CRG – CYBERSECURITY RESEARCH GROUP

CAPACIDADES ESENCIALES PARA UNA CIBERDEFENSA NACIONAL

29 Octubre 2013. Panamá

Dr. Jorge López Hernández-Ardieta

indra

IBSI 2013

ÍNDICE

01. CIBERESPACIO Y CIBER CONFLICTOS

02. CAPACIDADES DE CIBERDEFENSA

03. CONCLUSIONES

indra

ASPECTOS CLAVE

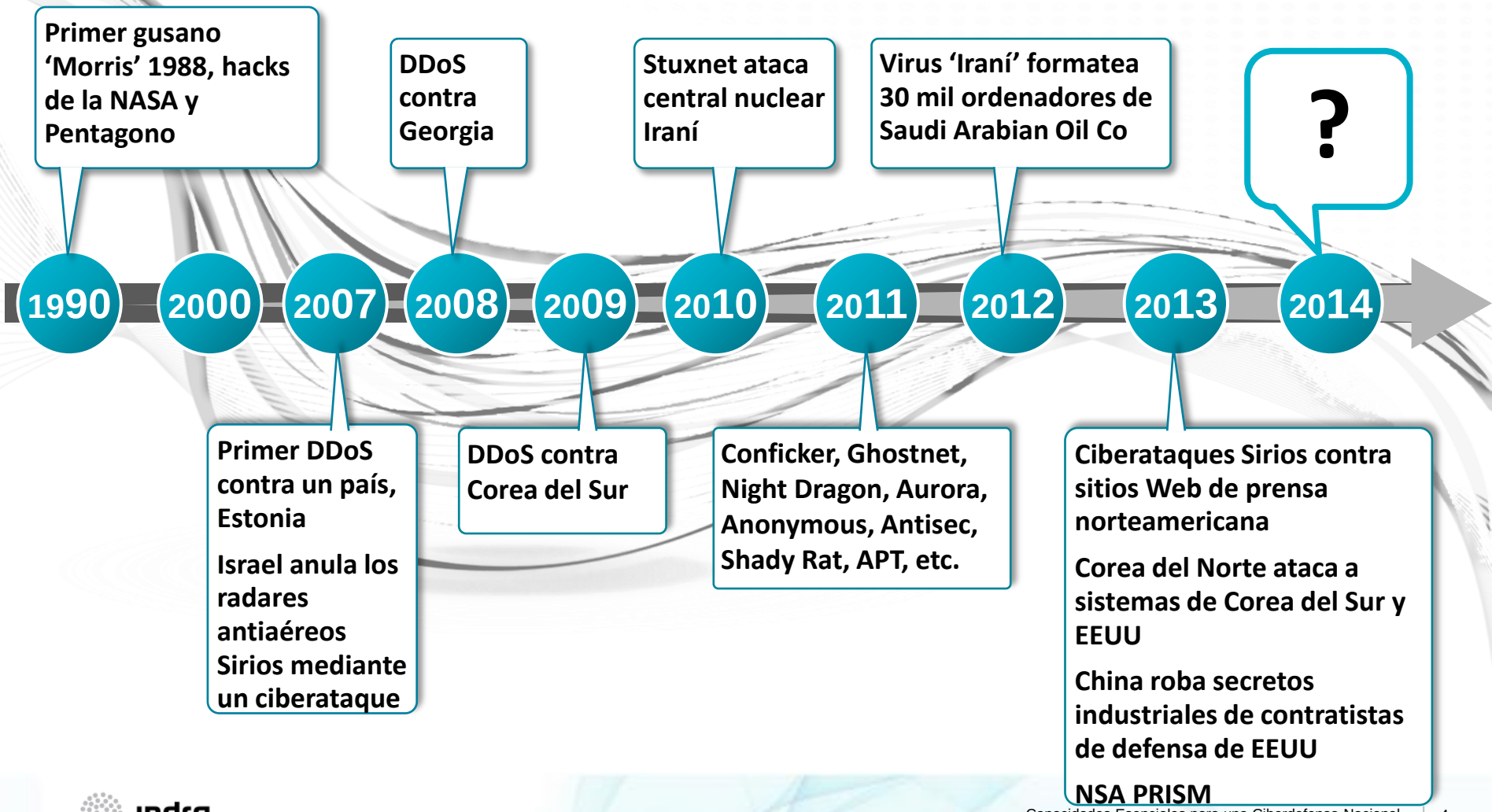
La evolución de las tecnologías de la información y las comunicaciones ha provocado un cambio de paradigmas que exige la adopción de procedimientos y herramientas especializadas para la neutralización y control de las amenazas cibernéticas.

EL INCREMENTO DE LA DEPENDENCIA EN E INTERCONEXIÓN DE LOS SISTEMAS DE INFORMACIÓN

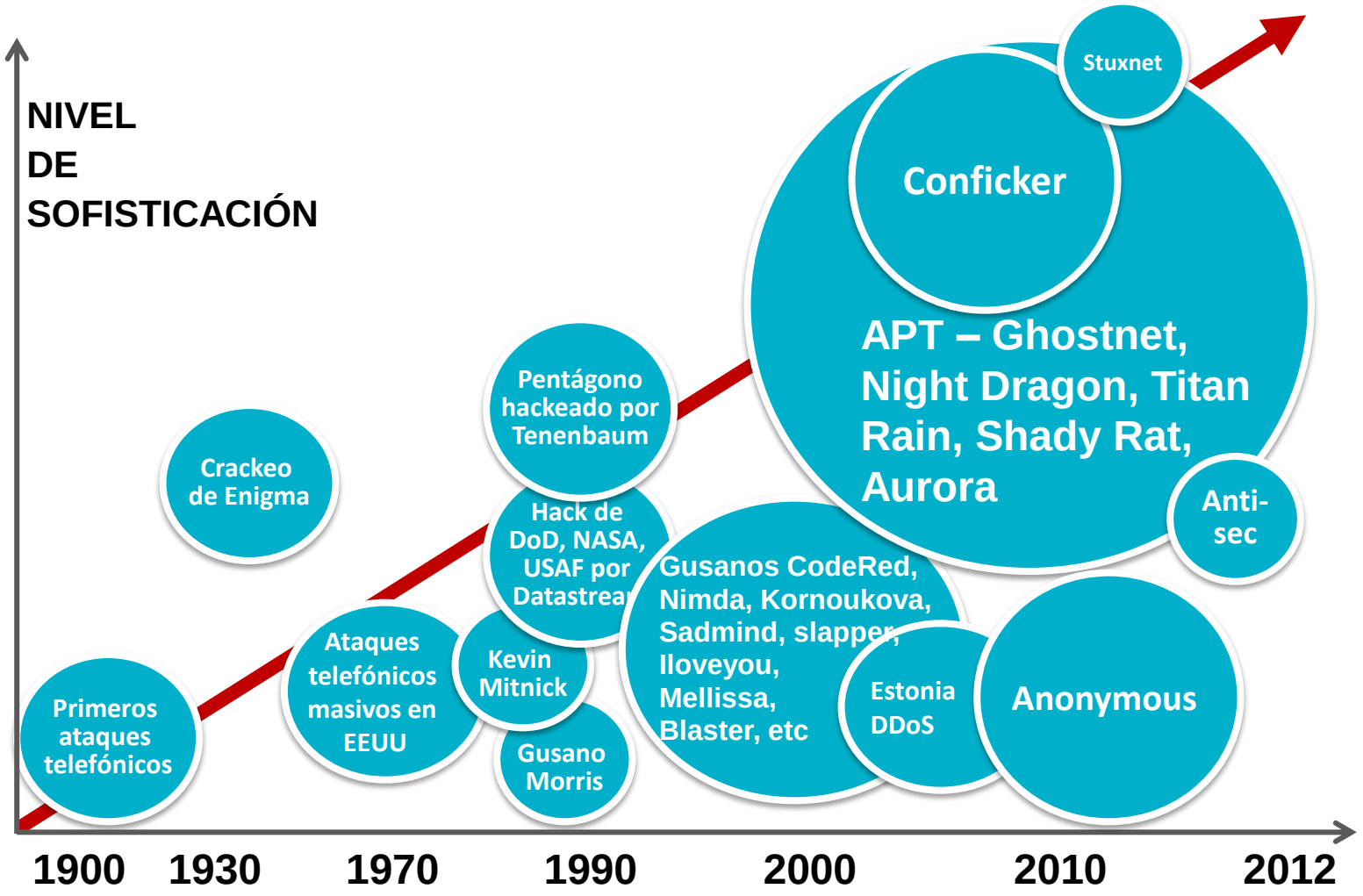
LA CRECIENTE COMPLEJIDAD DE LA TECNOLOGÍA

EVOLUCIÓN DE LAS CIBERAMENAZAS

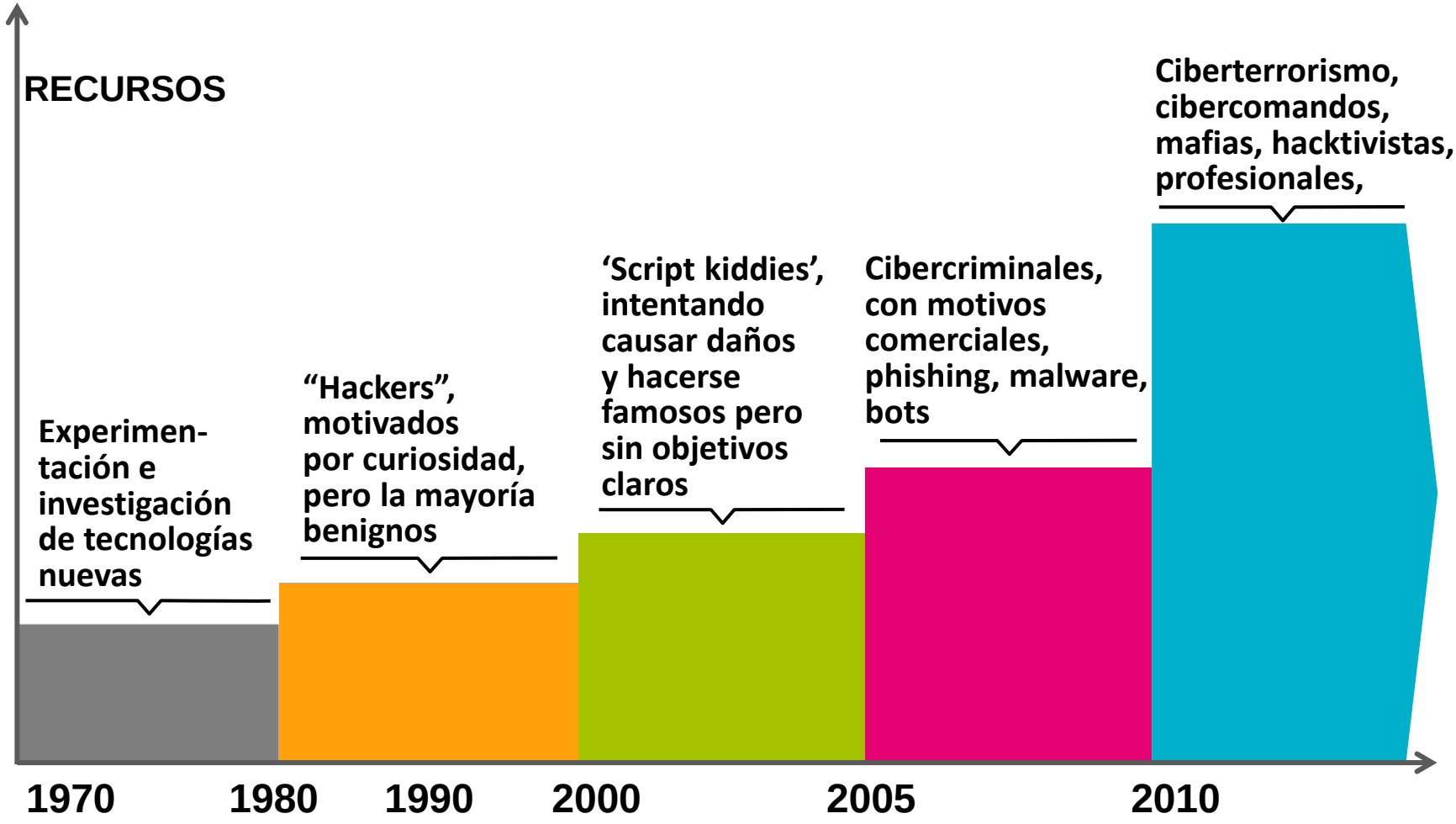
CRONOLOGÍA DE LOS CIBERATAQUES



AUMENTO EN SOFISTICACIÓN E IMPACTO



EVOLUCIÓN DE LOS ATACANTES



CIBER CONFLICTOS RECIENTES

EL PAÍS, viernes 20 de agosto de 2010

El ordenador de Spanair que anotaba los fallos en los aviones tenía virus

mente por unos programas 'troyanos'

BBC NEWS

Home | UK | Africa | Asia

12 October 2012 Last upd

US prepare

Cyber-attacks could in
damage on the US as t
attacks on 11 Septemb
defence secretary has

Leon Panetta said the co
to take pre-emptive actio
attack was imminent.

EL PAIS

INTERNACIONAL

Estados Unidos y China, ante la primera ciberguerra fría

Obama firmó una orden ejecutiva la pasada semana que le otorga poderes especiales

ANTONIO CAÑO | Washington | 19 FEB 2013 - 20:06 CET 135

Archivado en: Barack Obama Guerra electrónica Ataques informáticos China Ciberactivismo Seguridad internet Asia oriental Activismo Guerra Estados Unidos Internet Norteamérica Asia Telecomunicaciones Conflictos América Comunicaciones

TO al experto de Atlas Capital Ignacio Cantos

30.000 ordenadores

The New York Times

WORLD | U.S. | N.Y. / REGION

AFRICA AMERICAS ASIA PACI

Panetta Warns o

By ELISABETH BUMILLER and THOM
Published: October 11, 2012

Defense Secretary Leon E.
States was facing the possi
increasingly vulnerable to
dismantle the nation's pow

El presidente Barack Obama durante una intervención en Washington este martes. / JIM LO SCALZO (EFE)

La Casa Blanca describió este martes los reiterados ataques cibernéticos, que una investigación reciente vincula directamente con una unidad secreta del Ejército chino, como "un serio desafío para la seguridad y la economía de Estados Unidos", lo que es la señal de que una nueva guerra fría, en el desconocido e incontrolable espacio de Internet, ha comenzado entre las dos grandes potencias que se disputan la supremacía en el siglo XXI.

Sin acusar directamente a China, por

los 'ciberataques'
chino revela una
pocos esconden

Edificio de la 'Unidad 61398'. | Foto: City8.com, via Mandiant

REUTERS

Tech | Opinion | Breaking

Exclusive: Inside
cyber attack

By Jim Finkle
Fri Sep 7, 2012 4:52am EDT

(Reuters) - One or more insiders with high-lev
access are suspected of assisting the hacker
damaged some 30,000 computers at Saudi A
national oil company last month, sources fam
with the company's investigation say.

indra

espías australianos

JOSE REINOSO | Pekín 4

Piratas informáticos chinos roban los planos de la nueva sede de la agencia australiana de espionaje, según la cadena ABC

ro Mejía (Efe) | Washington

tualizado jueves 21/02/2013 10:11 horas

Comentarios

revelación de identidades y 'modus operandi' de los miembros de la
puesta unidad de 'hacking' más secreta del Ejército chino ha sido
al sector priva
el gobierno.
talladа hasta el extremo y los expertos consideran que China

CAMBIOS EN LA DOCTRINA MILITAR

Varios países, incluyendo EEUU, han reconocido el ciberespacio como el quinto dominio de la guerra, y están desarrollando formas de operar en estos nuevos teatros de operaciones.

SEGURIDAD | España

Defensa crea el Mando Conjunto de Ciberdefensa frente a las 'ciberamenazas'

Efe | Madrid

Actualizado martes 26/02/2013 13:19 horas

BBC News Sport Weather Travel Future

NEWS ASIA

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Envi

Asia Business China India

15 March 2013 Last updated at 09:10 GMT

North Korea says US 'behind hack attack'

Gobiernos y organismos internacionales, entre ellos la OTAN, han creado Centros de Ciberdefensa para defenderse contra las amenazas ciberneticas.

PROPIEDADES DE LOS CIBER CONFLICTOS

- El ciberespacio evoluciona continuamente y presenta un comportamiento impredecible
- La información disponible requiere un procesamiento y refinamiento constante
- Los ciberconflictos demandan respuestas rápidas cercanas al tiempo real, con alto impacto
- Efectos ciber-kinéticos de los ciberataques
- La cooperación como eje fundamental para el éxito, pese a las dificultades que implica
- El adversario juega un papel activo, y la atribución es altamente compleja

ÍNDICE

01. CIBERESPACIO Y CIBER CONFLICTOS

02. CAPACIDADES DE CIBERDEFENSA

03. CONCLUSIONES

indra

EL CONCEPTO DE CIBERDEFENSA

Se centra en las medidas técnicas, políticas y organizativas que protegen los sistemas y redes militares de ciberataques, e incluye las capacidades de reacción y ataque propias de un conflicto armado (utilizando el ciberespacio).

La protección puede extenderse a sistemas de información de terceros (civiles) que puedan resultar críticos para la nación o la misión.

Desde un punto de vista práctico, la ciberdefensa se sustenta mayoritariamente en tecnología de ciberseguridad ampliamente probada y desplegada en el sector civil.

No obstante, se está viendo la necesidad de desarrollar nuevas tecnologías así como reorientar las ya existentes.

CAPACIDADES ESENCIALES

Una ciberdefensa que garantice una protección y reacción eficaz frente a las ciberamenazas debe sustentarse en un amplio conjunto de soluciones, incluyendo aspectos organizativos, procedimentales y tecnológicos

CENTRO NACIONAL DE CIBERDEFENSA

La capacidad militar de ciberdefensa se basa en el concepto de un centro de ciberdefensa que provee el apoyo técnico y la coordinación para poder contrarrestar los ataques cibernéticos y desplegar acciones ofensivas y de respuesta activa.

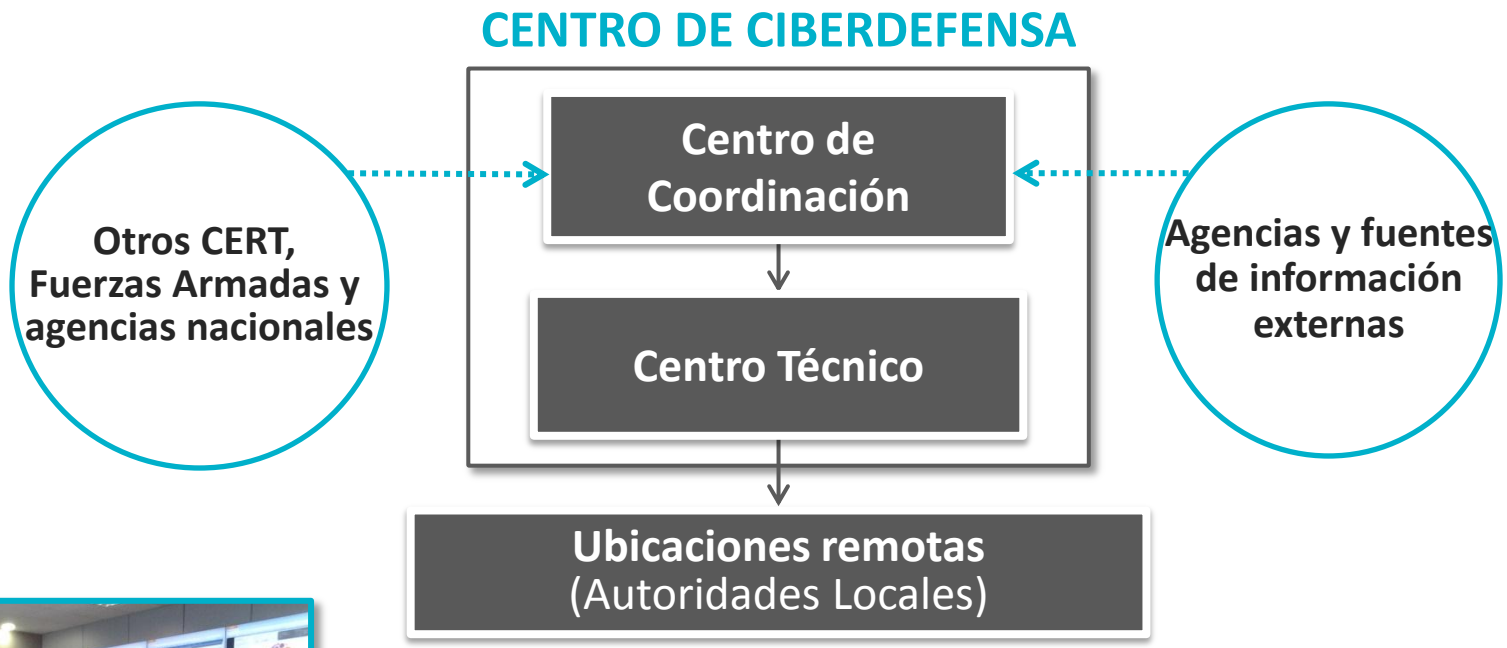
OBJETIVOS

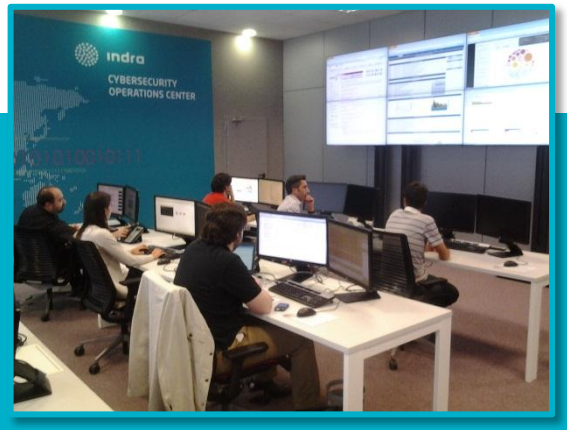
- Proveer y coordinar servicios de apoyo técnico y de creación de políticas
- Proveer y coordinar la capacidad de apoyo a las respuestas ante incidentes de seguridad cibernética (CERT)
- Ejecutar y coordinar ciberoperaciones

RESPONSABILIDADES

- Preparación de capacidades
- Protección de activos TI militares y críticos (civiles)
- Detección y análisis de incidentes
- Respuesta ante incidentes
- Respuesta activa y despliegue de ciberoperaciones
- Coordinación con agencias externas

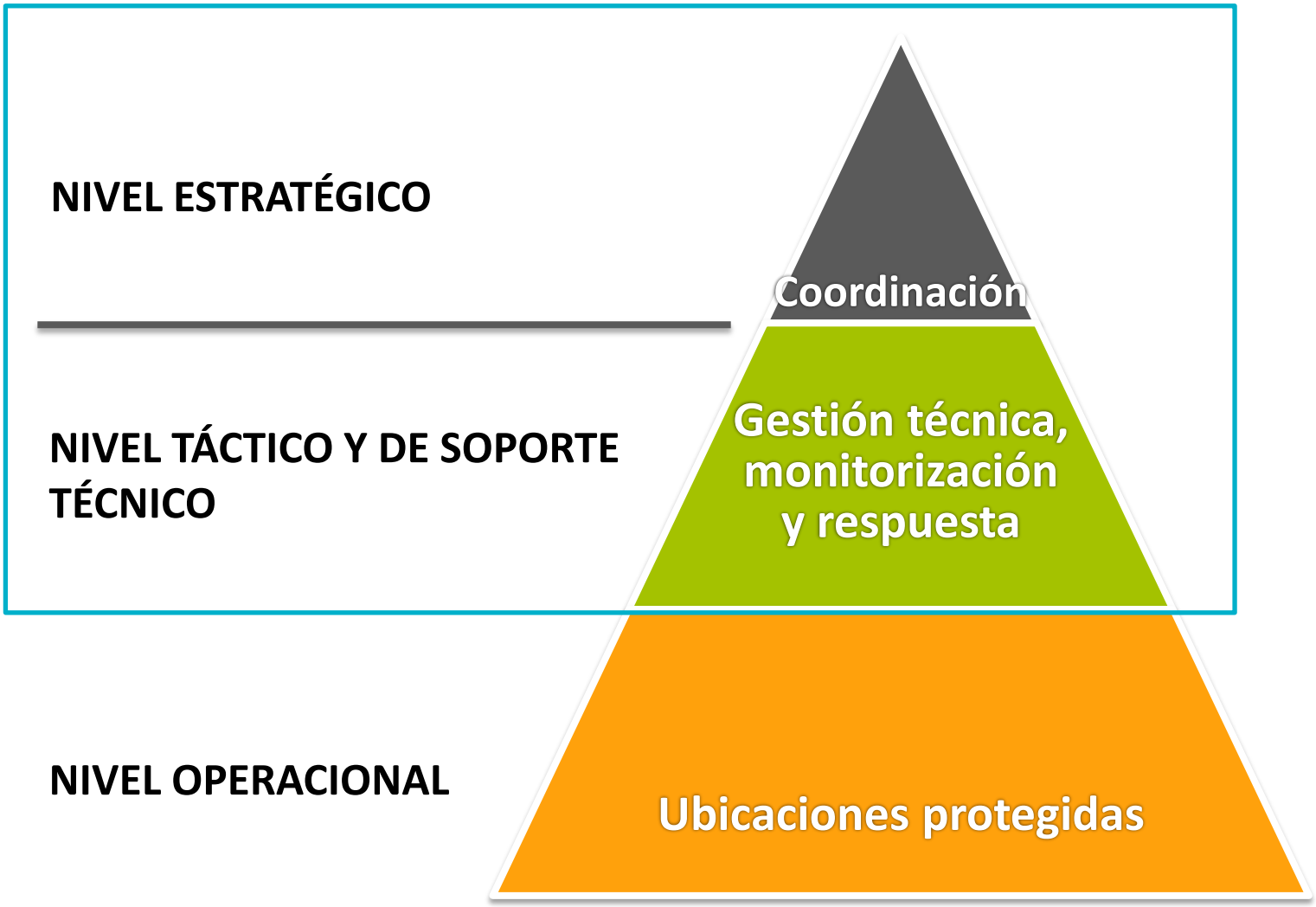
CENTRO NACIONAL DE CIBERDEFENSA



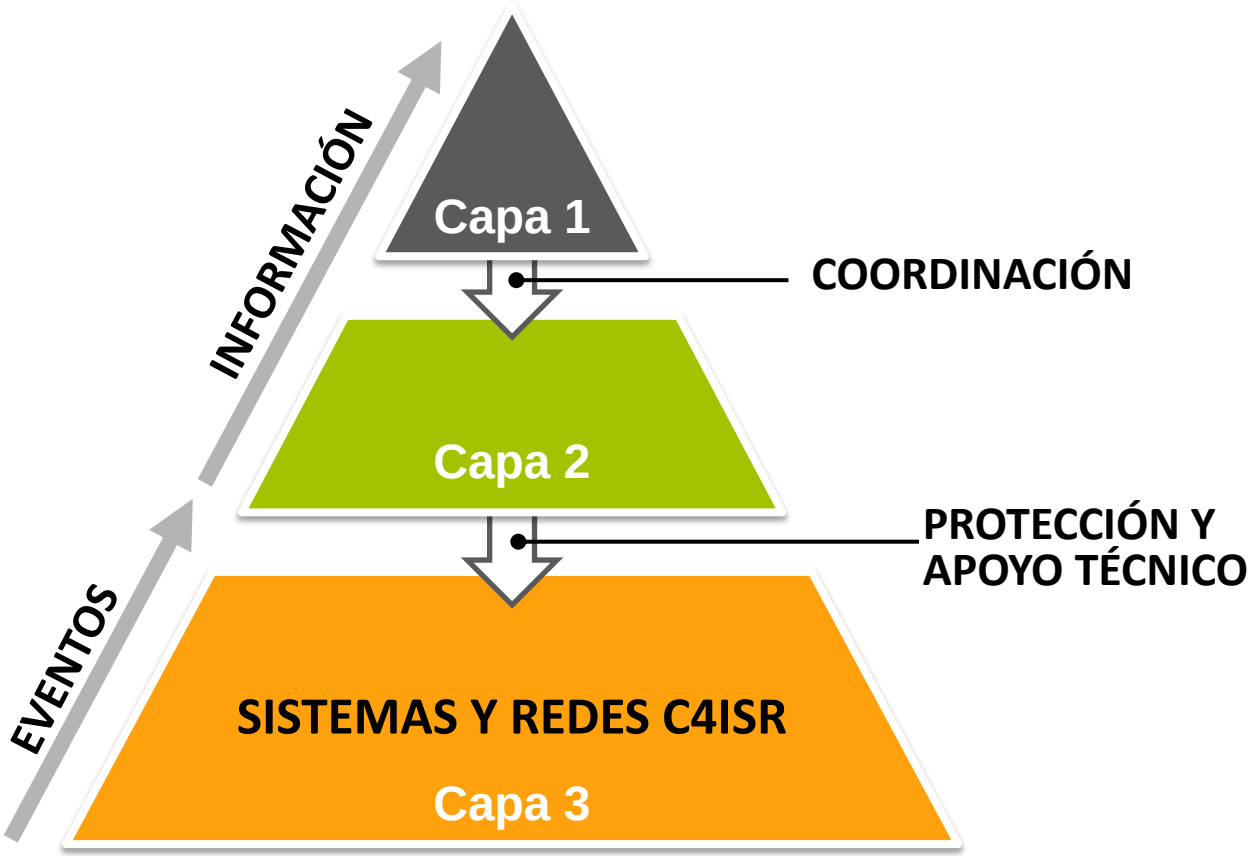


Un centro integrado de Ciberdefensa que coordina, monitoriza y provee la capacidad de detección y respuesta a la red operativa, cuyas autoridades locales son el responsable último de gestionar la seguridad de sus redes y sistemas

CENTRO NACIONAL DE CIBERDEFENSA

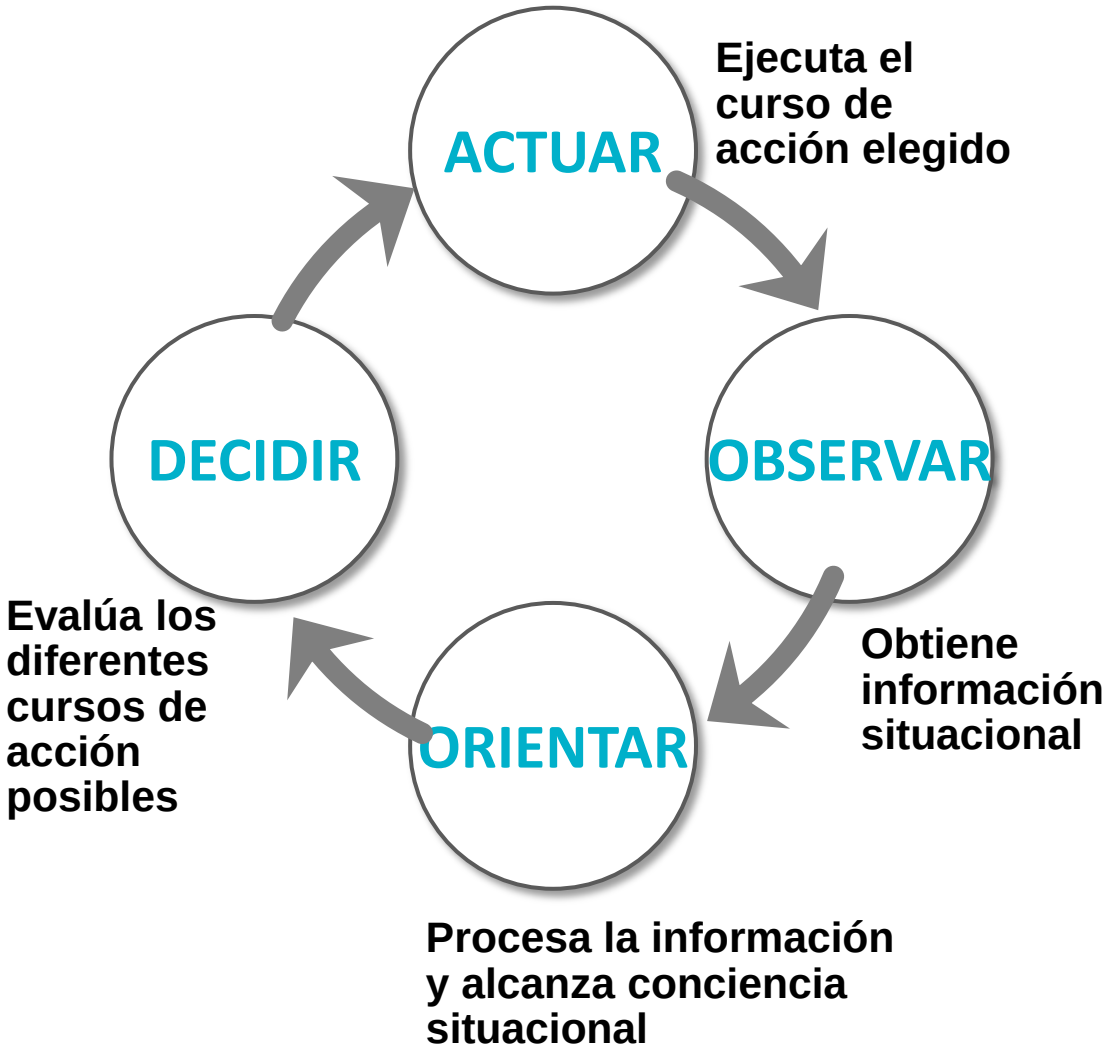


CENTRO NACIONAL DE CIBERDEFENSA



1. La capa 1 implementa la coordinación e inteligencia para dar conciencia situacional
2. La capa 2 monitoriza y provee respuesta a incidentes a la capa 3
3. La capa 3 administra sus sistemas y notifica los eventos de seguridad

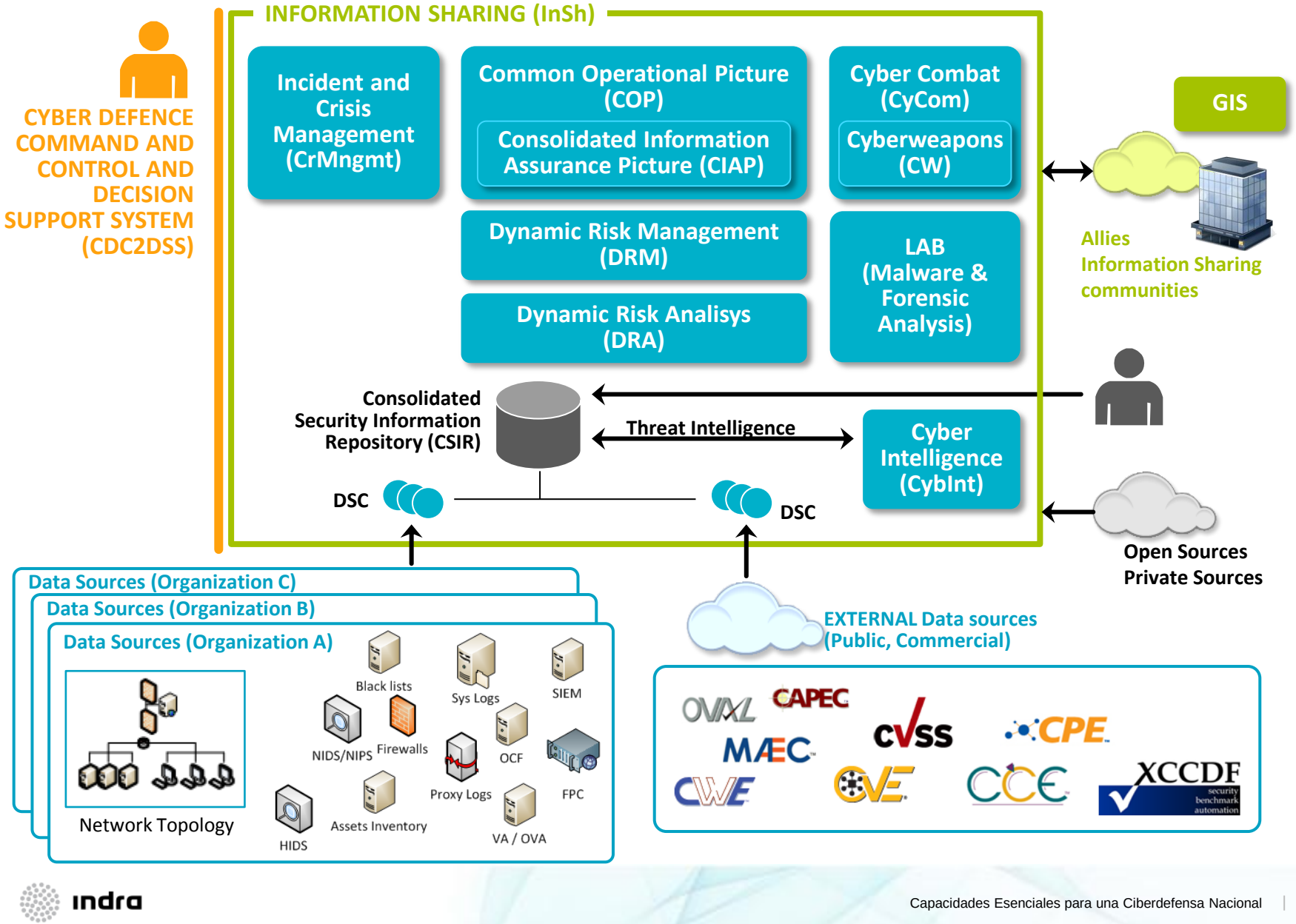
CICLO DE OPERACIONES



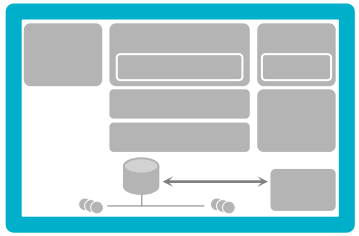
El bucle OODA debe adaptarse para evitar tomar decisiones basadas en información caduca (agilidad)

CICLO DE OPERACIONES

ARQUITECTURA FUNCIONAL



ARQUITECTURA FUNCIONAL



INSH
INFORMATION SHARING

Interdependencia de redes y sistemas.

Complejidad creciente de la tecnología.

Conocimiento disperso en múltiples entidades heterogéneas.

La autoridad para decidir y actuar se encuentra repartida en diferentes dominios.

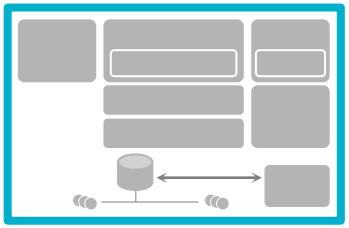
Evolución de las amenazas (ataques distribuidos, ciberarmas, actores financiados por Estados).

Ninguna entidad puede protegerse eficazmente por sí misma sin colaborar con otros socios y aliados.

Esto es especialmente relevante en los ciber conflictos, donde las acciones ofensivas y defensivas requieren aproximaciones multinacionales y multiorganizativas para operar en el ciberespacio.

LA COMPARTICIÓN DE INFORMACIÓN COMO ASPECTO CLAVE PARA LA CIBERDEFENSA COOPERATIVA

ARQUITECTURA FUNCIONAL



INSH
INFORMATION SHARING

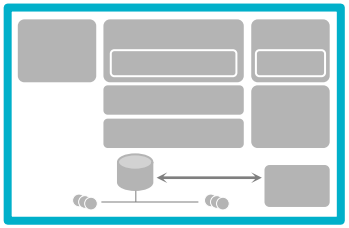
Un comportamiento egoísta puede ser dañino

- Baja calidad de conciencia situacional.
- Falta de conocimiento para resolver/atribuir un incidente de manera rápida y precisa.
- Socava la preparación propia y de los aliados.

Compartir información puede tener consecuencias negativas también

- Revelar una vulnerabilidad puede abrir la puerta a ataques dirigidos.
- Compartir cierta información colateral puede posibilitar al atacante inferir conocimiento sobre configuraciones vulnerables.
- ¿Quién controla el flujo de información?

ARQUITECTURA FUNCIONAL



INSH
INFORMATION SHARING

Existe una necesidad de razonar acerca de las repercusiones (coste-beneficio) de compartir información así como de estimar el riesgo de hacerlo.

Además, debemos afrontar las amenazas considerando la dimensión temporal.

- **Los ciberataques se extienden y pueden causar efectos en cascada en "tiempo máquina".**
- **En C4ISR, el tiempo es un factor crítico para la toma de decisiones.**
- **No podemos reaccionar a las amenazas en "tiempo humano".**

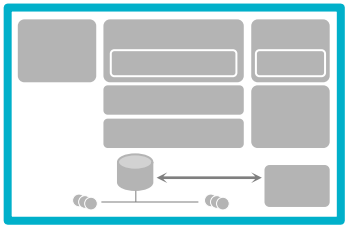
Necesitamos pasar de una compartición de información centrada en la persona a una automática en tiempo real que considere el riesgo

La complejidad de los ciber-incidentes y sus repercusiones exigen inevitablemente cierta participación de la persona durante la toma de decisiones.

El factor humano debería minimizarse, liberado de tareas que pueden automatizarse.

La automatización puede ofrecer mejores análisis cuantitativos del riesgo.

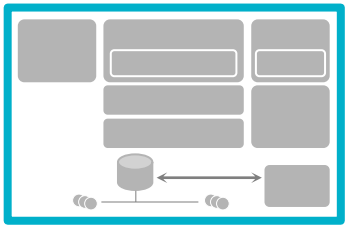
ARQUITECTURA FUNCIONAL



INSH
INFORMATION SHARING

- **Sistema INSH como middleware que ofrece mecanismos de compartición de información a los diferentes sistemas y capacidades que componen el sistema integral CDC2DSS**
- **Se espera que la compartición de información automatizada basada en políticas y consciente del riesgo que opere en tiempo (cuasi) real se convierta en una pieza central de cooperación en operaciones de ciberdefensa**
- **Los avances en otros dominios, especialmente las redes sociales y redes complejas, pueden contribuir a entender mejor y diseñar algoritmos y frameworks eficaces de compartición de información**
- **La confianza (Trust) y la privacidad son esenciales para adaptar la compartición de información a políticas y procedimientos de aplicación a cada ámbito concreto**

ARQUITECTURA FUNCIONAL



INSH
INFORMATION SHARING

Estándares sobre información estructurada de ciberseguridad y modelos formales pueden claramente ayudar a estudiar y razonar sobre muchos aspectos del problema de la compartición de información (coste-beneficio).

Assets (inventory) / Configuration guidance (analysis) / Vulnerability assessment (analysis) / Threat alerts (analysis) / Incident report (management) / Risk/attack indicators (intrusion detection)

	CPE	OVAL	SWID	XCCDF	CCE	OCIL	CCSS	CVE	CWE	CVSS	CAPEC	CVRF	MAEC	CybOX	IndEX	STIX	IODEF	CPE	CEE	RID	RID-T	CYBEX	CWSS
Asset	■	■	■															■					
Configuration		■		■	■	■	■																
Vulnerability		■						■	■	■		■											
Threat								■	■	■	■		■	■	■	■	■		■	■	■		
Incident	■							■					■	■	■	■	■	■	■	■	■		
Risk/attack	■	■			■			■	■	■			■		■	■	■			■	■	■	■

ÍNDICE

01. CIBERESPACIO Y CIBER CONFLICTOS

02. CAPACIDADES DE CIBERDEFENSA

03. CONCLUSIONES

indra

03. CONCLUSIONES

El ciberespacio es ahora el quinto dominio de la guerra

Las ciberoperaciones aumentan en número, impacto y sofisticación

Necesitamos desarrollar capacidades nacionales de ciberdefensa para proteger nuestras redes y activos tanto militares como civiles críticos para la nación

Las organizaciones civiles no protegidas bajo el marco nacional deben alcanzar un nivel de madurez adecuado, para mitigar el principio del eslabón más débil en un contexto interdependiente y sin fronteras

El análisis de un conjunto integrado de capacidades de ciberdefensa muestra que existen todavía numerosos retos que afrontar

Gracias

Dr. Jorge López Hernández-Ardieta
jlhardieta@indra.es

Avda. de Bruselas 35
28108 Alcobendas,
Madrid Spain
T +34 91 480 60 00
F +34 91 480 60 31
www.indracompany.com