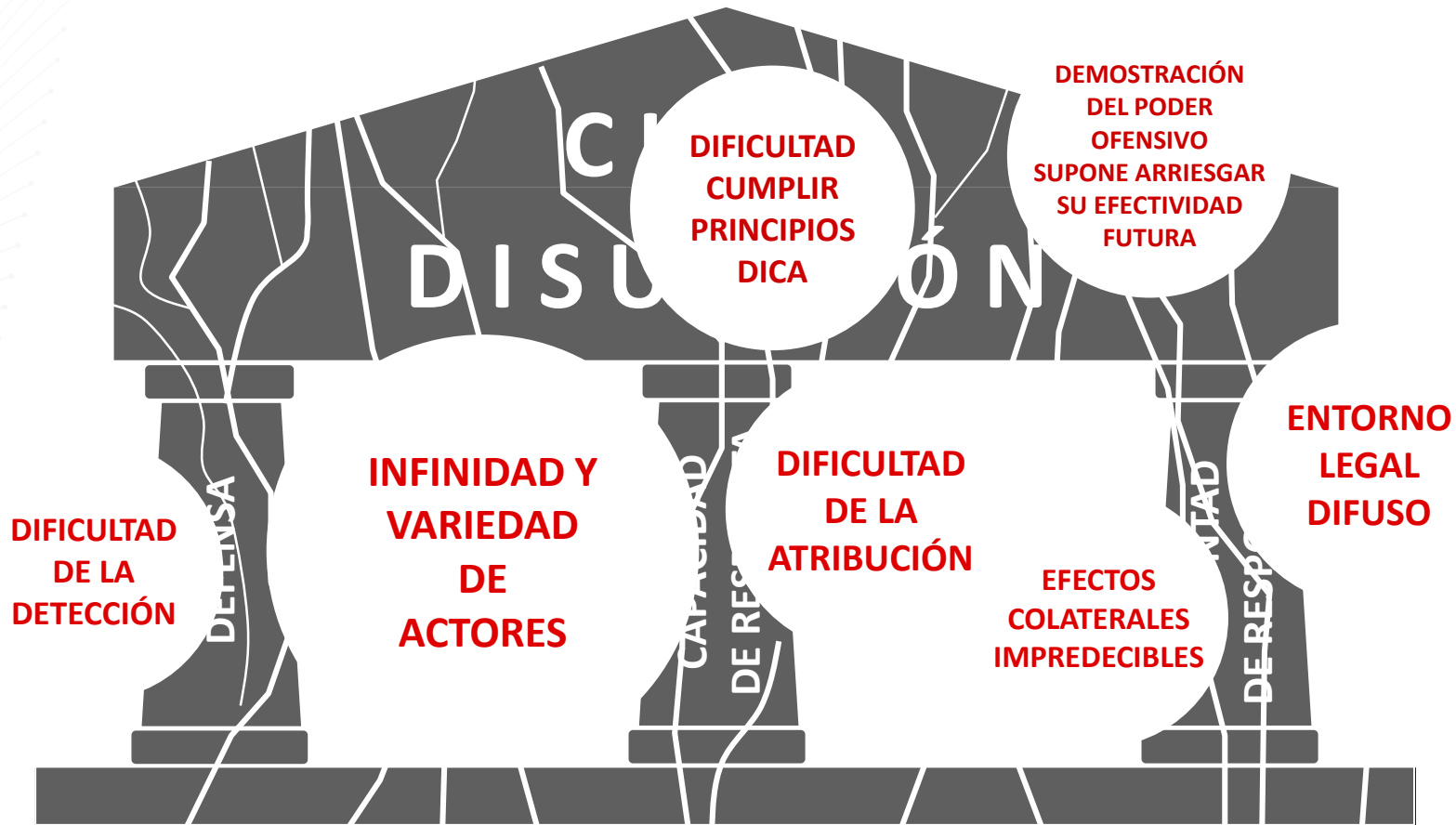
Complejidad de la respuesta

La demostración de capacidades ofensivas supone arriesgar su efectividad futura



Ciberspacio, nuevo campo de batalla

Ineficacia de la disuasión



La dimensión ciberespacial de los conflictos



La dimensión ciberespacial de los conflictos



La dimensión ciberespacial de los conflictos



WWW.ONEMAGAZINE.ES

NEWSLETTER

NEWS BUSINESS ONE HACKER MOTOR TECH LIFESTYLE



¿Ha sufrido Ucrania el primer ciberataque energético de la historia?

JOSÉ M. VERA

Viernes 08 de enero de 2016, 09:12h

europa **press**

Ucrania acusa a Rusia de un ciberataque contra el principal aeropuerto de Kiev

Publicado 18/01/2016 11:26:57 CET

KIEV, 18 Ene. (Reuters/EP) -

El principal aeropuerto de Kiev ha sufrido un ciberataque de un servidor ruso, según ha informado este lunes un portavoz del Ejército ucraniano. Por su parte, el Equipo de Respuesta de Emergencias Informáticas (CERT-UA) ha advertido de la posibilidad de nuevos ataques.

La dimensión ciberespacial de los conflictos

Guerra híbrida y ciberespacio



La dimensión ciberespacial de los conflictos

infobae

Martes 24 de Enero de 2017 AMÉRICA ARGENTINA TENDENCIAS TKM

🔍 "El Chapo" en EEUU Trump Presidente PWA y APP móvil Crisis en Venezuela Estado Islámico Especiales Data

MUNDO

La "doctrina Gerasimov": cómo hace Rusia para reclutar hackers de élite para su ciberguerra

Desde hace al menos tres años Moscú inició una intensa campaña para incorporar programadores a firmas controladas por el Ejército, que luego son utilizadas para tareas de espionaje

30 de diciembre de 2016



El General Valery V. Gerasimov, creador de la doctrina que lleva su nombre (AFP)

EL ESPAÑOL

ESPAÑA

OPINIÓN

MUNDO

ECONOMÍA

CIENCIA

CULTURA

INICIO ► MUNDO

EUROPA

AMÉRICA

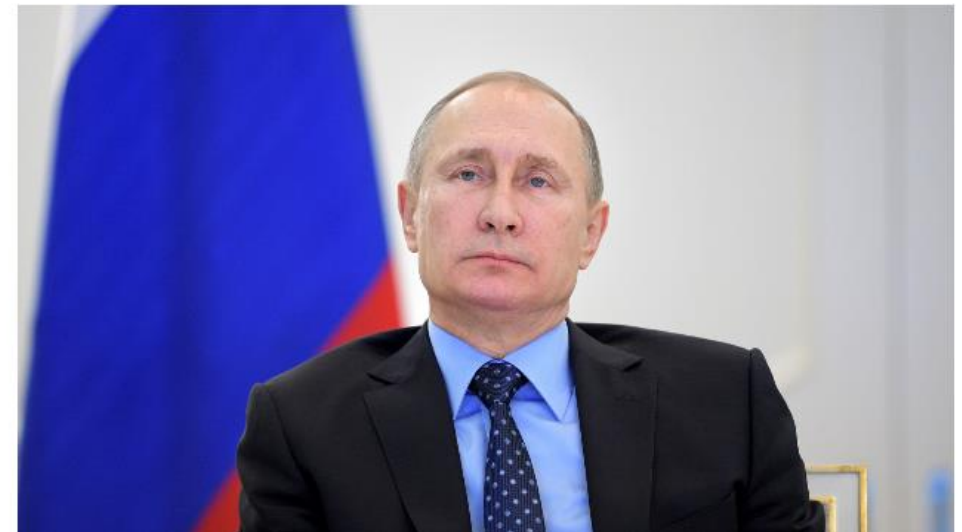
ORIENTE PRÓXIMO

ÁFRICA

ASIA

Europa y sus elecciones, objetivo de la ciberguerra rusa

Holanda, Francia y Alemania serán nuevos escenarios de intervención para el ciberespionaje ruso, según los expertos.



La dimensión ciberespacial de los conflictos

naked security by SOPHOS

Soldiers sent hate-SMS messages from rogue base stations

12 MAY 2017

by [John E Dunn](#)



Somebody has been bombarding Ukrainian soldiers with SMS messages – and they aren't nice ones, either.

According to evidence collected by Associated Press (AP), soldiers fighting pro-Russian separatists in the east of the country have received a steady stream of mystery propaganda texts since 2014, around the time the conflict started.

Examples can be viewed in Cyrillic or in English. As a flavour from November 11 2015:

Who is robbing your family while you are paid pennies waiting for your bullet?

Or a few days later:

Murderer from the Ukrainian Armed Forces. The East won't forgive you and the West won't remember you!

La dimensión ciberespacial de los conflictos



NEWS

NATO: Russia targeted German army with fake news campaign

Emails accusing German soldiers stationed in Lithuania of rape were sent to local news outlets and the parliamentary president. NATO officials allege that Russia is targeting the military alliance.



Ciberejércitos

Sun, Sep 16, 2018

Newsweek

SIGN IN SUBSCRIBE >

TECH & SCIENCE

CYBERWAR: HOW CHINESE HACKERS BECAME A MAJOR THREAT TO THE U.S.

BY DOROTHY DENNING ON 10/5/17 AT 7:00 AM



Ciberejércitos



Corea del Norte cuenta con un ciberejército de 7.000 hackers, según Seúl

Ante la "amenaza" que supone esta situación, el Ejército surcoreano ha decidido incrementar también su personal especializado en ciberseguridad desde los actuales 600 efectivos hasta un millar.

Redacción

11 de mayo del 2015 - 8:25 PM



Ciberejércitos

SUNDAY EXPRESS

Iranian hackers STEAL top secret information on nuclear power and cybersecurity

IRANIAN hackers have stolen sensitive British information on nuclear power and cybersecurity from UK universities, it has been revealed.

By LAURA MOWAT

PUBLISHED: 10:01, Sat, Sep 15, 2018 | UPDATED: 10:09, Sat, Sep 15, 2018

Ciberejércitos

Venezuela tiene el mayor ciberejército de América para defender al régimen

El régimen de Nicolás Maduro cuenta con al menos 500 personas dedicadas a la desinformación y manipulación



Por Sabrina Martín

— El Oct 24, 2019

NOTICIAS

RELACIONES INTERNACIONALES

SUR AMÉRICA



El país suramericano ocupa el puesto número 11 de las naciones con más personal sistematizado en tareas de esa índole en todo el mundo. (Kremlin)

Ciberejércitos

El cibercomando de Estados Unidos ya está operativo



TWITTEAR



COMPARTIR



ENVIAR

Por [jjvelasco](#) el 8 de noviembre de 2010, 12:04

El USCC coordinará y dirigirá las operaciones relativas a la defensa de las **redes de información** y se preparará para ejecutar acciones militares (ciberataques) en casos de guerra o en caso de ataque contra Estados Unidos, sus intereses o sus aliados. Dado su carácter transversal, estará formado por distintas unidades de las fuerzas armadas norteamericanas, sumando unos noventa mil efectivos.



Ciberejércitos

FRANCIA DEFENSA

Francia aumentará en 800 efectivos su ejército ante la amenaza terrorista

06/04/2016 15:07

París, 6 abr (EFE).- El presidente de Francia, François Hollande, decidió hoy reforzar los efectivos de su ejército ante la amenaza terrorista, que se traducirá en la creación neta de cerca de 800 puestos suplementarios en los tres próximos años en unidades operativas y de ciberdefensa.

Ciberejércitos

INTERNACIONAL

Martes, Abril 26, 2016

Alemania creará unidad de defensa cibernética en sus Fuerzas Armadas



Según explicó la ministra de Defensa, Ursula von der Leyen, la unidad contará con 13.500 efectivos.

Ciberejércitos

Israel potencia su unidad de ciberdefensa

Martes 11 de diciembre de 2012, 00:00h

El Ejército israelí ha lanzado una campaña para reclutar expertos en ordenadores para ampliar la Unidad 8200.

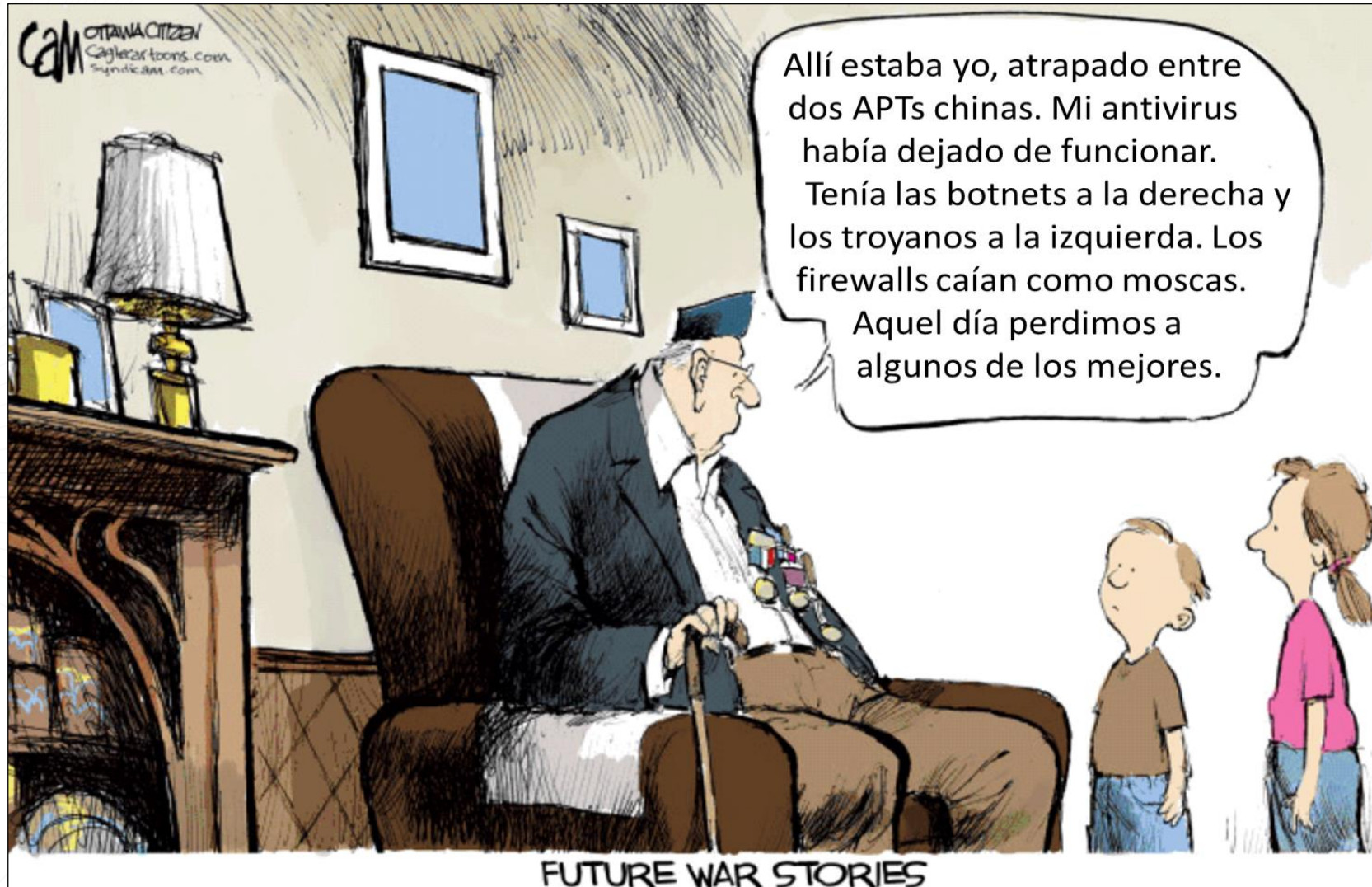
El Ejército israelí ha lanzado una campaña para reclutar expertos en ordenadores para ampliar la Unidad 8200, una organización altamente secreta que, supuestamente, estaría tras de los ataques cibernéticos contra Irán.

La ciberdefensa tiene prioridad en el actual plan quinquenal de desarrollo militar, a pesar de los recortes en defensa, habiéndose presupuestado 320 millones de dólares para el programa del Ejército de ciberdefensa, ya que la cibertecnología es un nuevo arma de guerra y para defenderse contra ella se debe dominar este nuevo campo, que es uno de los pilares del plan israelí de defensa.

Conclusiones

- Ciberespacio consolidado como ámbito de las operaciones militares.
- Ámbito muy peculiar:
 - Transversal.
 - Opaco.
 - Infinidad de actores (estatales y no).
 - Ineficacia de la disuasión.
- Todas las naciones están desarrollando capacidades para operar en el ciberespacio.
- El elemento humano cualificado/especializado es esencial.
- La cantidad también cuenta (efectivos, presupuesto).
- La importancia del ciberespacio en el devenir de los conflictos será cada vez mayor.

Preguntas





COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

CCN-cert
centro criptológico nacional