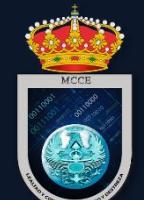




Has sido tú !!  
Te crees que no te he visto



#XVJORNADASCCNCERT



ccn-cert  
centro criptológico nacional



**EMILIO RICO RUIZ**

**TCol. (Cab) - Analista de Ciber Defensa  
Fuerza de Operaciones (FOCE) del MCCE**

**[ericorui@et.mde.es](mailto:ericorui@et.mde.es)**



**#XVJORNADASCCNCERT**

# ¿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.



#XVJORNADASCCNCERT

# 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

Gran dificultad en conseguir el éxito:

- Coste económico.
- Dificultad técnica.
- Posibilidad de ser detectado identificado.

## Disuasión por represalia

Riesgo elevado frente al beneficio obtenible:

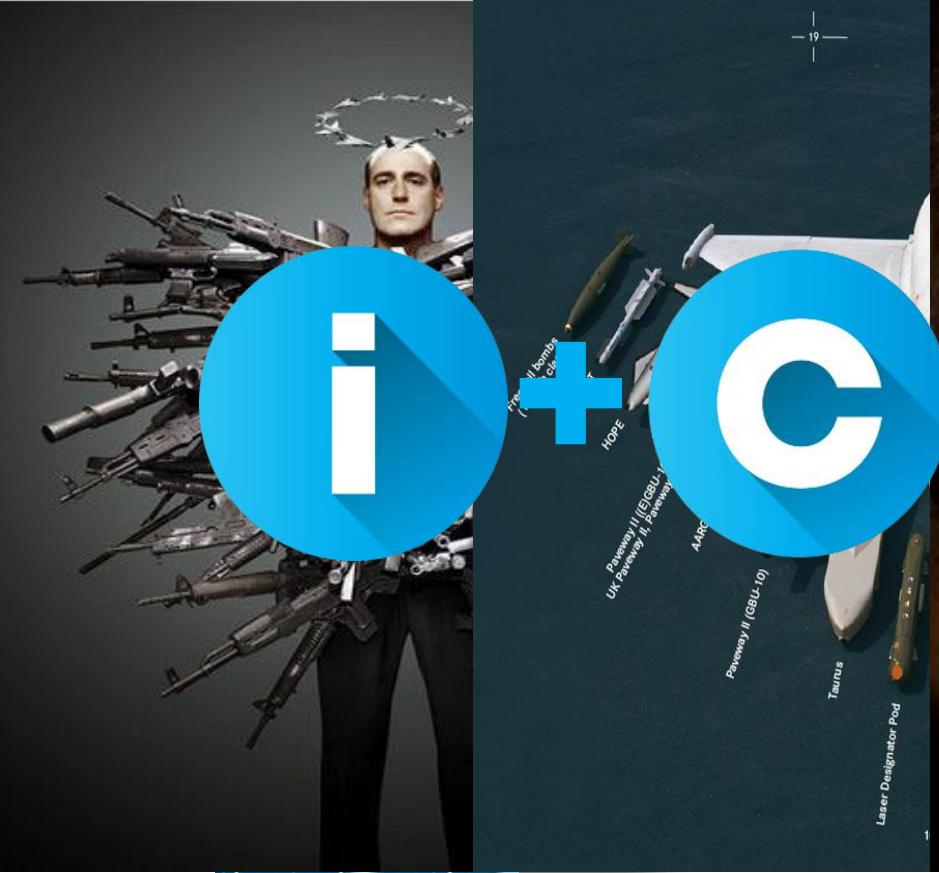
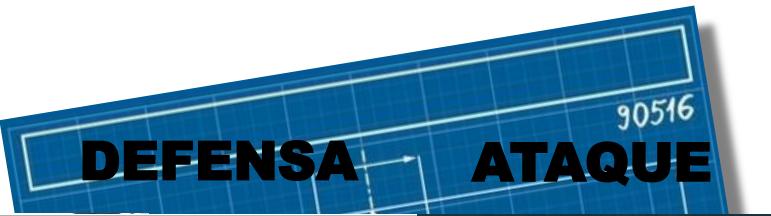
- Probabilidad de sufrir represalias o castigo



# CONSTRUYENDO la Disuasión



**CREDIBILIDAD**

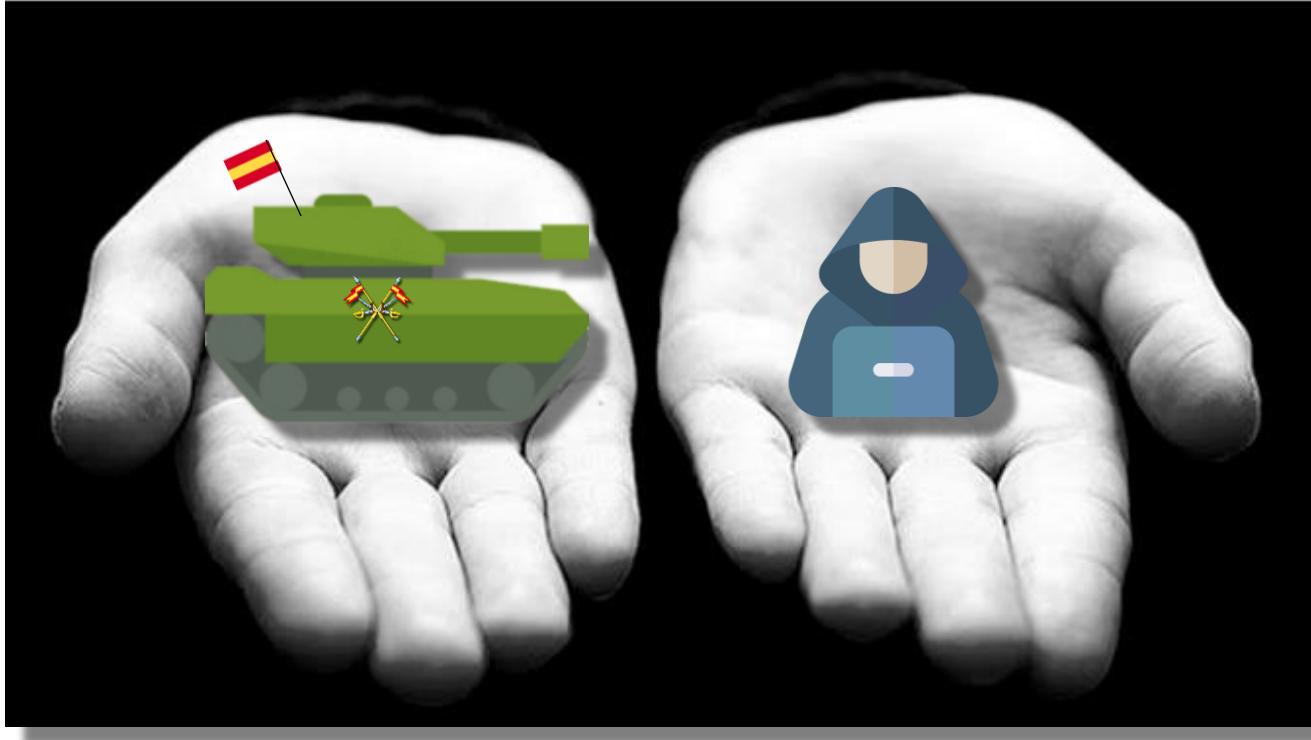


**VOLUNTAD**



#XVJORNADASCCNCERT

# 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



#XVJORNADASCCNCERT



# La atribución

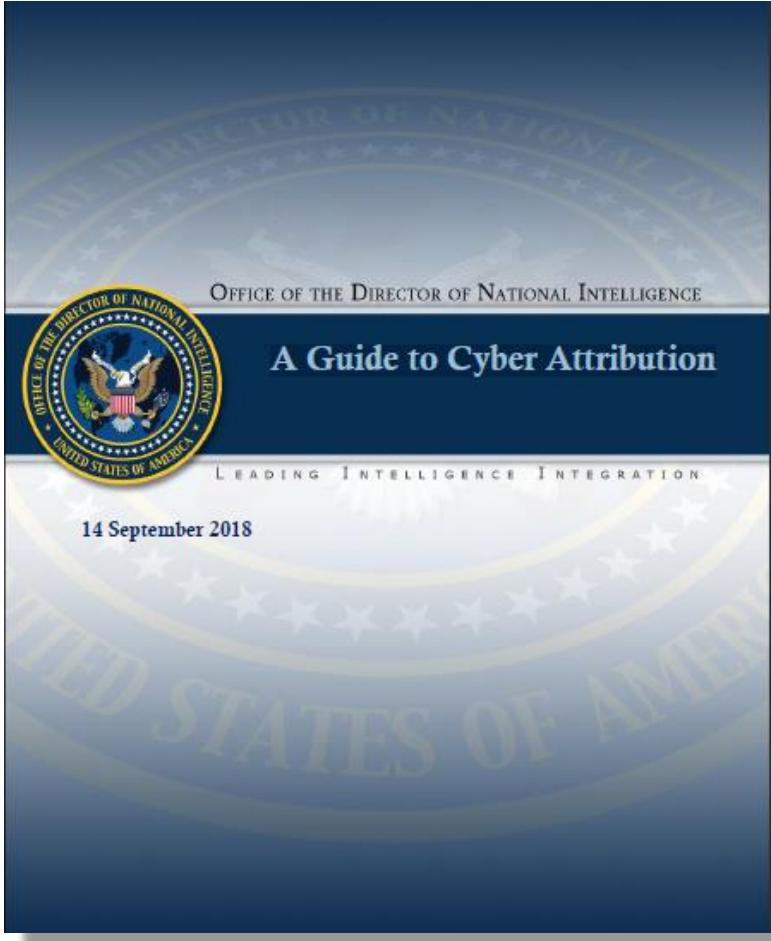
**atribución:** acción de atribuir.

**atribuir:** aplicar, a veces sin conocimiento seguro, hechos o cualidades a alguien o algo.



#XVJORNADASCCNCERT

# 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](https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf)



#XVJORNADASCCNCERT



# 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



1 Reconocimiento



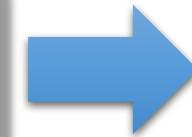
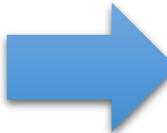
3 Entrega



5 Instalación



7 Acciones  
sobre  
objetivo



1 Reconocimiento



2 Armado



4 Explotación

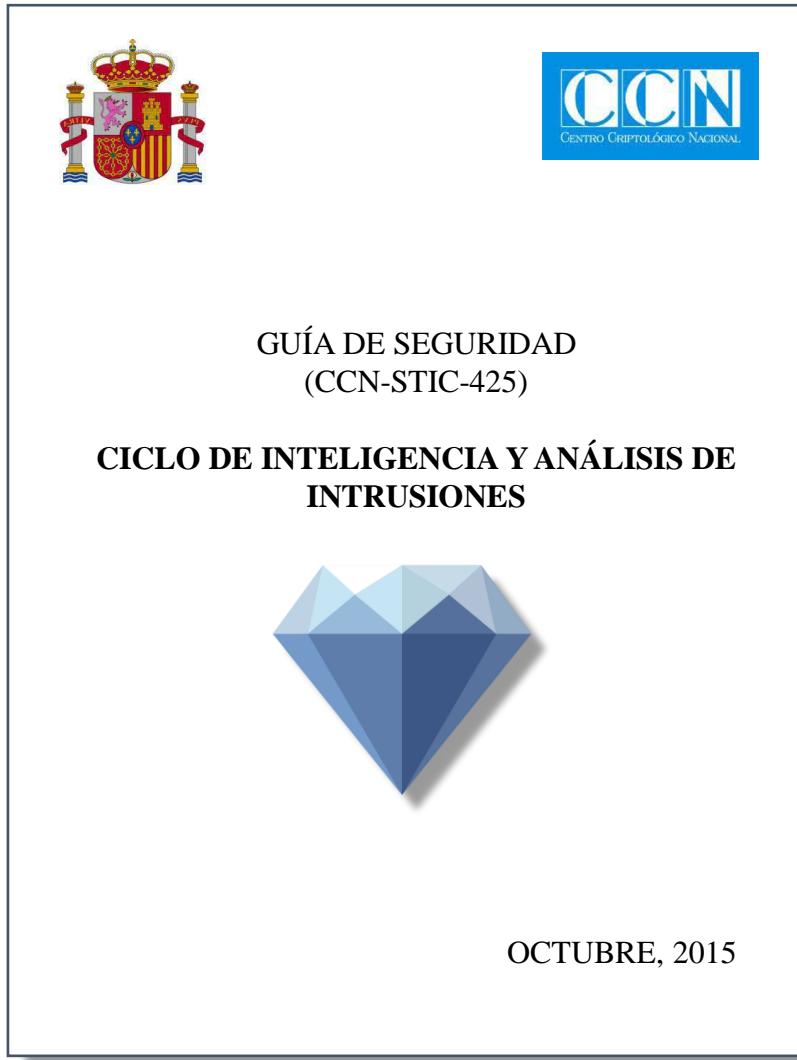


6 Comm. & Control



#XVJORNADASCCNCERT

# 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>

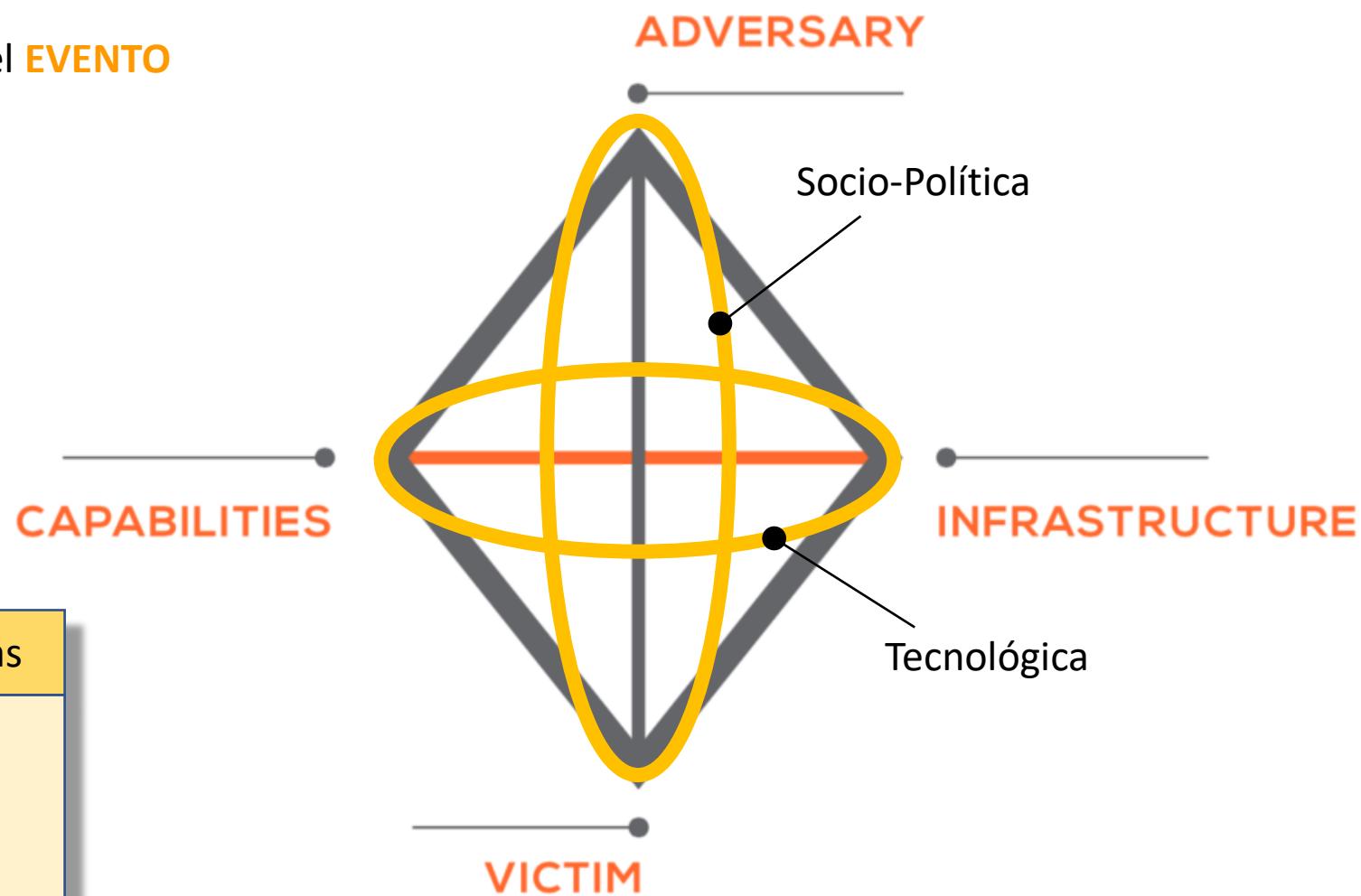


# El modelo diamante 2

- 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
<ul style="list-style-type: none"><li>▪ Sello de tiempo</li><li>▪ Fase</li><li>▪ Resultado</li><li>▪ Dirección</li><li>▪ Metodología</li><li>▪ Recursos</li></ul>





# El modelo diamante 3

THREATCONNECT INCIDENT 19770525F:

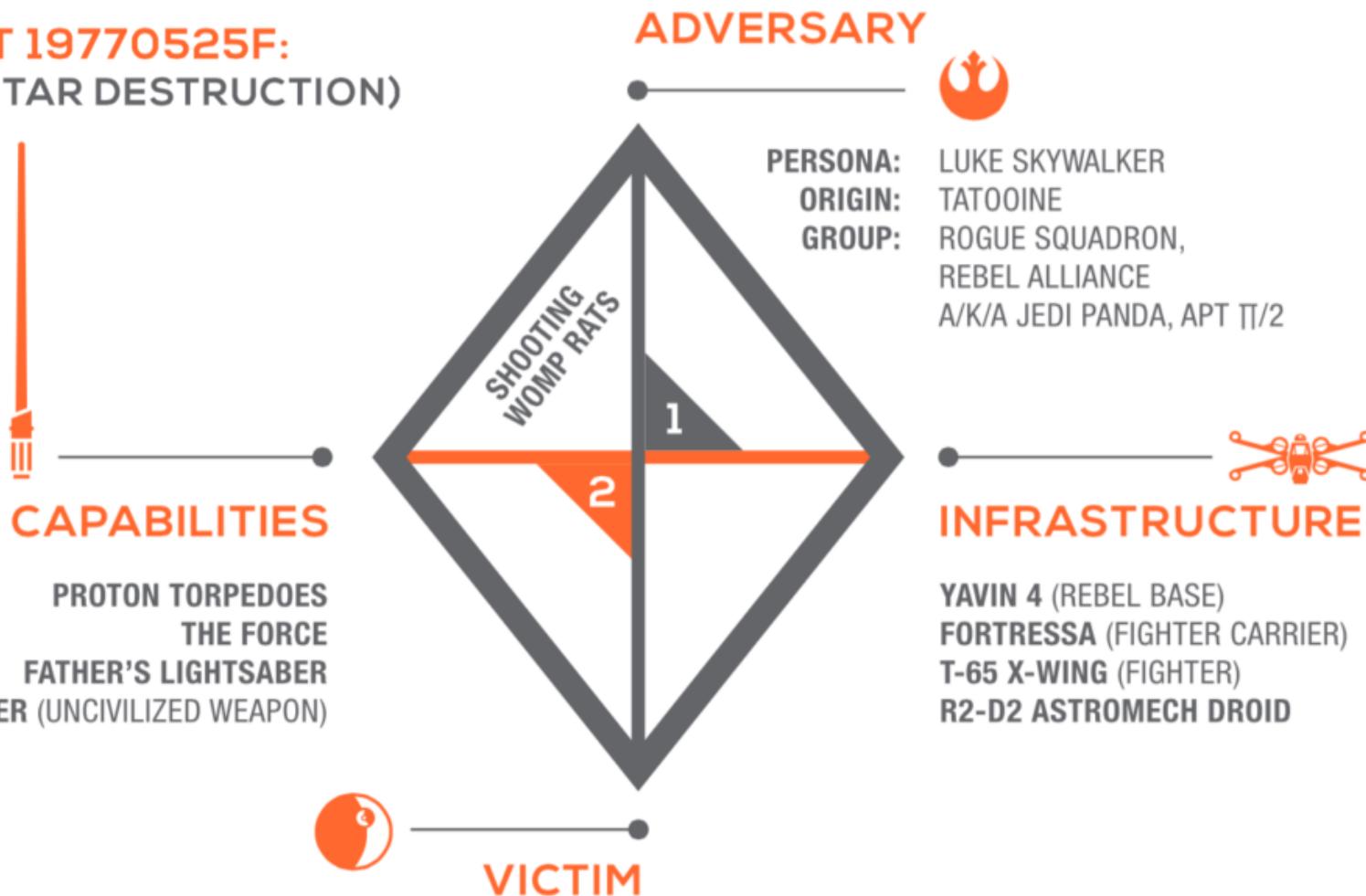
BATTLE OF YAVIN (EVENT: DEATH STAR DESTRUCTION)

## 1 SOCIO-POLITICAL AXIS

MOTIVE: IDEOLOGICAL; REVENGE  
INTENT: POLITICAL UPHEAVAL

## 2 TECHNICAL AXIS (TTPS)

PRECISION TARGETING  
FORCE-CONTROLLED FLIGHT  
FORCE COMMUNICATION



LUKE IN THE SKY WITH DIAMONDS

<https://threatconnect.com/blog/diamond-model-threat-intelligence-star-wars/>



#XVJORNADASCCNCERT

# El modelo diamante 4

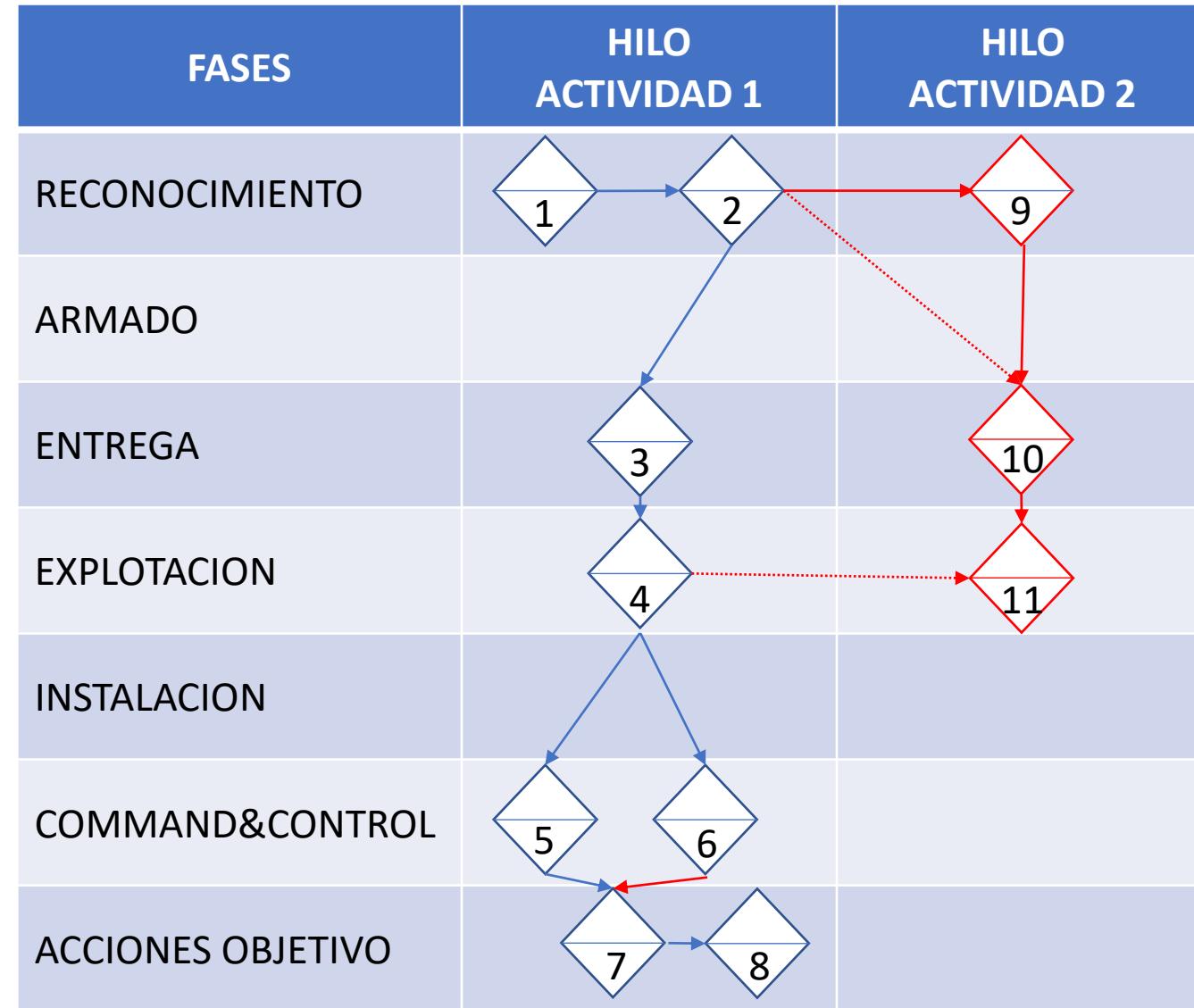


Hilos de actividad  
(grafo orientado a fases)



CYBER KILL CHAIN

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

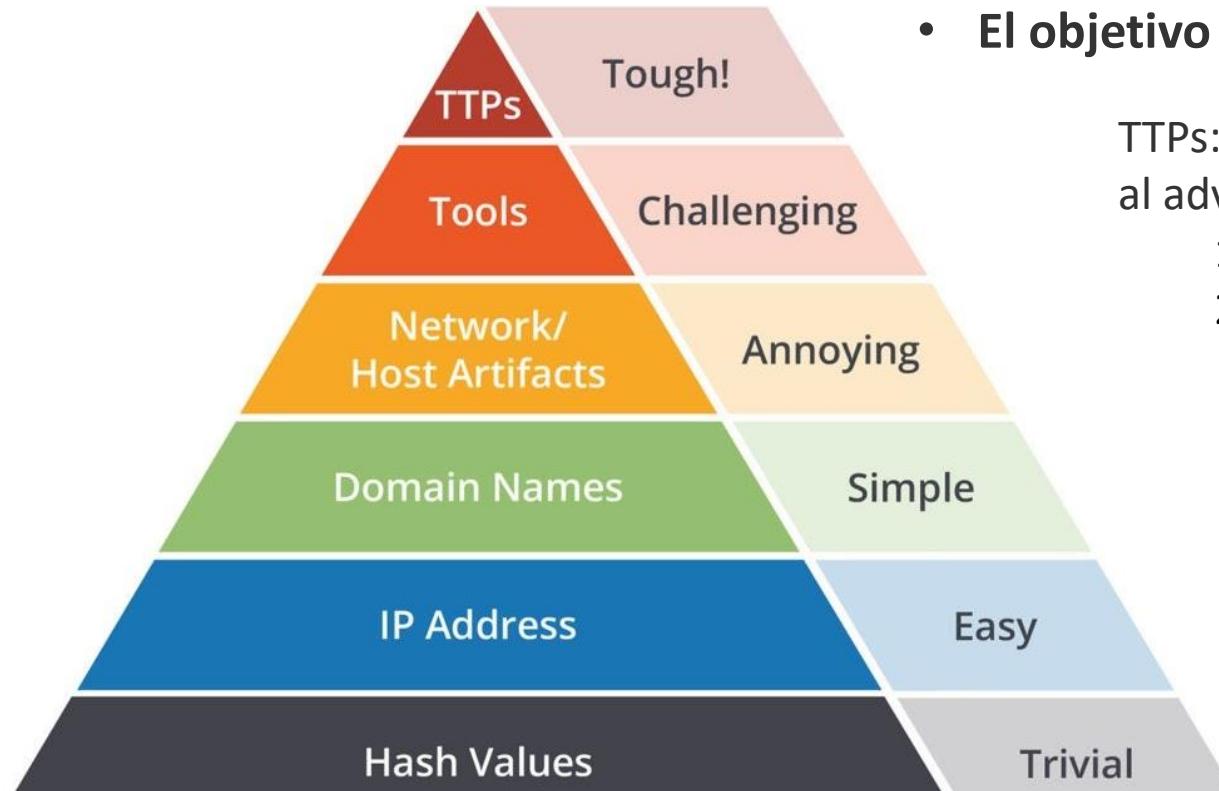


#XVJORNADASCCNCERT



# Nueva aproximación: las TTPs

Tácticas, Técnicas y Procedimientos



- 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

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



#XVJORNADASCCNCERT



MCCE



MCCE

Reconnaissance 10 techniques	Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/2)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/2)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Cloud Service Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Deploy Container	Direct Volume Access	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Cloud Service Discovery	Dynamic Resolution (0/3)	Exfiltration Over C2 Channel	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/6)	Create Account (0/3)	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Input Capture (0/4)	Container and Resource Discovery	Replication Through Removable Media	Encrypted Channel (0/2)	Exfiltration Over Other Network Medium (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Trusted Relationship	Shared Modules	Software Deployment Tools	Create or Modify System Process (0/4)	Escape to Host	Execution Guardrails (0/1)	Modify Authentication Process (0/4)	Domain Trust Discovery	Data from Configuration Repository	Fallback Channels	Inhibit System Recovery	Firmware Corruption
Search Open Websites/Domains (0/2)	Valid Accounts (0/4)	System Services (0/2)	User Execution (0/3)	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	File and Directory Permissions Modification (0/2)	File and Directory Discovery	Software Deployment Tools	Ingress Tool Transfer	Network Denial of Service (0/2)	Resource Hijacking
Search Victim-Owned Websites		Windows Management	External Remote Services	Hijack Execution	Hijack Execution Flow (0/11)	Hide Artifacts (0/9)	OS Credential Dumping (0/8)	Group Policy Discovery	Taint Shared Content	Multi-Stage Channels	Scheduled Transfer	Service Stop
					Impair Defenses (0/9)	Impair Defenses (0/9)	Steal Application Access Token	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Local System	Non-Application Layer Protocol	System Shutdown/Reboot
					Indicator Removal on Host (0/6)	Indirect Command Execution	Steal or Forge Kerberos Tickets (0/4)	Network Share Discovery		Data from Network Shared Drive	Non-Standard Port	
					Masquerading (0/7)	Two-Factor Authentication Interception	Steal Web Session Cookie	Network Sniffing		Data from Removable Media		
					Modify Authentication Process (0/4)	Unsecured Credentials (0/7)	Two-Factor Authentication Interception	Password Policy Discovery		Data Staged (0/2)		
					Scheduled Task/Job (0/6)	Modify Cloud Compute Infrastructure (0/4)	Unsecured Credentials (0/7)	Peripheral Device Discovery		Email Collection (0/3)		
					Server Software Component (0/4)	Modify Registry	Two-Factor Authentication Interception	Permission Groups Discovery (0/3)		Input Capture (0/4)		
					Traffic Signaling (0/1)	Modify System Image (0/2)	Unsecured Credentials (0/7)	Process Discovery		Screen Capture		
					Accounts (0/4)	Network Boundary Bridging	Two-Factor Authentication Interception	Query Registry		Video Capture		
							Two-Factor Authentication Interception	Remote System Discovery		Web Service (0/3)		
							Two-Factor Authentication Interception	Software Discovery (0/1)				
							Two-Factor Authentication Interception	System Information Discovery				

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

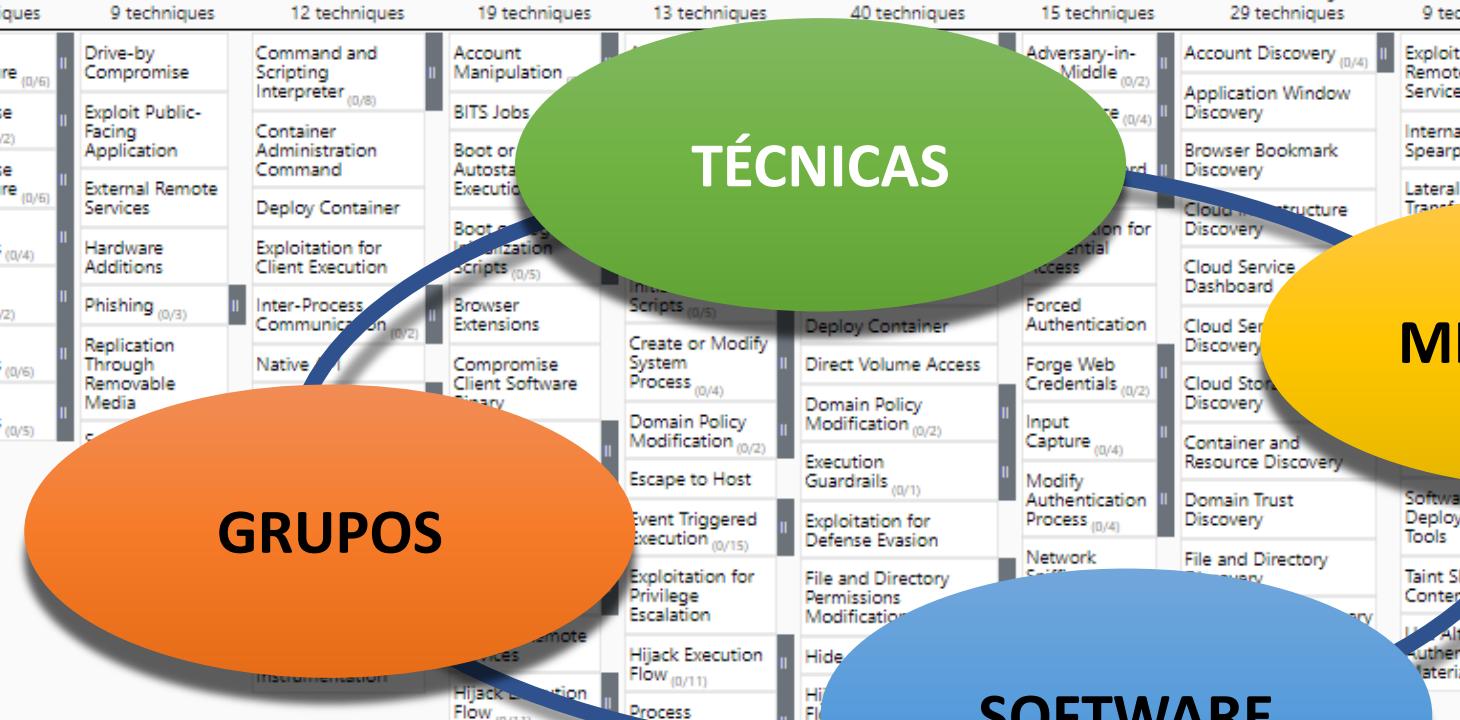
Reconnaissance	Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation	Adversary-in-Middle (0/2)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/2)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Data Transfer Size Limits	
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Adversary-in-the-Middle (0/4)	Application Window Discovery	Internal Spearphishing	Application Layer Protocol (0/4)	Communication Through Removable Media	Data Encrypted for Impact	Data Manipulation (0/3)	
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Autostart Execution	Adversary-in-the-Middle (0/4)	Browser Bookmark Discovery	Lateral Tool Transfer	Adversary-in-the-Middle (0/2)	Audio Capture	Defacement (0/2)	Exfiltration Over Alternative Protocol (0/3)	
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Autostart Execution Scripts (0/5)	Adversary-in-the-Middle (0/4)	Cloud Infrastructure Discovery	Cloud Service Dashboard	Cloud Service Discovery	Cloud Storage Discovery	Disk Wipe (0/2)	Exfiltration Over C2 Channel	
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Forced Authentication	Cloud Service Discovery	Container and Resource Discovery	Container and Resource Discovery	Container and Resource Discovery	Endpoint Denial of Service (0/4)	Exfiltration Over Other Network Medium (0/1)	
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native (0/1)	Compromise Client Software Binary	Forge Web Credentials (0/2)	Cloud Service Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Firmware Corruption	Inhibit System Recovery	
Search Closed Sources (0/2)	Stage Capabilities (0/5)			Threat Scripts (0/5)	Direct Volume Access	Cloud Storage Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	Network Denial of Service (0/2)	Non-Application Layer Protocol	
Search Open Technical Databases (0/5)				Deploy Container	Domain Policy Modification (0/2)	Container and Resource Discovery	Software Deployment Tools	Repository (0/2)	Repository (0/2)	Non-Standard Port	Protocol Tunneling	
Search Open Websites/Domains (0/2)				Exploit Volume Access	Execution Guardrails (0/1)	Domain Policy Modification (0/2)	Taint Shared Content	Ingress Tool Transfer	Ingress Tool Transfer	Proxy (0/4)	Remote Access Software	
Search Victim-Owned Websites				Exploit Volume Access	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Alternate Authentication Material (0/4)	Multi-Stage Channels	Multi-Stage Channels	Protocol Tunneling	Resource Hijacking	
				Exploit Volume Access	File and Directory Permissions Modification	File and Directory Permissions Modification	Data from Information Repositories (0/3)	Scheduled Transfer	Scheduled Transfer	Remote Access Software	Service Stop	
				Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Data from Local System	Non-Application Layer Protocol	Non-Application Layer Protocol	Transfer Data to Cloud Account	System Shutdown/Reboot	
				Implant Internal Image	Implant Internal Image	Implant Internal Image	Data from Network Shared Drive	Non-Standard Port	Non-Standard Port			
				Modify Authentication Process (0/4)	Modify Authentication Process (0/4)	Modify Authentication Process (0/4)	Data from Removable Media	Protocol Tunneling	Protocol Tunneling			
				Office Application Startup (0/6)	Office Application Startup (0/6)	Office Application Startup (0/6)	Data Staged (0/2)	Proxy (0/4)	Proxy (0/4)			
				Pre-OS Boot (0/5)	Pre-OS Boot (0/5)	Pre-OS Boot (0/5)	Email Collection (0/3)	Remote Access Software	Remote Access Software			
				Scheduled Task/Job (0/6)	Scheduled Task/Job (0/6)	Scheduled Task/Job (0/6)	Input Capture (0/4)	Traffic Signaling (0/1)	Traffic Signaling (0/1)			
				Server Software Component (0/4)	Server Software Component (0/4)	Server Software Component (0/4)	Screen Capture	Web Service (0/3)	Web Service (0/3)			
				Traffic Signaling (0/1)	Traffic Signaling (0/1)	Traffic Signaling (0/1)	Video Capture					
				Accounts (0/4)								

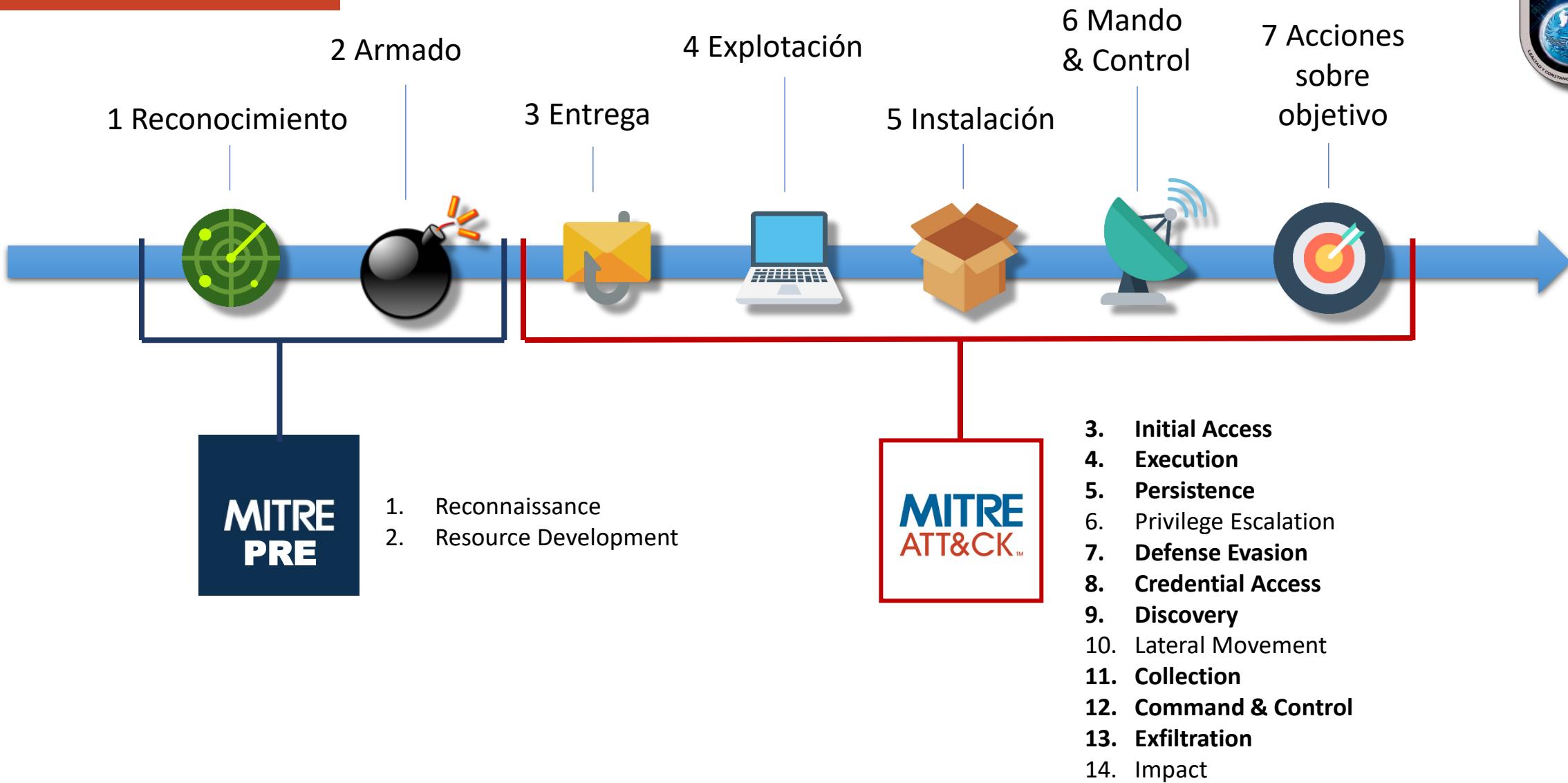
TÉCNICAS

GRUPOS

SOFTWARE

MITIGACIÓN







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



#XVJORNADASCCNCERT

# ATAQUES DE FALSA BANDERA



National Cyber Security Centre  
a part of GCHQ

National Security Agency

Advisory: Turla group exploits Iranian APT to expand coverage of victims

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.

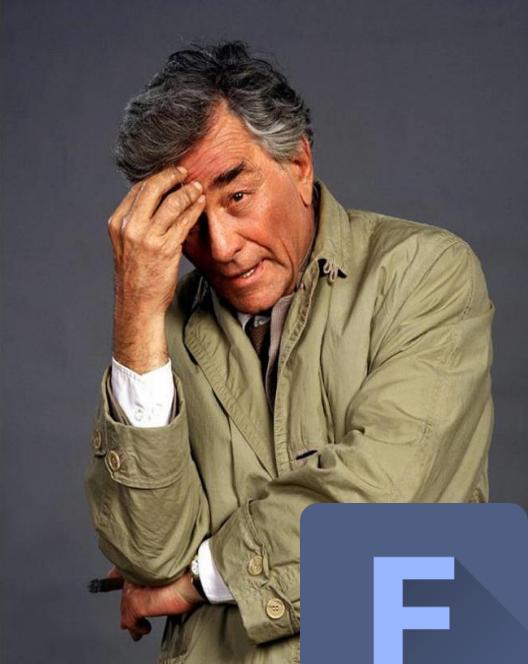
“Se puede crear un buen engaño, pero en última instancia **se ataca lo que interesa**” (Hultquist)



# 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)

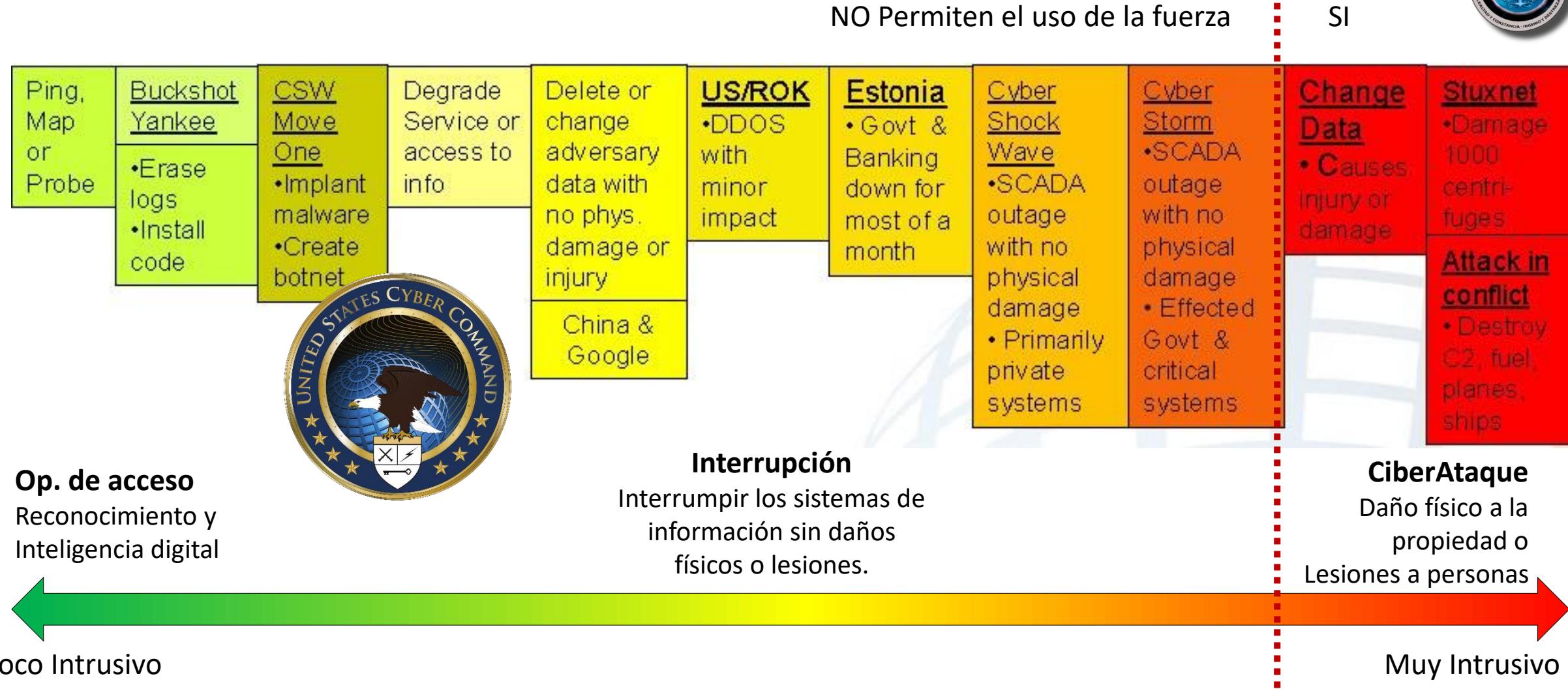


# Las NORMAS



**Art. 51**

# El espectro de las CiberOperaciones



# The EU Cyber Diplomacy Toolbox



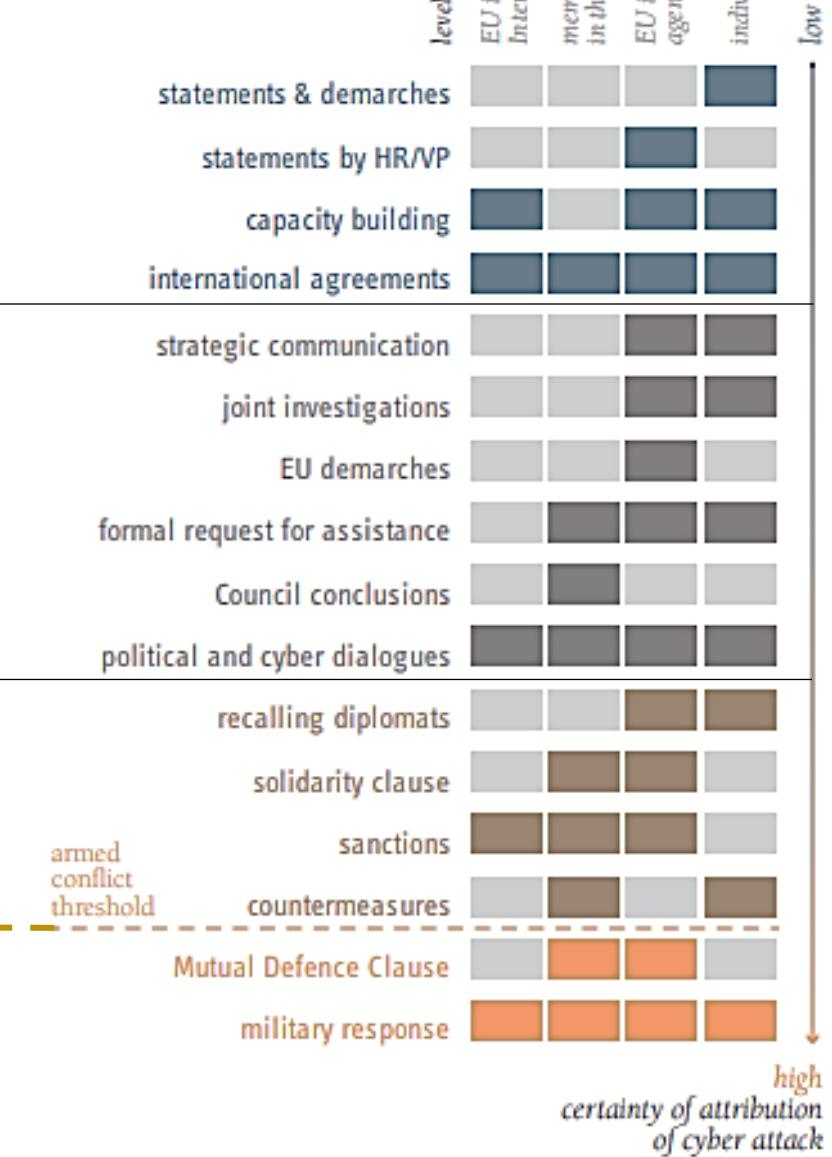
sólo se contemplan ciberataques deliberados con un efecto significativo

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

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

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

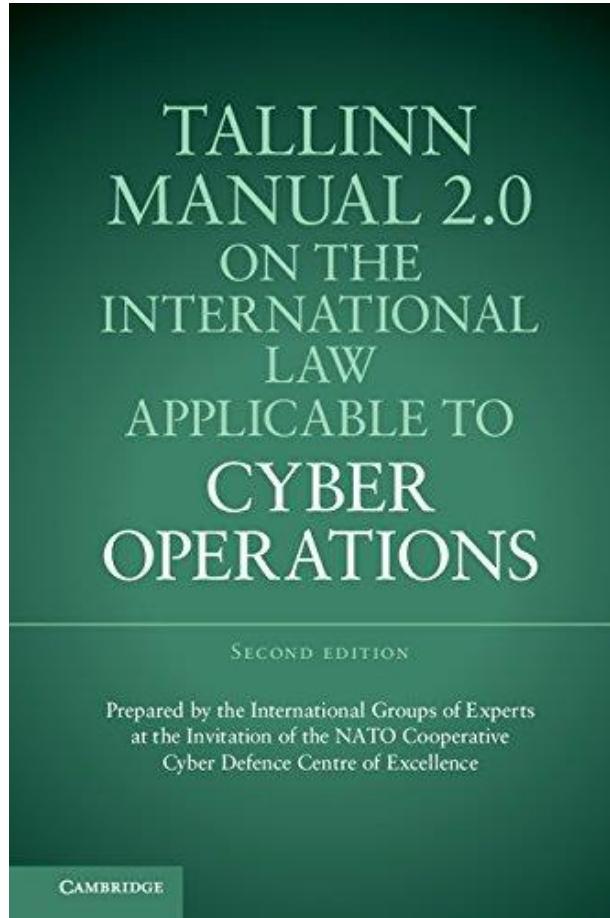
Acciones que requieren una **ABSOLUTA** certeza de atribución



#XVJORNADASCCNCERT



# 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

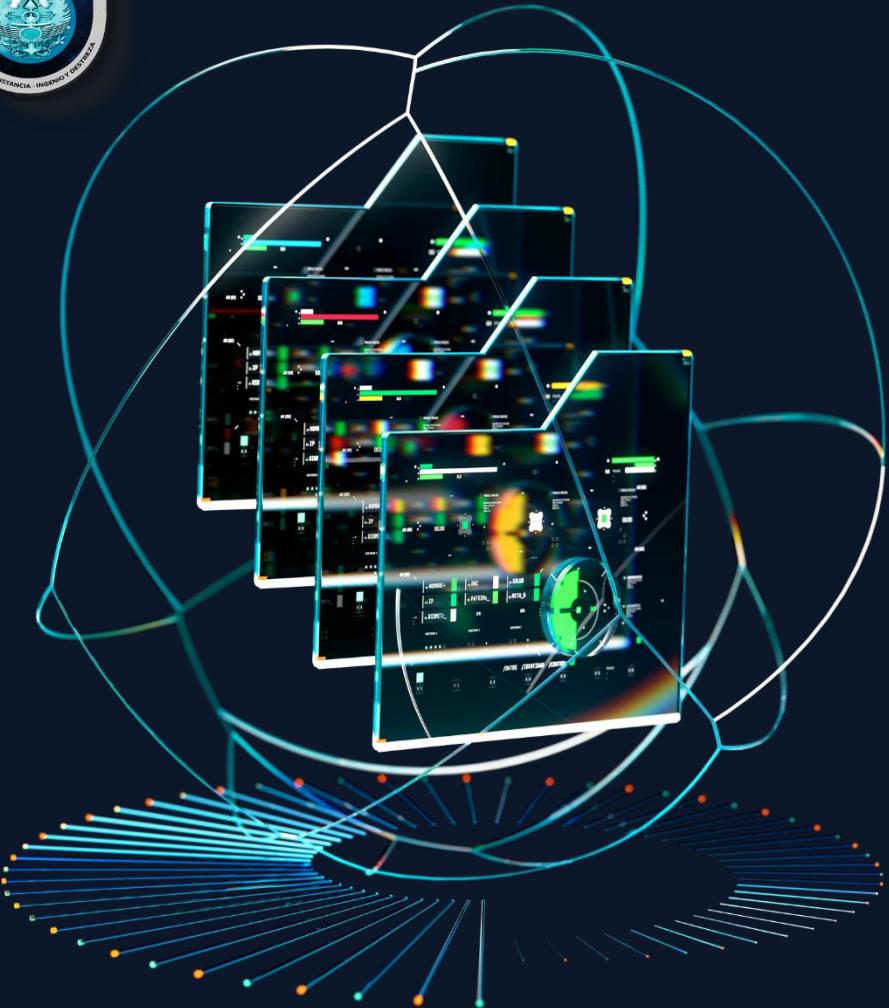


# CONCLUYENDO ...



- 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



#XVJORNADASCCNCERT

# 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



#XVJORNADASCCNCERT

# TOMAS FALSAS 3

## Defensa Activa: Deception Framework



Significado de  
**DECEPCIÓN**



#XVJORNADASCCNCERT

# 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?)



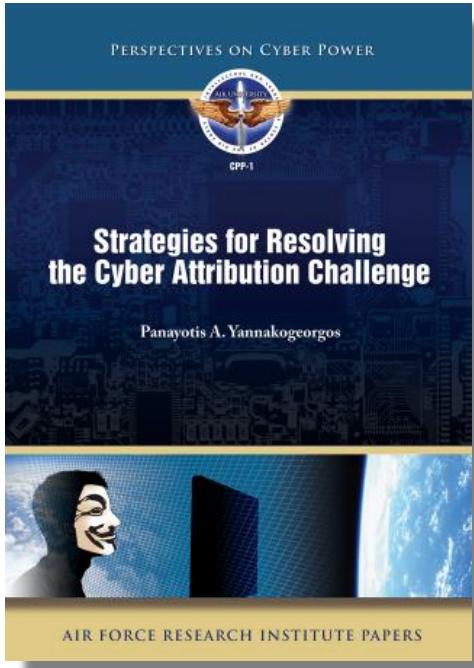
# DISUASION: bibliografía



- [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 cyberspace - 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](#)



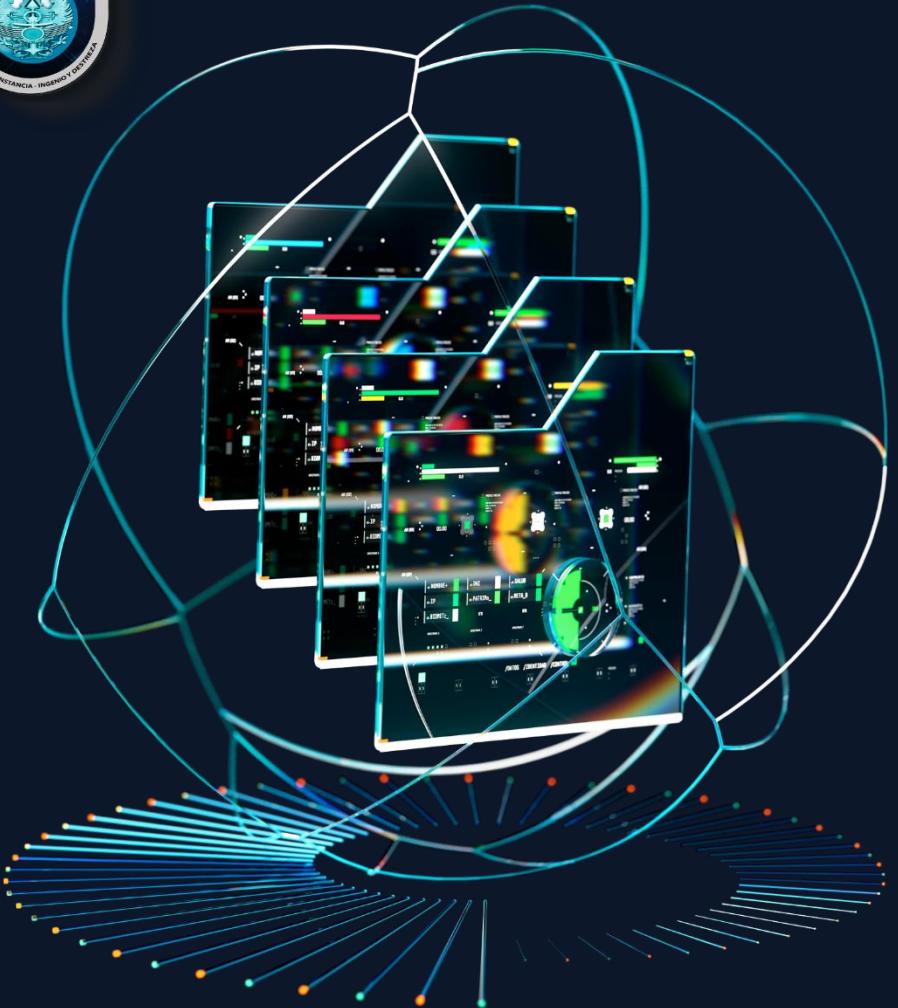
# TOMAS FALSAS 5

## Defensa Activa: Hacking Back?



PST BY ANDREW KNEEL CARTOONS





Otra vez  
MUCHAS  
GRACIAS

#XVJORNADASCCNCERT