

CiberSeguridad

Nociones básicas y aproximación militar

Viernes, 13 de Abril de 2018

Objetivos de la sesión

1. Introducir el concepto de “ciberseguridad” y relacionarlo con otros conceptos relacionados
2. Desmitificar (o explicar algunas de) las noticias que nos llegan relativas a la ciber-seguridad y la ciber-defensa
3. Introducir algunas propuestas para protegernos mejor

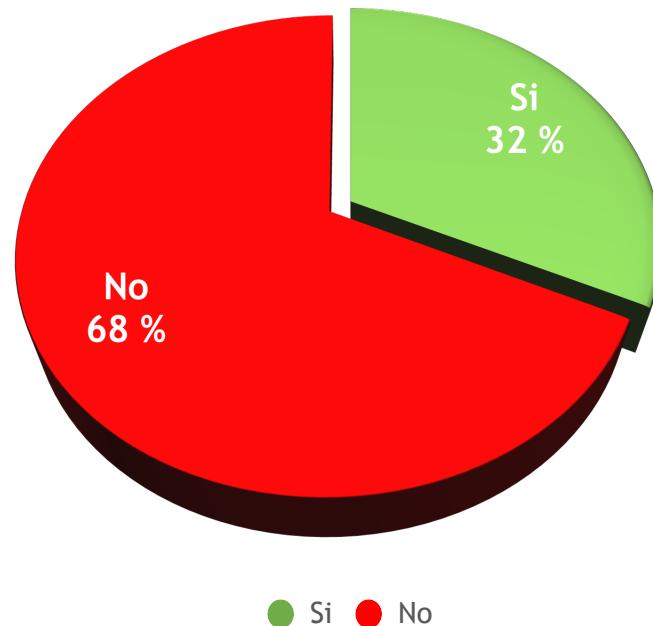
Vídeo introductorio

Concienciación (1/7)

- La seguridad de la información **NO** es parte activa de nuestra sociedad
- A pesar de ello, esta tiene:
 - Serias implicaciones en los negocios:
 - Competencia, espionaje industrial, competitividad
 - Serias implicaciones en la vida personal:
 - Seguridad y Privacidad
 - **Serias implicaciones en la vida de un país y en su defensa nacional:**
 - Nuevos vectores de riesgo, nuevas amenazas globales y nuevos tipos de conflictos (generalmente asimétricos)

Concienciación (2/7)

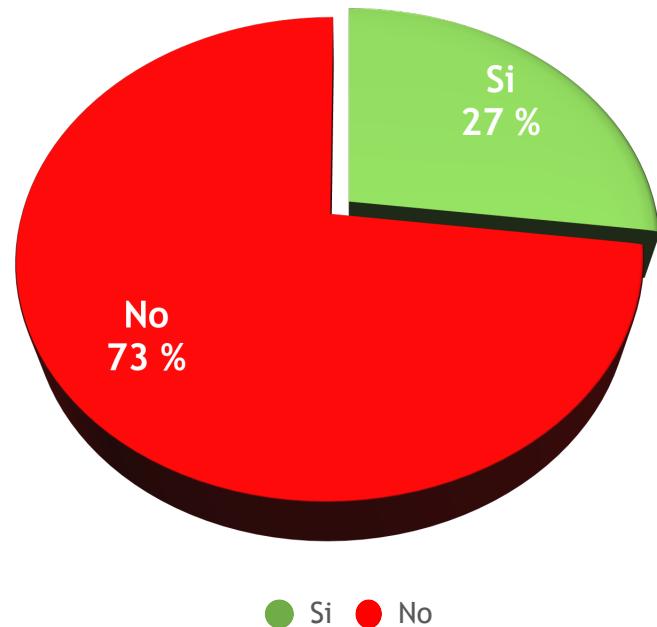
Personas que han recibido algún curso en materia de seguridad, seguridad de la información y/o ciberseguridad



Fuente: Savitz Research for ESET

Concienciación (3/7)

Personas que han recibido algún curso en materia de seguridad, seguridad de la información y/o ciberseguridad RELACIONADO CON REDES SOCIALES



Fuente: Harris poll for ESET

Concienciación (4/7)

- Los principales vectores de riesgo son:
 - Acceso no autorizado a información
 - Perdida de acceso a recursos y sistemas de información
 - Perdida de información
 - Corrupción de información
 - Robo de información
 - Ventaja informational (inteligencia)
 - Infoxicación

Concienciación (5/7)

- Los principales implicaciones son:
 - Empresas:
 - Perdida de beneficios
 - Perdida del negocio
 - Cuestiones de propiedad industrial, patentes y marcas
 - Multas, demandas judiciales
 - Publicidad negativa (salir en los titulares)
 - Sobrecostes

Concienciación (6/7)

- Los principales implicaciones son:
 - Personas:
 - Robo y suplantación de identidad
 - Bullying (acoso)
 - Pérdida de privacidad
 - *Intromisión en la intimidad de las personas*
 - Pérdida/robo de datos sensibles
 - Cuestiones de propiedad intelectual, patentes y marcas

Concienciación (7/7)

- Los principales implicaciones son:
 - **Los 3 poderes del Estado, FFyCCSE y FFAA:**
 - Intromisión en la vida de un país (por terceros)
 - Mediante alteración de datos e información (infoxicar)
 - Valiéndose de operaciones psicológicas (PsyOps)
 - **Acceso a datos clasificados**
 - Nuevos modelos de guerra electrónica (SIGINT) :
 - Basados en la informática y las redes de datos (COMINT)
 - Basados en la electrónica y las emisiones electromagnéticas (EM ~ ELINT)

Situación de partida

- Las organizaciones manejan **datos e información de diferentes tipos y niveles de criticidad**
- Cada día más **procesos**, de toda índole, **dependen de la informática**
 - Informática: mecanización de procesos de gestión de información

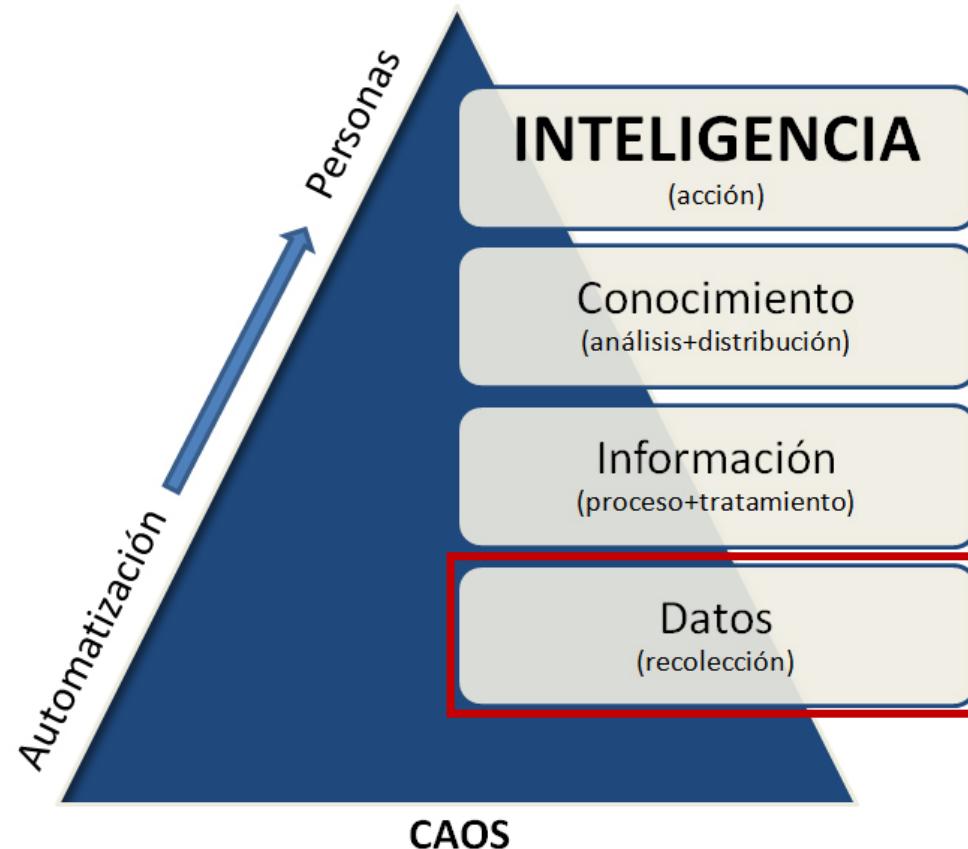
Datos, ¿qué son?

- El término “dato” proviene del latín "datum" cuyo significado es "lo que se da"
- Un dato es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa
- **Los datos describen hechos empíricos, sucesos y entidades**
- En informática, los datos alimentan todos los sistemas; **el dato es la unidad minima de procesamiento de información**

Información ¿qué es?

- La RAE dice que información es
 - “*5. f. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.*”
- *En información y documentación, la “información” es el resultado del tratamiento de datos*

Pirámide informacional



Ciber + Seguridad

Ciber-[] ¿a qué se refiere?*

- Etimología:

Término del griego clásico → *κυβερνητική*



- Refiere a “*kybernētēs*” (timonel) y se interpreta como el arte de gobernar una nave
- Otras referencias más cercanas:
 - Cibernética: Norbert Wiener, 1948, tratado de automática
 - Ciberespacio: William Gibson, 1984, novela “Nuromante”

Sobre la seguridad

- Según su definición:
 - RAE define “seguridad” como aquella situación
“libre o exenta de todo daño o riesgo”

Sobre seguridad de la información

- Según su definición:
 - Normas internacionales como ISO/IEC 27001 (ISMS) definen esta como:

“El conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.”

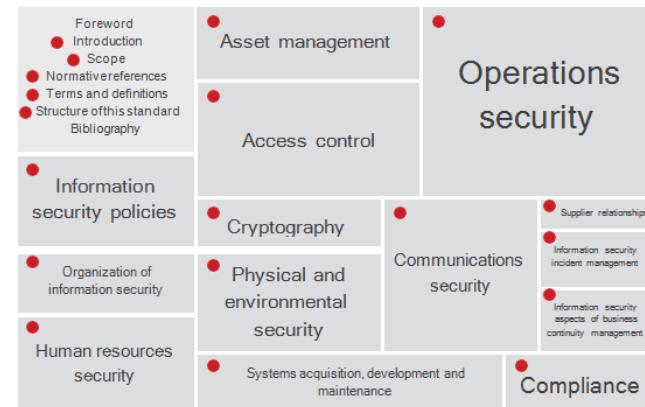
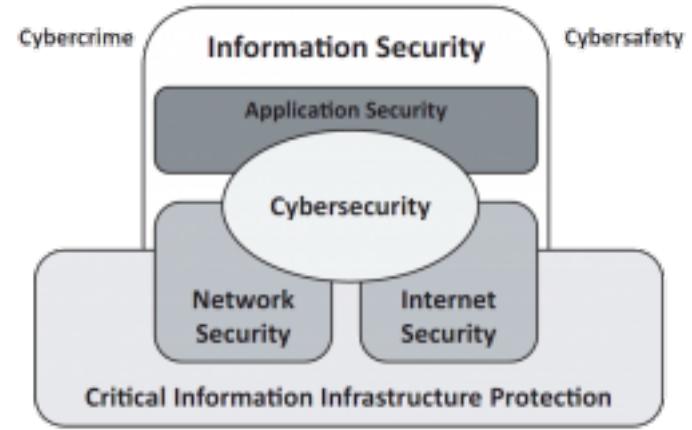
Sobre la ciberseguridad

- Según su definición:
 - ISACA define “ciberseguridad” como

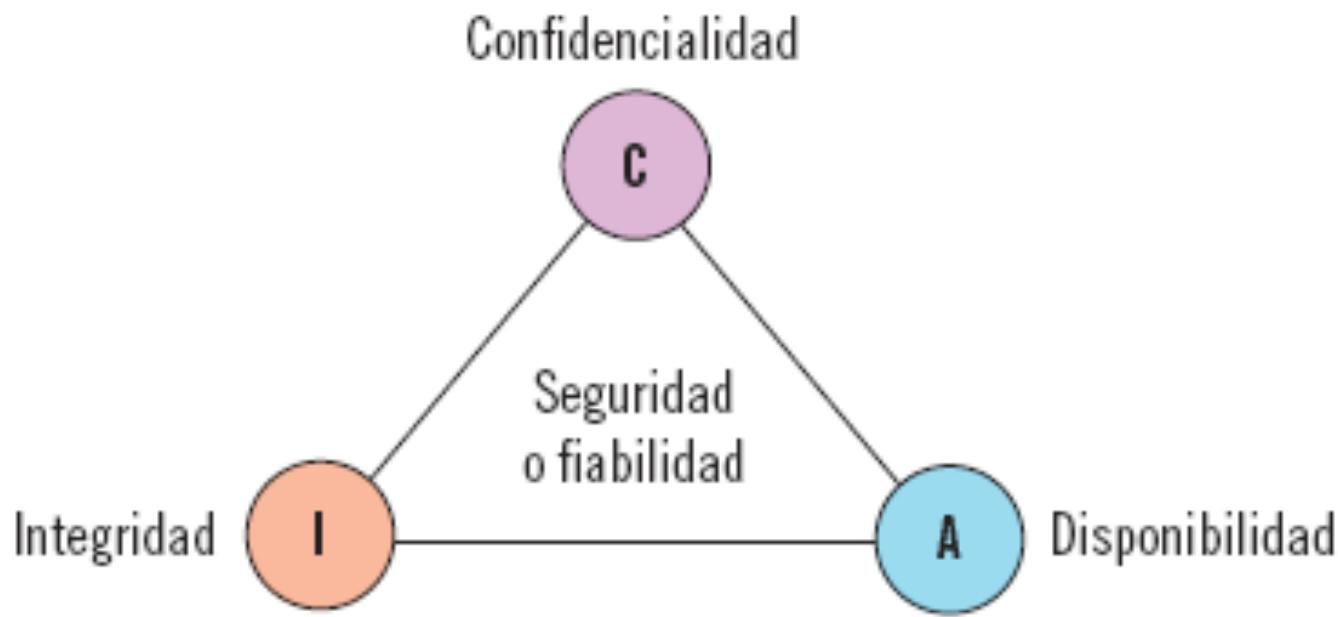
“la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”

Relación existente entre seguridad <-> ciberseguridad

- La **seguridad de la información** es un concepto más amplio, más general
- La **ciberseguridad** se enfoca en proteger la información en un entorno “ciber” o entorno “conectado”

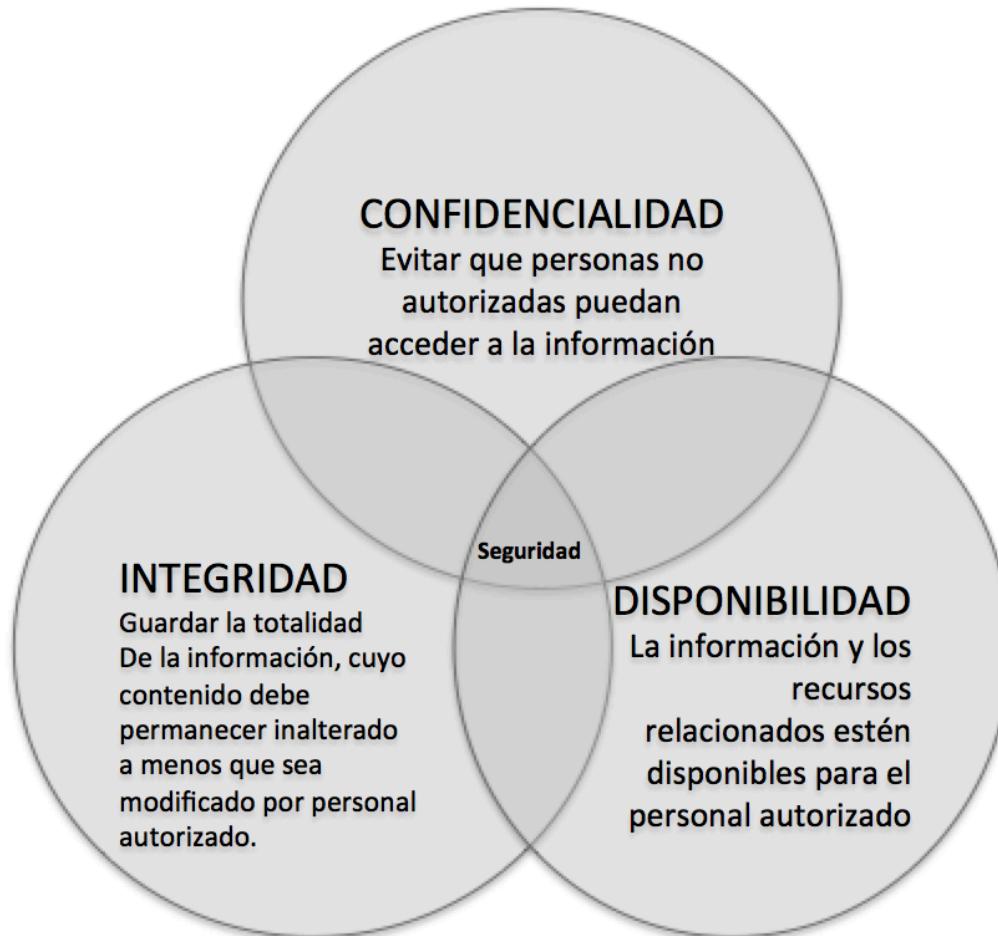


Seguridad de la Información



$$\text{Seguridad} = \text{Confidencialidad} + \text{Integridad} + \text{Disponibilidad}$$

Seguridad de la Información



PRIVACIDAD

Privacidad, ¿qué es?

- La RAE la define como:

“2. f. Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.”

- Pero en lo que refiere a la ciberseguridad esta queda mejor definida como:

“El control sobre la información relativa a un usuario, que se ve afectada por el intercambio de datos con servicios propios de las redes como lo es Internet”

Privacidad, ¿como nos afecta?

CNN politics 45 CONGRESS SECURITY THE NINE TRUMP/AMERICA 2018

f t g s

US military reviewing security practices after fitness app reveals sensitive info

By Joshua Berlinger and Maegan Vazquez, CNN
Updated 1514 GMT (2314 HKT) January 29, 2018



0:47 / 2:10

NOW PLAYING: Fitness app reveals troops info

New strains on U.S. bases in Japan

Rescue mission underway for US service members

Is the A-10 headed for the graveyard?

Navy launch

Nathan Ruser @Nrg8000 Follow

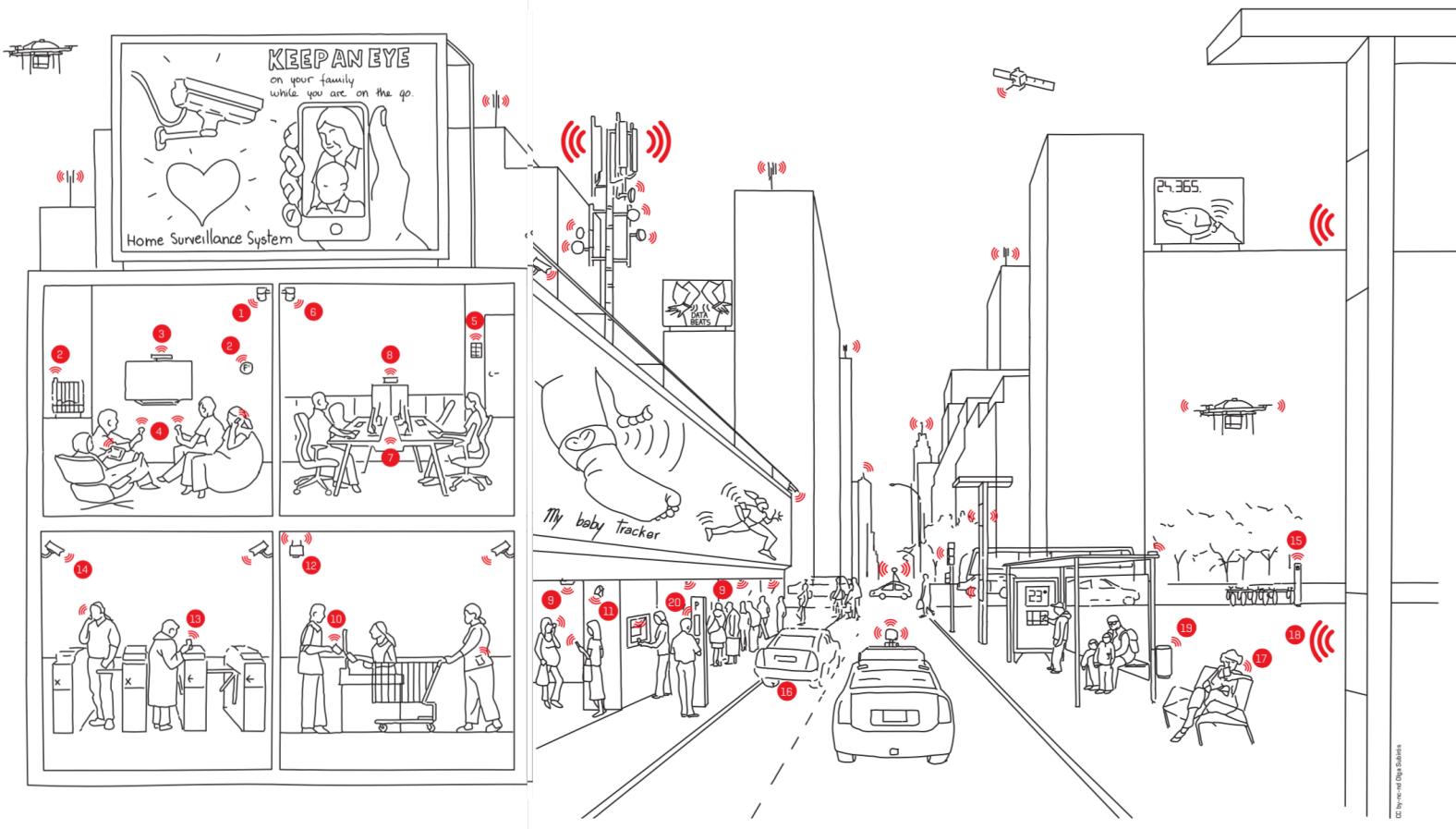
Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). medium.com/strava-engineer/... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable



7:24 PM - 27 Jan 2018

Privacidad, ¿qué hacer?

- Restringir tecnología personal en el entorno laboral y viceversa
 - Pulseras de actividad, móvil, GPS, cámaras de fotos, etc, tokens criptográficos,
- Restringir la información en los perfiles públicos de servicios contratados, gratuitos y de redes sociales.
 - Usar credenciales/passwords fuertes
- Utilizar sistemas informáticos seguros y siempre tener un respaldo
 - Sistemas operativos siempre parcheados y con antivirus
 - Copias de seguridad frecuentes



En casa: (1) videovigilancia doméstica, (2) contadores de luz y termostato, (3) televisiones inteligentes, (4) consolas de videojuegos

En el trabajo: (5) control de accesos biométrico, (6) videovigilancia, (7) monitorización remota, (8) bases de datos personales

En los espacios comerciales: (9) sensor de cuenta de personas, (10) tarjetas inteligentes, (11) iBeacons, (12) redes Wi-Fi gratuitas

En el transporte urbano: (13) abonos de transporte publico, (14) videovigilancia en andenes públicos, (15) redes de bicicletas publicas, (16) automóviles inteligentes y no inteligentes

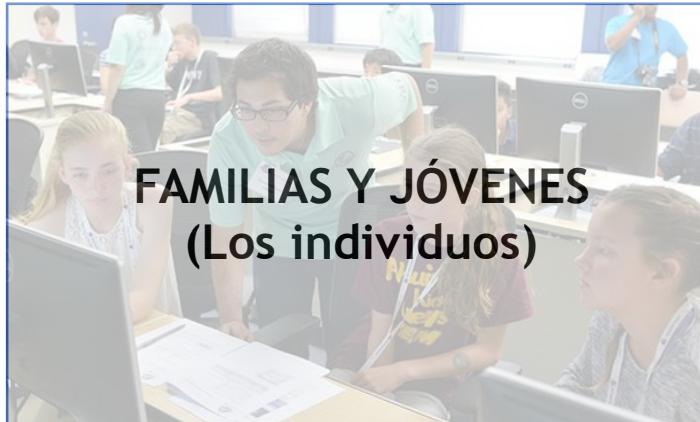
En la calle: (17) telefonía móvil, (18) cámaras térmicas y sensores sonoros, (19) movilidad urbano-inteligente y (20) sistemas de parking y cajeros automáticos / inteligentes / quioscos de servicios



**EMPRESAS Y ENTORNOS
CORPORATIVOS**
(Gran empresa)



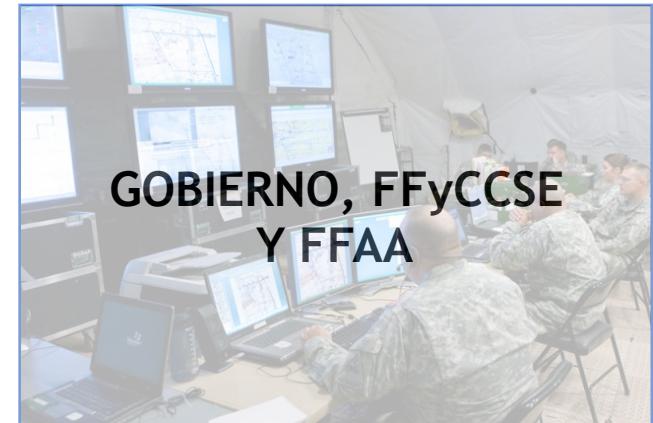
INDIVIDUOS Y PYMES
(Pequeña empresa)



FAMILIAS Y JÓVENES
(Los individuos)



**SISTEMAS INDUSTRIALES
E INFRAESTRUCTURAS
CRITICAS**



**GOBIERNO, FFyCCSE
Y FFAA**

La ciberseguridad es más que un individuo aislado que explota las vulnerabilidades de un sitio remoto



VS



99%

1%

Ese 1% no tiene las capacidades que se le atribuyen

Todos incidentes de ciberseguridad están coordinados; Son grupos, nunca lobos solitarios



EEUU National Security Agency (NSA)
(COMSEC & SIGINT)



UK Government Communications Headquarter
(SIGINT & Information Assurance)



Israel Unit 8200
Ha'Man, IDF
(SIGINT Corps)



NATO Communications & Information Agency



Joint Staff Department of the Central Military Commission
(Electronic Warfare)



Rusia Main Intelligence Directorate (GRU)
(6th Dir. SIGINT)

Todos incidentes de ciberseguridad están coordinados; Son grupos, nunca lobos solitarios



The Lulz Raft



LulzSec



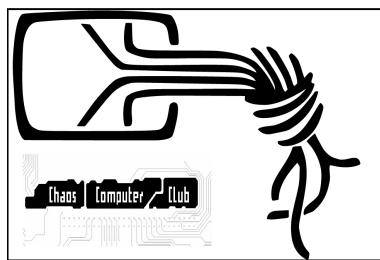
Máscara de Guy Fawkes



Anonymous



Tarh Andishan (Irán)



Otros: https://en.wikipedia.org/wiki/Category:Hacker_groups



Shadow Brokers

Idea fuerza

Todos los eventos de (ciber)seguridad responden a dos factores:

- Interés
- Oportunidad

INTERES	OPORTUNIDAD	
	NO	SI
NO	✗	✗
SI	✗	✓

The Adaptive Defense Security Model

UNDERSTANDING THE ATTACK

ATTACKERS UTILIZE MULTIPLE VECTORS
AND MULTIPLE FLOWS TO COMPLETE THEIR MISSION

EXPLOIT & CALLBACK

EXTERNAL RECON

IDENTIFY PEOPLE,
PLACES & THINGS

INITIAL COMPROMISE

GAIN INITIAL ACCESS
INTO TARGET

MALWARE & CALLBACK

ESTABLISH FOOTHOLD

STRENGTHEN POSITION
WITHIN TARGET

MAINTAIN PRESENCE

INTERNAL RECON

MOVE LATERALLY,
IDENTIFY TARGET DATA

DATA EXFILTRATION

COMPLETE MISSION

PACKAGE & STEAL
TARGET DATA

DETECTING THE EXPLOIT IS KEY SINCE EVERY PHASE AFTER THAT CAN BE ENCRYPTED BY THE ATTACKER

Buenas prácticas en el ciberespacio (Oficina, Viajes, Hogar)



Usar contraseñas seguras, robustas y custodiarlas con rigor



Mantener todas las aplicaciones de software y anti-virus al día



Entrar al sistema con los privilegios mínimos. Evitar navegar como administrador



No dejar las sesiones abiertas. Siempre hacer el *logout* de las sesiones



Comunicar cualquier actividad sospechosa al administrador de sistemas



No hacer click sobre enlaces. Siempre escribir la URL en el navegador y forzar <https://>



No confiar en dispositivos ajenos ni en WiFi's públicas, aunque requieran de contraseña



No ignorar los avisos del navegador sobre certificados digitales



No enviar información del trabajo al email personal ni viceversa



No descargar aplicaciones sin verificar su certificado, ni si quiera a móviles o tablets

NEED COFFEE!!



Ciberseguridad y Ciberdefensa

Ciber: Nuevo “campo de batalla”

- Desde que el hombre es hombre han existido conflictos, desarrollados en diferentes dominios de combate (tierra, mar, aire, espacio)
- Las naciones están interesadas en dominar el nuevo entorno, el entorno “ciber” o “ciberespacio”
 - Todo es nuevo, específico, sin demasiado control
 - Todo es distinto: es artificial, infinito, sin fronteras
 - Hay infinidad de partes interesadas (no solo ejércitos)
- En este entorno se combate por la información:
 - Defender la propia
 - Atacar la de otros

Características ciberespacio

- Entorno virtual sin límites geográficos
- Escasa seguridad por diseño (TCP/IP)
- Se desarrollan actividades vitales para la sociedad
 - *Existe una dependencia de la informática*
- Presencia de delincuencia, terrorismo y espionaje
 - *Búsqueda de beneficio económico, anonimato, acceso a información sensible o importante*
- Pero... ¿existen conflictos armados? Y.. ¿existe control armamentístico?
- Estas acciones, ¿están sujetas a la ley o hay anonimato?

Definición del ciberespacio

- DOCTRINA OTAN

NATO CyberDefense Taxonomy and Definitions (2014)

- Es un dominio global formado por sistemas TIC y otros sistemas electrónicos.
- Se incluye en esta definición también la interacción entre sistemas, la información que es almacenada y la que es transmitida.

Amenazas en el ciberespacio

- Los más importantes:

- Ciberguerra
- Cibercrimen
- Ciberespionaje
- Hacktivismo

Guerra Vs Ciberguerra (1/2)

- **Guerra:** lucha armada entre dos o más naciones o entre bandos de una misma nación
 - Escenarios:
 - Espacio Terrestre
 - Espacio Marítimo
 - Espacio Aéreo
 - Espacio Exterior (España no tiene)
 - Espacio CiberEspacio

Guerra Vs Ciberguerra (2/2)

- **Ciberguerra:** hace referencia al desplazamiento de escenario de un conflicto, que toma el ciberespacio y las tecnologías de la información como teatro de operaciones
- Persigue: generar alteraciones en la información del enemigo, incluidos sus sistemas de procesamiento, a la vez que se protege la información propia de los sistemas ofensivos del atacante/enemigo.

Quienes son los actores (1/3)

- **Estados:** la amenaza más peligrosa:
 - Tienen recursos, personal y tiempo
 - Conducen operaciones directamente o a través de terceros (mercenarios tecnológicos)
- **Actores transnacionales:** Organizaciones formales o informales no ligadas a fronteras nacionales
 - Pueden ejercer su “hacktivismo” o acciones terroristas haciendo uso del ciberespacio

Quienes son los actores (2/3)

- **Organizaciones criminales**
 - No tienen fronteras
 - Persiguen lucro (beneficio económico)
 - Pueden prestar servicios (como mercenarios tecnológicos) a estados o actores transnacionales.

La mayor cantidad de las acciones sufridas en el ciberespacio se debe a este tipo de actor

Quienes son los actores (2/3)

- **Actores individuales o pequeños grupos**
 - Pueden tener motivaciones diversas
 - Generalmente “demostrar capacidad”
 - Pueden prestar servicios al resto de actores y organizaciones

Son los menos representativos

Asimetría con los actores

- Ciberarmas:
 - Bajo coste de producción
 - Elevada eficacia
 - Son difíciles (imposibles) de trazar
- Ejércitos tradicionales:
 - No ven en rango de igualdad la situación
 - Pueden no estar preparados para responder

España: Marco legal y normativo

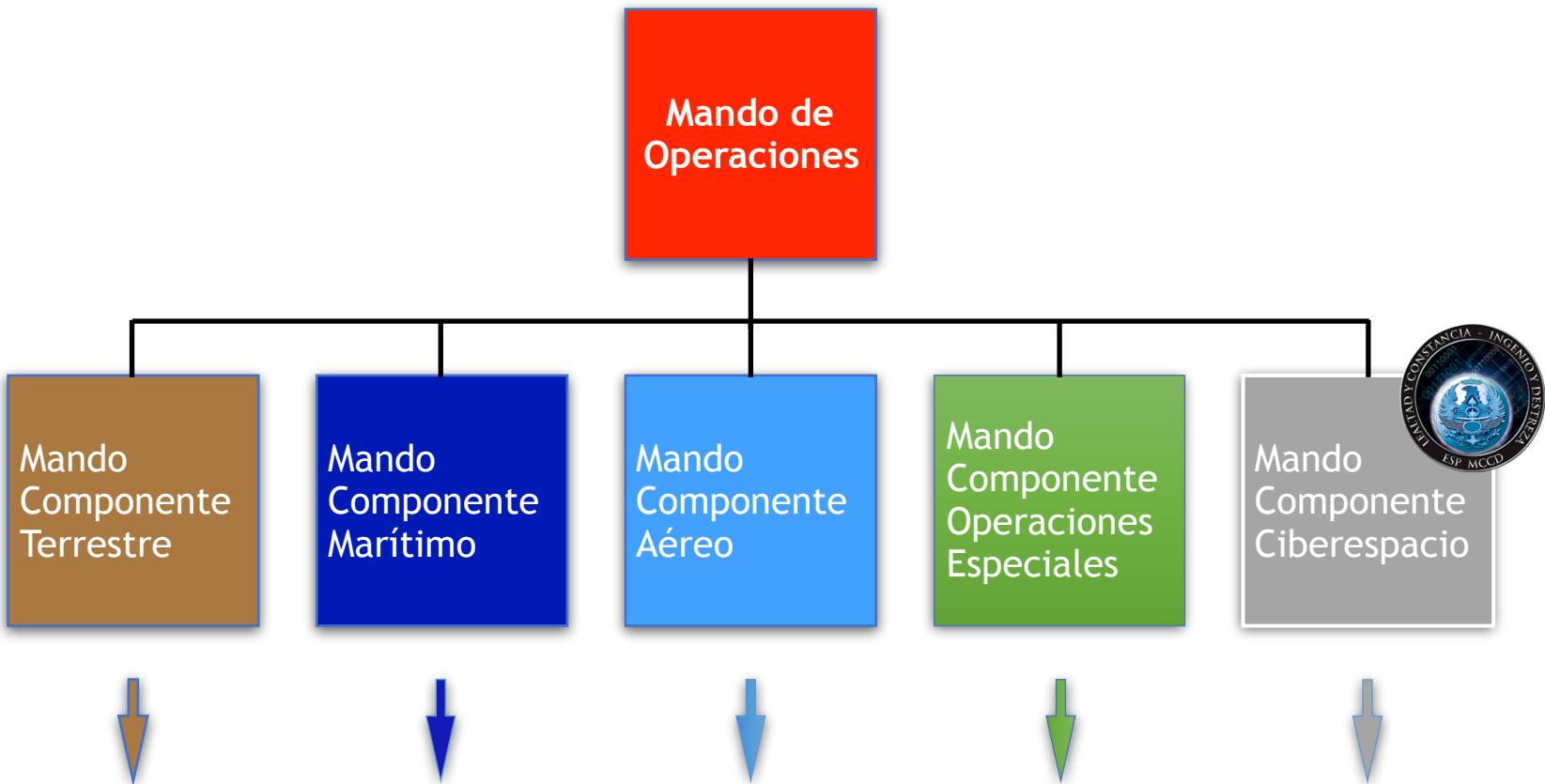


España: MCCD. Cometidos.



- RD 872/2014 (Organización de las FAS) → MCCD
 - Acciones de ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudieran ser encomendadas.
 - Operaciones en el exterior de nuestras FAS
 - Agregadurías militares
 - Respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Estructura operativa MCCD



OBJETIVOS OPERACIONALES

Operaciones militares (1/3)

- MCCD PERSIGUE LA GENERACIÓN DE EFECTOS EN EL CIBERESPACIO:
 - Se persigue mermar, reducir o anular las capacidades de los sistemas de información de sus objetivos:
 - Confidencialidad (confidentiality)
 - Integridad (integrity)
 - Disponibilidad (availability)

Operaciones militares (2/3)

- Una **OPERACIÓN MILITAR** en el ciberespacio es:

“una operación en la que se emplean capacidades ‘ciber’ con el objetivo de alcanzar objetivos militares en el ciberespacio o a través de él”

Operaciones militares (3/3)

- Un **ATAQUE ARMADO** en el ciberespacio es:

“una acción originada en el ciberespacio en la que se producen daños a personas u objetos”

Esta definición está relacionada con el concepto legal de **AUTODEFENSA (DE LOS ESTADOS)** en el derecho internacional.

Area de operaciones CIBER (1/2)

- Area fija:
 - Redes y Sistemas de información (CIS) de consideradas “Territorio Nacional”:
 - Ministerio de Defensa
 - Despliegues de las FAS en operaciones en el exterior
 - Las que se encomienden al MCCD por mandato legal

Area de operaciones CIBER (2/2)

- Area variable:
 - La parte de ciberespacio de interés militar, necesario para:
 - Desarrollar operaciones específicas
 - Responder a amenazas o agresiones que afecten a la Defensa Nacional

**NO SE PUEDE ABORDAR TODO EL CIBERESPACIO,
NI PARA DEFENSA NI PARA ATAQUE.**

Planeamiento de operaciones (1/2)

- Igual que operaciones de otros componentes o dominios
 - No hay una forma diferente de hacer las cosas por ser un entorno “cibernético”
- Se planean todas las acciones en conjunto con otros componentes o dominios
- Generalmente, se integran dentro de operaciones comunes a todos los niveles:
 - táctico
 - operacional
 - estratégico

Planeamiento de operaciones (2/2)

- **Búsqueda de objetivos / CyberTargeting**
 - Selección y priorización de objetivos
 - Definición de efectos a producir en ellos
- **Selección de armamento / CyberWeaponeering**
 - Determinación de cantidad y tipo de ciberarmamento a utilizar en función del efecto deseado sobre los objetivos

Tipos de operaciones (1/3)

- **Operaciones Defensivas**

- Objetivo: mantener la libertad de acción, evitando impacto en confidencialidad, integridad y disponibilidad de la información y los sistemas que la albergan
- Comprende: protección, monitorización, análisis y respuesta a actividades no autorizadas en sistemas de información propios.
- Tipos:
 - *Permanentes*: sobre sistemas del M. de Defensa
 - *En misión*: para proteger un sistema específico bajo una amenaza definida

Tipos de operaciones (1/3)

Capacidades defensivas

- **Preventivas.** Tareas:

- Seguridad física, control de accesos, control de emanaciones electromagnéticas, actualizaciones de HW, SW, AV/AM, etc...
- Securización de sistemas, análisis de vulnerabilidades, formación y adiestramiento del personal, sistemas de alerta temprana, formación y concienciación de seguridad

- **Proactivas.** Tareas:

- Inspecciones y auditorías, monitorización de sistemas y redes, test de penetración

- **Reactivas.** Tareas:

- Gestión de incidentes de seguridad, restauración de sistemas, análisis forense, acciones legales (si hay atribución)

Tipos de operaciones (2/3)

- Operaciones de Explotación
 - Objetivo(s):
 - Obtención de información de los sistemas de adversarios
 - Obtención de información de orígenes de ataques a sistemas propios
 - Tipos:
 - OSINT (Inteligencia de Fuentes abiertas)
 - Reconocimiento pasivo del objetivo (fingerprinting)
 - APT (penetración y exfiltración permanente de datos de los objetivos)

Tipos de operaciones (3/3)

- **Operaciones Ofensivas**

- Objetivo(s):

- Degradar, interrumpir, denegar o destruir sistemas de información (**Mando y Control**) de un objetivo, o la información en sí misma.

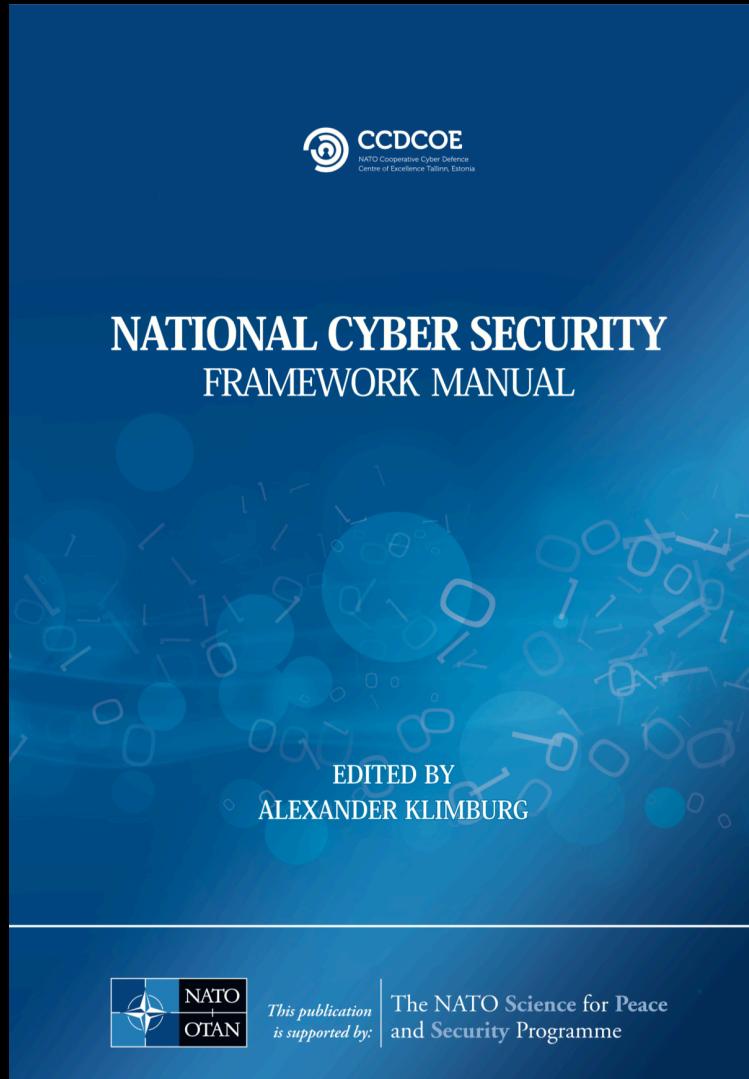
- Requiere:

- Sincronización con las acciones en otros dominios para alcanzar objetivos militares asignados
 - Operaciones de Explotación previamente ejecutadas para la consecución de los objetivos con éxito

Legislación / Normativa

- **Tratados internacionales** → SI
 - Tanto en tiempo de paz como en tiempo de conflicto
 - No hay tratados específicos para el ciberespacio
 - Hay grupos de trabajo en la ONU pero no hay consenso entre los países
 - Por ahora, solo existe como referencia el “**Manual Tallin**”
 - Legislación internacional aplicable a la ciberguerra.

Manual “Tallin”



Legislación / Normativa

- Cuestiones de soberanía
 - Los estados ejercen control sobre las “ciber-infraestructuras” y las actividades dentro de su territorio soberano (Manual Tallin)
 - Por lo tanto:
 - Los estados son responsables, ante terceros, del uso de sus infraestructuras en tiempo de conflicto

ius ad bellum (1/2)

Justicia antes de la guerra; legislación en tiempo de paz

- En España
 - Código penal → **penas de prisión**
 - Acceso no autorizado
 - Interrupción no autorizada
 - Aplicable tanto en el país de origen, los de paso, como el de destino final del ciberataque

ius ad bellum (2/2)

Justicia antes de la guerra; legislación en tiempo de paz

- Derecho Internacional
 - Carta de Derechos Humanos de Naciones Unidas
 - Prohibe el uso de la fuerza, excepto en dos supuestos:
 - Por decisión del Consejo de Seguridad: para mantener y restaurar la paz y seguridad
 - A través de su Artículo 51: reconoce el uso de la fuerza en *autodefensa* en caso de *ataque armado*
 - *Caso de daño a personas u objetos*

ius in bellum

Justicia en tiempos de guerra

- Aplicable Derecho Internacional Humanitario
 - Regula el uso de la fuerza
 - Exige discriminación clara entre objetivos militares y civiles
 - Fuerza la proporcionalidad en los daños; no pueden ser excesivos
 - Debe de responder a una necesidad militar justificada
 - Debe de preservar la vida de la población y de las infraestructuras civiles

Operaciones - Ejemplos (1/5)

- Red October (~2007 / se desconoce si esta en activo todavía)
 - Tipo de operación: ofensiva
 - Objetivo: agencias diplomáticas y gobiernos de todo el mundo
 - Efectos provocados: exfiltración de información
 - Vector de ataque: phishing via email
 - Categoría: ciberespionaje
 - No es un acto de guerra

Operaciones - Ejemplos (2/5)

- Estonia, Tallin (2007)
 - Tipo de operación: ofensiva
 - Objetivo: activos de la red de administración del estado
 - Efectos provocados: Denegación de servicio (DDoS)
 - Vector de ataque: botnets (+170 países)
 - Categoría: cibersabotaje
 - No es un acto de guerra

Operaciones - Ejemplos (3/5)

- Buckshot Yankee (2008)
 - Tipo de operación: ofensiva / defensiva
 - Objetivo: Departamento de Estado EEUU
 - Efectos provocados: Exfiltración de información
 - Vector de ataque: llave de memoria USB “abandonada” en un parking
 - Categoría: ciberespionaje
 - No es un acto de guerra

Operaciones - Ejemplos (4/5)

- Georgia, región de Osetia del Sur (2008)
 - Tipo de operación: ofensiva
 - Objetivo: Activos en la red de administración del estado de Georgia
 - Efectos provocados:
 - Denegación de servicio (DOS / DDoS)
 - Desvío de tráfico informático a través otros servidores
 - Vector de ataque:
 - Botnets
 - Toma de control (en remoto) de servidores
 - **Categoría: ciberataque dentro de un conflicto armado y previo a una ofensiva militar (en guerra con Rusia)**
 - **Esto SI es un acto de guerra**

Operaciones - Ejemplos (5/5)

- Irán (2010)
 - Tipo de operación: ofensiva
 - Objetivo: instalaciones nucleares
 - Efectos provocados:
 - Malfunción de las centrifugadoras de una planta de enriquecimiento de uranio
 - Retraso de dos (2) años en el programa nuclear iraní
 - Vector de ataque: llave de memoria USB “abandonada” en un aparcamiento (troyano Stuxnet)
 - Categoría: cibersabotaje
 - No es un acto de guerra

Knowing is not understanding.

There is a great difference between knowing and understanding: you can know a lot about something and not really understand it.

(Charles Kettering)

Muchas gracias