II Foro de Ciberseguridad y Ciberdefensa 2015

Nuevos retos y perspectivas en Latinoamérica

Fundación IN-NOVA Centro de Innovación

Los retos y desafíos del **ciberespacio** en el ámbito de la **Seguridad** y la **Defensa**

FUNDACIÓN IN-NOVA - ESPAÑA

D. SAMUEL ÁLVAREZ – SECRETARIO GENERAL

Contenido

- Introducción. Contexto general.
- Conceptos básicos del entorno.
- Antecedentes. Un poco de génesis
- Los principales ataques y sus tecnologías asociadas.
- Datos y cifras reales de los últimos años.
- Concepto operativo de la Ciberdefensa
- **Los principales retos y desafíos**
  - Tecnológicos
  - Humanos
  - Organizativos

Introducción. Contexto general

La sociedad actual se ha vuelto muy **dependiente** de las Tecnologías e Información y Comunicaciones (TIC). Conectamos personas, pero también "cosas".

Mayor riesgo de interrupción económica, social, y física debido a las **vulnerabilidades que estas tecnologías intrínsecamente** poseen.

Nueva disciplina **Ciberdefensa** dentro del marco de la Ciberseguridad o seguridad de las TIC (STIC). **Nuevo *leit motiv***.

Varias naciones ya han comenzado a obtener capacidades de Ciberdefensa. La posibilidad de "**ciberconflictos**" ha dejado de ser una hipótesis.

Introducción. Contexto general

Fuerzas Armadas (FAS) inmersas en un proceso de adaptación al concepto Network Enable Capability (NEC) → incrementar sus capacidades de mando y control.

Sistemas con dispositivos de proceso → incrementan la capacidad de combate, pero también pueden convertirse en vulnerabilidades.

Ciberseguridad - Ciberdefensa

Fundación IN-NOVA Centro de Innovación

CIBERSEGURIDAD (STIC)

- "La capacidad de proteger la su integridad, confidencialidad, disponibilidad de la información procesada, almacenada o transmitida por los sistemas TIC, así como autenticidad de sus componentes y la trazabilidad de sus acciones".

CIBERDEFENSA

- "La capacidad de proteger la prestación y gestión de los servicios TIC en respuesta tanto a potenciales como efectivas acciones maliciosas originadas en el ciberespacio".

Ciberseguridad - Ciberdefensa

Ciberseguridad - Ciberdefensa

Ciberdefensa

- Subconjunto de la anterior, que tiene lugar en la **fase operativa** y se materializa mediante los ciberataques y su defensa.

Ciberseguridad

- Centrada en la defensa y **protección de sus redes** frente a intrusiones en las mismas. Incluye medidas tanto preventivas como reactivas.

ASPECTO	CIBERSEGURIDAD	CIBERDEFENSA
Ciclo de vida del Sistema de Incidentes Sucesos	Comprende todas las fases	Fase de operación
	Fortuitos y maliciosos	Maliciosos
	Desastres naturales y ciberataques	Ciberataques

CIBERESPACIO

Definición:

Conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos, junto con los usuarios que interactúan con estos sistemas.

Composición:

capas **física**, **lógica** y **social**

Características:

Anonimato.

No tiene fronteras definidas.

Falta de regulación.

Escaso coste de las acciones en relación con otros dominios.

Alcance para todas las personas de manera sencilla.

Construido a base de tecnologías inseguras en su diseño.

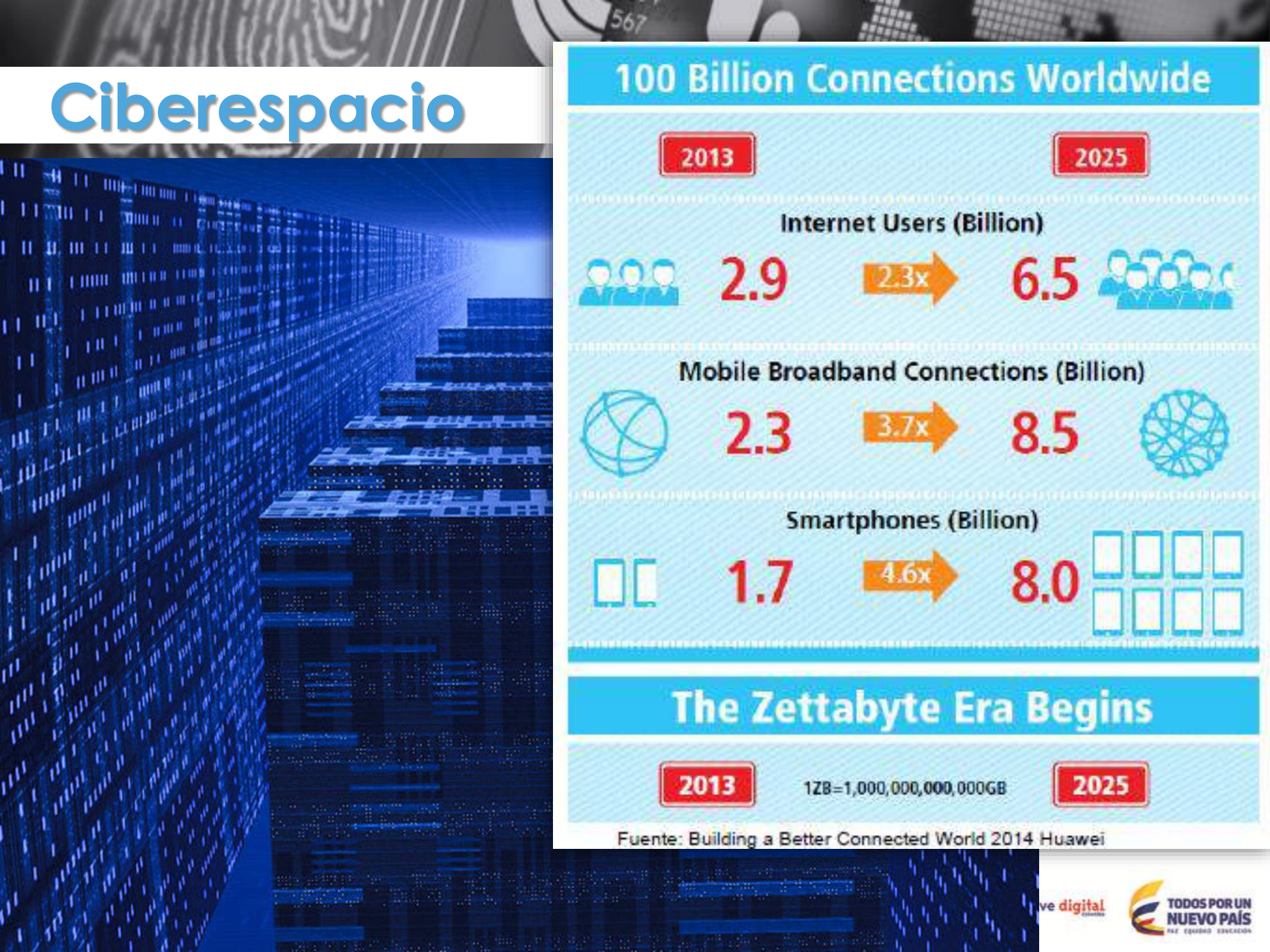
Un gran TABLERO DE JUEGO. Y creciendo:

Relación entre la población mundial y el uso de Internet por regiones del planeta

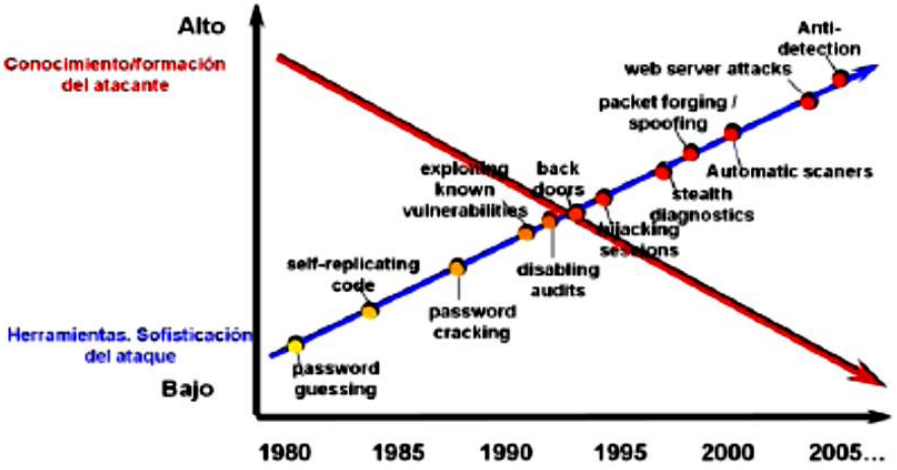
WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2014 - Mid-Year Update						
World Regions	Population (2014 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2014	Users % of Table
Africa	1,125,721,038	4,514,400	297,885,898	26.5 %	6,498.6 %	9.8 %
Asia	3,996,408,007	114,304,000	1,386,188,112	34.7 %	1,112.7 %	45.7 %
Europe	825,824,883	105,096,093	582,441,059	70.5 %	454.2 %	19.2 %
Middle East	231,588,580	3,284,800	111,809,510	48.3 %	3,303.8 %	3.7 %
North America	353,860,227	108,096,800	310,322,257	87.7 %	187.1 %	10.2 %
Latin America / Caribbean	612,279,181	18,068,919	320,312,562	52.3 %	1,672.7 %	10.5 %
Oceania / Australia	36,724,649	7,620,480	26,789,942	72.9 %	251.6 %	0.9 %
WORLD TOTAL	7,182,406,565	360,985,492	3,035,749,340	42.3 %	741.0 %	100.0 %

Fuente: Internet World Stats. ttp://www.internetworldstats.com/stats.htm

Ciberespacio



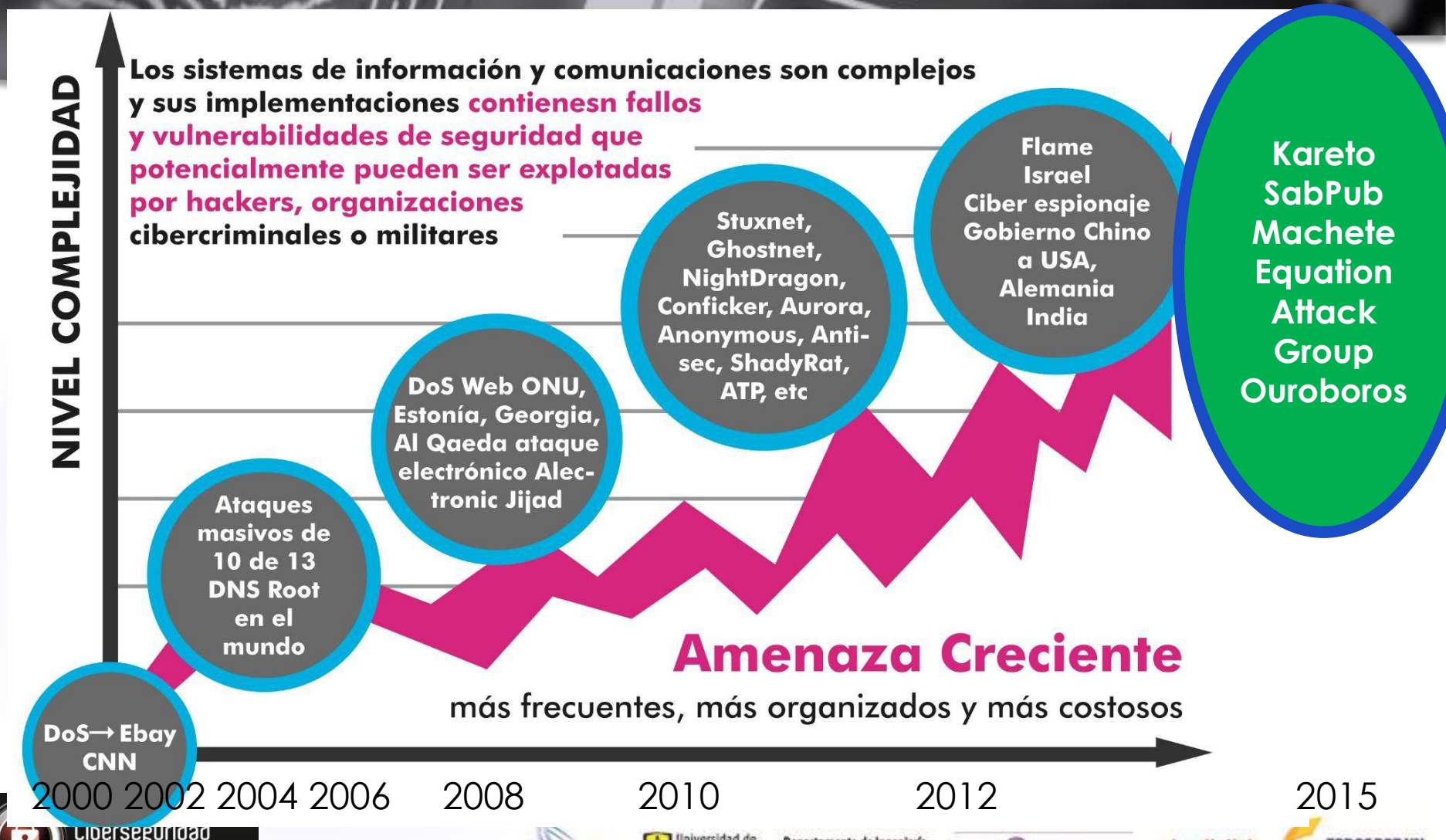
Amenazas conocidas



- Guerra asimétrica
- Irrupción de ciberactivistas y ciberterroristas.
- Nuevos tipos de amenazas:
  - Amenazas Persistentes Avanzadas (APT, APA).
  - Subversive Multi-Vector Threats (SMT).
  - Advanced Evasion Techniques (AETs).

La identificación de estas amenazas es clave para poder protegerse de las mismas, así como lo es el intento de predicción de futuras amenazas todavía desconocidas

Antecedentes. Haciendo memoria…

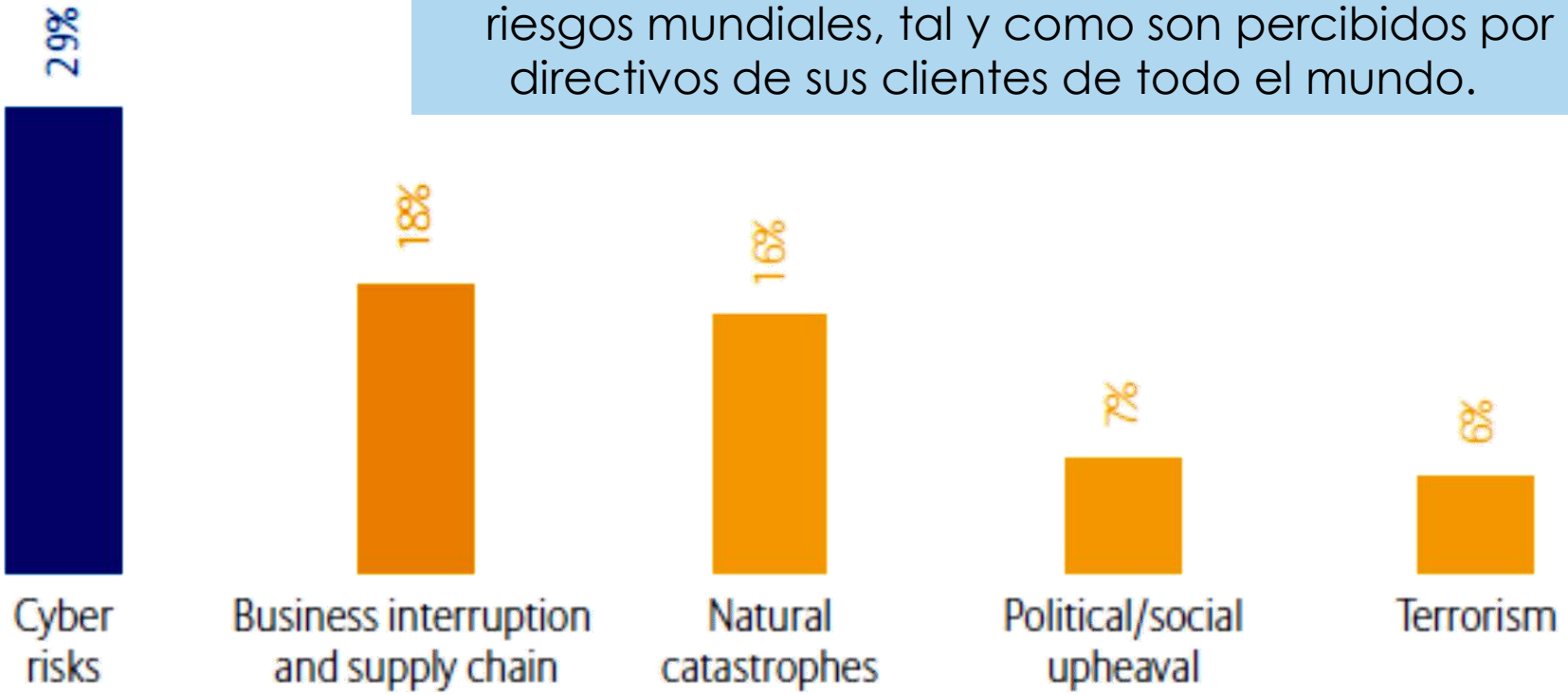


Tendencias futuras para el 2016

- Ciberespionaje
- Los ataques como servicio
- Fusión de técnicas y procedimientos utilizadas por el ciberespionaje y la ciberdelincuencia
- Estabilización de los ataques hacktivistas.
- Herramientas de ataque para dispositivos móviles (principalmente ANDROID)
- El "secuestro" de organizaciones por ransomware.
- Incremento de los ataques contra Cajeros Automáticos y procedimientos de pago.
- Ataque contra infraestructuras críticas

Análisis de Riesgos Mundiales 2014

ALLIANZ desarrolló en 2014 un estudio relativo a los riesgos mundiales, tal y como son percibidos por los directivos de sus clientes de todo el mundo.



Histórico de ciber-agresiones entre estados

1982 Logic Bomb. Desde EEUU. Agredido: Rusia
Objetivo: gaseoducto soviético

1998-2000 Moonlight Maze. Desde Rusia (piratas informáticos). Agredidos: EEUU
Objetivo: sistemas informáticos del pentágono, NASA, Departamento de energía

2003-2005 TITAN RAIN. Desde China. Agredido: EEUU
Objetivo: sistema informático militar y la NASA

2007 Operación Huerto. Agredido: Siria
Objetivo: Defensas antiaréreas de Siria

2007 Black Hat. Desde Rusia. Agredido Estonia -> **PRIMER ACTO CONSIDERADO DE CIBERGUERRA**
Objetivo: sistemas informáticos de empresas y organismos estonios. Sistema financiero.

2008 OSETIO. Desde Rusia. Agredidos: Georgia y Azerbaiyán -> **Precedió a ataques físicos. 5º DOMINIO DE LA GUERRA**
Objetivo: webs de medios de comunicación y de instituciones públicas

2009 Operación Aurora. Desde China. Agredidos: EEUU
Objetivo: sistemas informáticos de grandes compañías estadounidenses (google, Yahoo, Symantec, Abode, etc

2008-2010 STUXNET (Juegos Olímpicos). Desde EEUU e Israel. Agredidos: Irán
Objetivo: instalaciones nucleares iraníes, sistemas de gestión industrial (SCADA).

2012 FLAME. Desde Israel. Agredidos: Irán (principalmente), Palestina Arabia Saudí, Sudán, Líbano y Egipto
Objetivo: recopilar información masiva para inteligencia (desde emails a documentos secretos)

2012 SHAMOON. Desde Irán. Agredidos: Arabia Saudí y Qatar
Objetivo: sistemas informáticos de compañía saudí de petróleo Aramco y la empresa gasística RasGas.

2011-2013 DARKSEOUL. Desde Corea del Norte. Agredidos: Corea del Sur
Objetivo: canales de televisión y sistemas informáticos de bancos

2013 SNOWDENGATE (PRISMA). Desde China Agredidos: EEUU, Europa, Japón, Corea del Sur, India, ONU, Turquía
Objetivo: instituciones, empresas, sistema financiero….

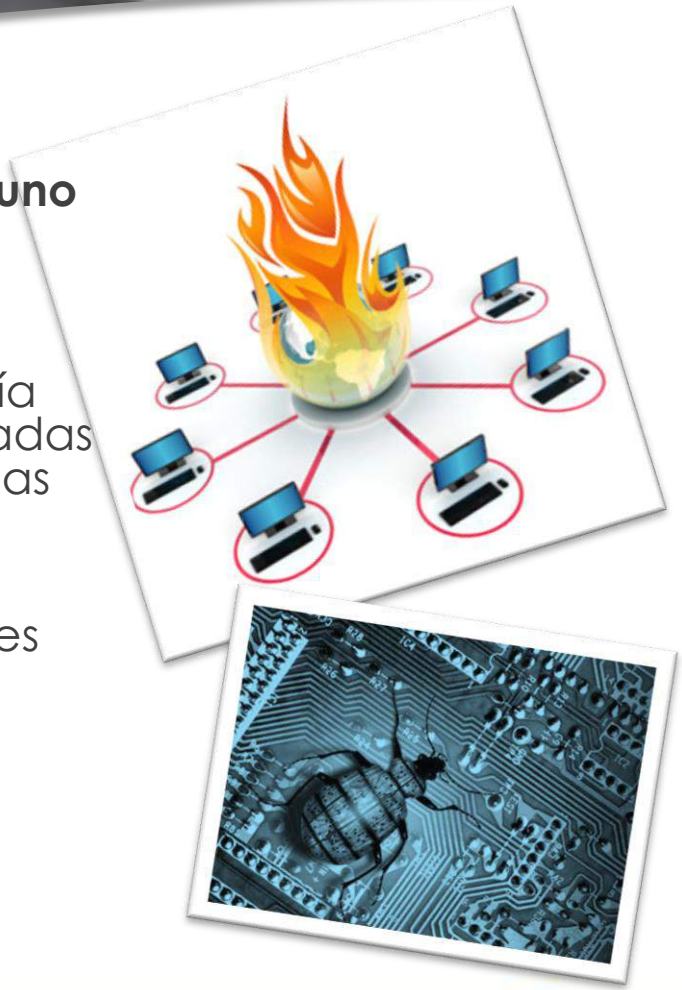
LAS TECNOLOGÍAS Y TÉCNICAS EMPLEADAS EN LOS ÚLTIMOS AÑOS QUE HAN SIDO MÁS DAÑINAS

APT's

ADVANCED PERSISTENT THREAT

Advanced Persistent Threat

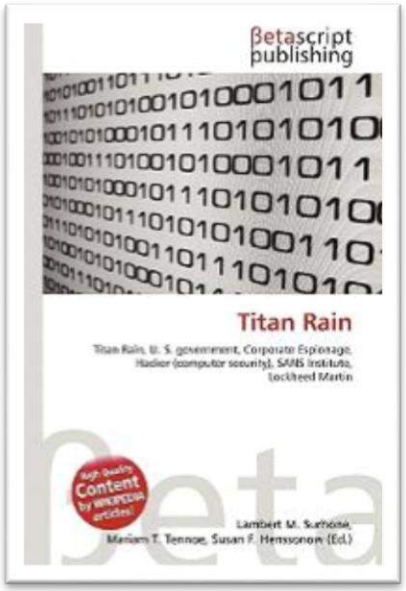
- **APT: sofisticado de ciberataque organizado, de rápida progresión y largo plazo, que constituye uno de los desafíos de seguridad más importante y peligroso, que deben afrontar hoy en día las organización.**
- Aprovechan vulnerabilidades conocidas o de día cero de los sistemas y aplicaciones TIC, combinadas con técnicas de ingeniería social para explotar las debilidades o **vulnerabilidades de la naturaleza humana.**
- Se caracteriza por cada uno de los componentes de su término descriptivo:
  - **Avanzada.**
  - **Persistente.**
  - **Amenaza.**



Tipos de Malware *"Titan Rain"*

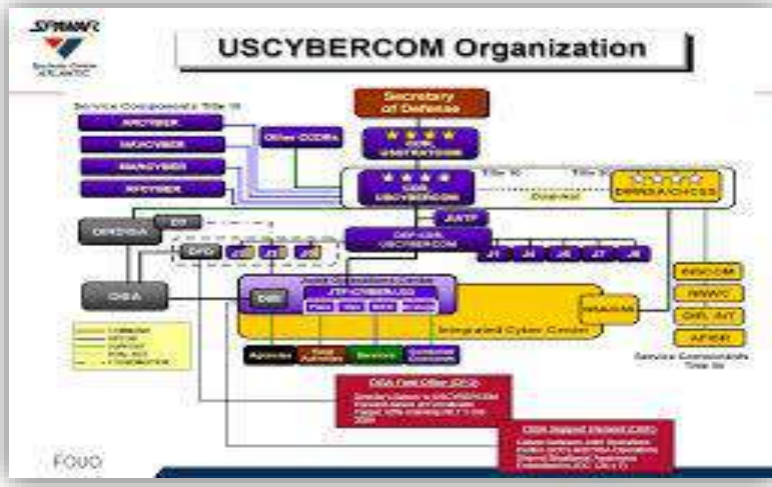
APT que realizó intrusiones en las redes de DoD de los EEUU, la NASA y empresas de defensa.

- Este tipo del malware dio origen **al nombre de que se utiliza comúnmente** hoy en día para referirse a los ataques a nivel de estado "**Advanced Persistent Threat (APT)**"

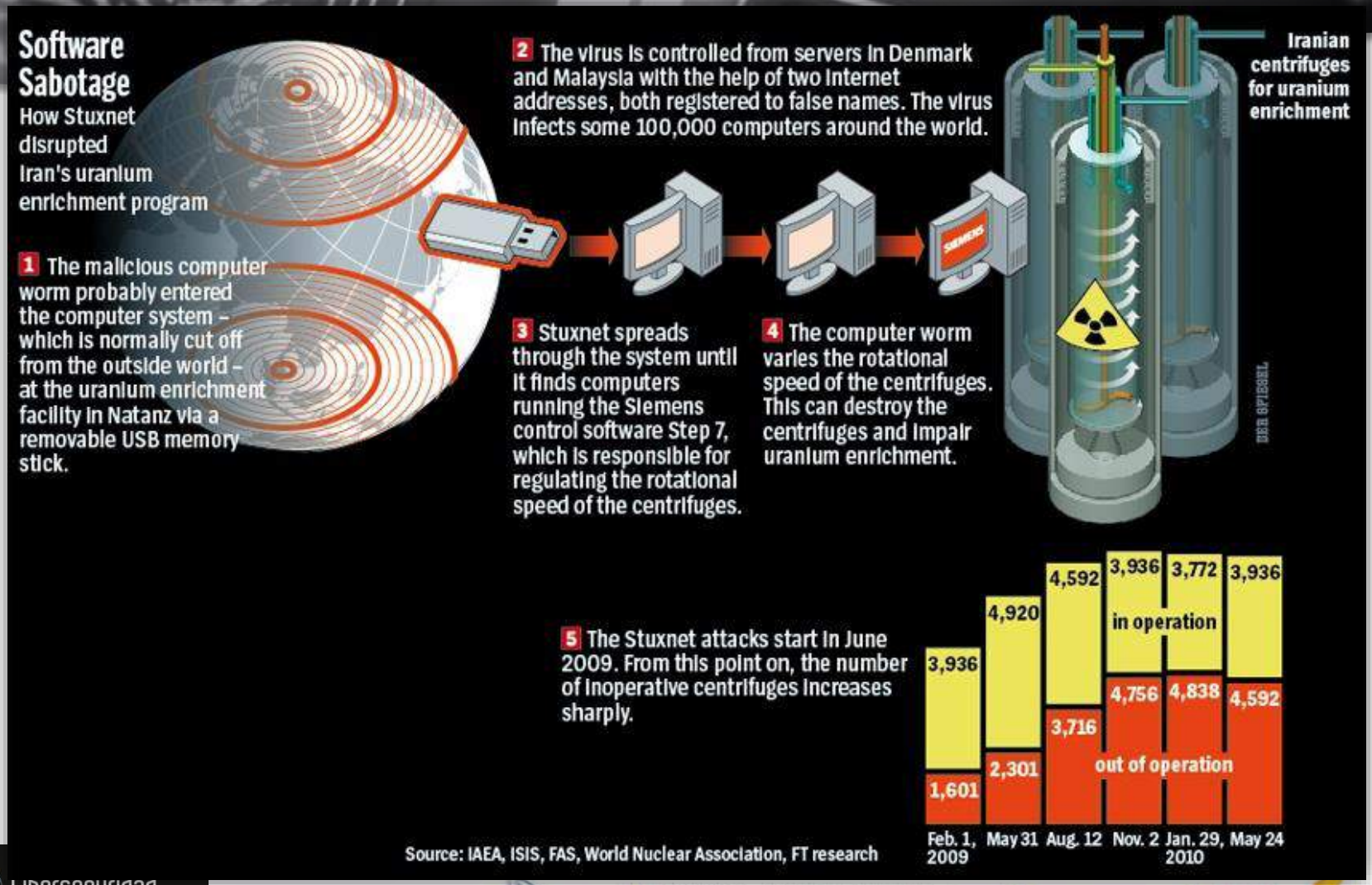


Tipos de Malware **"Buckshot Yankee"**

- APT, diseñado para usar **memorias USB como el vector de ataque** que dio lugar su prohibición en las redes del Departamento de Defensa.
- Tuvo un **impacto operacional grande** pues consiguió entrar en sistemas clasificados y no se sabe cuanta información consiguió extraer el malware.
- El DoD tardó **14 meses en quitar el gusano de su red** y el incidente.
- **Propulsor para la creación de USCYBERCOM.**

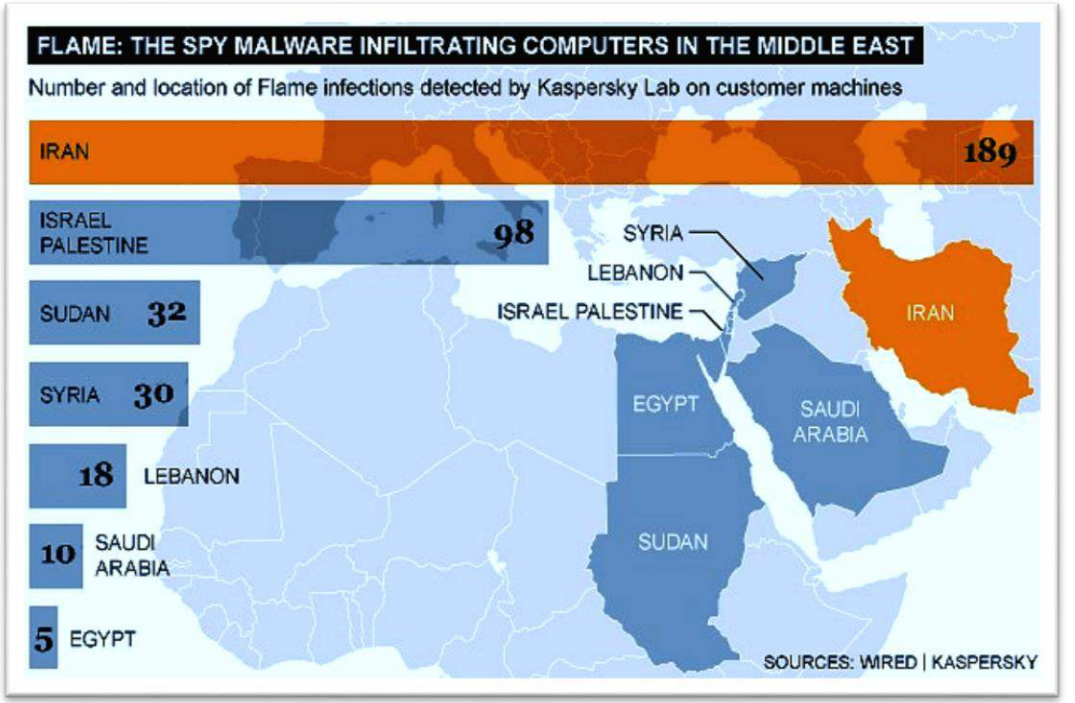


Tipos de Malware *"Stuxnet"*



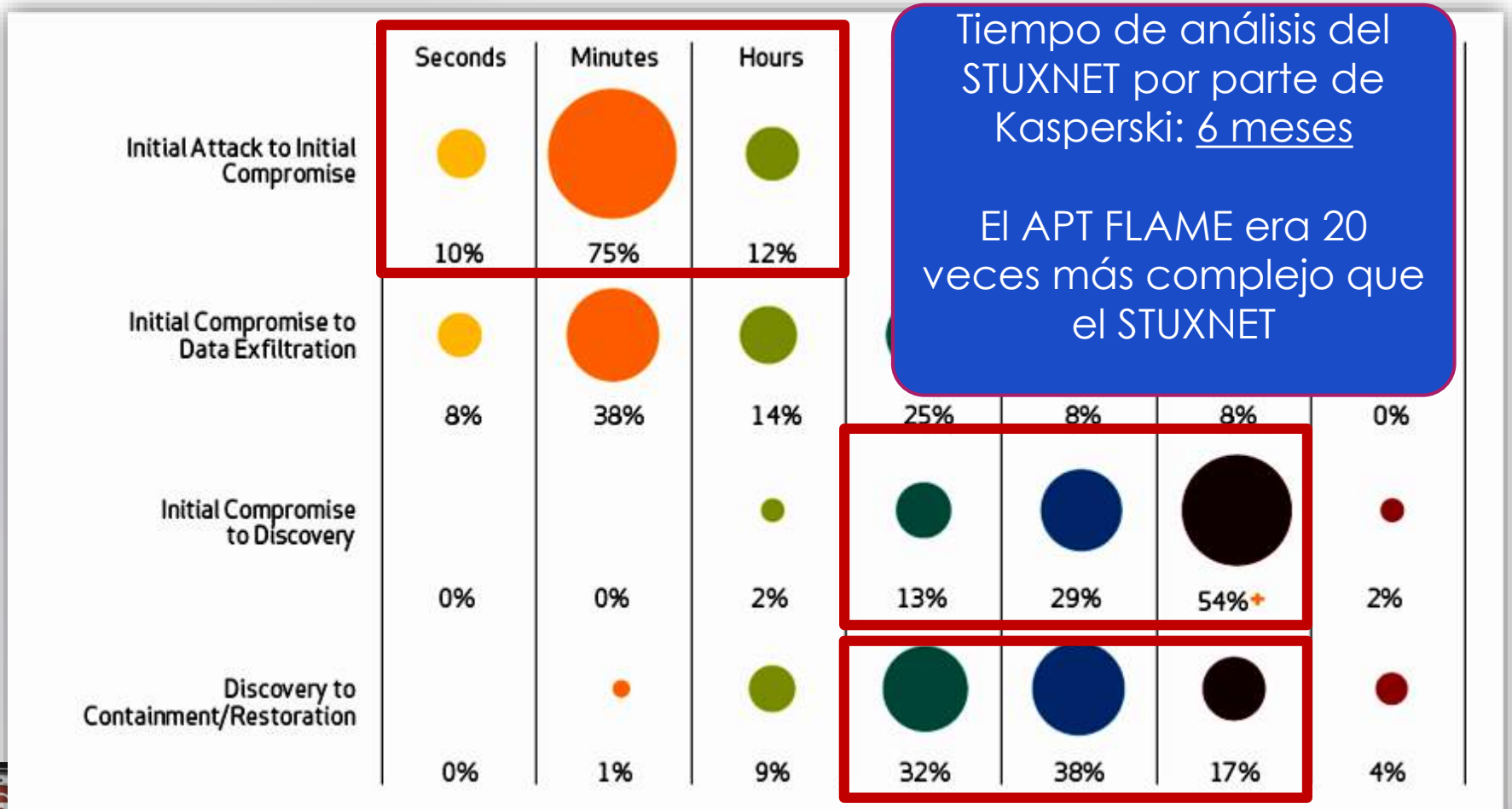
Tipos de Malware *"Flame"*

- Diseñado para rastrear de forma secreta redes informáticas de Irán y controlar los ordenadores de los funcionarios iraníes, enviando un flujo constante de información.
- Fue descubierto por la empresa de seguridad Kaspersky y se le considera uno de los **más complejos y dañinos** realizados hasta el momento.
- Sus principales capacidades son las de **replicar información de los sistemas infectados y controlar sus funciones enviando la información a un centro de mando y control (C2)**.



ADVANCED PERSISTENT THREAT

Situación Actual. Falta de efectividad ante APT



Tiempo de análisis del STUXNET por parte de Kasperski: 6 meses

El APT FLAME era 20 veces más complejo que el STUXNET

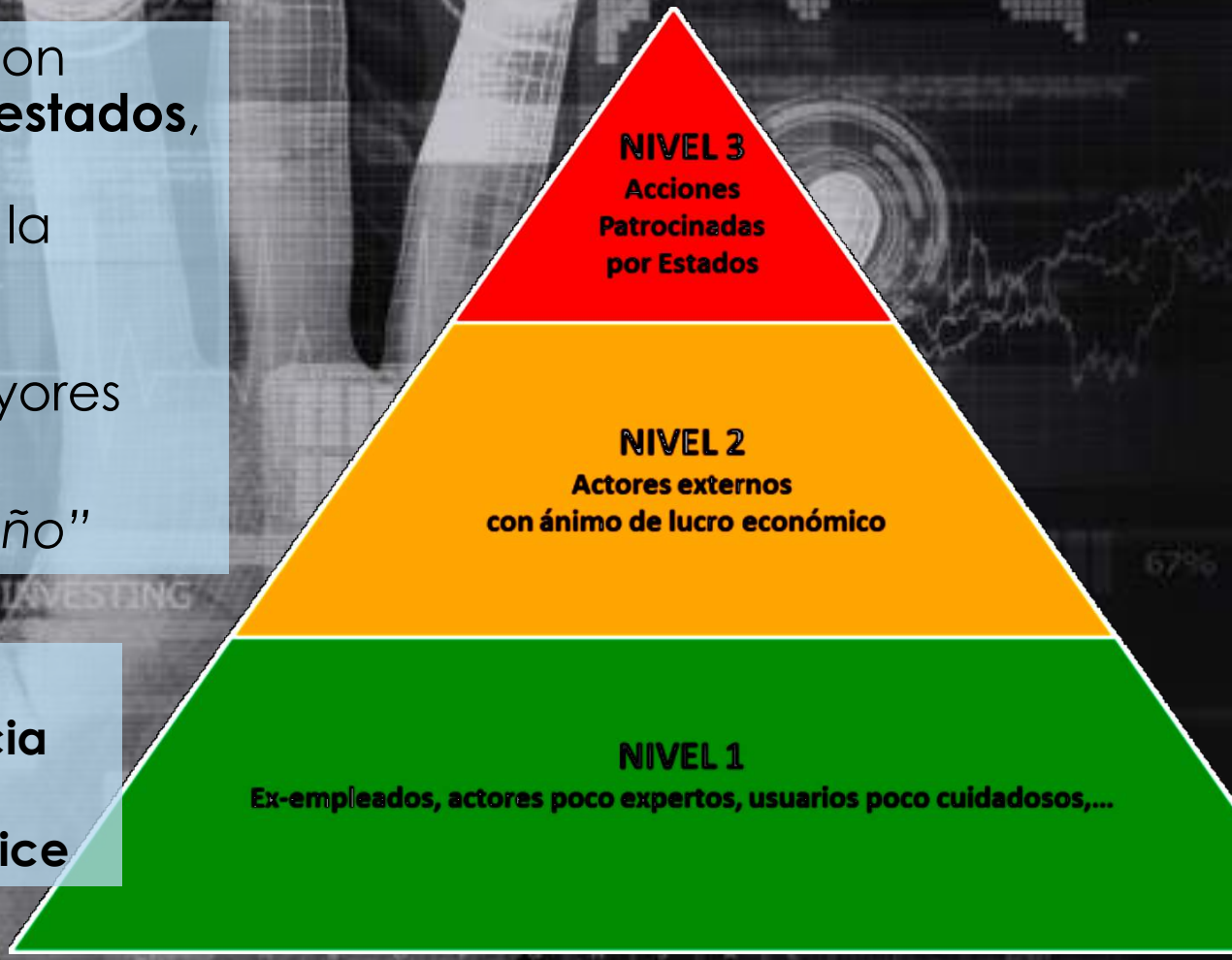
SOURCE: Verizon Business, *2012 Data Breach Investigations Report*

Realidades significativas del 2014

UNO. Las amenazas con **origen en los propios estados**, así como la profesionalización de la delincuencia en el ciberespacio, siguen constituyendo los mayores peligros

"Pirámide del Daño"

- **Técnicas APT**
- **Ciberdelincuencia**
- **Ransomware**
- **Crime-as-a-Service**



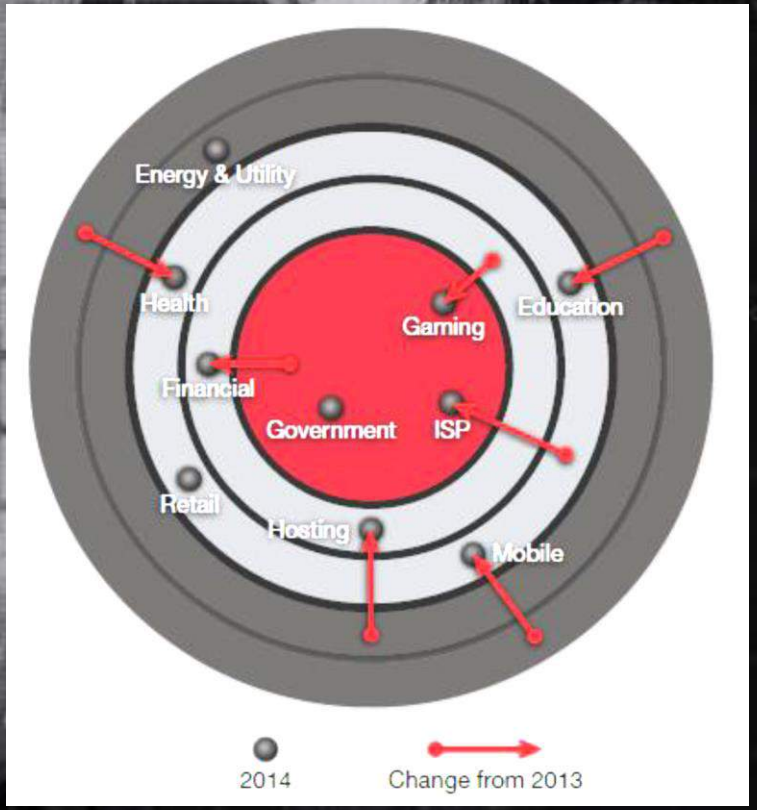
Tripwire. Layared Security. 2014.

Realidades significativas del 2014

DOS. El **impacto potencial** en los sistemas de información víctimas de los ciberataques se está incrementando a medida que lo hace la digitalización de la sociedad

TRES. Los problemas derivados del **software no-actualizado**.

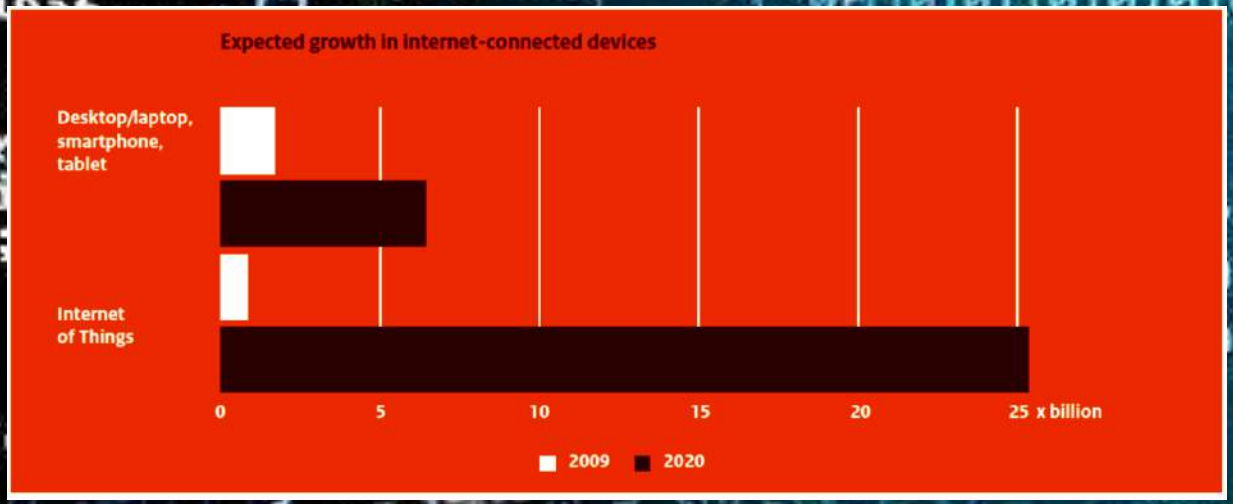
CUATRO. Los problemas de privacidad derivados de la recolección masiva de datos (**Big Data**).



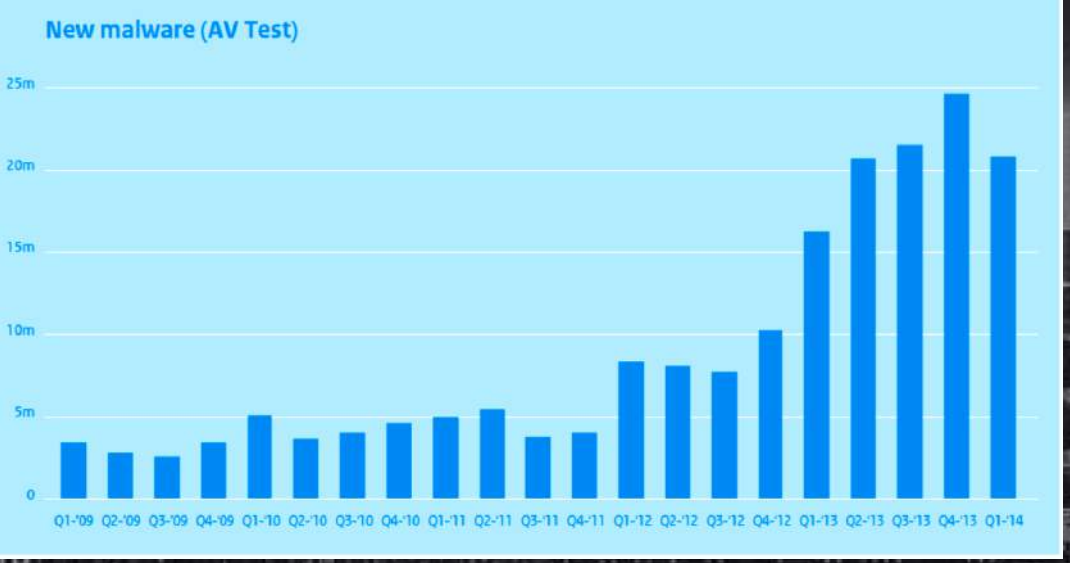
Radware: Global Application & Network Security Report 2014-2015.

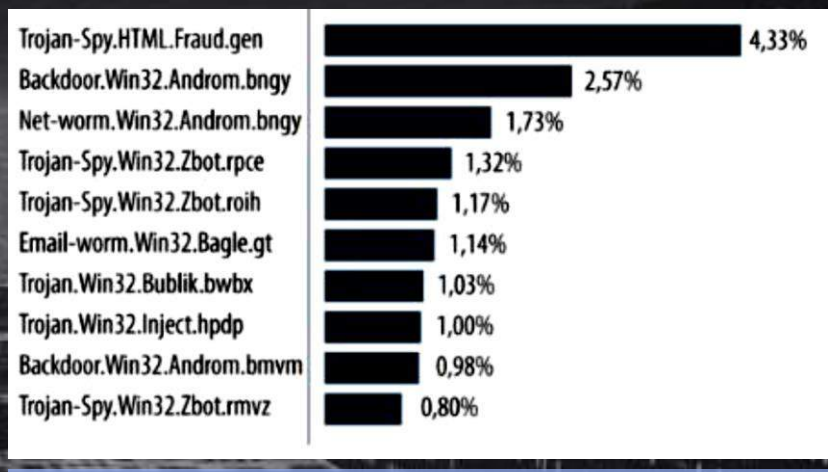
Agentes de la Amenaza (2014)

- El **ciberespionaje** ha constituido la mayor amenaza en el 2014.
- También se ha evidenciado la creciente profesionalización de las organizaciones delincuenciales -> **Crime-as-a-service (CaaS)**
- Por otro lado el desarrollo de lo que se ha denominado **Internet of Things**, supone uno de los mayores retos en el campo de la ciberseguridad



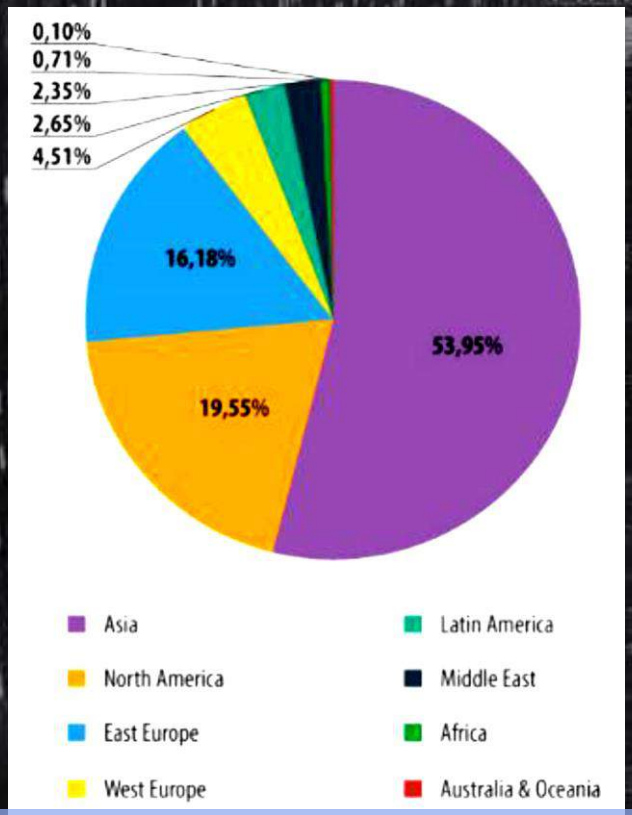
http://www.gartner.com/newsroom/id/2684915



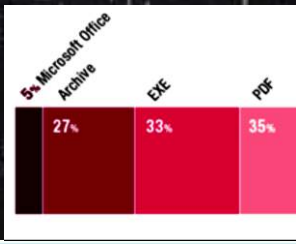


Diez muestras mas significativas de código dañino

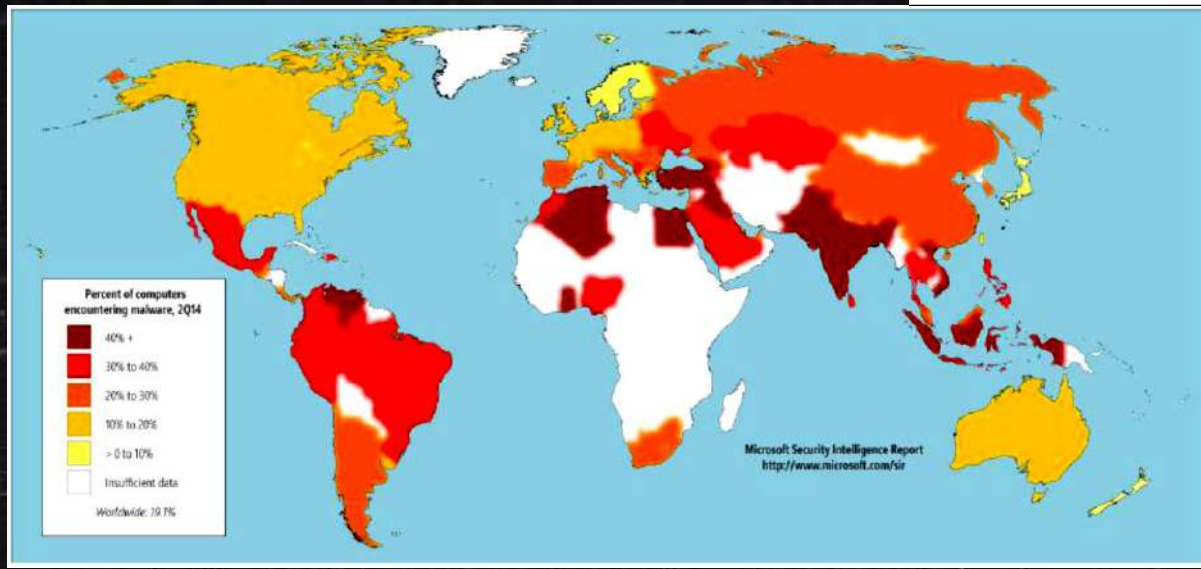
Kaspersky: Spam Report. (Feb., 2014)



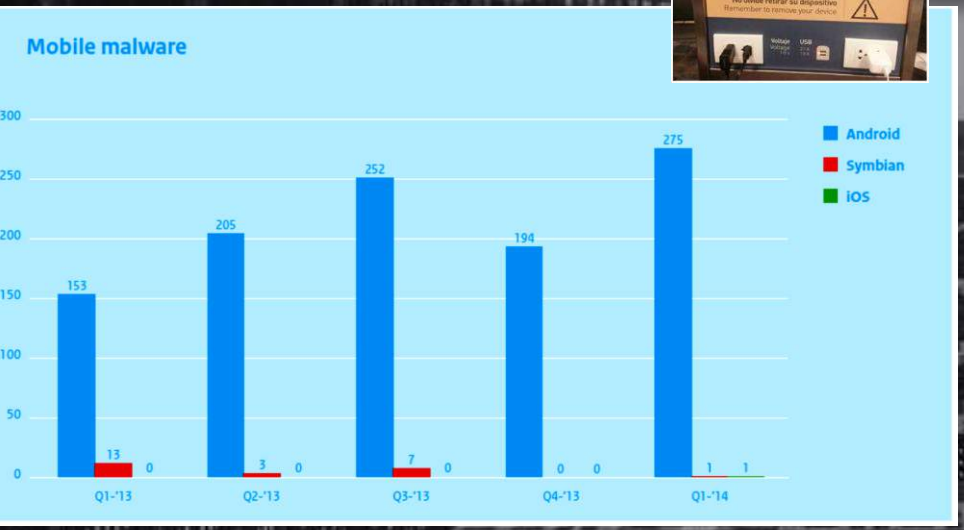
Regiones productoras de SPAM



Código dañino
Distribución Geográfica de Detecciones (segundo trimestre 2014)

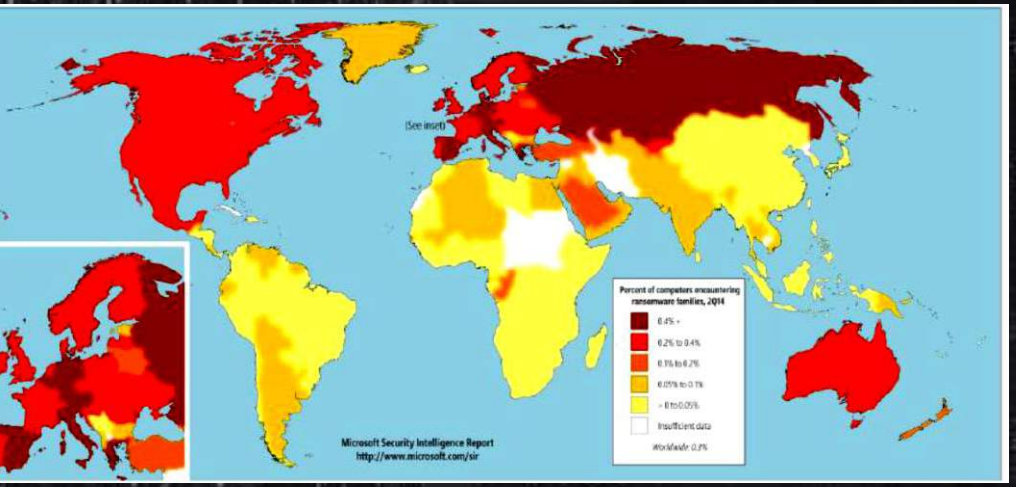


Código dañino para dispositivos móviles

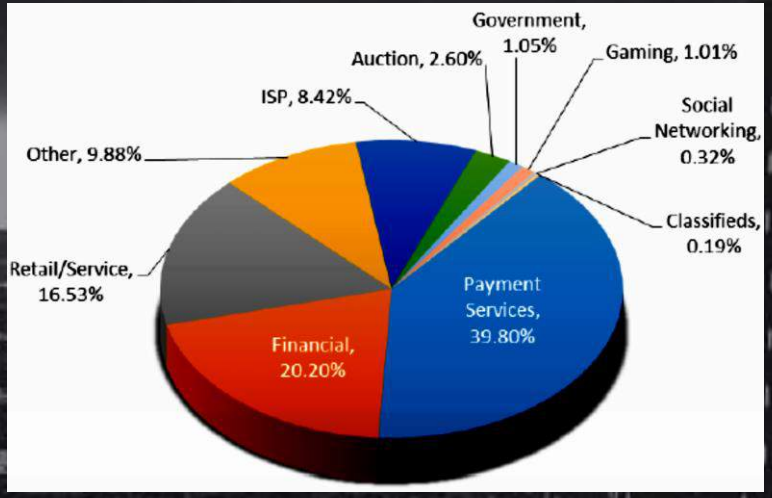


nte: http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2014.pdf

Herramientas de acceso remoto RAT

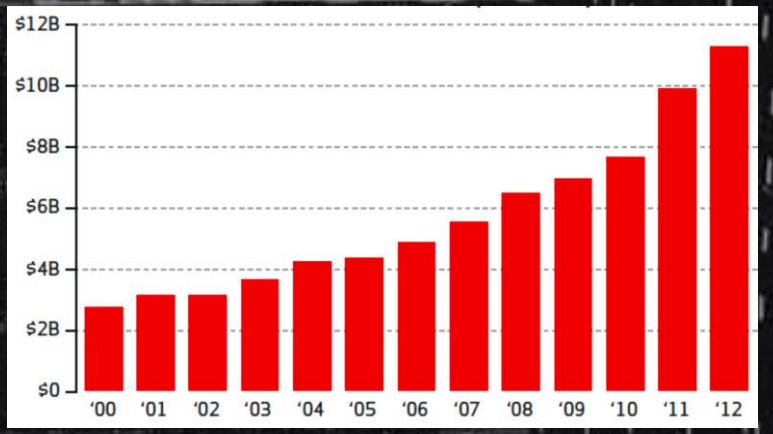


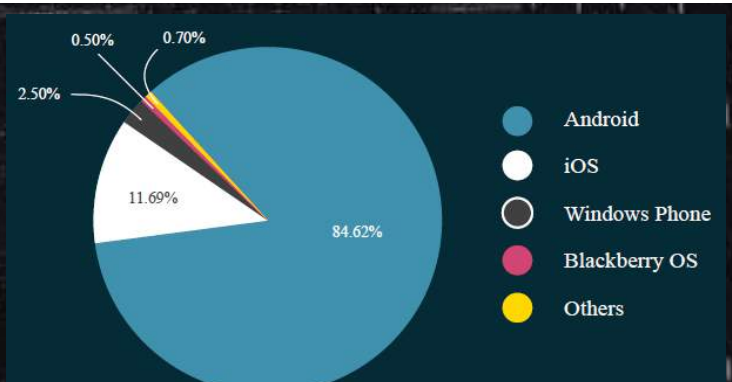
Vulnerabilidades en dispositivos móviles



Phishing

Crime-as-a-Service





CIBERESPACIO

- Estonia vs Rusia 2007
- Irán vs EEUU 2010
- Corea del Sur Vs Corea del Norte 2011
- Ucrania Vs Rusia 2104
- ¿¿¿2016??? ¿Drones?

HASTA AHORA LOS CIBERATAQUES HAN CAUSADO NUMEROSOS DAÑOS MATERIALES Y ECONÓMICOS, CRISIS POLÍTICAS QUE HAN SIDO GESTIONADAS....

....PERO, ¿UN CIBERATAQUE PUEDE PROVOCAR DIRECTAMENTE BAJAS DE VIDAS HUMANAS?. ¿ESTAMOS PREPARADOS PARA ESE ESCENARIO?

NAPT's

España es, tras EE UU y Reino Unido, el país que sufre más ciberataques

• Margallo revela que en 2014 se registraron más de 70.000 incidentes cibernéticos

MIGUEL GONZÁLEZ | Madrid | 5 FEB 2015 - 12:48 CET

183 355 313 46

Archivado en: José Manuel García Margallo Ataques informáticos Seguridad Internet España Telecomunicaciones Comunicaciones

España fue en 2014 el tercer país con más ciberataques. / KACPER PEMPEL (REUTERS)

Enviar Imprimir Guardar

Con más de 70.000 ciberincidentes, España fue el año pasado el tercer país del mundo, tras Estados Unidos y Reino Unido, que más ataques cibernéticos sufrió. Así lo ha revelado este jueves el ministro de Asuntos Exteriores, José Manuel García-Margallo, durante la presentación del monográfico sobre ciberguerra editado por Vanguardia Dossier. El ministro no ha detallado la gravedad de estos ataques, sus orígenes o destinatarios, pero ha dicho tanto a la Administración

Cyber attacks on drones

Perimeter Security | Access Control | Technology | Aircraft | Strategic Sites | Airport Security | Applications | Big Data | C4I | Security | Counter Terror | Cyber | Cyber Crime | Cyber Security | Infrastructure Security | Geo-politics | Iran | Communications | Networking | News | Technology News | Unmanned Systems | UAV | USA | world news

By Ziv Ithzaki - Feb 2, 2015

Illustration

The number of missions unmanned systems are tasked with, as well as their diversity, is expanding each year. The roles they play include a wide range of missions, such as intelligence gathering, analysis, storag and dissemination. Movement of forces, weather conditions, images, statistics and so on are merely some the types of data unmanned systems are capable of processing. At the same time, securing the data association with the operation of unmanned systems has become one the most important fields in this

Pero, con este panorama y estos antecedentes…..

¿ESTAMOS PREPARADOS?
¿ESTAMOS ORGANIZADOS?
¿QUÉ NECESITAMOS?

…. UN MÉTODO

¿Cómo definimos un mecanismo operativo para atender a esta realidad?

Principios de la Ciberdefensa

- Anticipación.
- Carácter permanente.
- No duplicidad.
- Colaboración e Interoperabilidad.
- Flexibilidad y Adaptabilidad.

Objetivos de la Ciberdefensa

- Libre Acceso de los Sistemas.
- Ámbito de operación seguro.
- Mantener superioridad.
- Garantizar la operación en condiciones críticas.
- Obtener, analizar y explotar la información del adversario.
- Ejercer la respuesta necesaria.

CIBERDEFENSA: enfoque operativo

Capacidades	Funcionalidades
Detección de ataques cibernéticos y actividades maliciosas	• Gestión y Control de los sensores. • Análisis de Actividad Maliciosa.
Prevención y mitigación de ciberataques	•Sistema Alerta Temprana •Aplicación de Inteligencia
Recuperación frente a ciberataques	• Configuración de Aplicaciones CIS • Recuperación ante Ciberataques
Evaluación dinámica del riesgo	• Valoración Dinámica del Riesgo • Valoración de Daños (análisis forense)
Conciencia de la situación	• Conducción y Seguimiento Operaciones de Ciberdefensa. • Conciencia de la Situación.

CIBERDEFENSA: enfoque operativo

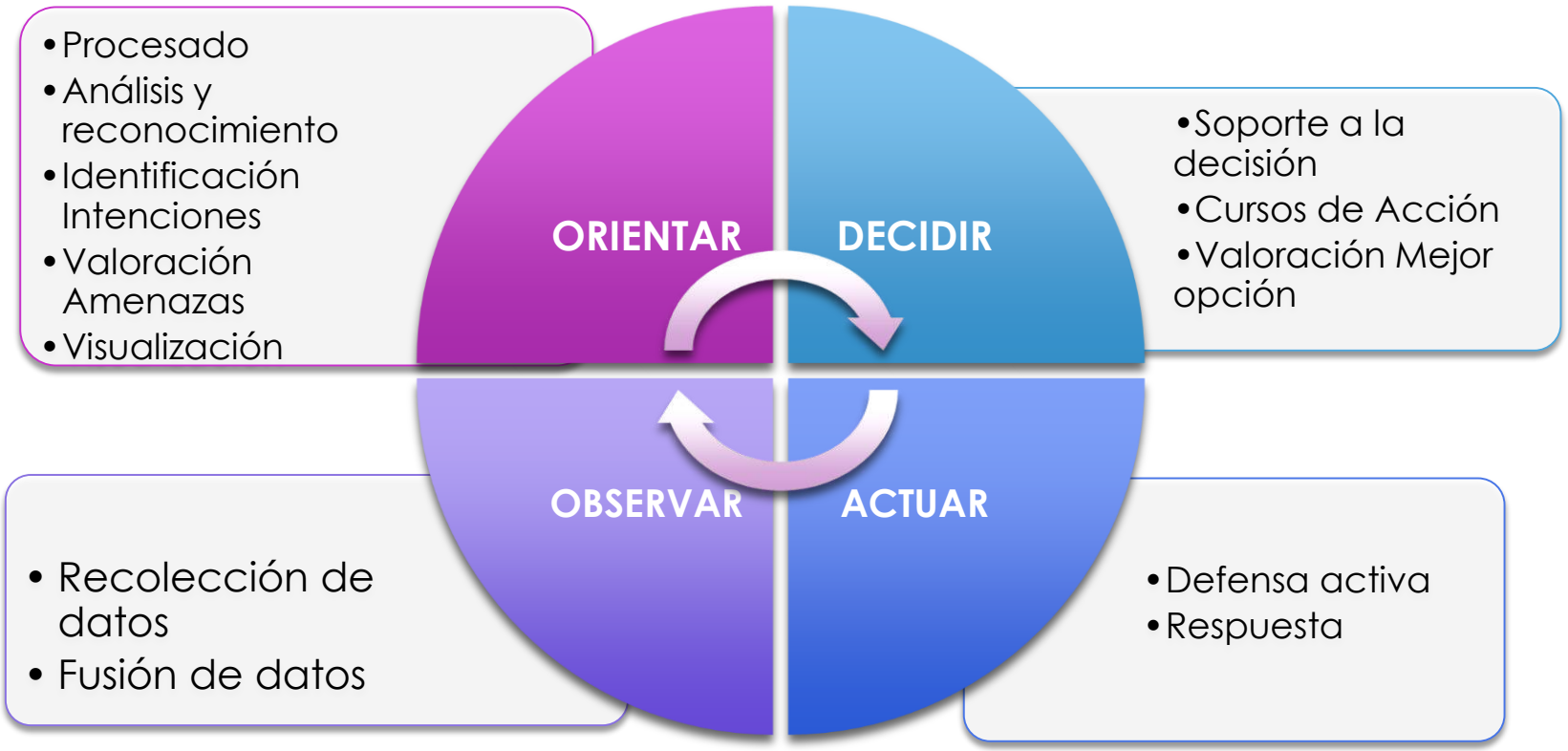
Capacidades	Funcionalidades
Toma de decisiones en tiempo oportuno	• Soporte a la decisión. • Cursos de acción.
Defensa activa (hacking ético)	• Plataforma de Ciberataques
Colaboración y compartición de información	• Servicio WEB intercambio de datos XML. • Herramientas colaborativas
Análisis de malware	• Aplicación de Análisis Malware • Sistema de Decepción (Honeynet).
Entrenamiento	• Plataforma Simulación y Sistemas Reales de Entrenamiento y adiestramiento.

NECESIDAD DE CONCEPTO OPERATIVO PARA ABORDAR LA GESTIÓN DE LA CIBERDEFENSA: **MODELO OODA**

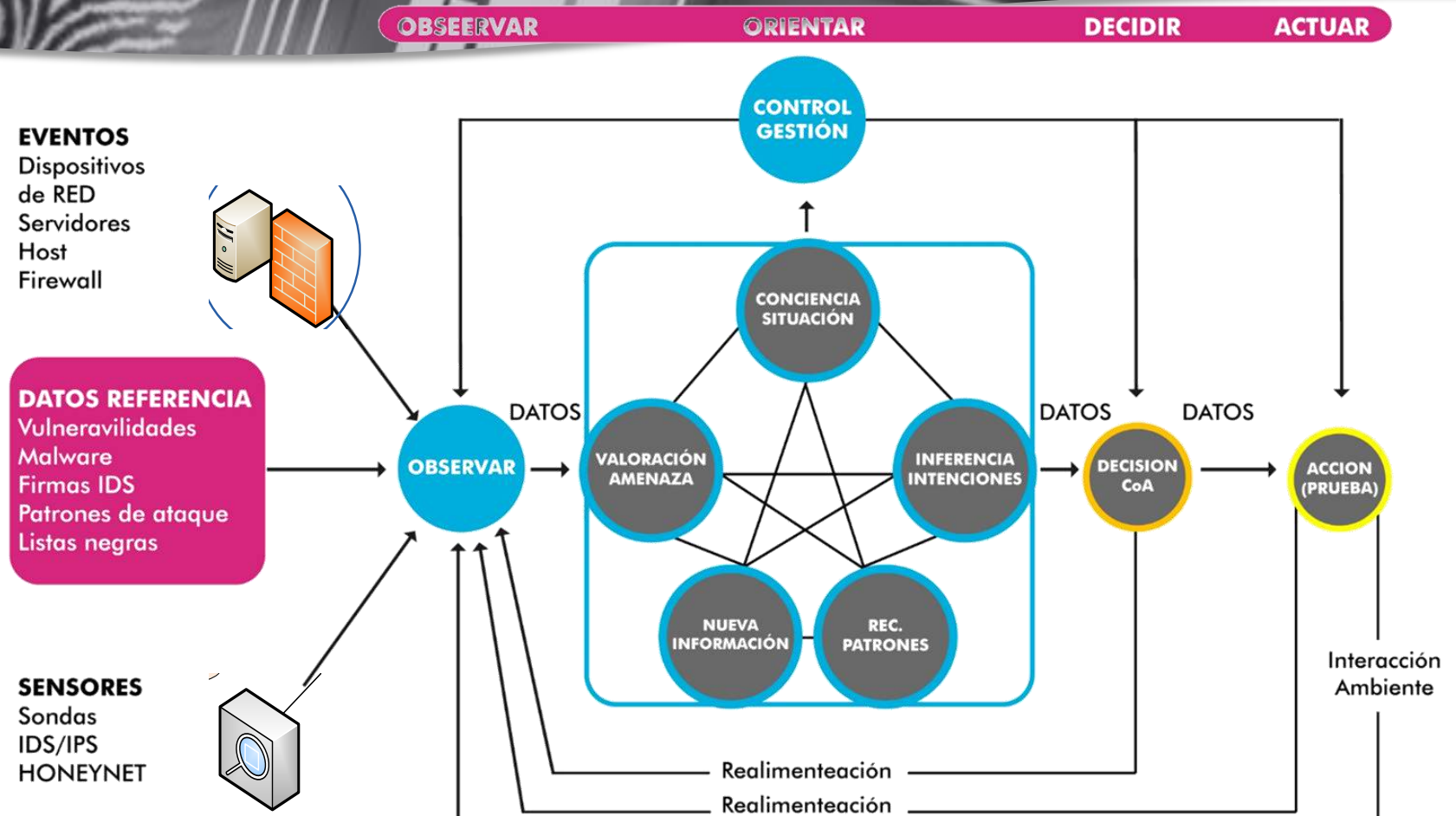
Coronel John Boyd

Concepto Operativo

Desglosa las actividades de ciberdefensa con respecto las cuatro fases del bucle de toma de decisiones Observar-Orientar-Decidir-Actuar (OODA).



Concepto operativo



Ciberdefensa: Retos y Desafíos

Incrementar el nivel de eficacia en el uso del ciberespacio en las operaciones militares proponiendo mecanismos de mejora, lecciones aprendidas y buenas prácticas basándose en el análisis del estado de seguridad de los sistemas TIC

MUCHOS RETOS Y DESAFÍOS Y ADEMÁS DE DIFERENTE NATURALEZA

Algunos retos y desafíos

Ámbito Tecnológico

- ¿Big data?
- Software en tiempo real
- Semántica y ontologías.
- ¿Infraestructuras de experimentación. Laboratorios?
- Inteligencia artificial y sistemas expertos y predictivos. Apoyo a la decisión.

Ámbito legal y organizativo

- Normalización de la Ciberdefensa.
- Legislación internacional. Derechos humanos.
- Doctrina.
- **Ciberdefensa COOPERATIVA**.

RRHH, ¿un nuevo tipo de soldado?

- Adiestramiento.
- Formación, entrenamiento
- Planes de carrera.

MANDO CONJUNTO DE CIBERDEFENSA: CASO ESPAÑA.

Constituido en septiembre de 2013

- Joint Force Commander
  - CC Land
  - CC Maritime
  - CC Air
  - CC Special Operations
  - CC Cyber

ESTRATEGIA DE CIBERSEGURIDAD NACIONAL: Líneas de actuación

Fundación IN-NOVA Centro de Innovación

- Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas.
- Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas.
- Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas.
- Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia.
- Seguridad y resilencia de las TIC en el sector privado.
- Conocimientos, competencias e I+D+i
- Cultura de la ciberseguridad
- Compromiso internacional

Ámbito de actuación del MCCD

Ámbito de actuación del MCCD

- Redes y sistemas de información y telecomunicaciones del Ministerio de Defensa.
- … u otras que pudiera tener encomendadas. Según OM 08/2015, "… que específicamente se le encomienden y que afecten a la Defensa Nacional".

Misión del MCCD

- Planeamiento y ejecución de las acciones relativas a la ciberdefensa.
- Contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Cometidos del MCCD

- El MCCD ejerce las responsabilidades que le encomienda el art.15 del RD 872/2014 y en particular, entre otras, las siguientes:
  - Dirige y coordina, en materia de ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos.
  - Ejerce la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.
  - Define, dirige y coordina la concienciación, la formación y el adiestramiento especializado de esta materia.


DESAFÍOS TECNOLÓGICOS
SOLUCIÓN = I+D

CD&E Ciberdefensa

Desarrollo de Conceptos y Capacidades

TTCP GUIDEx – Guide for Understanding and Implementing Defense Experimentation

BIG DATA en Seguridad y Defensa

Aplicaciones Big Data en Defensa y Seguridad
Detección de intrusión física en grandes espacios o infraestructuras abiertas
Computación sobre información encriptada
Análisis automático de vulnerabilidades de red (máquinas-tráfico de datos)
Criminología computacional
Uso fraudulento de recursos corporativos y/o sensibles
Análisis de video en tiempo real / Búsqueda y recuperación rápida en librerías de video.
Inteligencia visual en máquinas
Identificación de anomalías, patrones y comportamiento en grandes volúmenes de datos.
Análisis de texto (estructurado y no estructurado) como apoyo a la toma de decisión en tiempo real en entornos intensivos en datos.
Consciencia situacional
Traducción automática a gran escala (en número de idiomas y en volumen)
Predicción de eventos

- Vigilancia y Seguridad perimetral.
- Vigilancia y Seguridad de fronteras
- Seguridad física de infraestructuras críticas.
- Comunicaciones y redes seguras
- Bancos de datos para los ámbitos financiero, seguridad interior, inteligencia, defensa.
- Protección (redes IT) de Infraestructuras críticas
- Ciberdefensa / Ciberseguridad
- Lucha contraterrorista y contra crimen organizado
- Lucha contra el fraude
- Control y seguridad de recursos informáticos y datos en organizaciones
- Gestión del conocimiento en grandes organizaciones
- Seguridad ciudadana
- Inteligencia militar
- Planeamiento táctico de misiones.
- Toma de decisión en tiempo real para operaciones (Defensa/seguridad).
- Inteligencia industrial
- En ámbito militar en HUMINT/operaciones en entornos urbanos.
- Preparación de seguridad de eventos singulares (deportivos, políticos, etc.)
- Control y comportamientos de multitudes
- ...

Fuente: IEES. Instituto Español de Estudios Estratégicos "Big Data en los Entornos de Seguridad y Defensa" 2013

Factores impulsores y limitadores en la aplicación del Big Data en Seguridad y defensa

Fuente: IEES. Instituto Español de Estudios Estratégicos
"Big Data en los Entornos de Seguridad y Defensa"
2013

La importancia del BIG-DATA en la Ciberseguidad y en la Ciberdefensa

Fundación IN-NOVA Centro de Innovación

- Análisis automático de vulnerabilidades de red (máquinas-tráfico de datos)
- Criminología computacional
- Uso fraudulento de recursos corporativos y/o sensibles
- Identificación de anomalías, patrones y comportamiento en grande volúmenes de datos.
- Conciencia situacional
- Predicción de eventos

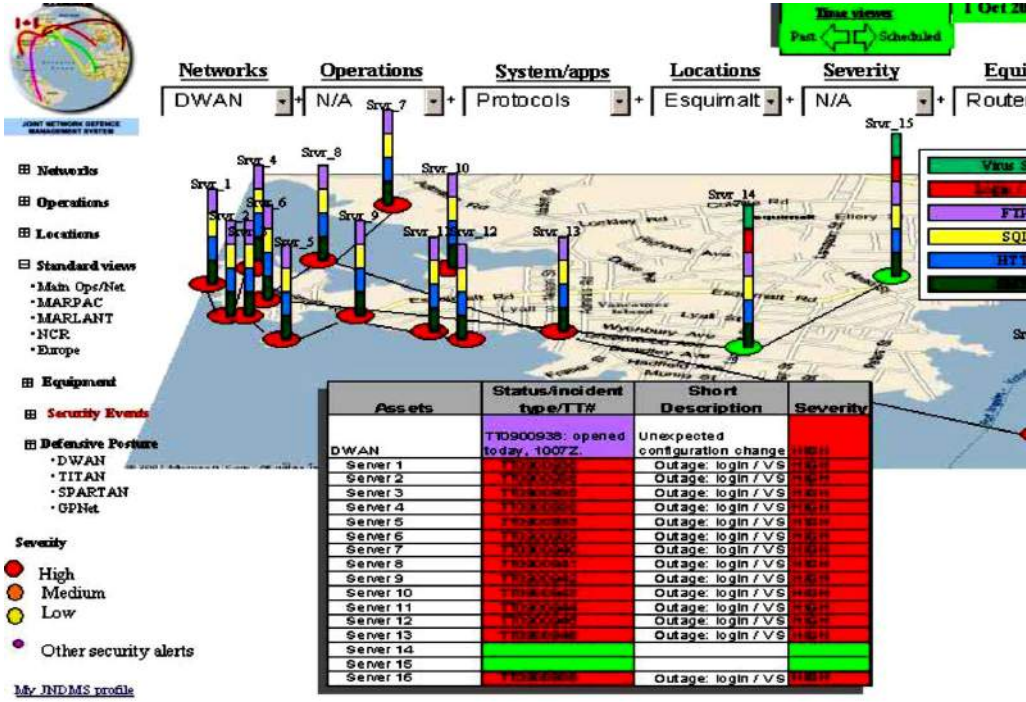
Desde un punto de vista de operaciones, el hándicap tecnológico es aún mayor:

SOFTWARE EN TIEMPO REAL & BIG DATA

La Combinación Extrema

Conciencia de Situación. Sistemas de Apoyo a la Decisión

- Representar el dispositivo vulnerado
- Indicadores de compromiso
- Características del ataque
- Origen del ataque
- Niveles de representación:
  - Estratégico
  - Operacional
  - Táctico



Extraída de Mr. Marc Grégoire, Mr. Luc Beaudoin. Visualisation for Network Situational Awareness in Computer Network Defence

DESAFÍOS SOBRE LA PREPARACIÓN DE LOS RRHH

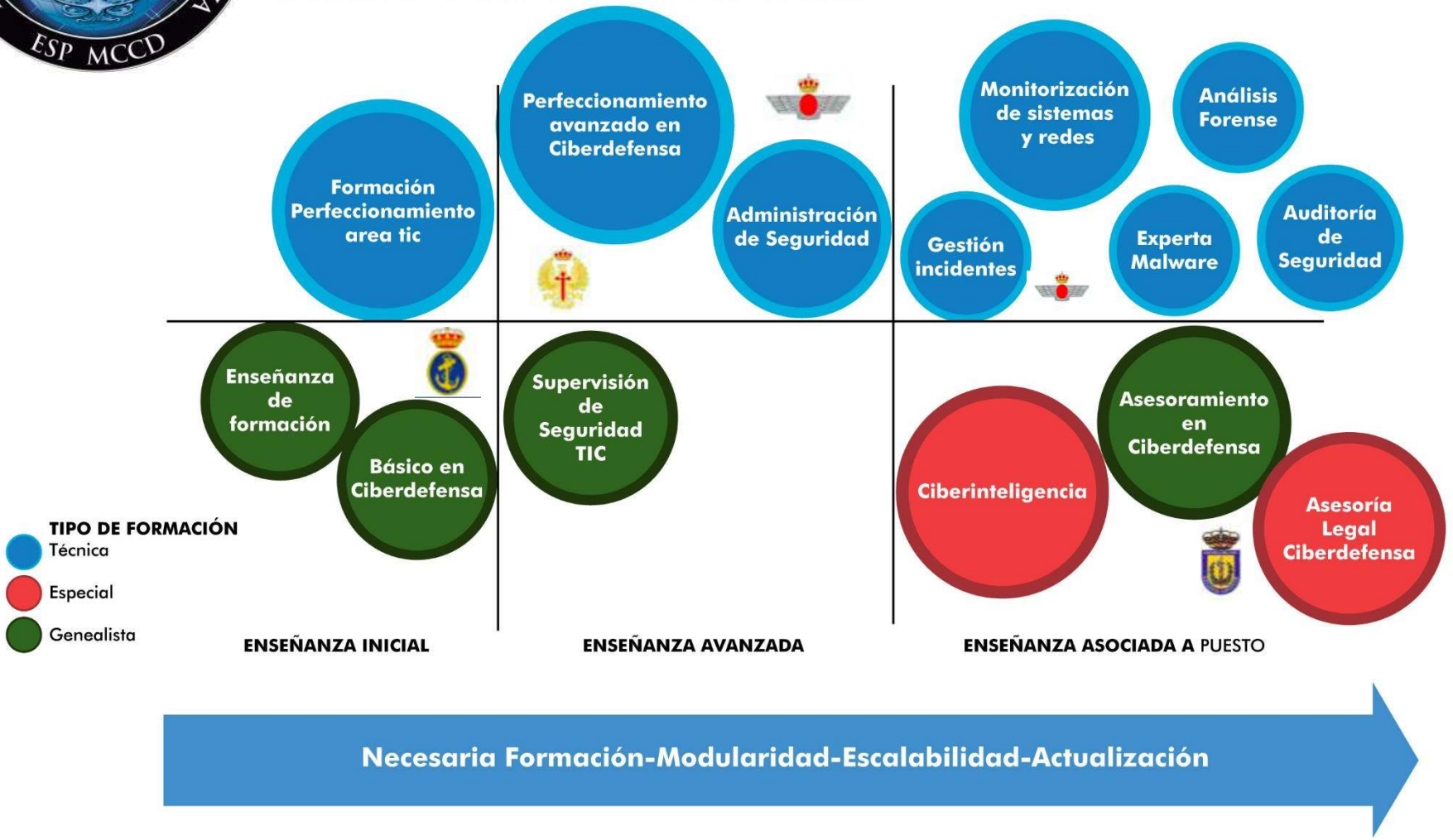
SOLUCIÓN = PLAN DE CARRERA ADIESTRAMIENTO Y FORMACIÓN A LOS DIFERENTES PERFILES

Disponer de infraestructuras de adiestramiento, ejercicios y validación de estrategias: Cyber Range.

Formar a los recursos humanos con titulaciones específicas de Ciberdefensa

FORMACIÓN, ADIESTRAMIENTO, PLAN DE CARRERA

ESQUEMA DEL PLAN DE FORMACIÓN EN CIBERDEFENSA



Necesaria Formación-Modularidad-Escalabilidad-Actualización

Formación, Adiestramiento, Plan de carrera

FORCIBE FORMACIÓN POR GRUPOS			FORMACION										
			BÁSICA	SSTIC	FUNCIONES TÉCNICAS						OTRAS FUNCIONES		
			Formación Basica CD	Supervisión de Seguridad TIC	Formación Avanzada CD	Gestion de Incidentes	Administración de Seguridad	Monitorización de redes y sistemas	Analisis Forense	Experto Malware	Auditoria de Seguridad	Asesoramiento en CD	Ciberinteligencia	Asesoramiento Legal en CD
GRUPOS DE FORMACIÓN	FUNCIONES TÉCNICAS	Auditor de Seguridad			x		x				x			
		Supervisor de Seguridad de las TIC		x										
		Administrador de Seguridad (ASS)			x		x							
		Gestor de Incidentes			x	x								
		Operador de Monitorización			x			x						
		Analista Forense			x				x					
		Experto Malware			x					x				
		Administradores de red, sistemas y dispositivos móviles	A través de la Enseñanza de Formación. Ámbito específico/organizativo.											
	FUNCIONES DE ASOSARAMIENTO	Asesor Ciberdefensa	x		*							x		
		Analista Ciberinteligencia	x		*								x	
		Asesor Legal Ciberdefensa	x											x
	OTROS	Cuadros de Mando	A través de la Enseñanza de Formación y Ámbito específico/organizativo.											
		Alta Dirección	No se contempla formación particular dentro del Plan FORCIBE.											
		Autoridades de Sistemas	Para las Autoridades Operación de los sistemas (AOS/AOSTIC) y Autoridad de Seguridad TIC (ASTIC): No se contempla formación particular dentro del Plan FORCIBE. Cometidos según regulación vigente.											
			*	Debe haber realizado la Formación Básica CD o Avanzada CD (en caso de proceder de entorno TIC)										

DESAFÍOS SOBRE LAS PLATAFORMAS TECNOLÓGICAS PARA EL ADIESTRAMIENTO

SOLUCIÓN = CENTRO DE EXPERIMIENTACIÓN DE CIBERDEFENSA

Infraestructura Científica y Tecnológica.
CENTRO DE EXPERIMENTACIÓN EN CIBERDEFENSA

1. Subsistema de Gestión y Control
2. Subsistemas de Análisis y Monitorización de Datos
3. Subsistema de Experimentos
4. Subsistema de Ataque
5. Subsistema de Almacenamiento
6. Subsistema Obtención del Malware
7. Subsistema de Reingeniería y Análisis de Malware
8. Subsistema de Simulación
9. Subsistema DMZ

ENTORNOS REALES DE EXPERIMENTACIÓN, NO SIMULADOS

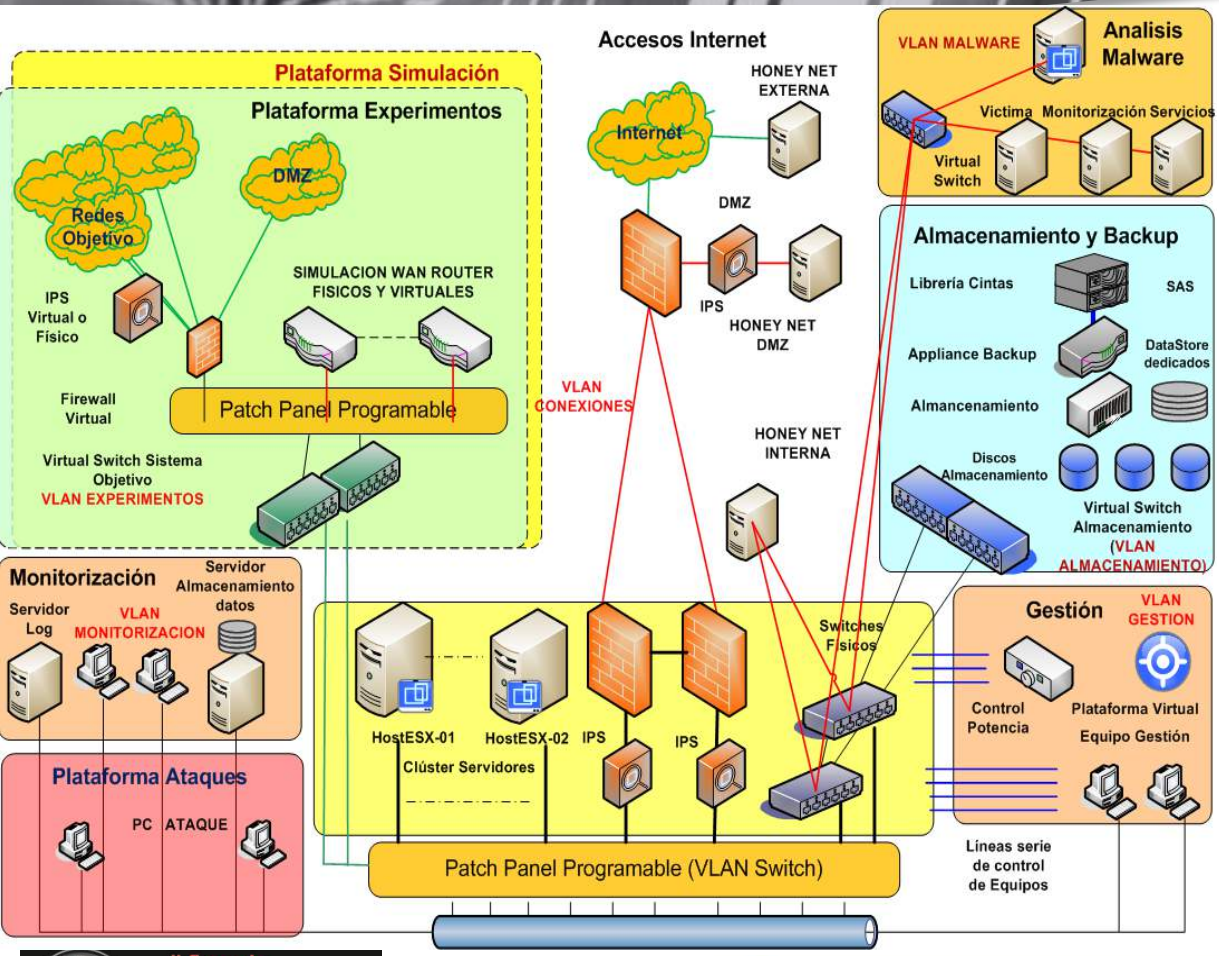
METAS del Centro de Experimentación

- Facilitar la experimentación y la identificación de las nuevas amenazas cibernéticas.
- Realizar el Desarrollo y Experimentación de Conceptos (CD&E) en el ámbito de la ciberdefensa.
- Plataforma segura de experimentación.
- Acceso a la infraestructura de experimentación a una amplia comunidad de usuarios.
- Desarrollo científico de metodologías de prueba rigurosa para las defensas contra ataques cibernéticos (infraestructura en red y sistemas de información).
- Obtención de una comprensión más profunda de los diferentes tipos de ataques cibernéticos para proporcionar el necesario apoyo y asesoramiento técnico a los diferentes organismos del MINISDEF y concienciarlos sobre la gravedad de estas nuevas amenazas.
- Difusión del conocimiento para contribuir al desarrollo de las capacidades nacionales de ciberdefensa.
- Desarrollar prototipos (nuevos desarrollos) estableciendo líneas de referencia para la validación.

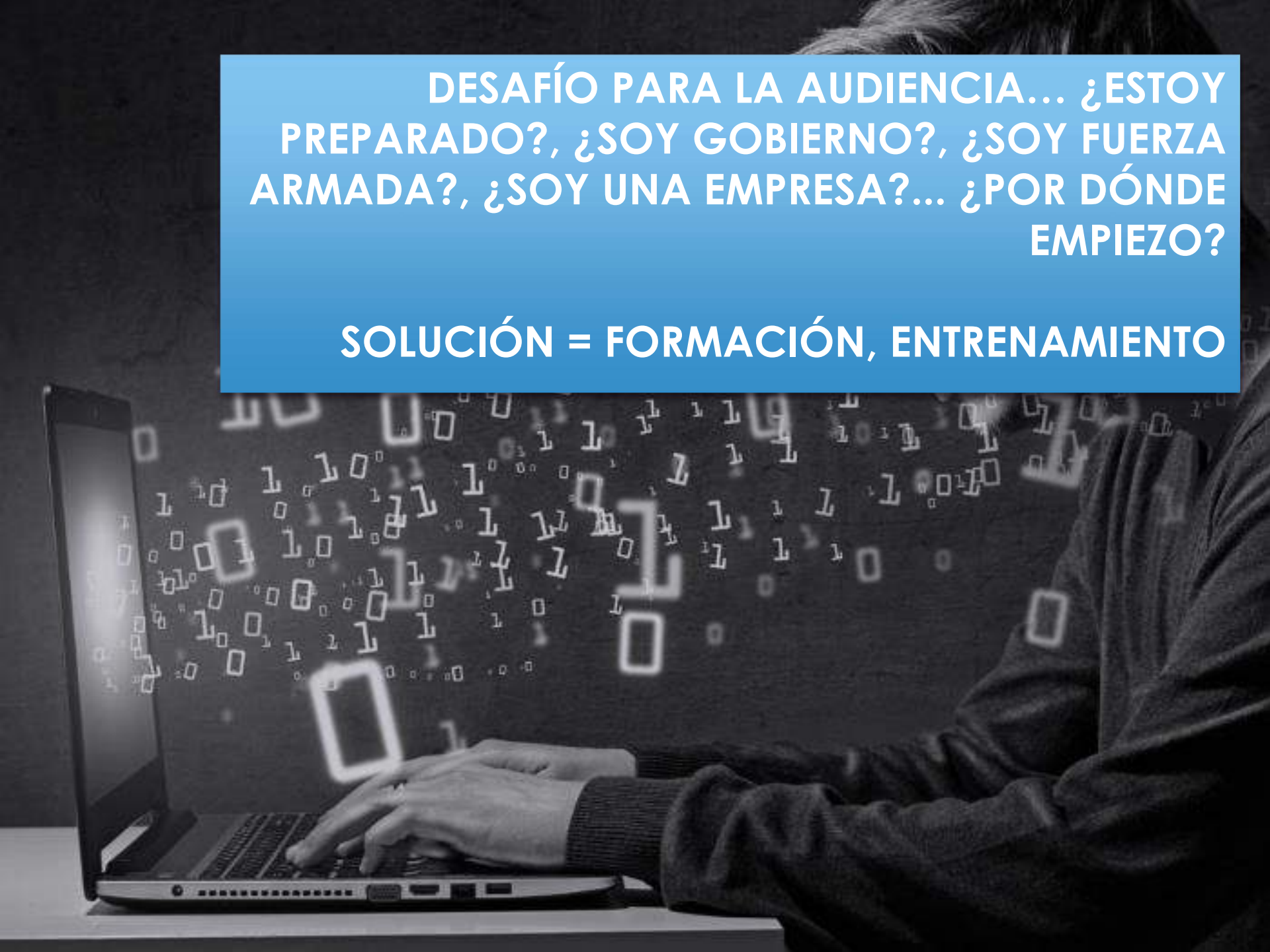
CAPACIDADES del Centro de Experimentación

- Capacidades de Experimentación Básicas: gestión y monitorización de eventos de seguridad, correlación de eventos, detección de intrusos y control de acceso a datos y redes, sistemas de auditoria de vulnerabilidades y herramientas de hacking ético y herramientas de bastionado y parcheo.
- Capacidades de Experimentación Avanzadas: simuladores, sistemas anti-fuga de datos, análisis forense y sistemas robustos.
- Capacidades de Experimentación en Nuevas Tecnologías: neutralización de botnets, gestión dinámica de riesgos, mitigación de ataques DDoS y ataques contra dispositivos de enrutamiento de redes de comunicaciones.
- Inteligencia: recolección de información de fuentes abiertas, filtrado de datos y alerta temprana.
- Capacidades de Experimentación en Ciberarmas: investigación y desarrollo de malware, automatización de malware, análisis de vulnerabilidades en software (certificación de desarrollos seguros) y malware y utilización de vulnerabilidades (creación de exploits).

Infraestructuras de adiestramiento, ejercicios y validación de estrategias



- Plataforma Virtualizada: diez mil nodos.
- Integración de entornos físicos y virtuales, y permitiendo la simulación de múltiples arquitecturas.
- Rápida configuración de red.
- Generación tráfico de Red.
- Red de almacenamiento.
- Análisis, configuración y gestión de red.
- Control de acceso físico y por red.
- Análisis y recolección de datos.


DESAFÍO PARA LA AUDIENCIA… ¿ESTOY PREPARADO?, ¿SOY GOBIERNO?, ¿SOY FUERZA ARMADA?, ¿SOY UNA EMPRESA?... ¿POR DÓNDE EMPIEZO?
SOLUCIÓN = FORMACIÓN, ENTRENAMIENTO

Conclusiones

- Las amenazas en el Ciberespacio cada vez son mas frecuentas, organizadas, costosas y complejas.
- Una de las prioridades marcadas de los países en la actualidad es la obtención de capacidades de experimentación en CIBERDEFENSA.
- La formación y el adiestramiento de los recursos humanos es fundamental para la realización con eficacia de las operaciones en el ciberespacio.
- Es necesaria la implantación de Infraestructuras de Adiestramiento, Ejercicios y Validación de Estrategias para el adiestramiento.
- Es necesario que los recursos humanos de Ciberdefensa estén formados con titulaciones específicas.
- Es IMPRESCINDIBLE una coordinación internacional, con una normativa, una legislación, una doctrina y unos tratados de operación.

MUCHAS GRACIAS

Samuel Álvarez
salvarez@in-nova.org

Fundación IN-NOVA
Centro de Innovación