

**XIII
JORNADAS
STIC
CCN-CERT**



Planeamiento operativo en el ciberspacio (Targeting)

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT





CTE. JOSE MANUEL LAGUNA GARCIA

Analista de Operaciones del EM del M CCD

M CCD / Ministerio de Defensa

Índice

1. Referencias, documentación
2. Ciclo de targeting conjunto
3. Acciones ofensiva en el ciberespacio
4. Efectos de las operaciones en el ciberespacio
5. Estimación del Daño Colateral (CDE)
6. Battle Damage Assessment (BDA)
7. Target folder (Joint Targeting System & Functional Area Service for Dynamic and Time Sensitive Targeting)



Joint Targeting es el proceso de **selección de objetivos y de adecuación de la respuesta** a los mismos, teniendo en cuenta las **limitaciones operativas y legales**.

Comprende la **identificación** de un sistema, estructura, persona, grupo u objeto **(FIVE-O)** en el que se haya seleccionado un elemento crítico o un punto vulnerable adecuado, contra la cual la **aplicación de la menor fuerza militar posible** debería alcanzar el **objetivo político-militar deseado**.

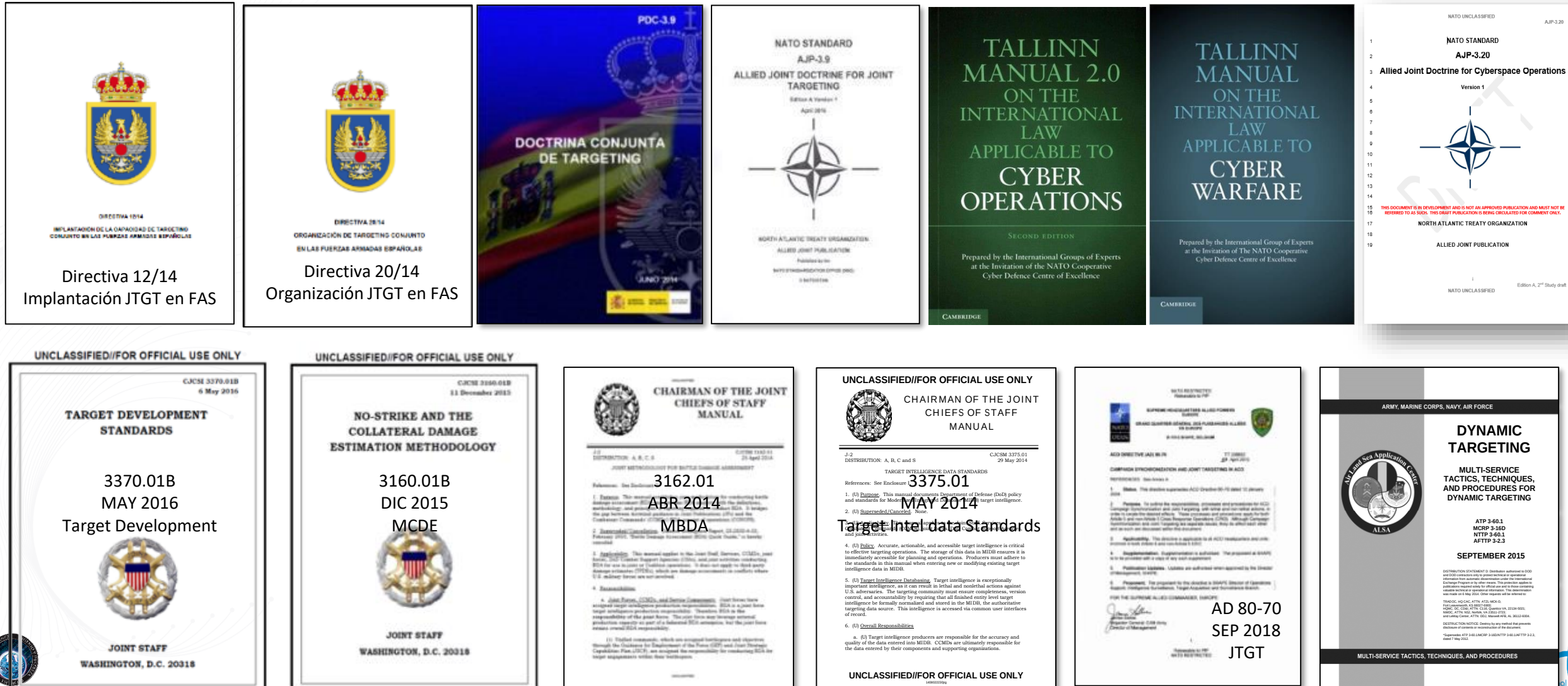
La función principal de Targeting and Weaponneering es permitir a un analista reunir una lista priorizada, mensurada y armada de objetivos (tanto instalaciones como unidades) para su inclusión en las órdenes de trabajo (por ejemplo, ATO) para el día siguiente.



Referencias, documentación

1.- REFERENCIAS

1.1.- DOCUMENTACIÓN

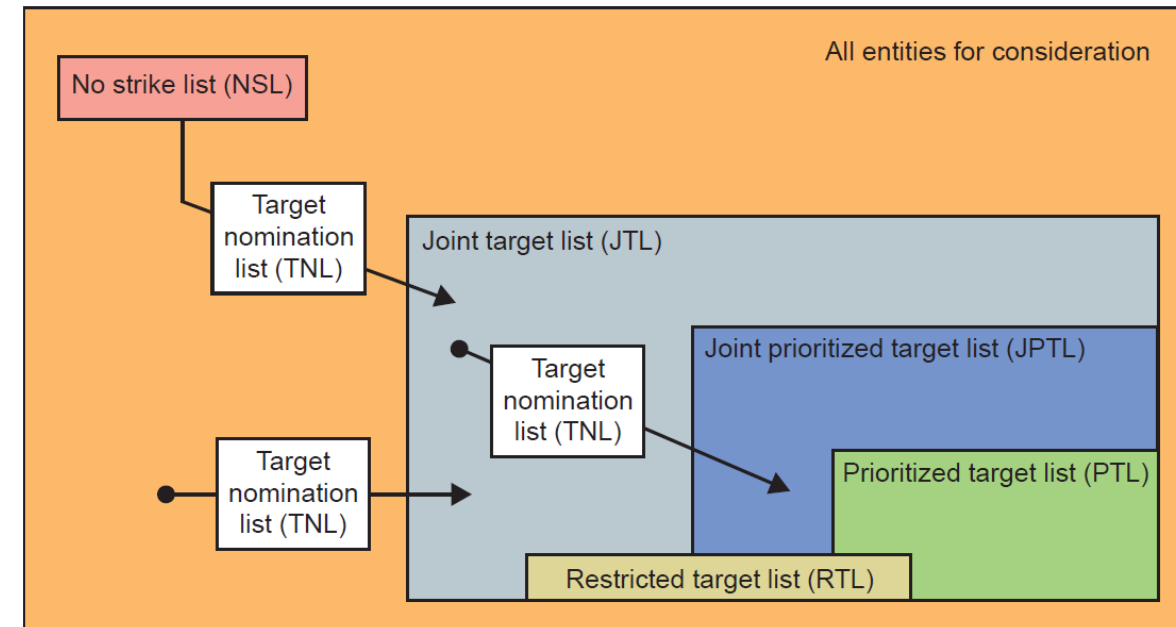
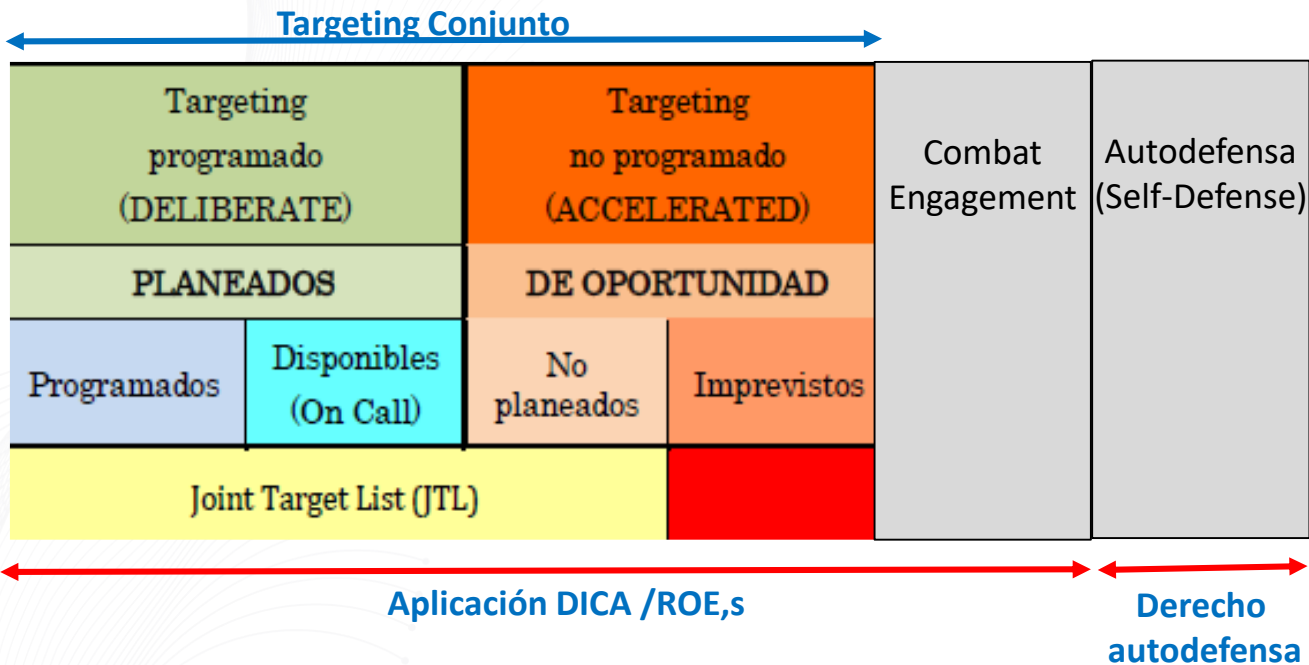


Ciclo de targeting conjunto (CTJ)



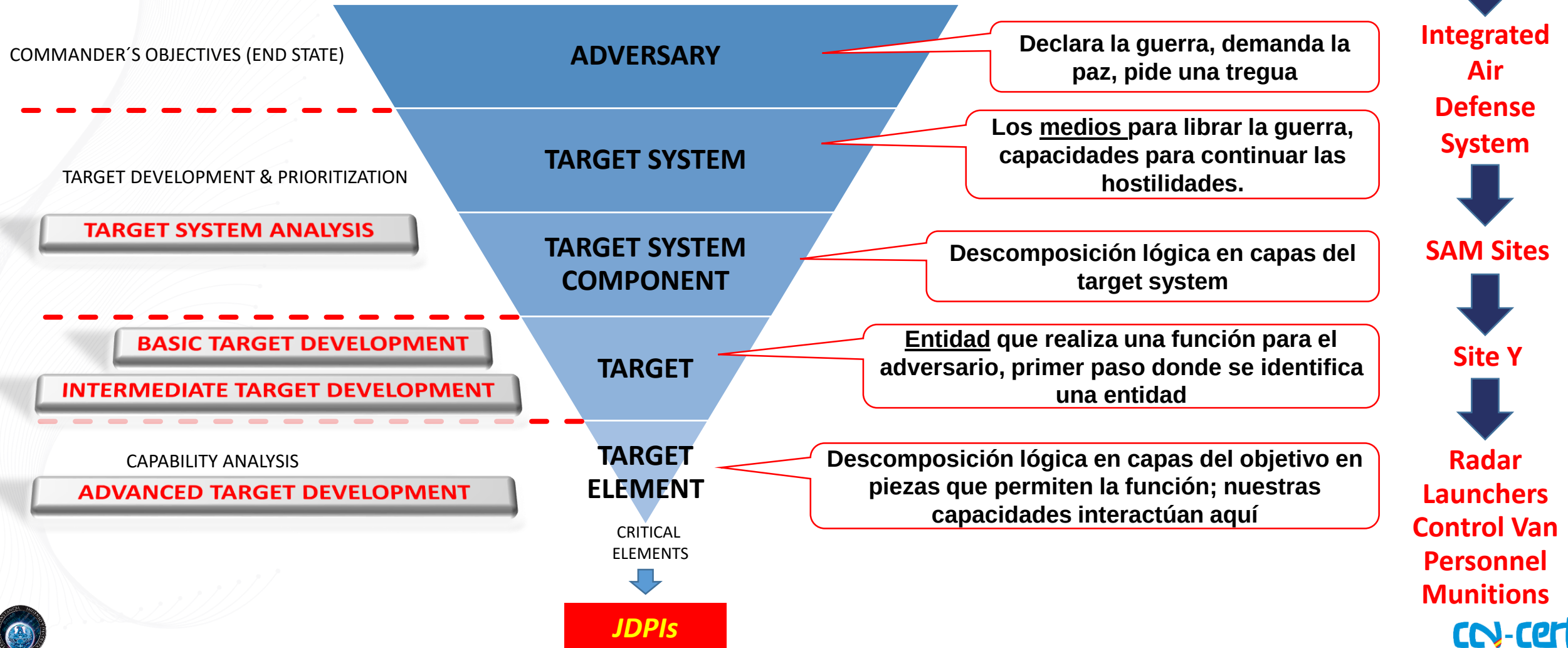
2.- CICLO DE TARGETING CONJUNTO

2.1.- TARGET DEVELOPMENT TAXONOMY



2.- CICLO DE TARGETING CONJUNTO

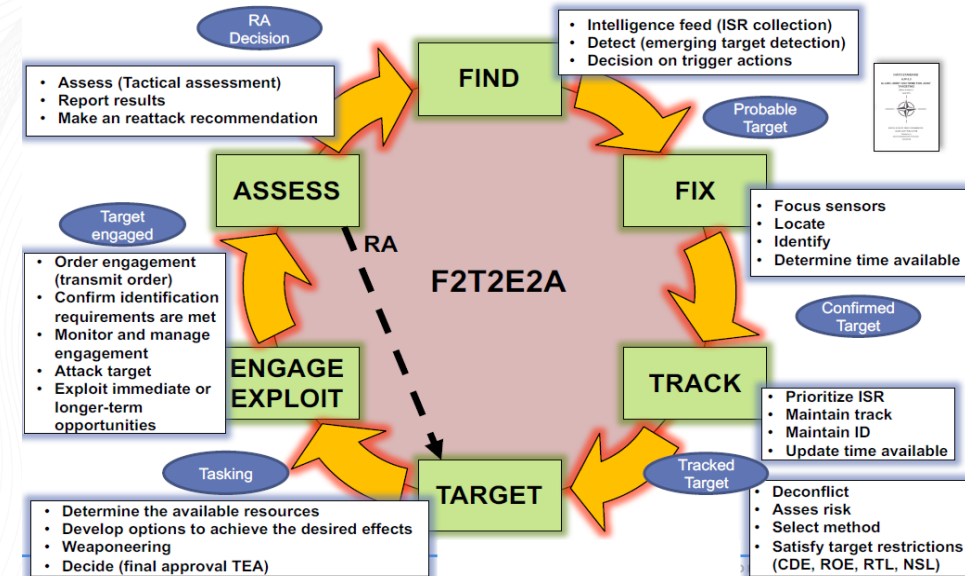
2.2.- TARGET DEVELOPMENT TAXONOMY



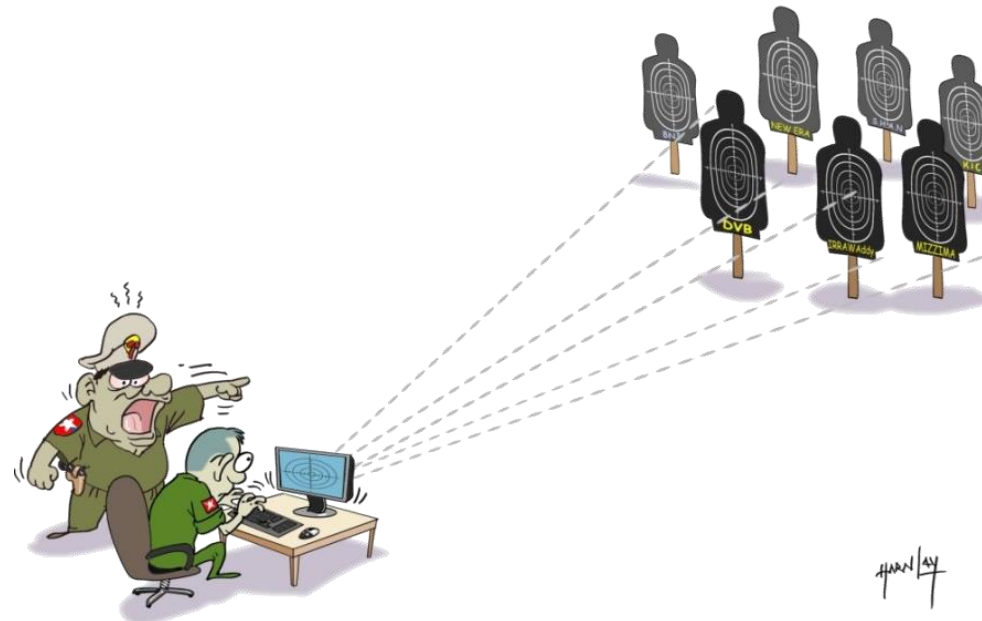
2.- CICLO DE TARGETING CONJUNTO

2.3.- PASOS DEL PROCESO

1. Identificación de Cyber Key Terrain.
2. Análisis de amenazas.
3. Análisis de vulnerabilidades.
4. Análisis de impacto.
5. Riesgos y gestión de riesgos.

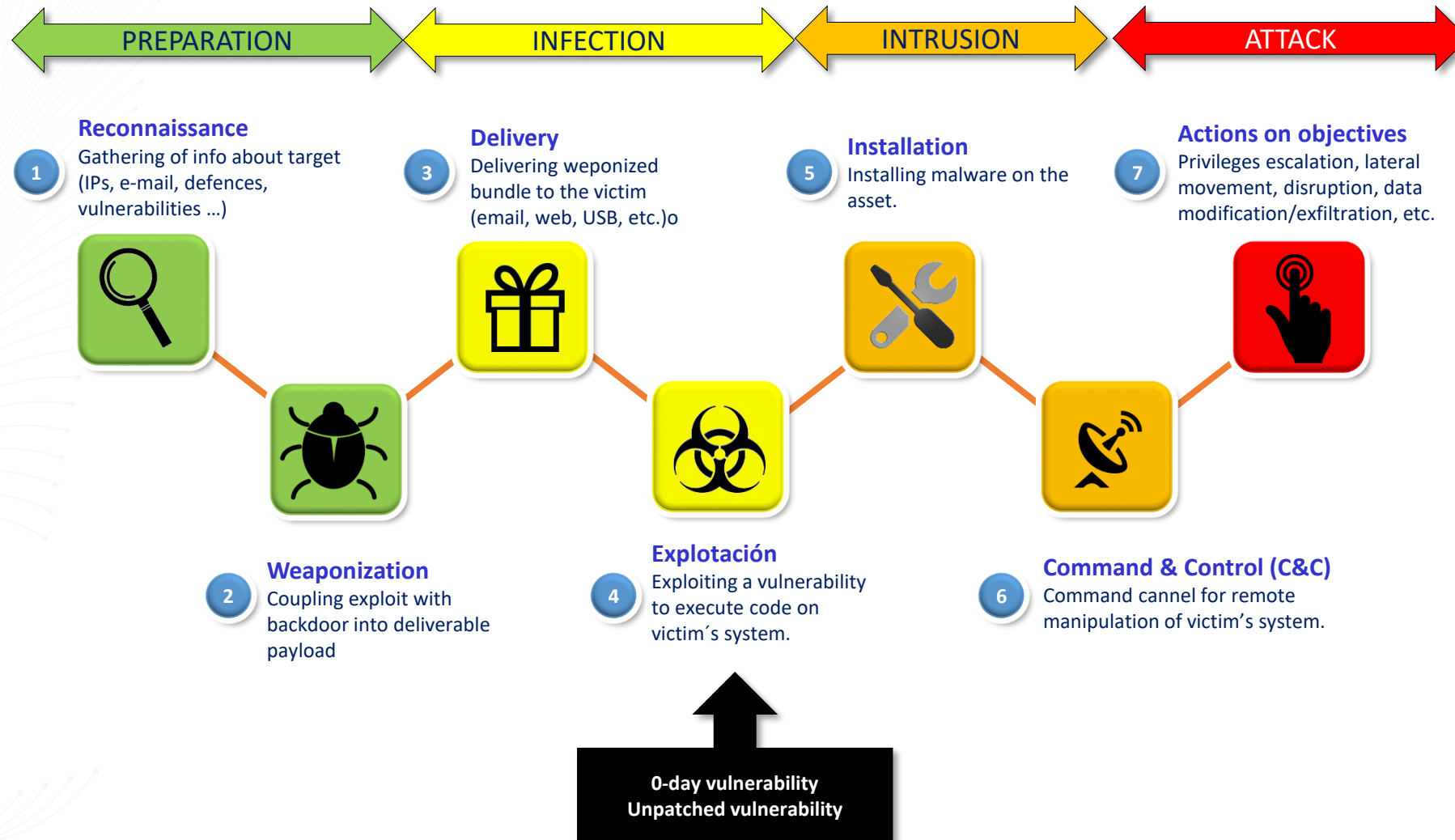


Acciones ofensivas en el ciberespacio



3.- ACCIONES OFENSIVAS EN EL CIBERESPACIO

3.1.- FASES DE UNA ACCIÓN OFENSIVA EN EL CIBERESPACIO



Efectos de las operaciones en el ciberespacio



4.- EFECTOS DE LAS OPERACIONES EN EL CIBERESPACIO

4.1.- CATEGORIAS DE GRAVEDAD POR LOS EFECTOS

La gravedad potencial y el alcance de una ciberarma o los efectos de la ciberoperación dictan el grado de control necesario para actuar de acuerdo con los principios del jus in bello..

Se definen **tres categorías de gravedad para los efectos**:

- ✓ Los **efectos primarios** tienen el potencial de afectar **directamente** los bienes físicos y las vidas humanas.
- ✓ Los **efectos secundarios** degradan o alteran los activos físicos como una **consecuencia** de segundo orden de los efectos en el dominio cibernético.
- ✓ Los **efectos indirectos** **permanecen** dentro del ciberdominio, teniendo sólo un impacto informativo.

Una ciberoperación pueden tener el **potencial de causar múltiples efectos**, posiblemente causando diferentes combinaciones de efectos primarios, secundarios e indirectos sobre diferentes objetivos. Debemos considerar cada probable combinación de objetivo y efecto para el cumplimiento de los principios de **jus in bello**.

4.- EFECTOS DE LAS OPERACIONES EN EL CIBERESPACIO

4.2.- CATEGORIAS POR PERSISTENCIA DE LOS EFECTOS

También definimos **tres grados de persistencia** para los efectos:

- ✓ **Permanente.** Este nivel de persistencia incluye efectos que **requieren la sustitución de hardware o reparaciones extensas** que requieren mucho tiempo. También incluye la **destrucción de datos primarios y copias de seguridad** de tal manera que la restauración oportuna sea imposible.
- ✓ **Temporal.** Los efectos temporales también **persisten una vez finalizada la operación**; Sin embargo, a diferencia de los efectos permanentes, **la recuperación** aquí **implica** acciones de **menor costo en recursos y tiempo**.
- ✓ **Transitorio.** Los efectos transitorios **disminuyen rápidamente** después de que el ataque termina, con poco esfuerzo por parte de la entidad objetivo.

Un ciberarma o ciberoperación pueden tener el **potencial de causar múltiples efectos**, posiblemente causando diferentes combinaciones de efectos por su persistencia sobre diferentes objetivos. Debemos considerar cada probable combinación de objetivo y efecto para el cumplimiento de los principios de **jus in bello**.

Estimación del daño colateral (CDE)



5.- ESTIMACIÓN DE DAÑO COLATERAL (CDE)

5.1.- CONSIDERACIONES

La estimación del daño colateral es una **parte fundamental del ciclo de Targeting** programado y no programado.

Es una metodología que **proporciona un proceso para predecir y mitigar los daños colaterales** de ataques letales o no letales.

El armamento empleado por las unidades del CCC no requiere el cálculo del CDE según normativa OTAN (no existiendo normativa nacional al respecto), no existiendo además un sistema que permita la estimación del mismo.

Preguntas:

- PID
- Límites laterales del TGT
- LoW/ROE
- Objetos colaterales/Escudos humanos
- Doble uso
- Amenaza NBQ
- Amenaza medioambiental



5.- ESTIMACIÓN DE DAÑO COLATERAL (CDE)

5.2.- CONSIDERACIONES LEGALES



5.- ESTIMACIÓN DE DAÑO COLATERAL (CDE)

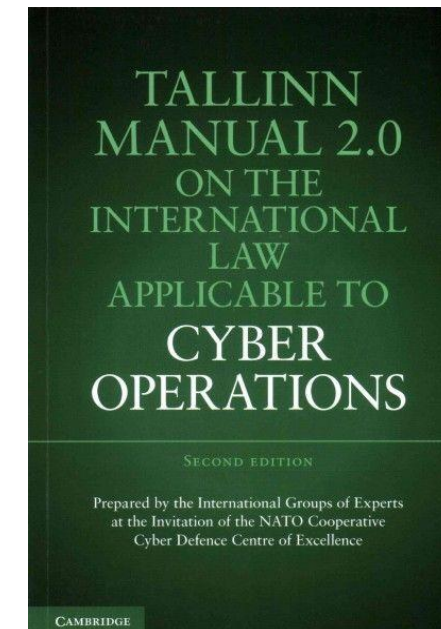
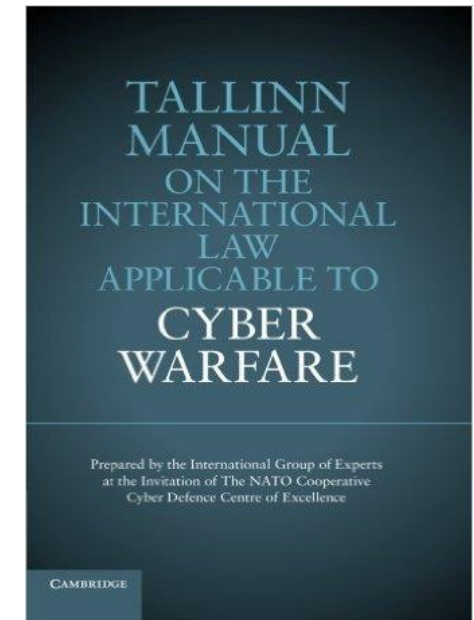
5.2.- CONSIDERACIONES LEGALES



5.- ESTIMACIÓN DE DAÑO COLATERAL (CDE)

5.3.- CONSIDERACIONES LEGALES

- Auspiciado por el CCD CoE.
- Opiniones de grupo de expertos.
- No vinculante (no reconocido internacionalmente).
- Aplicación del DIH al ciberespacio (95 normas).
- Principal conclusión: *Jus in bellum* y *Jus ad bellum* son aplicables al ciberespacio.
- Interpretaciones muy discutidas.



5.- ESTIMACIÓN DE DAÑO COLATERAL (CDE)

5.4.- COLLATERAL DAMAGE ESTIMATION

Aunque el cálculo de CDE está dirigido a los efectos físicos, no se pueden olvidar los efectos psicológicos o virtuales, algunos de los cuales pueden ser no deseados. En el ciberespacio es de especial interés los targets restringidos y las entidades de doble uso.

CJCSI 3370.01B: TARGET DEVELOPMENT STANDARDS

ANNEX C TO APPENDIX B TO ENCLOSURE D VIRTUAL TARGETS

Collateral Damage Considerations. Collateral damage considerations should not be limited to the distance or physical connections, but should consider any second and third order cascading effects.

CJCSI 3160.01B: NO-STRIKE AND THE COLLATERAL DAMAGE ESTIMATION METHODOLOGY

ENCLOSURE D – COLLATERAL DAMAGE ESTIMATION (CDE) POLICY AND GUIDANCE

h. (U) The CDM does not account for secondary explosions

Battle Damage Assessment (BDA)



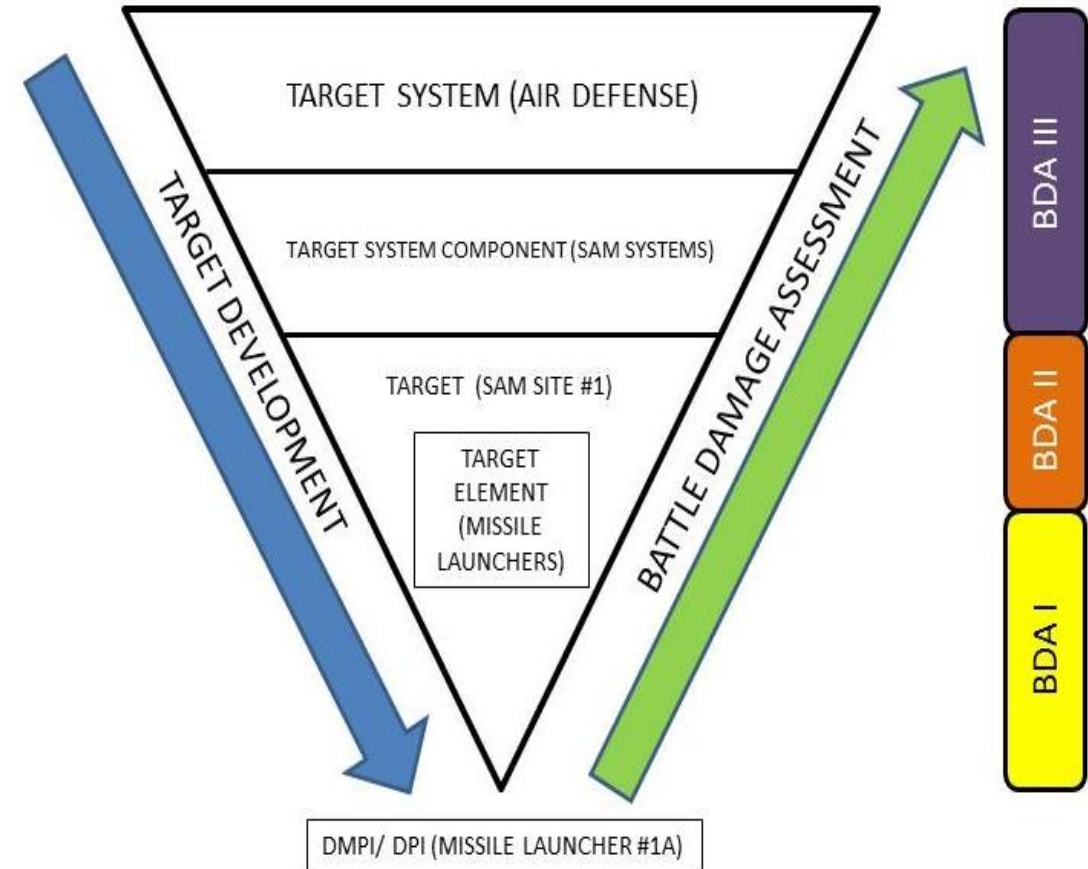
6.- BATTLE DAMAGE ASSESSMENT (BDA)

6.1.- VALORACION

La valoración de los efectos logrados por las acciones contra los *targets* se consigue mediante el análisis, en tres diferentes niveles, de los daños causados por estas:

- **Daño físico** (o Indicador de cambio para *Info Ops*), en cada *target element*.
- **Daño funcional**, del *target*.
- **Daño en los *target components* y *target system*.**

Es posible que, para llegar a valorar el daño en un determinado sistema de *targets*, haya que valorar el daño infligido a cada uno de los *targets* que lo componen. Para ello, se tendrá en cuenta el **daño funcional alcanzado y el tiempo de recuperación** estimado tras la ejecución de la acción



6.- BATTLE DAMAGE ASSESSMENT (BDA)

6.3.- BDA I / BDA II

OPER/OPLAN IB//
MSGID/INTEL TGT BDA / **BDAREP PHASE1 //**
BDAREPID/N000007//
ICOD/251030LJUN18//
BDA CELL/CCC / TGT BDA / //

GENTEXT/PURPOSE/THIS PHASE 1 BDA REPORT CONTAINS INITIAL PHYSICAL DAMAGE ASSESSMENTS IAW AD 80-70 AND OPLAN IB TARGETING DIRECTIVES//

TARGET/NBET5/60/CELTIA TELEKOM/83220/CEL/0041.0000N00036.0000W//
TGT SYS/SCT/ELECTRONIC ATTACK//
BDA SUMMARY/ PÁGINA WEB DE CELTIA TELEKOM. [HTTPS://WWW.CELTIA TELEKOM.CE/](https://www.celtiatelekom.ce/) (IP 61.6.241.125). PÁGINA OFICIAL DE CELTIA TELEKOM, DONDE EL PERSONAL CIVIL ESTA COLGANDO INFORMACIÓN SOBRE LA CAMPAÑA DE DECEPCION DE ISBETFOR.//

ADDMG/NTR//
COLDMG/NTR//
ENVDMG/NTR//

TGTEL/PLANNED:Y/TGTEL-CELTIA TELEKOM/NUMAIMPOINTS:1//
ELDMG/PHYDMG:SEV DMG/CONF:CNFRM//

GENTEXT DAMAGE/ATAQUE DE ACUERDO CON TIME LINE. 100% DE RESULTADOS DE EFECTIVIDAD DE MALWARE.//
AIMPOINT/AAA01/SERVIDOR/PHYDMG:SEV DMG/CONF:CNFRM/GEO:0041.0000N00036.0000W//

MSNDAT/GA/20180623-08/CS:N/A/UNIT:GA-ECC-03/PLTFRM:EXPLOITING
WEB/NUMWPN:1/WPNTYPE:WEBSHELL/N/A//

BDASRC/GA//
IMAGERY/NO//

REMARKS:/HA QUEDADO CIFRADO SU CONTENIDO Y DAÑADOS SUS BACKUPS.//

OPER/OPLAN IB//
MSGID/ INTEL TGT BDA/ **BDAREP PHASE 2//**
BDAREPID/N000007//
ICOD/251030LJUN18//
BDA CELL/CCC / TGT BDA / //

GENTEXT/PURPOSE/THIS PHASE 2 BDA REPORT PROVIDES AN ALL-SOURCE ASSESSMENT OF DETAILED PHYSICAL AND FUNCTIONAL DAMAGE TO CELTIA TELEKOM USING INFORMATION DERIVED FROM PHASE 1 BDA REPORTING AND ADDITIONAL INTELLIGENCE AS APPLICABLE. REPORT IS IAW AD 80-70 AND OPLAN IB TARGETING DIRECTIVE//

TARGET/NBET5/16/CELTIA TELEKOM/83220/CEL/0041.0000N00036.0000W//
TGT SYS/SCT/ELECTRONIC ATTACK//
GENTEXT/TARGET OBJECTIVE:DD//

TGTDMDG/FUNCDMDG:FUNC DSTR/STCHG:Y//

GENTEXT/BDA SUMMARY/SE ESTA MONITORIZANDO EL SERVIDOR Y NO SE DETECTA ACTIVIDAD. EL MALWARE SIGUE INSTALADO Y NEGANDO EL ACCESO A LOS SISTEMAS. HA QUEDADO CIFRADO SU CONTENIDO Y DAÑADOS SUS BACKUPS.//

ADDMG/NSTR//
COLDMG/NSTR//
ENVDMG/NSTR//

TGTEL/PLANNED:Y/TGTEL-CELTIA TELEKOM/NUMAIMPOINTS:1//

ELDMG/PHYDMG:DES EFCT ACHVD/CONF: CNFRM/FUNCDMDG:FUNC DSTR/STCHG:Y/MINRECUP:NO ESTIMABLE/MAXRECUP:NO ESTIMABLE//

GENTEXT DAMAGE NARRATIVE/LOS DAÑOS LOGICOS AFECTAN A TODOS LOS SISTEMAS Y COPIAS DE SEGURIDAD, QUE SE ENCUENTRAN INFECTADAS IMPOSIBILITANDO LA RESTAURACIÓN. EL SOPORTE INFORMATICO QUE DA EL SISTEMA ESTA INUTILIZADO, SIENDO NECESARIO LA REPOSICIÓN FISICA DE TODOS LOS SISTEMAS. HA QUEDADO CIFRADO SU CONTENIDO Y DAÑADOS SUS BACKUPS.//
AIMPOINT/AAA01/SERVIDOR/PHYDMG:SEV DMG/CONF:CNFRM/0041.0000N00036.0000W//

MSNDAT/GA/20180623-08/MISSION:N/A/CS:/UNIT:GA-ECC-01/PLTFRM:EXPLOITING
WEB/NUMWPN:1/WPNTYPE:WEBSHELL/N/A//

GENTEXT/MUNITIONS EFFECTIVENESS SUMMARY/EL MALWARE HA AFECTADO AL TARGET SEGÚN LO ESPERADO.//

BDASRC/MONITORIZACIÓN//

IMAGERY/NA//

BDAREF/MONITORIZACION DE LOS SISTEMAS POR EL GE//

AMPN/BDAREP II HA SIDO REALIZADO EN BASE A LA MONITORIZACION D ELOS SISTEMAS POR EL PROPIO MANDO EJECUTANTE//

Target Folder

Joint Targeting System (JTS)

Functional Area Service for Dynamic and Time Sensitive Targeting (FAST)



7.- TARGET FOLDER

7.1.- Joint Targeting System (JTS)

JTS proporciona capacidad para la designación de objetivos, la gestión de la lista de objetivos y la evaluación del combate de las operaciones a nivel operacional y táctica en tiempos de paz, ejercicios, crisis y conflictos. Por lo tanto, JTS soporta completamente el ciclo de targeting conjunto entre el JFC y escalones superiores y los diversos mandos Componentes (CC) y subordinados (p.ej. CAOCs)..

La aplicación JTS **puede ser utilizada en cada uno de los pasos del proceso del Joint Targeting Process** y en **todos los niveles de Mando**. Se ajusta a la **doctrina de la OTAN** sobre objetivos conjuntos y a la estructura C2.

JTS es básicamente la herramienta de targeting para:

- almacenar la inteligencia producida del target
- mantener listas de targets
- crear/mantener los targets
- Almacenar los informes de BDA



7.- TARGET FOLDER

7.2.- Functional Area Service for Dynamic and Time Sensitive Targeting (FAST)

En su esencia, FAST es un **instrumento de colaboración y coordinación**, diseñado para ayudar en el **seguimiento y enjuiciamiento de Time Sensitive Targets**. Debido a la sensibilidad en el tiempo de los objetivos, FAST está diseñado para ser lo más fácil posible de usar, minimizando la cantidad de navegación y el número de clics de ratón necesarios para un uso óptimo. La parte central de la ventana FAST, el apartado Joint Time Sensitive Targets, ha sido diseñado para presentar los datos relativos al estado actual de seguimiento del target de una manera condensada, pero fácil de entender.

Para coordinar el ciclo de TST, FAST gestiona 3 cosas :

- **Targets:** todos los objetivos sensibles en el tiempo real.
- **Participants:** Los miembros de la célula TST, a cada uno de los cuales se le pueden asignar tareas
- **Tasks:** Tareas que deben realizar los participantes para determinar si un objetivo puede ser adquirido



TARGET PRESENTATION

(CLASSIFICATION when completed)

NAME: CELTIA TELEKOM (PAGINA WEB)

TGT NAT: CEL

TGT LOC: 0041.0000N00036.0000W (RADIUS 25KM)

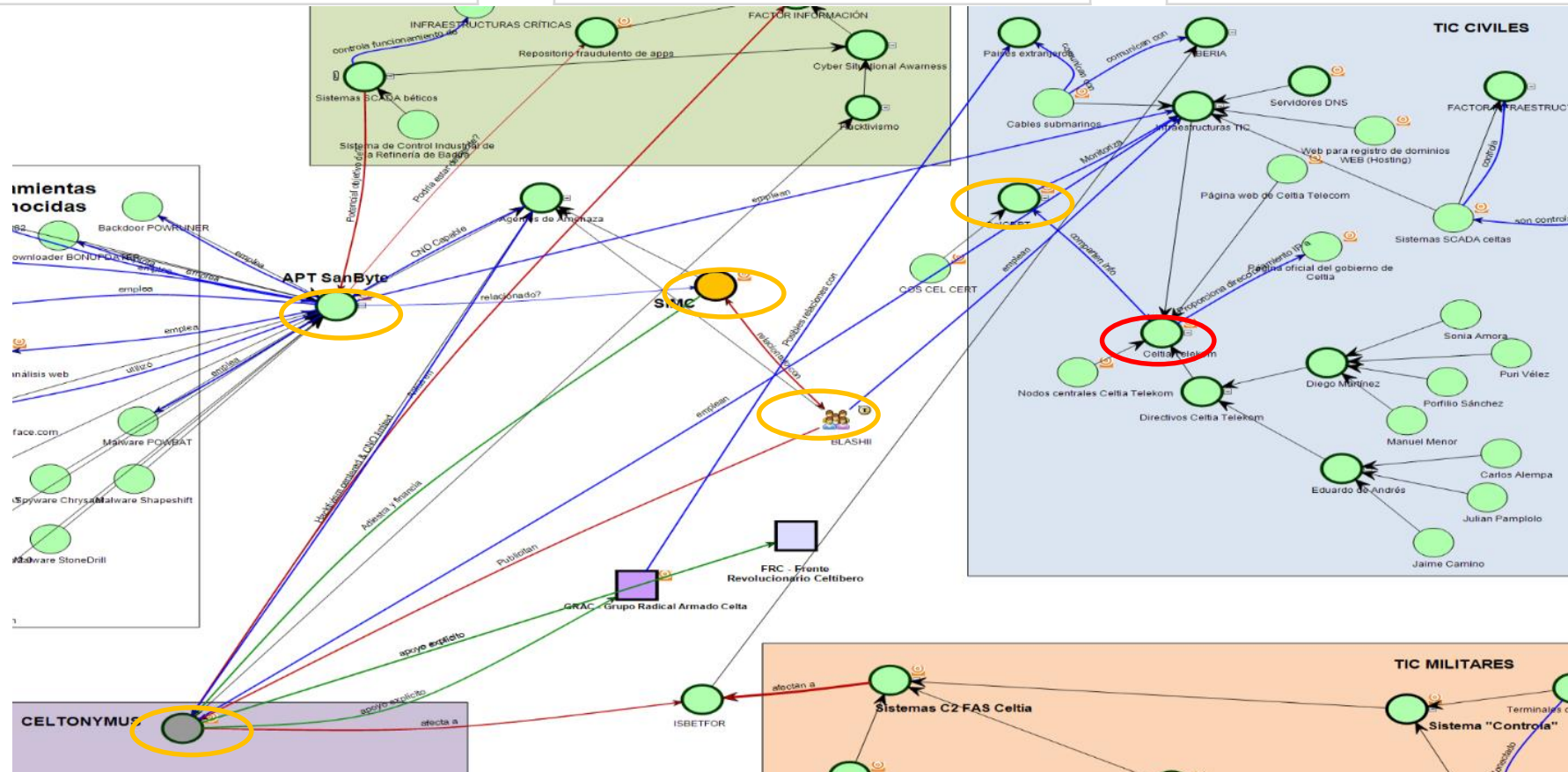
TGT ID: XCELCCC00016V

TOT: NO TIME CONSTRAINT

CATEGORY		INDIVIDUAL
	X	GROUP

PRIORITY	1	URGENCY	A
----------	---	---------	---

NOMINATING AGENCY:	CCC	CURRENT STATUS:	JTL	TGT VALID AS OF:
SERVICING AGENCY:	CCC	PROPOSED STATUS:	JPTL	11/05/2018



TARGET JUSTIFICATION

(CLASSIFICATION when completed)

NAME: CELTIA TELEKOM (PAGINA WEB)
TGT NAT: CEL
TGT LOC: 0041.0000N00036.0000W (RADIUS 25KM)
TGT ID: XCELCCC00016V
TOT: NO TIME CONSTRAINT

TGT SET	HN	ROE	D-USE	HAZARD	H-SHIELD	LEGAD	POLAD
CYF							

TARGET DESCRIPTION
PAGINA OFICIAL DE CELTIA TELEKOM,
FUNCTIONAL CHARACTERIZATION
LA ARQUITECTURA DEL SISTEMA TIENE UNA IP CONOCIDA: https://www.celtiatelecom.ce/ (IP 61.6.241.125)

ROE
AL AMPARO DE LAS ROE DEL GRUPO 120-129 SERIE 122 (12203, 12204, 12205, 12206, 12207A/B, 12208, 12209) SE HAN LLEVADO A CABO LAS CYISR DE PENTESTING, (ESCANEOS DE PUERTOS Y LEVANTAMIENTO DE ESTRUCTURA DE RED). AL AMPARO DE LAS ROE DEL GRUPO 120-129 SERIE 122 (12213A , 12214A/B, 12215A) SE PRETENDEN LLEVAR A CABO LAS OCO CONDUCTENTES A DEGRADAR LAS CAPACIDADES EN EL CIBERESPACIO DEL REPOSITORIO FRAUDULENTO DE USO POR PARTE DE APT SANBYTE.

TARGET SIGNIFICANCE
PAGINA OFICIAL DE CELTIA TELEKOM, DONDE EL PERSONAL CIVIL ESTA COLGANDO INFORMACIÓN SOBRE LA CAMPAÑA DE DECEPCION DE ISBETFOR.
CRITICAL TARGET ELEMENTS
AAA01 https://www.celtiatelecom.ce
OPERATIONAL OBJECTIVE - DECISIVE CONDITIONS - INFO SUPPORT EFFECT
OO: DC:J07 – CAPACIDAD DE PROXIES DE CELTIA REDUCIDA ISE:J071 – NODOS
DESIRED EFFECT(S)
DD (DISRUP COMUNICATION)
EXPECTATION STATEMENT
UN ATAQUE A ESTA PAGINA PODRIA ACARREAR EL DESPRESTIGIO DE LA EMPRESA Y POR ENDE DEL GOBIERNO CELTA
CONSTRAINT(S)
NECESIDAD DE APROBACIÓN DADO EL CDE. CDE 5H POR POSIBLES CONSECUENCIAS POLÍTICAS EN LA EJECUCIÓN DE LA ACCIÓN SOBRE EL TARGET AL ATRAVESAR ESPACIOS CYBER DE SOBERANÍA NACIONAL DE PAÍSES AMIGOS
INFO ACTIVITIES COORDINATION
Virtual – Equipment - Organization

TARGET ACTION PLAN

(CLASSIFICATION when completed)

NAME: CELTIA TELEKOM (PAGINA WEB)
TGT NAT: CEL
TGT LOC: 0041.0000N00036.0000W (RADIUS 25KM)
TGT ID: XCELCCC00016V
TOT: NO TIME CONSTRAINT

OVER CDE CALL	CDE 5-HIGH HST
Por posibles consecuencias políticas en la ejecución de la acción sobre el target al atravesar espacios cyber de soberanía nacional de países amigos.	

WEAPON SOLUTION 1

SERIAL	DESCRIPTION	SERVICING UNIT/ORG	METHOD & MESSAGE	TIME FRAME
	LOCATION			
01	AAA01 https://www.celtiatelecom.ce	CCC	VECTOR: EXPLOITNG WEB MALWARE: WEBSHELL	A/O (TIME FRAME BDA 72H)
	Equipos (COMUNICACIONES) IP 61.6.241.125			



BDA REP I y II

OPER/OPLAN IB//
MSGID/INTEL TGT BDA **BDAREP PHASE1 //**
BDAREPID/N000007//
ICOD/251030LJUN18//
BDA CELL/CCC / TGT BDA / //

GENTEXT/PURPOSE/THIS PHASE 1 BDA REPORT CONTAINS INITIAL PHYSICAL DAMAGE ASSESSMENTS IAW
AD 80-70 AND OPLAN IB TARGETING DIRECTIVES//

TARGET/NBET5/60/CELTIA TELEKOM/83220/CEL/0041.0000N00036.0000W//
TGT SYS/SCT/ELECTRONIC ATTACK//
BDA SUMMARY/ PÁGINA WEB DE CELTIA TELEKOM. [HTTPS://WWW.CELTIA TELEKOM.CE/](https://www.celtiatelekom.ce/) (IP 61.6.241.125).
PAGINA OFICIAL DE CELTIA TELEKOM, DONDE EL PERSONAL CIVIL ESTA COLGANDO INFORMACIÓN SOBRE
LA CAMPAÑA DE DECEPCION DE ISBETFOR.//

ADDMG/NTR//
COLDMG/NTR//
ENVDMG/NTR//

TGTEL/PLANNED:Y/TGTEL-CELTIA TELEKOM/NUMAIMPOINTS:1//
ELDMG/PHYDMG:SEV DMG/CONF:CNFRM//

**GENTEXT DAMAGE/ATAQUE DE ACUERDO CON TIME LINE. 100% DE RESULTADOS DE EFECTIVIDAD DE
MALWARE.//**
AIMPOINT/AAA01/SERVIDOR/PHYDMG:SEV DMG/CONF:CNFRM/GEO:0041.0000N00036.0000W//

MSNDAT/GA/20180623-08/CS:N/A/UNIT:GA-ECC-03/PLTFRM:EXPLOITING
WEB/NUMWPN:1/WPNTYPE:WEBSHELL/N/A//

BDASRC/GA//
IMAGERY/NO//

REMARKS:/HA QUEDADO CIFRADO SU CONTENIDO Y DAÑADOS SUS BACKUPS.//

OPER/OPLAN IB//
MSGID/ INTEL TGT BDA **BDAREP PHASE 2//**
BDAREPID/N000007//
ICOD/251030LJUN18//
BDA CELL/CCC / TGT BDA / //

GENTEXT/PURPOSE/THIS PHASE 2 BDA REPORT PROVIDES AN ALL-SOURCE ASSESSMENT OF DETAILED
PHYSICAL AND FUNCTIONAL DAMAGE TO CELTIA TELEKOM USING INFORMATION DERIVED FROM
PHASE 1 BDA REPORTING AND ADDITIONAL INTELLIGENCE AS APPLICABLE. REPORT IS IAW AD 80-70
AND OPLAN IB TARGETING DIRECTIVE//

TARGET/NBET5/16/CELTIA TELEKOM/83220/CEL/0041.0000N00036.0000W//
TGT SYS/SCT/ELECTRONIC ATTACK//
GENTEXT/TARGET OBJECTIVE-DD//

TGTDMG/FUNCDMG:FUNC DSTR/STCHG:Y//
**GENTEXT/BDA SUMMARY/SE ESTA MONITORIZANDO EL SERVIDOR Y NO SE DETECTA ACTIVIDAD. EL
MALWARE SIGUE INSTALADO Y NEGANDO EL ACCESO A LOS SISTEMAS. HA QUEDADO CIFRADO SU
CONTENIDO Y DAÑADOS SUS BACKUPS.//**

ADDMG/NSTR//
COLDMG/NSTR//
ENVDMG/NSTR//

TGTEL/PLANNED:Y/TGTEL-CELTIA TELEKOM/NUMAIMPOINTS:1//
ELDMG/PHYDMG:DES EFCT ACHVD/CONF: CNFRM/FUNCDMG:FUNC DSTR/STCHG:Y/MINRECU: NO
ESTIMABLE/MAXRECU: NO ESTIMABLE//

**GENTEXT DAMAGE NARRATIVE/LOS DAÑOS LOGICOS AFECTAN A TODOS LOS SISTEMAS Y COPIAS DE
SEGURIDAD, QUE SE ENCUENTRAN INFECTADAS IMPOSIBILITANDO LA RESTAURACIÓN. EL SOPORTE
INFORMATICO QUE DA EL SISTEMA ESTA INUTILIZADO, SIENDO NECESARIO LA REPOSICIÓN FISICA DE
TODOS LOS SISTEMAS. HA QUEDADO CIFRADO SU CONTENIDO Y DAÑADOS SUS BACKUPS.//**
AIMPOINT/AAA01/SERVIDOR/PHYDMG:SEV DMG/CONF:CNFRM/0041.0000N00036.0000W//

MSNDAT/GA/20180623-08/MISSION:N/A/CS:/UNIT:GA-ECC-01/PLTFRM:EXPLOITING
WEB/NUMWPN:1/WPNTYPE:WEBSHELL/N/A//

**GENTEXT/MUNITIONS EFFECT/VENESS SUMMARY/EL MALWARE HA AFECTADO AL TARGET SEGÚN LO
ESPERADO.//**

BDASRC/MONITORIZACIÓN//
IMAGERY/NA//
BDAREF/MONITORIZACION DE LOS SISTEMAS POR EL GE//

**AMPN/BDAREP II HA SIDO REALIZADO EN BASE A LA MONITORIZACION D ELOS SISTEMAS POR EL
PROPIO MANDO EJECUTANTE//**



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

CCN-cert
centro criptológico nacional