Has sido tú !!
Te crees que no te he visto

EMILIO RICO RUIZ

TCol. (Cab) - Analista de Ciber Defensa

Fuerza de Operaciones (FOCE) del MCCE

ericorui@et.mde.es

¿De qué va esta charla?

Reino Unido construirá un centro de ciberdefensa capaz de lanzar ataques contra "estados hostiles"

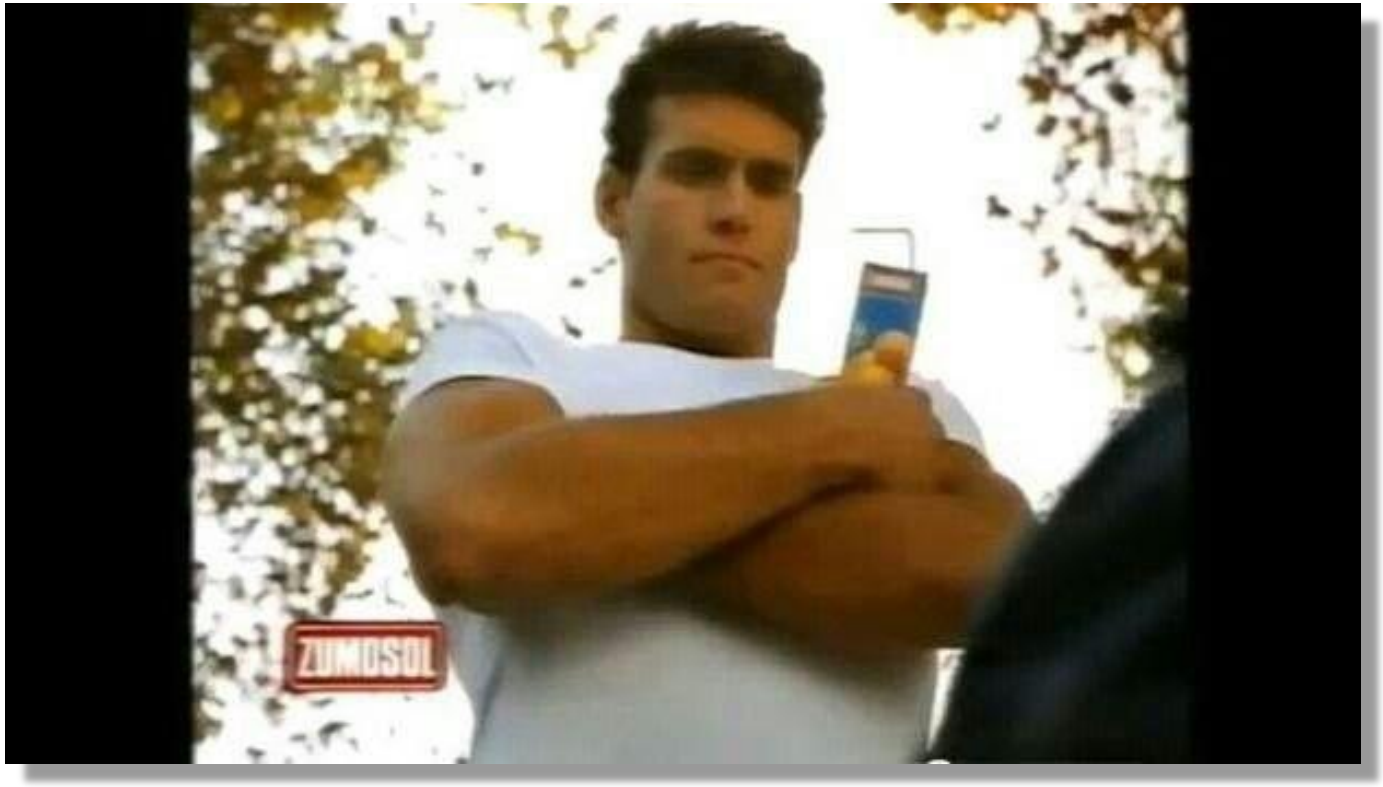
El ministro de Defensa de Reino Unido, Ben Wallace / (3 OCT - EUROPA PRESS)

"Mi deber es defender, pero parte de ello consiste en tener la habilidad de desmantelar las capacidades de tus adversarios para atacarte"

- La oficina empleará a miles de analistas y 'hackers' en 2030, poniendo al país "**a la cabeza**" de las naciones capaces de realizar ataques de este tipo

LA DISUASIÓN

Disuasión: Acción y efecto de disuadir.
Disuadir: Inducir, mover a alguien con razones a mudar de dictamen o a desistir de un propósito.



DISUASION: los dos caminos

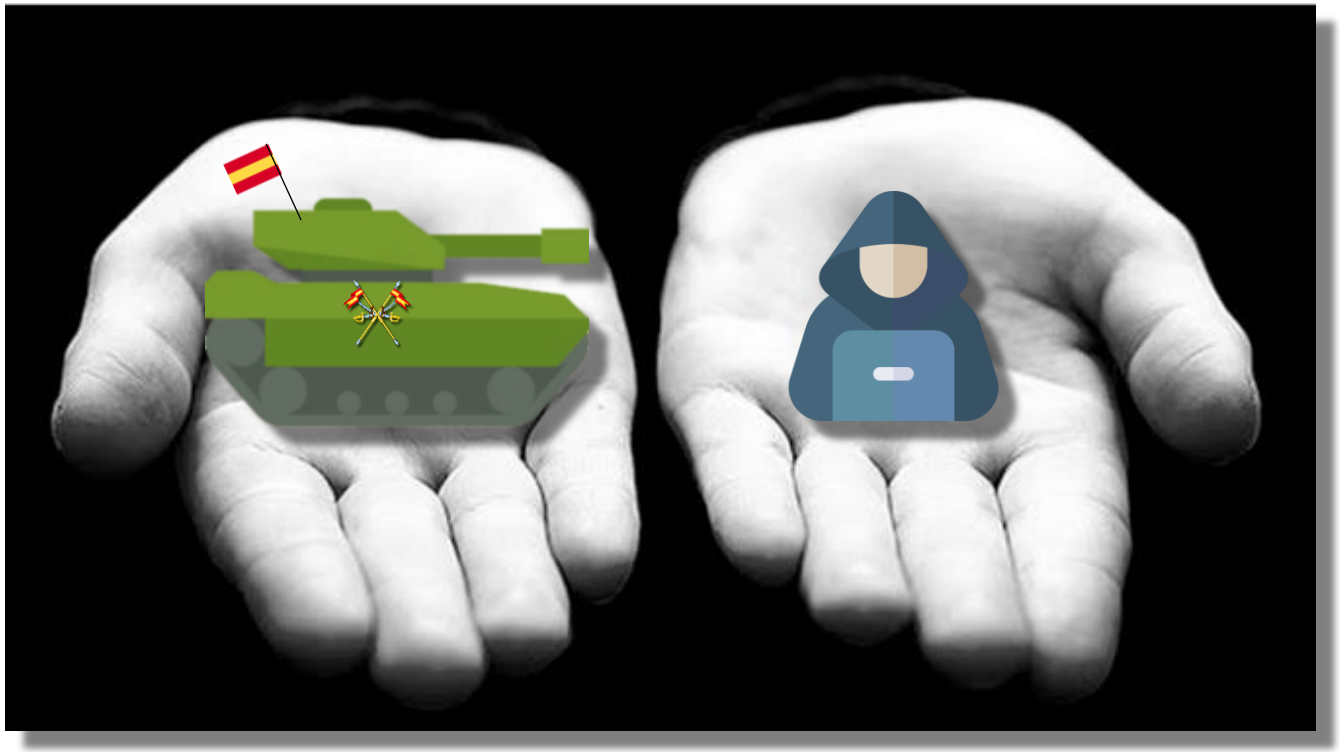
El potencial atacante ha de percibir (correcta o incorrectamente):
un **riesgo elevado frente al beneficio** que puede obtener con sus actividades

Disuasión por negación	Disuasión por represalia
Gran dificultad en conseguir el éxito: ▪ Coste económico. ▪ Dificultad técnica. ▪ Posibilidad de ser detectado identificado.	Riesgo elevado frente al beneficio obtenible: ▪ Probabilidad de sufrir represalias o castigo

CONSTRUYENDO la Disuasión

CREDIBILIDAD **DEFENSA** **ATAQUE** **VOLUNTAD**

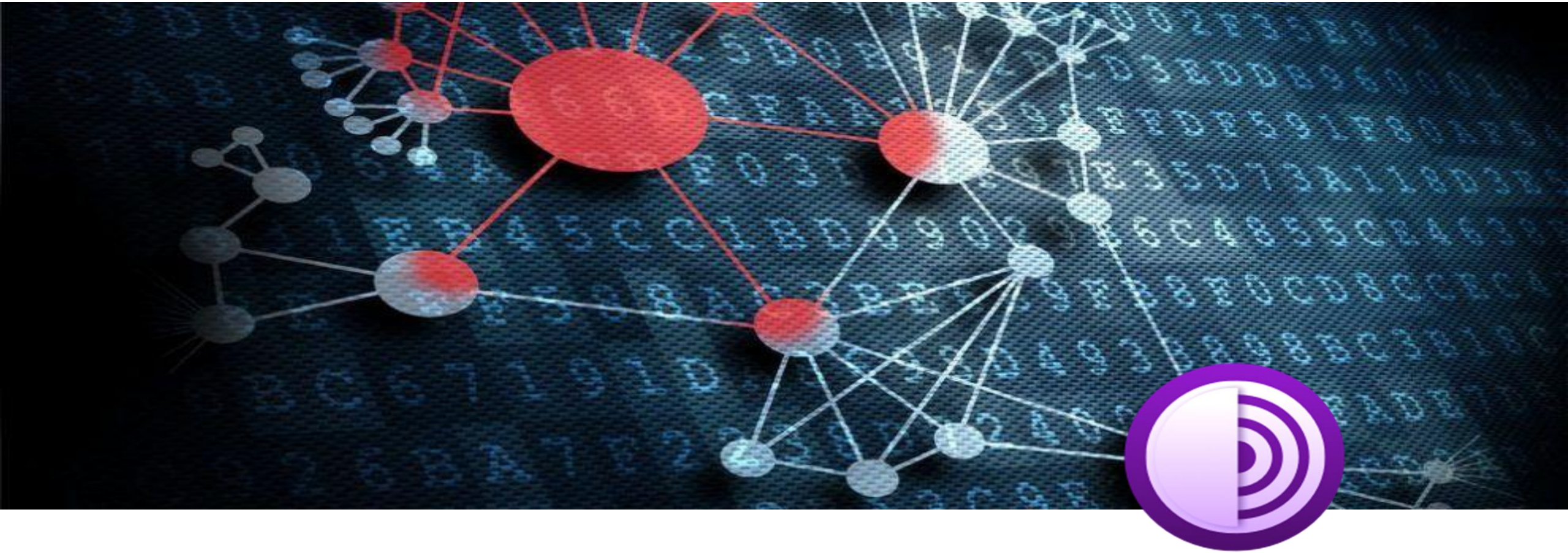
SÍ, sin RENUNCIAR a la Capacidad de Ataque



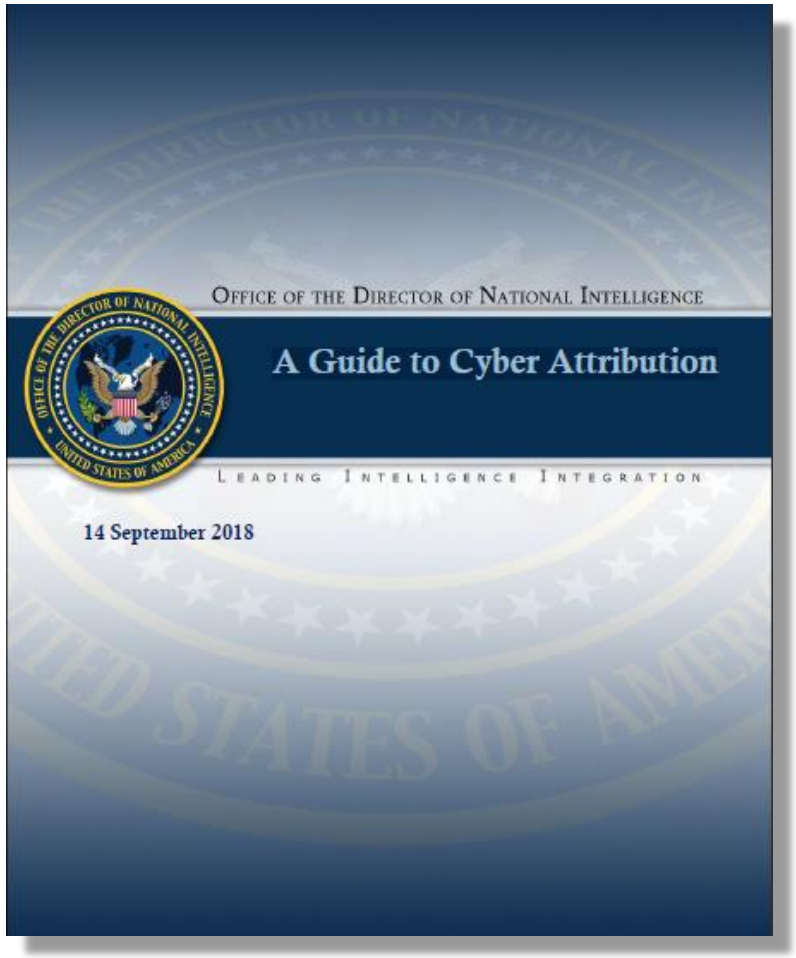
Descubrir procedimientos operativos, infraestructuras de ataque, fuentes de inteligencia, capacidades o limitaciones, proporcionan una información demasiado valiosa a terceros

La atribución

atribución: acción de atribuir.
atribuir: aplicar, a veces sin conocimiento seguro, hechos o cualidades a alguien o algo.



Referencias



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

A Guide to Cyber Attribution (2018)

- Todo tipo de operación cibernética, maliciosa o no, deja un rastro.
- No existe un proceso técnico simple o una solución automatizada para determinar la responsabilidad de las operaciones cibernéticas.
- Atribuir un ataque a un país o actor en particular requiere recopilar la mayor cantidad de datos posible para establecer conexiones con actores, individuos y entidades en línea.

https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf

A Guide to Cyber Attribution

Indicadores clave que permiten la atribución

01

Forma de trabajo

Comportamiento habitual al llevar a cabo un ciberataque. Los hábitos suelen ser más difíciles de cambiar que las herramientas empleadas.

02

Infraestructura

Estructuras de comunicaciones físicas o virtuales empleadas para llevar a cabo una cibercapacidad o mantener las capacidades de C2 (compra, alquiler, compartida, comprometida).

03

Malware

Software malicioso empleado para habilitar la ejecución de acciones no autorizadas en el sistema comprometido.

04

Intención

Compromiso del atacante a la hora de realizar ciertas acciones a partir del contexto

05

Fuentes externas

Informes procedentes de agentes externos para proporcionar datos o compartir hipótesis sobre los potenciales autores del ataque.

Los MÉTODOS

3 enfoques para rastrear y analizar las diversas características de las intrusiones por parte de actores de amenazas avanzadas.

(2011)
the Cyber Kill Chain

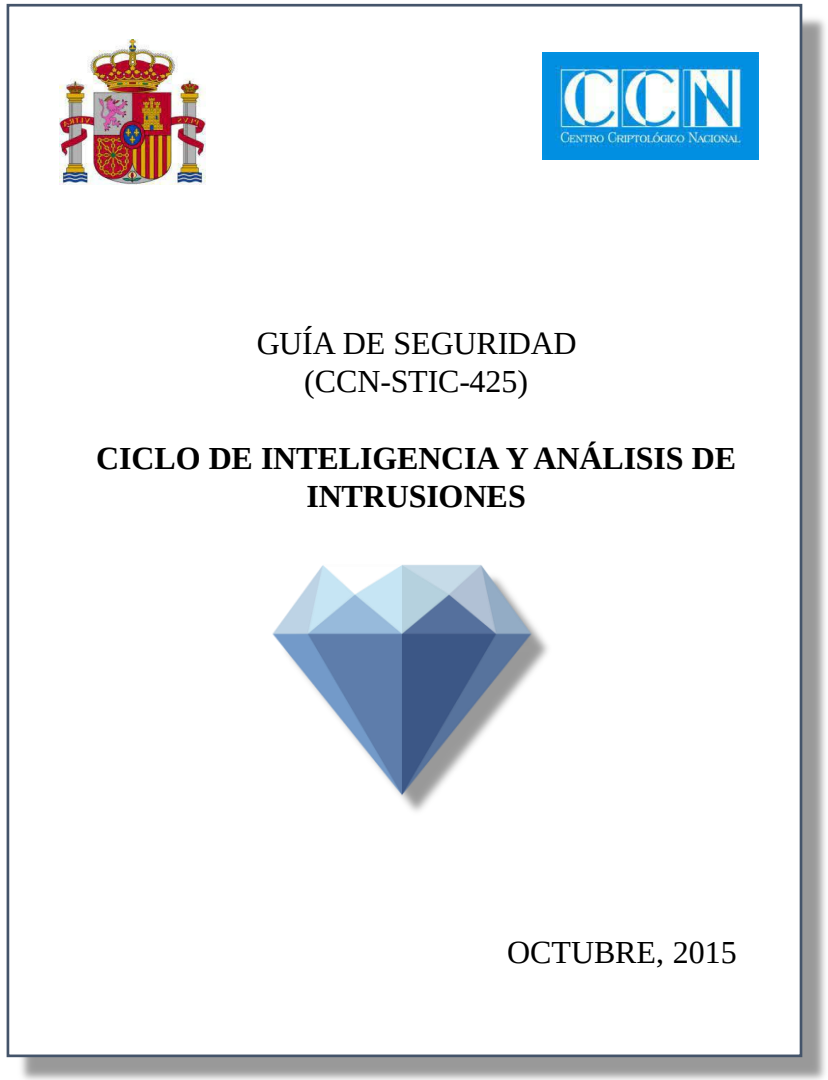
(2013)
the Diamond Model

(2015)
MITRE- matrix

The Cyber KILL CHAIN

Lockheed Martin - 2011

El modelo diamante



Sergio Caltagirone / Andrew Pendergrast / Christopher Betz

GUÍA CCN-STIC-425

El **Análisis de Intrusiones** pretende:

- DOTAR a los responsables de seguridad de las organizaciones-víctimas …
- de los MÉTODOS, PROCEDIMIENTOS y HERRAMIENTAS más adecuados …
- para DESCUBRIR, COMPRENDER y NEUTRALIZAR las operaciones del atacante.

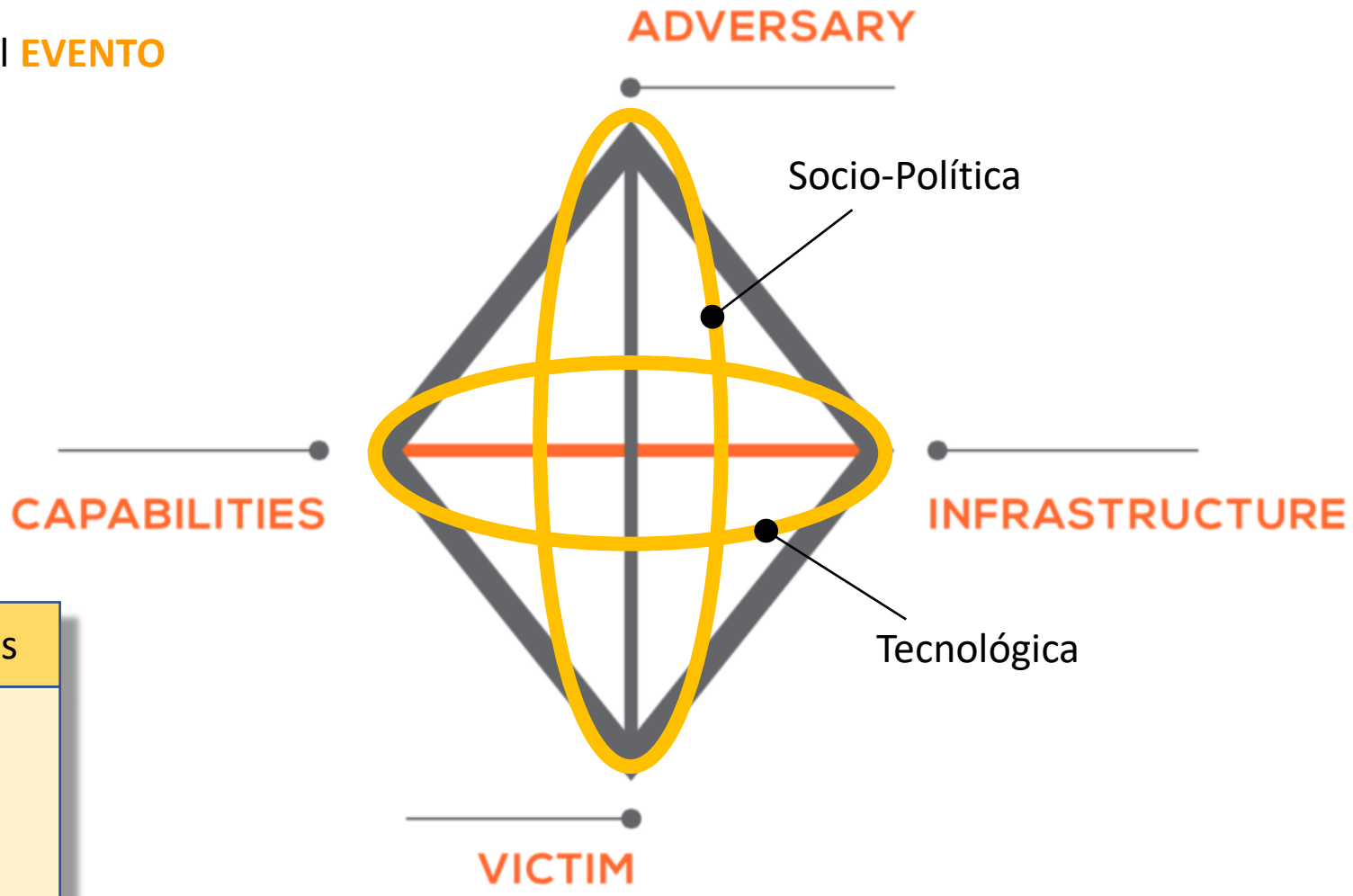
https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html

El modelo diamante 2

- El elemento básico del modelo es el **EVENTO**

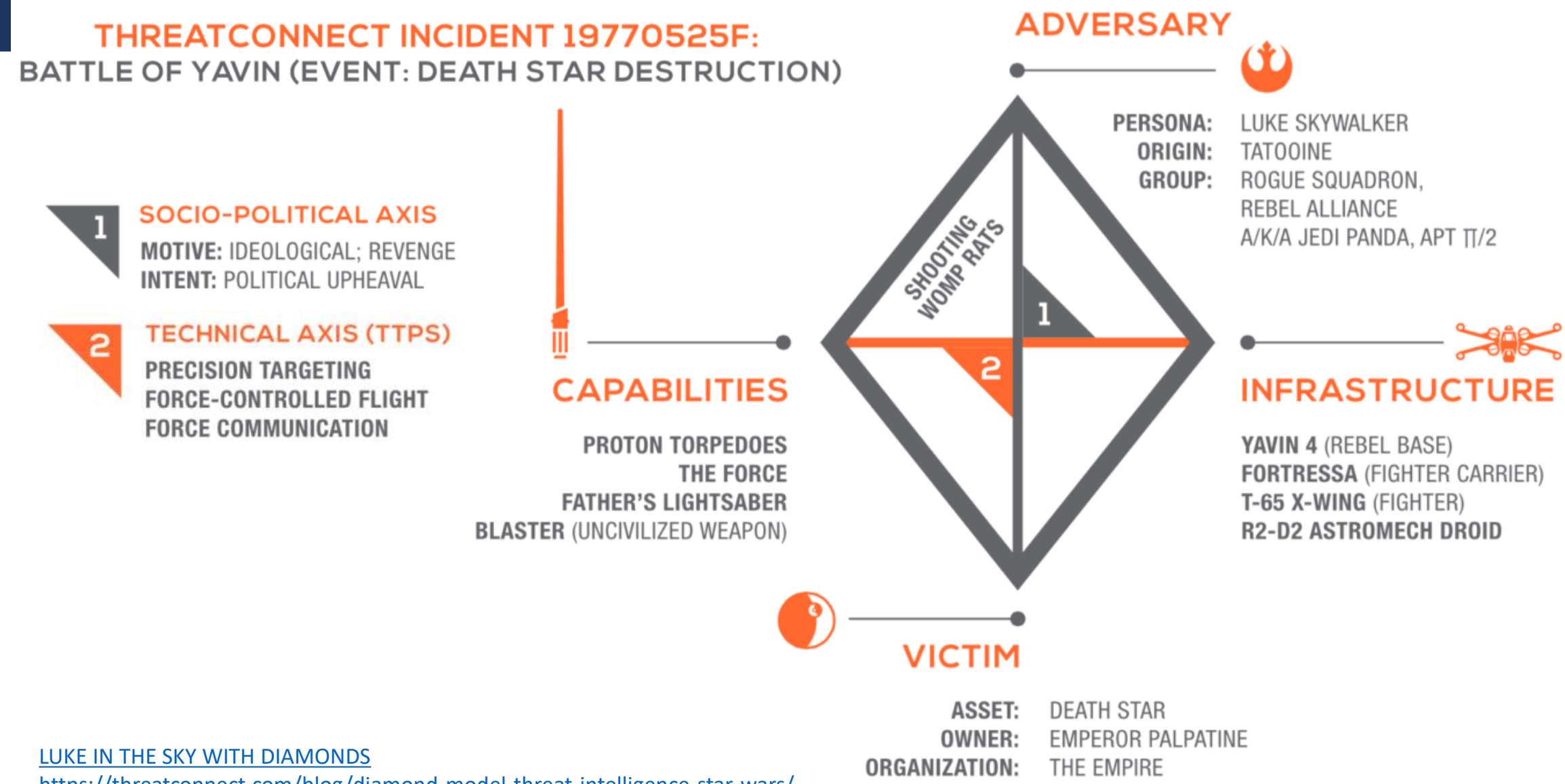
AXIOMA 1

Para cada Evento existe un **ADVERSARIO** que, haciendo uso de una **CAPACIDAD** desplegada sobre una **INFRAESTRUCTURA**, ataca a una **VÍCTIMA**, produciendo un determinado resultado.



META-Características
▪ Sello de tiempo ▪ Fase ▪ Resultado ▪ Dirección ▪ Metodología ▪ Recursos

El modelo diamante 3



LUKE IN THE SKY WITH DIAMONDS
https://threatconnect.com/blog/diamond-model-threat-intelligence-star-wars/

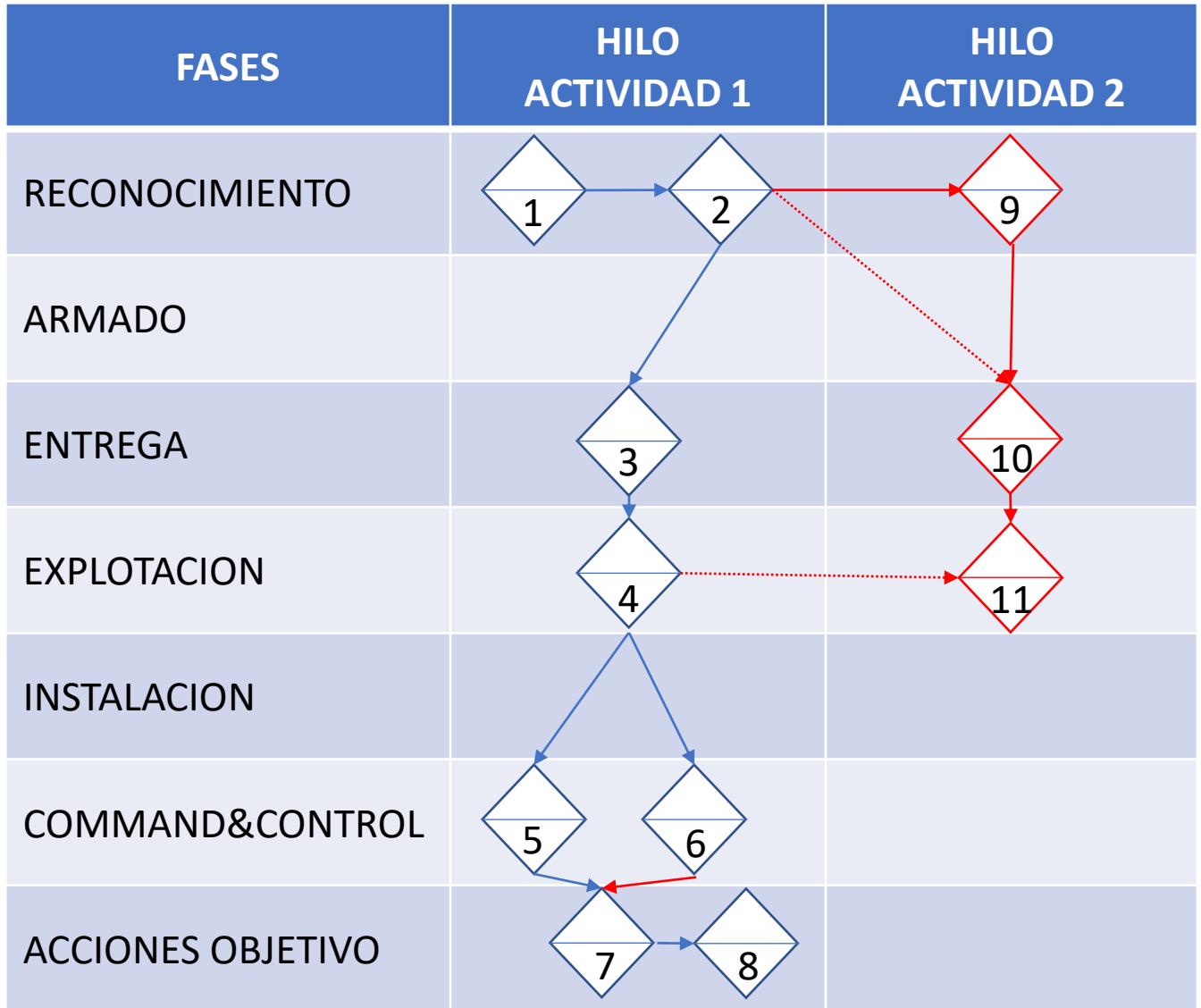
El modelo diamante 4

Hilos de actividad
(grafo orientado a fases)

↓

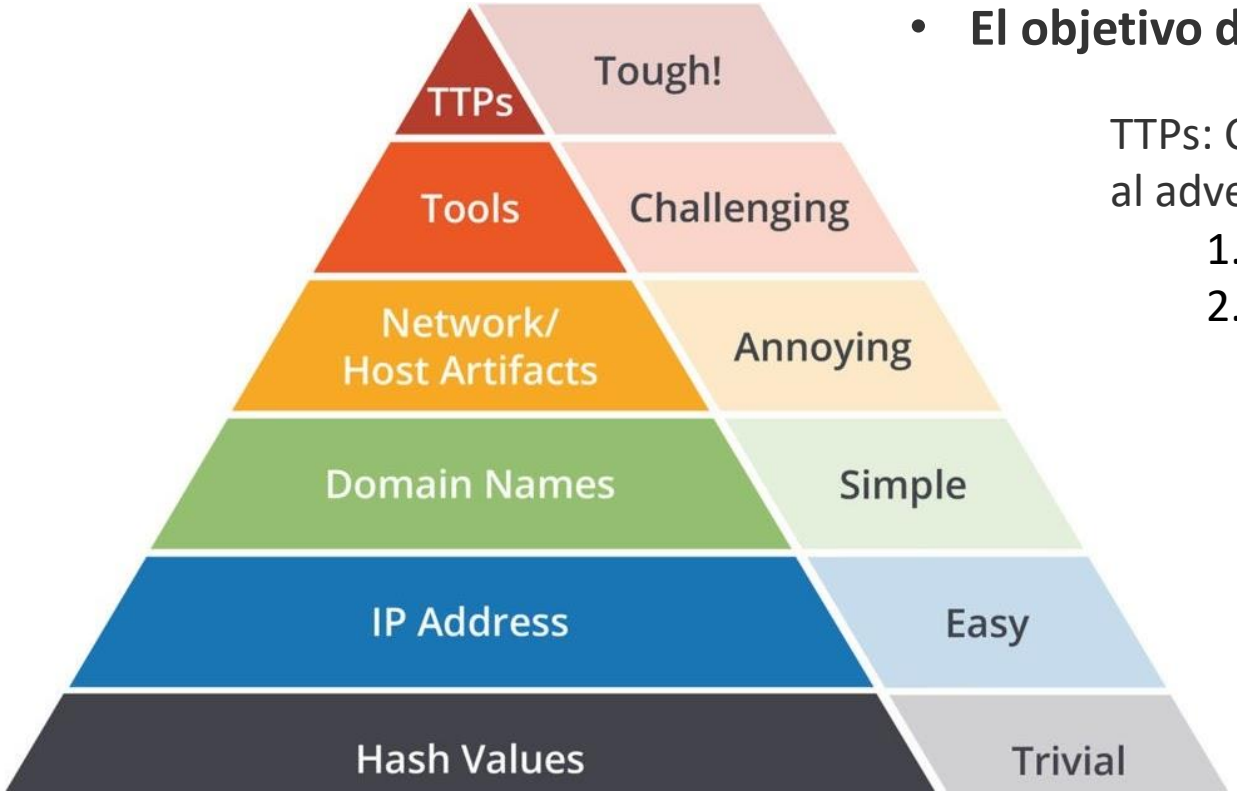
CYBER KILL CHAIN

Grafos de actividad-ataque
(soporte al análisis de hipótesis)



Nueva aproximación: las TTPs

Tácticas, Técnicas y Procedimientos



DavidJBianco (01/03/2013) - http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

- **El objetivo de detectar indicadores es responder a ellos.**

  TTPs: Cuando detectas y respondes a este nivel , al adversario solo le quedan dos opciones:

  1. Darse por vencido, o
  2. Reinventarse desde cero

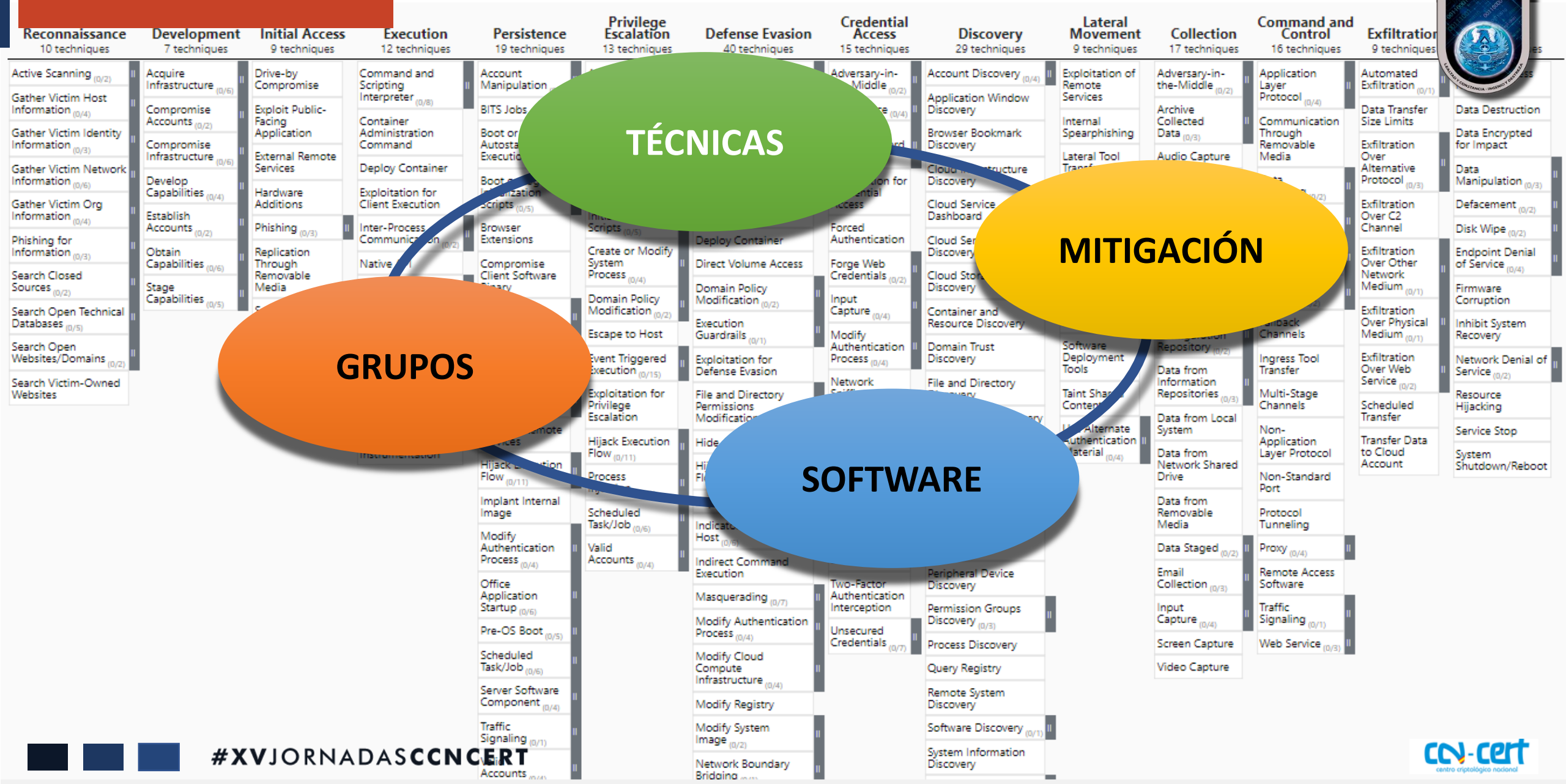
MITRE | ATT&CK®

Permite:

- Desarrollar analíticas
- Visualizar la amenaza
- Realizar una evaluación de las defensas
- Emular a los potenciales adversarios

V.01: 16 ENE 2018
V.10: 21 OCT 2021

MITRE | ATT&CK®



#XVJORNADASCCNCERT

MITRE | ATT&CK®

ENTERPRISE

MITRE PRE

1. Reconnaissance
2. Resource Development

MITRE ATT&CK™

3. **Initial Access**
4. **Execution**
5. **Persistence**
6. Privilege Escalation
7. **Defense Evasion**
8. **Credential Access**
9. **Discovery**
10. Lateral Movement
11. **Collection**
12. **Command & Control**
13. **Exfiltration**
14. Impact

MITRE | Engage

METAS

Prepare	Expose		Affect			PROVOCAR		Understand
Planning	Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation	Analysis
Define Exit Criteria	API Monitoring	Decoy Artifacts and Systems	Baseline	Decoy Artifacts and Systems	Decoy Artifacts and Systems	Application Diversity	Application Diversity	Distill Intelligence
Develop Threat Model	Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity	Hotwash
Persona Creation	Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware	Inform Threat Model
Strategic Goal	System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation	Refine Operation Activities
Storyboarding			Security Controls	Network Manipulation		Information Manipulation	Personas	
				Peripheral Management		Network Diversity	Network Diversity	
				Security Controls		Peripheral Management		
				Software Manipulation		Pocket Litter		

DEFENSA ACTIVA y DECEPCION

DEFENSA ACTIVA: "El empleo de acciones ofensivas limitadas y contraataques para negar un área o posición en disputa al enemigo".

OBJETIVO: mantener a los intrusos lejos de los activos reales y atraparlos o detenerlos en áreas con la intención de minimizar el daño y obtener la oportunidad de aprender de los métodos y el comportamiento del atacante

¿CÓMO? Con Integración de tácticas de engaño en herramientas de seguridad y automatización

SIMONE

ATAQUES DE FALSA BANDERA

Un ciberataque de bandera falsa *(false flag attack)* se produce cuando alguien (persona, organismo, ...) realiza un ataque de una manera que intenta engañar a sus víctimas y al mundo sobre quién es responsable o cuáles son sus objetivos.

"Se puede crear un buen engaño, pero en última instancia **se ataca lo que interesa**" (Hultquist)

La capacidad FORENSE DIGITAL (DF)

El analista debe tener claro cuándo su valoración es una intuición (fiabilidad baja) o resultado del análisis estructurado de múltiples fuentes de datos (fiabilidad alta)

Las NORMAS

El espectro de las CiberOperaciones

NO Permiten el uso de la fuerza | SI

Ping, Map or Probe	Buckshot Yankee •Erase logs •Install code	CSW Move One •Implant malware •Create botnet	Degrade Service or access to info	Delete or change adversary data with no phys. damage or injury China & Google	US/ROK •DDOS with minor impact	Estonia • Govt & Banking down for most of a month	Cyber Shock Wave •SCADA outage with no physical damage • Primarily private systems	Cyber Storm •SCADA outage with no physical damage • Effected Govt & critical systems	Change Data • Causes injury or damage	Stuxnet •Damage 1000 centri-fuges Attack in conflict • Destroy C2, fuel, planes, ships

Op. de acceso
Reconocimiento y Inteligencia digital

Interrupción
Interrumpir los sistemas de información sin daños físicos o lesiones.

CiberAtaque
Daño físico a la propiedad o Lesiones a personas

Poco Intrusivo — Muy Intrusivo

The EU Cyber Diplomacy Toolbox

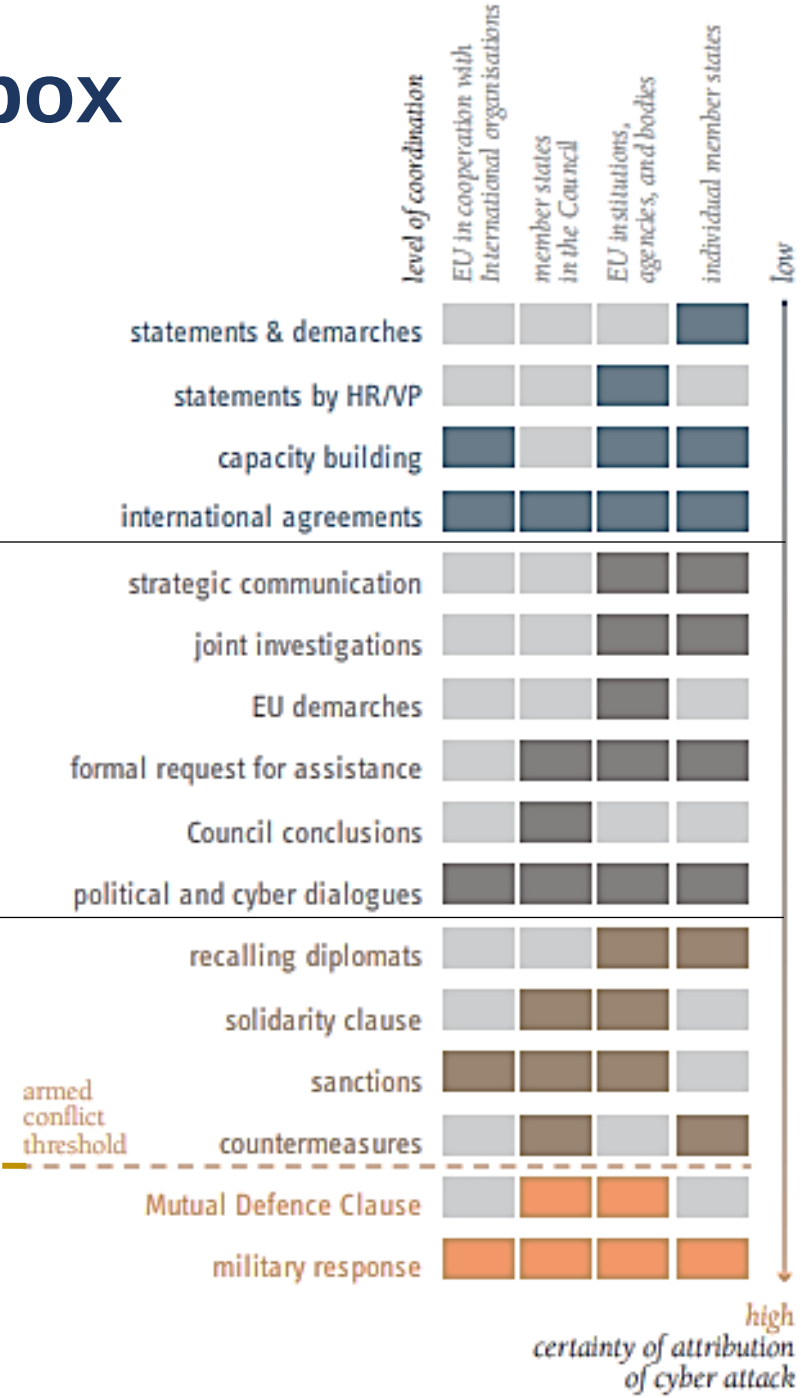
Acciones que requieren una **BAJA** certeza de atribución

Acciones que requieren una **MODERADA** certeza de atribución

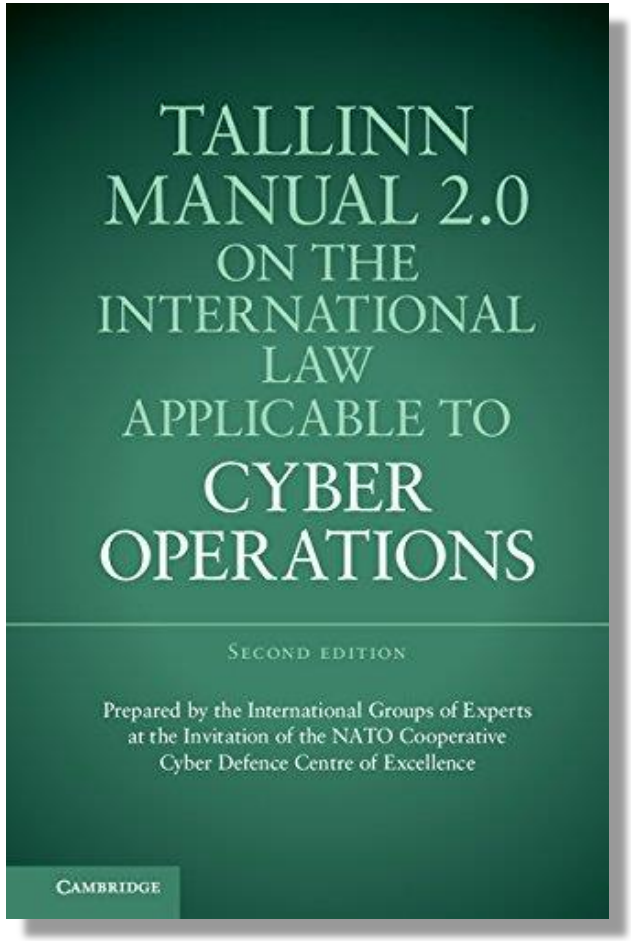
Acciones que requieren una **ALTA** certeza de atribución

Acciones que requieren una **ABSOLUTA** certeza de atribución

sólo se contemplan ciberataques deliberados con un efecto significativo



El Manual de Tallinn (2.0)



Atribución y responsabilidad de los estados en los ciberataques

Regla 14 – Ciber Operaciones que sean **atribuibles al Estado**.

Regla 15 – Ciber Operaciones realizadas **por órganos de un Estado**, o por personas o entidades facultadas o con autoridad gubernamental.

Regla 17 – Ciber operaciones realizadas por un **actor no estatal** cuando:

a) el Estado reconoce las operaciones como propias, o
b) … bajo su dirección o control.

¿Afinamos más?

a) ¿Conseguir que el Estado reconozca las operaciones como propias?

ESCOLLO: NEGACIÓN PLAUSIBLE

b) ¿… bajo su dirección o control?
DEFINE "control" estatal" → 2 doctrinas

- La Doctrina de CONTROL EFECTIVO (ECD): cuando actores NO-estatales se desempeñan en completa dependencia del estado ← Prueba más allá de cualquier duda

- La Doctrina de CONTROL GENERAL (OCD): el estado juega un papel en la organización, coordinación o apoyo al actor NO-estatal ← Prueba más allá de la duda razonable

TENDENCIA: de la atribución → a la responsabilidad

CONCLUYENDO …

- Las ciber operaciones han venido para quedarse.
- DISUASIÓN y ATRIBUCIÓN no son asuntos binarios.
- La atribución llega con el tiempo, ergo … el problema de la atribución no debe resolverse, debe **GESTIONARSE.**
- Capacidades ofensivas → SI, pero ¡Ojo con arriesgarlas!
- La legislación debe adaptarse.

MUCHAS GRACIAS

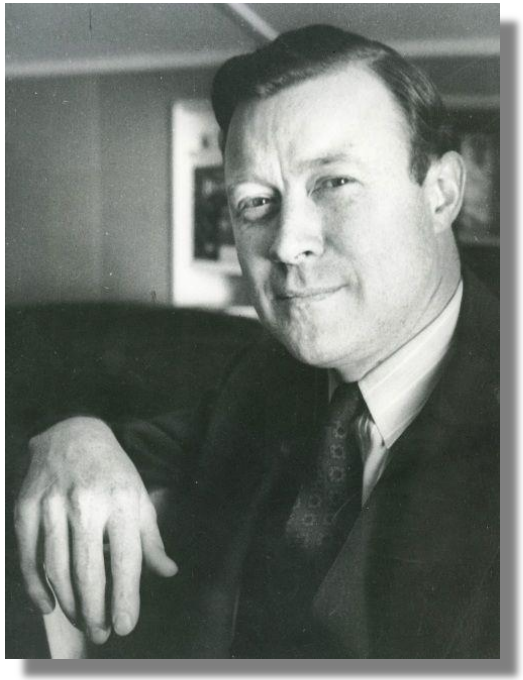
#XVJORNADASCCNCERT

TOMAS FALSAS 1

La atribución: nada es lo que parece

"Si parece un pato, anda como un pato y hace 'cuac' como un pato, entonces debe ser un pato"

Walter Reuther



... o NO

TOMAS FALSAS 2

Capacidades Ofensivas

"En la guerra, la verdad es tan preciosa

que siempre debe ser protegida …

… por un conjunto de mentiras."

Winston Churchill

TOMAS FALSAS 3

Defensa Activa: Deception Framework

Significado de

DECEPCIÓN

TOMAS FALSAS 4

Disuasión: es parte del engaño

- **“La invencibilidad es una cuestión de defensa, la vulnerabilidad, una cuestión de ataque.”**

- **“Hago que el enemigo vea mis fortalezas como debilidades y mis debilidades como fortalezas mientras hago que sus fortalezas se conviertan en debilidades y descubro dónde no es fuerte”**

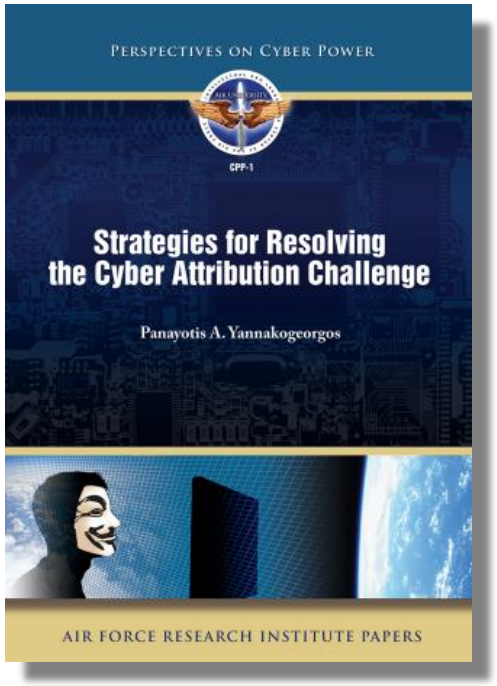
- Sun Tzu
- The Art of War, c. 500 BC

(¿De verdad alguien pensaba que Sun Tzu no aparecería?)

DISUASION: bibliografía

- Is cyber deterrence possible - McKenzie
- Una idea para potenciar la ciber disuasion de la OTAN - E. Cubeiro
- Cross-Domain Deterrence and Credible Threats - James A Lewis
- Cyber deterrence and cyberwar - Martin Libicki
- The fallacy of attribution to achieve deterrence in cybespace - Robert J. Johnson
- The Myth of Cyber Deterrence - Rhea Siers

ATRIBUCION: bibliografía



- ODNI - A Guide to Cyber Attribution
- Strategies for Resolving the Cyber Attribution Challenge (Yannakogeorgos)
- The Ultimate Challenge for Attribution for Cyber Operations - Hill
- Opportunities for Public and Private Attribution of Cyber Operations - Tallinn Papers
- Applying Cyber Kill Chain® Methodology to Network Defense
- The Diamond Model of Intrusion Analysis
- A Method of Cyber-Attack Attribution Based on Threat Intelligence - Qiang, Ze-Ming
- NSA-CSA Turla Group Exploits Iranian APT

ASPECTOS JURÍDICOS: bibliografía

- Manual de Tallín 2.0 (online)
- The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?
- ON THE SPECTRUM OF CYBERSPACE OPERATIONS
- Sanciones contra ciberataques: la acción de la UE - M. Robles

TOMAS FALSAS 5

Defensa Activa: Hacking Back?

Otra vez

MUCHAS GRACIAS

#XVJORNADASCCNCERT