Seminario Regional de Ciberdefensa
Buenos Aires (mayo 2014)

UNIVERSIDAD DE ALCALÁ

ALCALÁ DE HENARES – MADRID - ESPAÑA

Dr. Carlos Rodríguez-Solano (carlos.solano@uah.es)

information engineering
research unit

Indice

- Objetivo
- Grupo de Investigación (ieru)
- Proyectos Europeos Recientes
- Investigación y desarrollo entorno civil-militar
- Ciberdefensa
- Centro de Experimentación en Ciberdefensa
- Investigación y Análisis de Malware
- Generación Escenarios de Ciberdefensa
- Estrategias futuras
- Cooperación

Objetivo

- Comentar experiencias en proyectos I+D relacionadas con el trabajo conjunto en entornos colaborativos académico-militar, entre el Ministerio de Defensa de España y la Universidad de Alcalá de Henares.

- Aproximación a los temas actuales de investigación en Ciberdefensa acometidos en ese entorno de trabajo colaborativo.

- Estrategias futuras en I+D+i

- Cooperación

Grupo de Investigación (ieru)

ESCUELA POLITECNICA SUPERIOR

Oficialmente reconocido por la UAH dentro del Depto. de Cs. de la Computación, y cuya sede central está en el laboratorio O-24 de la Escuela Politécnica Superior (Campus Universitario); con capacidad de trabajo para 20 personas, complementado por una sala con servidores.
Interdisciplinario ; 25/30 personas (profesores, técnicos, colaboradores externos, doctorandos)

Áreas de interés

❖ WEB SCIENCE / DATA SCIENCE

- Semántica (Ontologías, Inferencia,KBS)
- E_learning
- E_health
- Seguridad - Ciberdefensa

Proyectos Europeos Recientes

- Altamente competitivos
- Calidad de la investigación auditable; duración proyecto : 3 años
- Experiencia y posicionamiento internacional del grupo de investigación

- VOA3R (€ 3,6 mill/consorcio: España, Bélgica, Italia, Alemania, Francia, Suecia, Dinamarca, Grecia, República Checa /coord:UAH (ieru))
- Organic.Lingua (€ 3,5 mill/consorcio: España, Austria, Italia, Reino Unido, Francia, Grecia, República de Estonia, Turquía /coord:UAH (ieru))
- Semagrow (€ 3,146,747 /consorcio: España, (Academia de Cs. China,Agric.) China, (FAO)Italia, Serbia, Grecia, Austria/coord:UAH (ieru))
- agInfra (€ 4,285,480 /consorcio: España, (Academia de Cs. China /,Agric.) China, (FAO) Italia, Serbia, Grecia, Austria, Reino Unido /coord:UAH (ieru))
- ODS (€ 15,320,000 /consorcio: 50 instituciones de 21 países distintos, coord : corporación Luxemburgo, finaliza 2015/principal socio técnico : UAH (ieru))

Investigación y desarrollo entorno civil-militar

- SAVCE (sitema de razonamiento de emergencias, usando ontologías de infraestructuras críticas; dominio: infraestructuras de energías trasladable a infraestructuras de comunicación digital;contrato multinacional INDRA UME)
- FOSSIL (entorno de interoperabilldad sintáctica + semántica (ontología de sensores y capac. plataformas) para Mando y Control militar en operaciones multinacionales; se usaron versiones ontológicas del estándar OTAN JC3IEDM; participación: unidad de Mando y Control del Área TICS del ITM; continuación proyecto: Rules of Engagement (ROE)
- INTEGRA (aplicación aprendizaje automático(ML) sobre sistemas Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance(sistemas C4ISR) relativo a misiones militares;aplicado a plataformas físicas; trasladable a agrupamiento automático de hosts en ataques coordinados; UAH + multinacional de Seguridad y Comunicaciones Amper)
- Perfil Repositorio de Objetos de Aprendizaje del Ejército de Tierra (academia de logística del ET)
- Programa RETOS (generación automática de escenarios de ciberdefensa y análisis de datos; ITM + UAH)
- Investigación y análisis de Malware (desarrollo de honeynets; ITM + UAH)

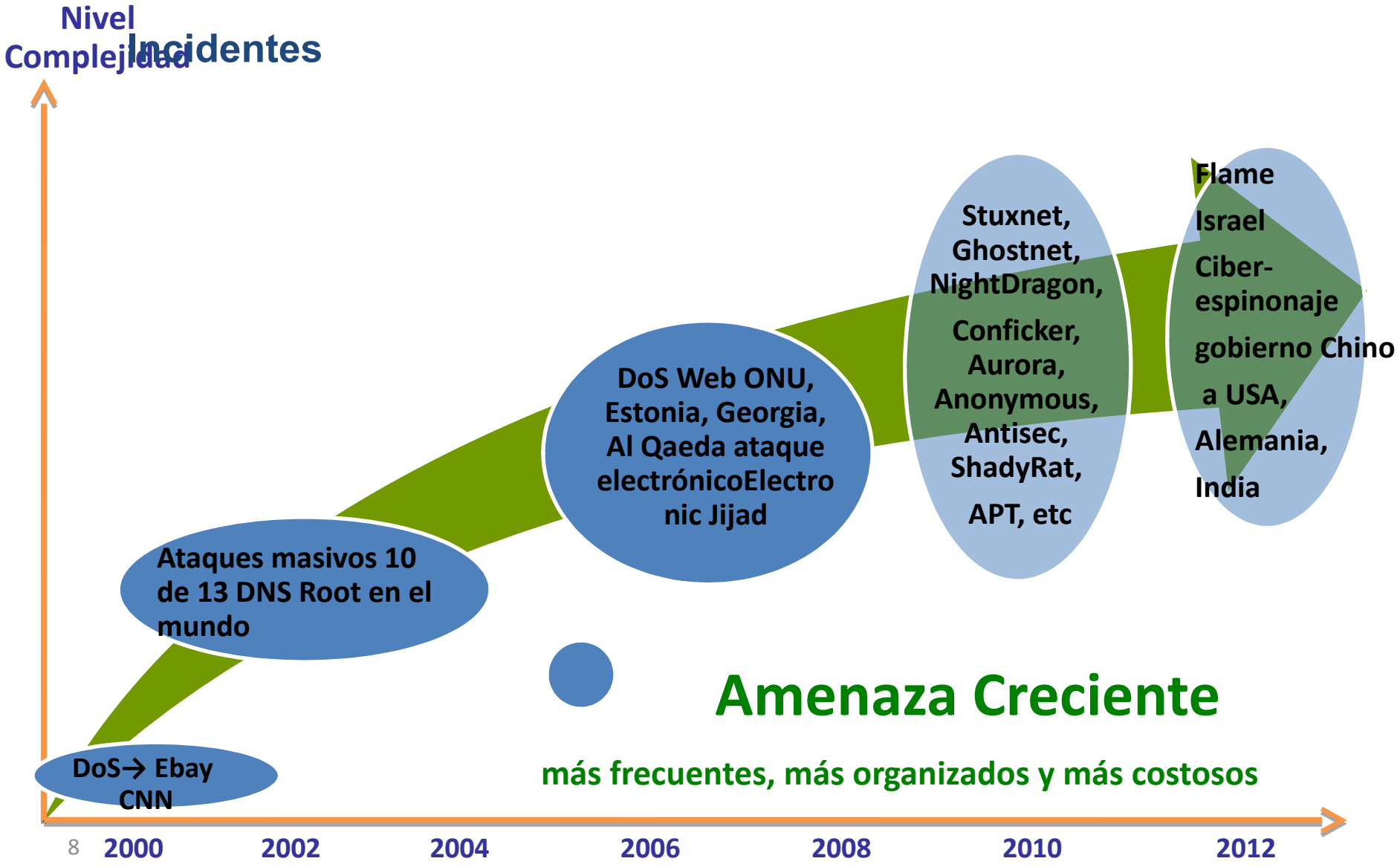
Ciberdefensa (I)

- **CIBERDEFENSA** *"La capacidad de proteger la prestación y gestión de los servicios CIS en respuesta tanto a potenciales como efectivas acciones maliciosas originadas en el ciberespacio"*. **(OTAN)**

- **CAPACIDADES DE CIBERDEFENSA:**

  - Detección de ataques cibernéticos y actividades maliciosas.
  - Prevención y mitigación de ciberataques.
  - Recuperación frente a ciberataques.
  - Evaluación dinámica del riesgo.
  - Conciencia de la situación, en cuanto a la capacidad de evaluar el estado de la seguridad de los sistemas y los daños producidos por los ciberataques.
  - Defensa activa (hacking ético).
  - Análisis de malware.

Ciberdefensa (II)



Centro de Experimentacion en Ciberdefensa (I)

- **Experimentación en Ciberdefensa**: Es una investigación controlada para descubrir información, confirmar o desaprobar una hipótesis o validar un concepto formalmente.

- **Aplicación metodología de la OTAN:** "Desarrollo y experimentación de conceptos (CD&E)"

MC 0583 – ***MC Policy for NATO Concept Development and Experimentation*** **(Sept 2009)**
MCM 0056-2010 – ***NATO Concept Development and Experimentation (CD&E) Process*** **(July 2010)**

BRINGING NATO CD&E TO THE NATIONS

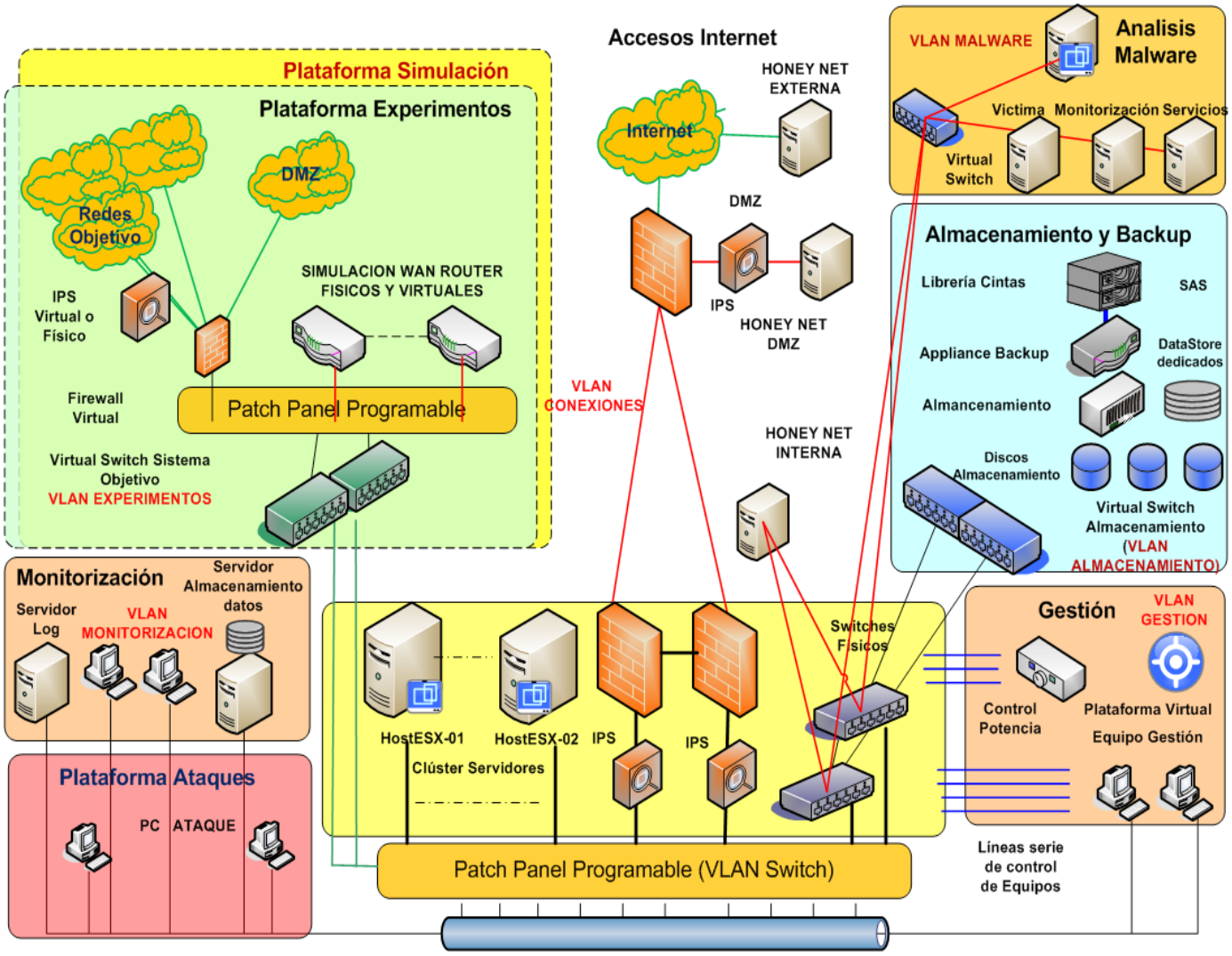
Centro de Experimentacion en Ciberdefensa (II)

SUBSISTEMAS

- *Gestión y Control* → Control de la infraestructura de virtualización, experimentos, asignación de recursos, configuraciones, etc.
- *Análisis y Monitorización de Datos* → Recolección de todo tipo de datos para poder realizar un análisis de la operación y resultados.
- *Experimentos* → Albergaría los diferentes nodos virtuales y físicos que compondrían el experimento.
- *Ataque* → Albergaría una plataforma con diversas herramientas de ataque.
- *Almacenamiento* → Almacenar las máquinas virtuales de los nodos y datos obtenidos en un experimento.
- *Recolección de Malware* → Captura y análisis de datos producidos por la actividad del malware recogido
- *Reingeniería y Análisis de Malware* → Entorno aislado mixto de equipos físicos y virtuales para la realización de análisis y reingeniería de malware.
- *Simulación* → Albergar simuladores de ciberdefensa.
- *DMZ* → Zona desmilitarizada de dos capas para conexión segura internet.

Centro de Experimentacion en Ciberdefensa (III)

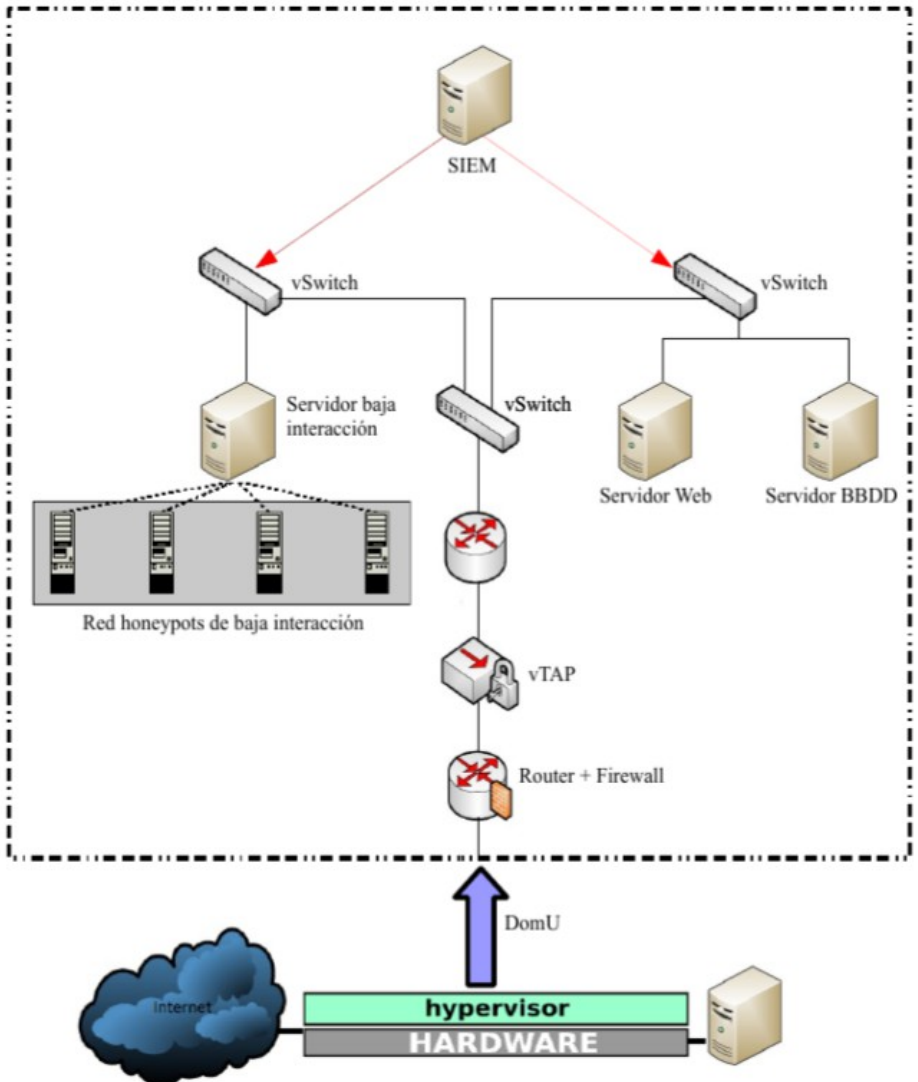
Esquema Arquitectura Centro Experimentación



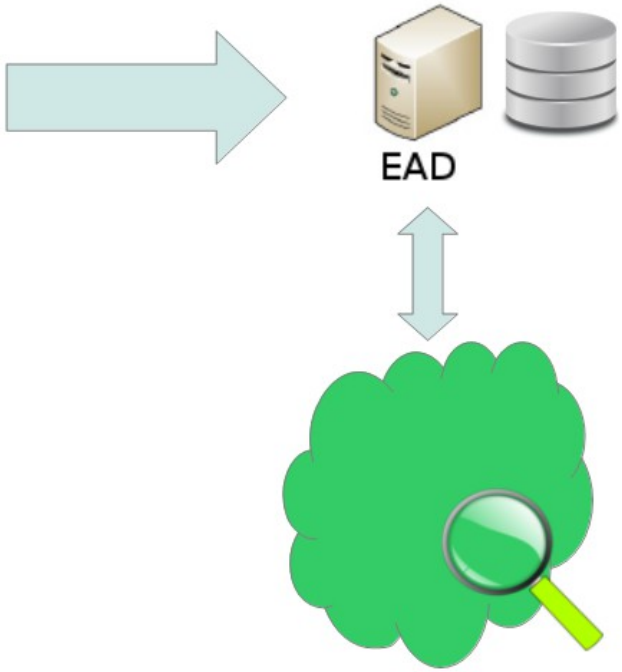
- Plataforma Virtualizada: mil nodos simultáneos.
- Integración de entornos físicos y virtuales, y permitiendo la simulación de múltiples arquitecturas.
- Capacidad de replicar experimentos
- Generación tráfico de Red.
- Red de almacenamiento.
- Análisis, configuración y gestión de red.
- Análisis y recolección de datos.

Investigación y Análisis de Malware (I)

HONEYNETS PARA LA DETECCIÓN Y ESTUDIO DE INTRUSIONES

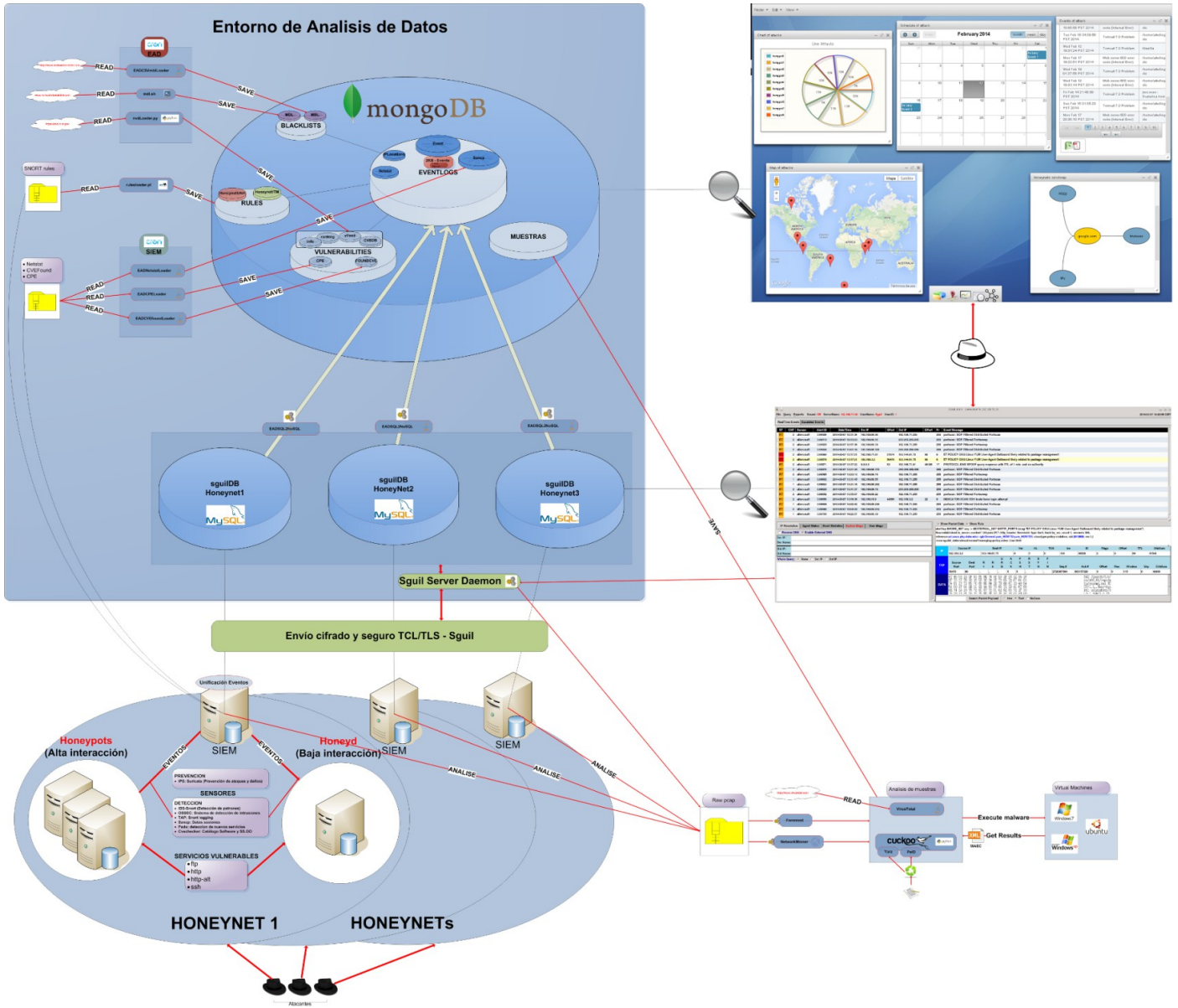


- Plataforma **virtual.**
- Honeynet **alta interacción.**
- Honeynet de **baja interacción.**
- Plataforma **centralizada de gestión para varias honeynet.**



Investigación y Análisis de Malware (II)

- **Honeynet: Arquitectura del sistema.**



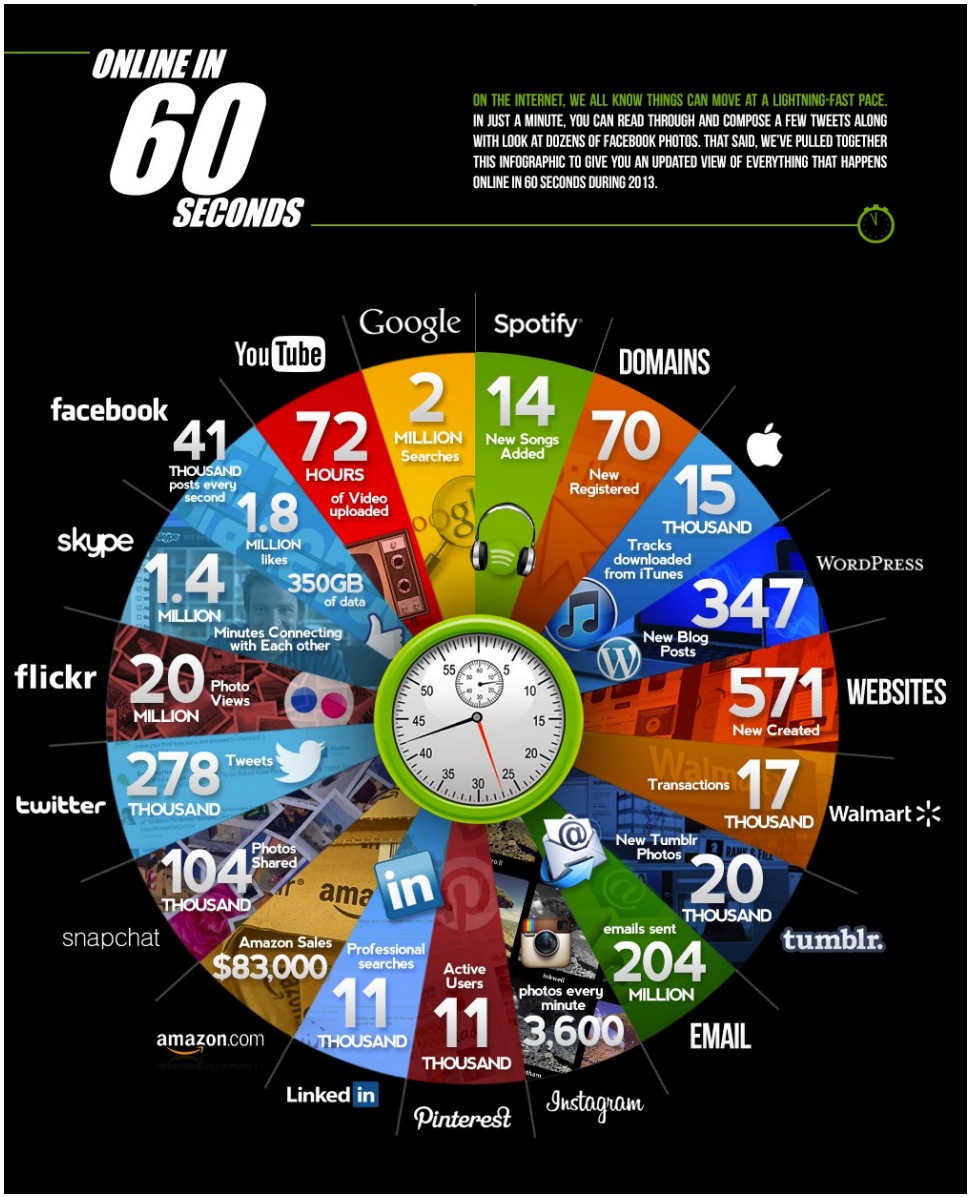
Investigación y Análisis de Malware (III)

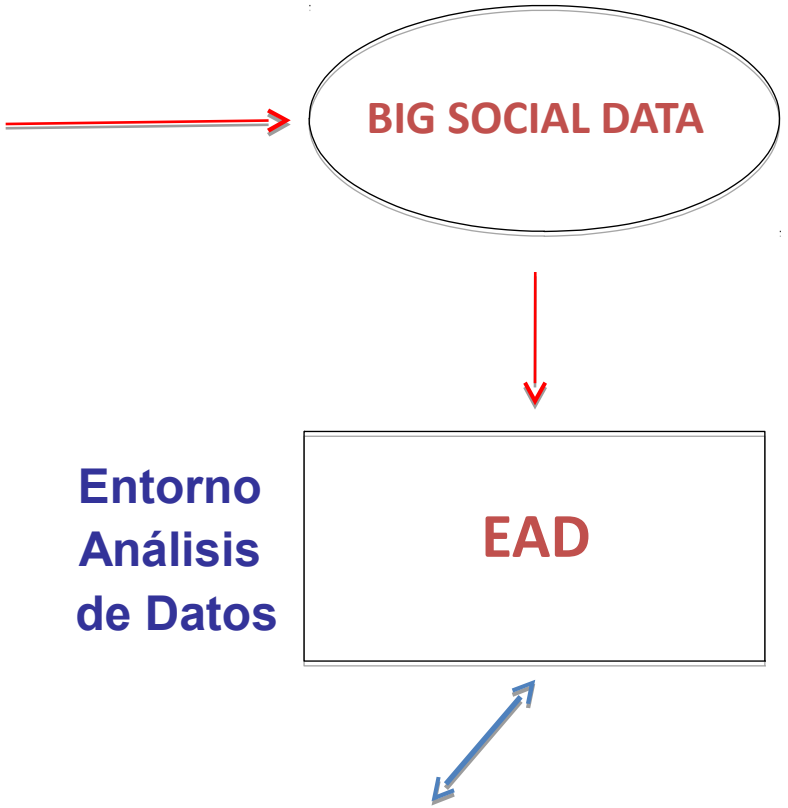
Entorno Análisis de Datos (*EAD*)

EAD *workbench* para análisis de datos generados por la Honeynet mediante técnicas de ***Inteligencia Artificial*** que permite**:**

- *Agrupación* de eventos de seguridad en un único punto.
- Categorización de los datos recogidos mediante *ontologías* que recojan el estado del arte (malware) y posibiliten mecanismos de inferencia
- *Análisis de tendencias* de ataque y *detección de orígenes comunes* de los atacantes (País, IP , métodos utilizados).
- *Reconocimiento de patrones* mediante conexiones a repositorios y herramientas de terceros (DDBB vulnerabilidades y malware; herramientas de análisis dinámico ejecutadas en *sandboxes*)
- Aplicación *técnicas de ML (aprendizaje automático)* para encontrar patrones ocultos para comprender e interpretar mejor la información producida y gestión del conocimiento en entornos de producción

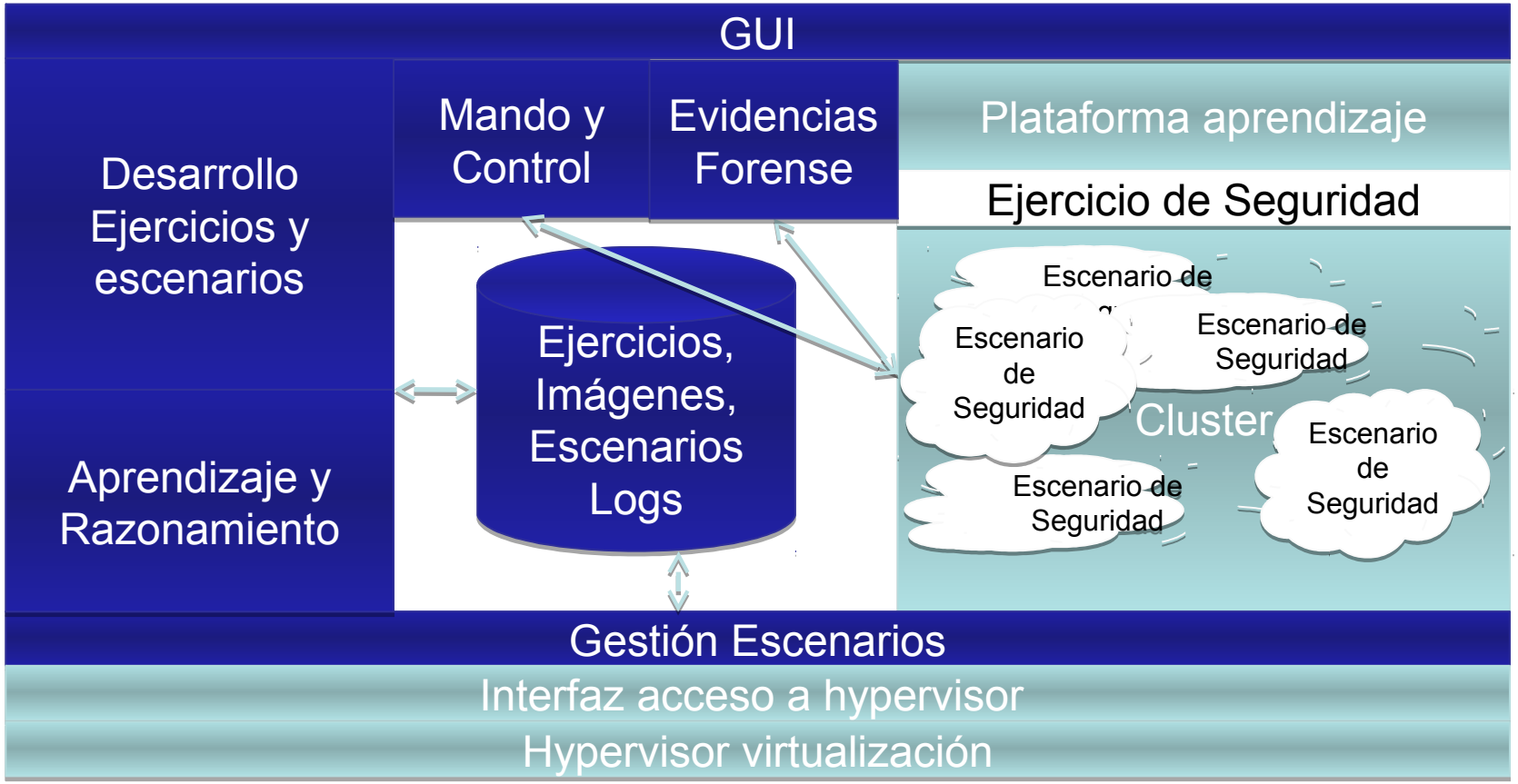
Investigación y Análisis de Malware (IV)





- Patrones sociales, económcos, políticos (Social Network Análisis)
- Tendencias sociales o económicas (Sentiment Analysis)
- Terrorismo (DarkWeb)

Generación Escenarios de Ciberdefensa (I)



Estrategias Futuras en I+D+i (I)

APT (Advanced Persistent Threat)

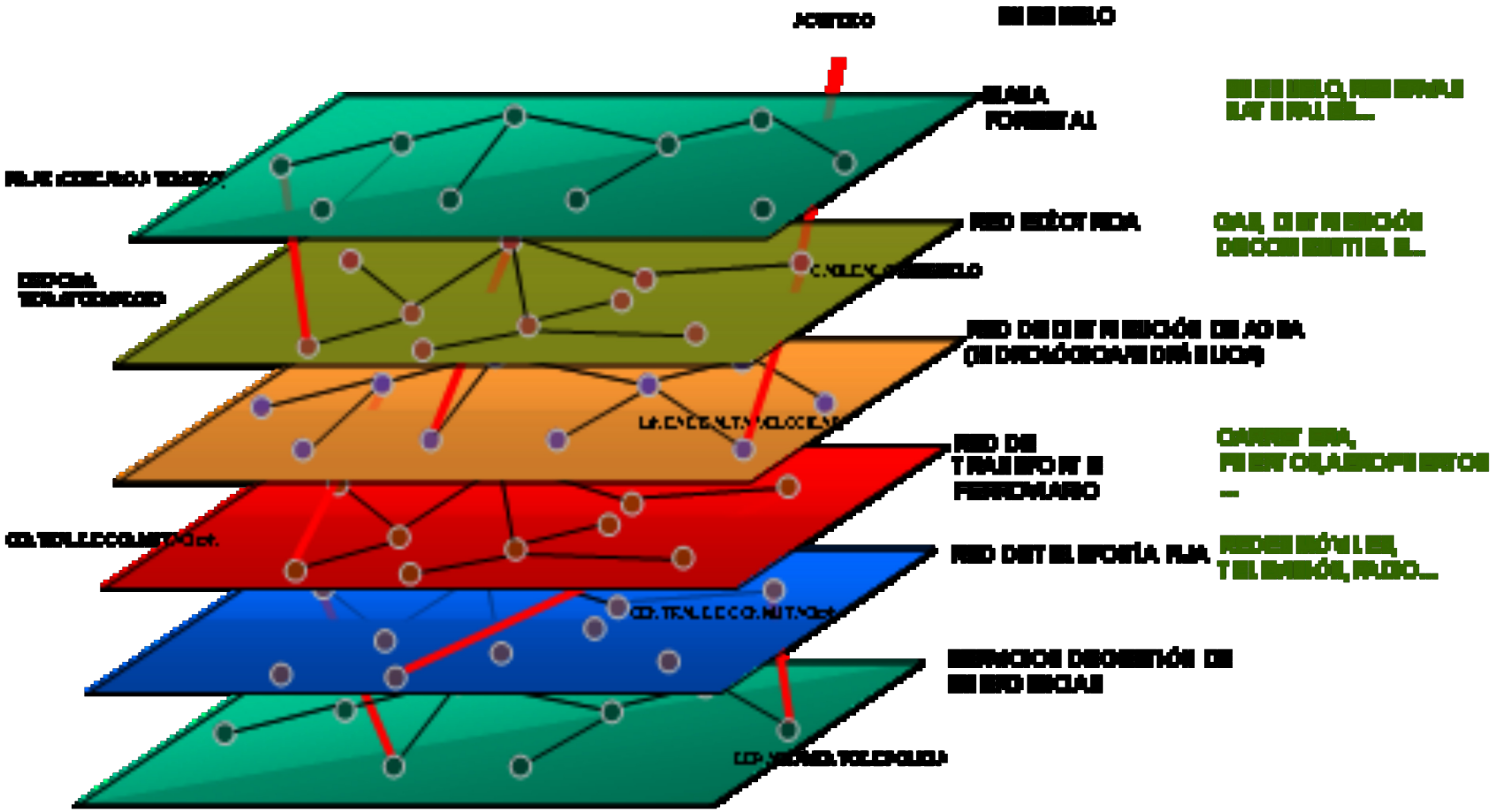
- Sofisticado ciberataque organizado, de *rápida progresión* y *largo plazo*, que constituye uno de los desafíos de seguridad más importante y peligroso, que deben afrontar hoy en día, las organizaciones e Infraestructuras Críticas.

- Aprovechan vulnerabilidades conocidas o de día cero de los sistemas y aplicaciones TIC, combinadas con técnicas de ingeniería social.

- El ciberatacante cuenta con varios métodos de ataque propagación u ocultamiento

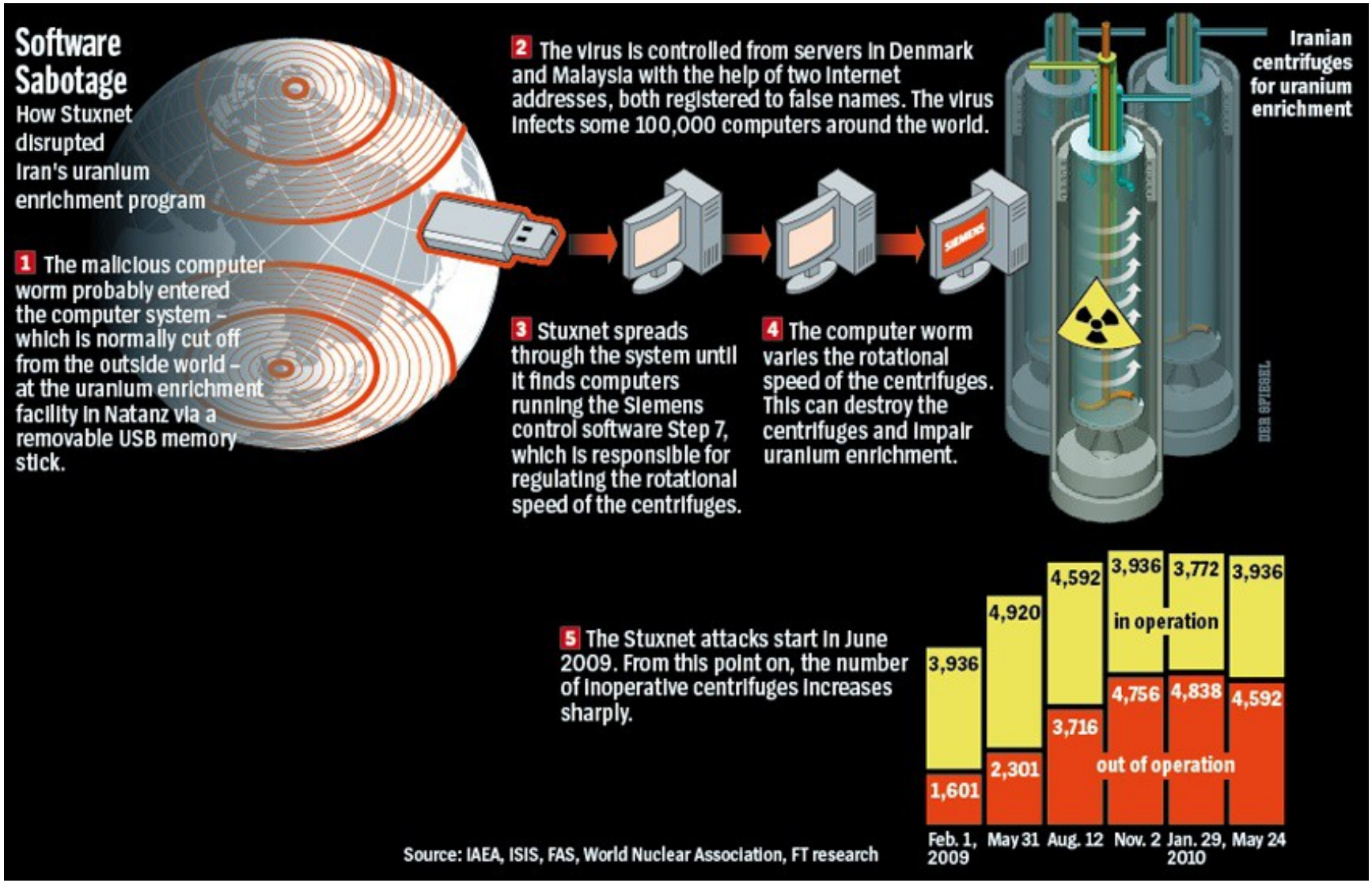
Estrategias Futuras en I+D+i (II)

Nodos Críticos



Estrategias Futuras en I+D+i (III)

Stuxnet



Estrategias Futuras en I+D+i (IV)

Propuesta de proyecto en el marco el programa H2020 de la Unión Europea.

"Secure societies – Protecting freedom and security of Europe and its citizens"

DS-3-2015: The role of ICT in Critical Infrastructure Protection

Estimated budget: 5,5 Meuros

- Objetivos :
- Desarrollar nuevas herramientas capaces de detectar malware APT a través de la agregación y fusión de datos procedentes de diferentes tipos de sensores.
- Diseño de una nueva arquitectura para los sistemas de detección de APT que se pueden implementar de forma transparente en sistemas integrados TIC-Sistemas Control Industrial.
- Evaluar los nuevos modelos y enfoques en los ensayos de campo en estudios de casos críticos de la infraestructuras críticas.

Cooperación

LATINOAMÉRICA

colaboración

Participam do LATIn:

Univ. Presbiteriana Mackenzie, Escuela Superior Politécnica del Litoral (Equador), Univ. de la República (Uruguai), Univ. Nacional de Rosario (Argentina), Univ. Autónoma de Aguascalientes (México), Univ. Austral de Chile, Univ. Central de Venezuela, Univ. Católica San Pablo (Peru), Univ. del Cauca (Colômbia), Universiteit Leuven (Bélgica), Univ. de Alcalá (Espanha) e Univ. Paul Sabatier (França)

ESPAÑA

Periódico
“Estado de Sao Paulo”
(250.000 ejemplares/día)
6 de mayo 2014

http://www.estadao.com.br/noticias/vida,professores-criam-plataforma-para-escrever-e-publicar-livros-gratuitamente-1162603,0.htm