Universidad Internacional de La Rioja (UNIR)

ESIT

Máster universitario en Seguridad Informática

Operaciones de Defensa en el Ciberespacio desde una perspectiva MILDEC

Trabajo Fin de Máster

presentado por: Daton Medenou, Roumen
Directores:
Martínez Monterrubio, Sergio Mauricio. PhD
Maestre Vidal, Jorge. PhD

Misión MILCYBDEC: Madrid
Fecha: 2 Marzo 2022

Índice

Índice de Figuras

Glosario

Sigla	Definición
ACA	Ciber Área de Actuación
AJP-3.20	Doctrina Conjunta de la OTAN para Operaciones en el Ciberespacio
AOR	Área de Responsabilidad
BDA	Daño de Batalla
C2	Mando y Control
CCMD	Mando de Combate
CCDR	Comandante de Combate
CJCSM	Jefe de Estado Mayor Conjunto
CI	Contrainteligencia
CIO	Jefe de Información; Chair Information Officer
CO	Operaciones Cibernéticas (Cyber Operations)
COA	Contramedida (Course of Action)
CO-IPE	Elemento de Planificación de CiberOperación
COP	Imagen Operacional Común
CMT	equipo de combate
CPT	equipo de ciberdefensa
CS	Análisis Situacional
CSA	Agencia de Soporte al Combate
CSSP	proveedor de servicios de ciberseguridad
CYBDEC	Engaño Ciber ; Cyber Deception
CYSA	Ciber conciencia Situacional
DCO	CO Defensivas
DCO-IDM	DCO de Medidas Defensivas Internas
DCO-RA	DCO de Respuesta
DISA	Organismo de Sistemas Informáticos de Defensa
DOD	MOD
EMS	Soporte de Guerra Electrónica
EW	Guerra Electrónica (Electromagnetic Warfare)
EXORD	orden de ejecución
FM3-12	Doctrina sobre Operaciones en el Ciberespacio y Guerra Electrónica
GCC	Mandos geográficos de Combate
IGL	ganancia/pérdida de inteligencia
ISR	Inteligencia, Vigilancia y Reconocimiento
JFC	Mando de Fuerzas Conjuntas
JOA	Área de Operaciones Conjuntas
JP3-12	Doctrina de Operaciones en el Ciberespacio
JP3-13.4	Doctrina conjunta de EEUU, sobre MILDEC
JPP	Proceso de Planificación Conjunta
JTL	lista conjunta de objetivos
IJSTO	operaciones técnicas especiales conjuntas integradas

TIC	Tecnologías de la Información y Comunicaciones
TIP	TIC de Plataforma

Tabla 1: Glosario

Resumen

Durante años, el ciberespacio ha sido considerado como el quinto dominio de batalla. No es de extrañar que las tácticas de guerra tradicionales se hayan traducido al Ciberespacio, tales como las tácticas de guerrilla, guerra asimétrica, engaño, atribución, entre otros. Recientemente, en las doctrinas de OTAN y Países Miembros se empieza a hablar de Operaciones Ofensivas en el Ciberespacio. Dichas operaciones son de apoyo o de actuación directa en dicho quinto dominio de batalla, como parte de una planificación inherentemente conjunta y/o combinada. Sin embargo, en el año de 2022, las operaciones en el ciberespacio siguen predominantemente basadas en efectos, donde su finalidad típicamente escala hacia una pretensión de objetivos estratégicos no convencionales (diplomáticos, económicos, sociales, políticos, etc.). No es de extrañar pues su proximidad a las operaciones MILDEC ('Military Deception' o Engaño Militar), siendo su uso en operaciones de defensa vinculado a conceptos como la estratagema o la disuasión; en ocasiones vinculadas a operaciones psicológicas y/o de información (de cara a articular una misión o narrativa paralela a la realidad englobando esta narrativa de engaño todos los dominios excepto el de ciberespacio). De ahí que es necesario realizar una síntesis del uso del ciberespacio como campo de batalla desde una perspectiva OTAN y proponer puntos de entrada de procedimientos MILDEC.

Palabras Clave: MILDEC; Engaño militar; Ciberdefensa; OTAN

Capítulo 1: Introducción

1.1. Motivación

El engaño militar (MILDEC) surge, de entre otros, de la necesidad de ejecutar una Misión Alternativa dedicada a ocultar las actuaciones de la Misión Principal (verdadera), o a hacer que las fuerzas adversarias realicen o se abstengan de realizar ciertas acciones. Al público en general, algunos de los procesos más conocidos de misiones militares son la Inteligencia, Contrainteligencia, Inteligencia de Señales (SIGINT), y más recientemente se han popularizado (divulgado) procesos de Guerra Electrónica. Sin embargo, técnicas de engaño y ocultación modernas datan de Siglo XX (Stech, Heckman, & & Strom, 2016) y documentos sobre ellas no son de amplio conocimiento. Hay muchas aplicaciones de MILDEC que, a primera vista, no parecen necesarias en el dominio cibernético de batalla. A modo de ejemplo, una de las aplicaciones de MILDEC es ocultar la relación de fuerzas, ante el adversario. (MILDEC JP3-13.4 Military Deception, 2012) En el domino cibernético, ¿cómo cuantificamos las fuerzas y capacidades? ¿Cómo las comparamos? Dicha cuantificación está muy abierta a interpretaciones. En el dominio cibernético del mundo presente, no parece haber asimetría entre adversarios, ya que, hoy, las operaciones cibernéticas ofensivas no suelen venir acompañadas por atribución (Rico, 2021), por miedo a una respuesta cinética del afectado. Sin embargo, en un futuro es muy probable que aparezcan disparidades (desigualdad) de capacidades ofensivas y defensivas entre distintos actores internacionales. (Peñas, 2021) En tales casos, el uso de CYBDEC y MILDEC en el dominio cibernético, sería esencial.

1.2. Planteamiento del Problema

Existen cierto tipo de ataques cibernéticos a los que no se ha sabido dar respuesta convencional. Por lo tanto, es fundamental crear una metodología de engaño cibernético, que es un método suplementario de defensa contra ataques a Terrenos Cibernéticos Clave (CKT), tales como radares, estaciones de Mando y Control, Servidores GIS, routers, servidores DNS, y otros activos y procesos cibernéticos que dan soporte a operaciones en el ciberespacio.

1.3. Estructura del Trabajo

El presente trabajo se estructura en tres grandes bloques

Objetivos, que vienen a plantear el Objetivo General y Objetivos Específicos de la propuesta de Metodología aplicada a CYBDEC y MILDEC

Estado del Arte, que hace un extenso repaso por las metodologías y enumera conceptos necesarios para entender la presente propuesta de Metodología

Propuesta de Metodología, que viene a contribuir y ampliar al estado de arte existente. (En ámbito militar, viene a contribuir a las doctrinas existentes mediante contribuciones del ámbito civil)

1.4. Objetivos

1.4.1.1.1. Objetivo General

A 2018, el Departamento de Defensa de EEUU publica la doctrina sobre Operaciones en el Ciberespacio JP3-12 (DOD, Cyberspace Operations JP3-12, 2018).
A 2020, OTAN publica la Doctrina Conjunta para Operaciones en el Ciberespacio AJP-3.20. ((NSO), 2020)
A 2021, el Departamento de Defensa de EEUU publica su última doctrina sobre Operaciones en el Ciberespacio y Guerra Electrónica FM3-12, (DOD, CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE , FM3-12, 2021) que es bastante más amplio que la doctrina conjunta de la OTAN.

SI bien en el ámbito civil se habla profusamente de CYBDEC o Engaño Cibernético (Jajodia & Subrahmanian, 2016) , dicha familia de tecnologías sólo hace mención a aplicaciones civiles.

El presente trabajo tiene como objetivo ser un punto de encuentro entre FM3-12, JP3-13.4, JP3.12, AJP-3.20.

El objetivo general es el Desarrollo de una Metodología de Evaluación y Evolución de Misiones de Ciber engaño orientadas a planificar, articular y llevar a cabo una Misión dedicada a MILDEC.

Dicha metodología se basará las doctrinas FM3-12, JP3-13.4, JP3.12, AJP-3.20.

1.4.1.1.2. Objetivos Específicos

1. Conectar la Doctrina de MILDEC y Doctrina de Guerra Electrónica exponiendo las necesidades y/o requisitos extendidos
2. Tratar de solventar dichas necesidades mediante una propuesta metodológica basada en el Estado del Arte de CYBDEC presente en el sector civil y lo expuesto en Objetivo 1.

1.4.1.1.3. Hipótesis

1.4.1.1.4. Hipótesis Nula (H0)

Los Procesos de Ciberengaño dentro de la Planificación y Ejecución de la Misión en el Sector Militar, se ejecutan como tareas aisladas de una misión principal en el sector militar tipo MILDEC (JP3-4), y FM3-12.

1.4.1.1.5. Hipótesis Alternativa (HA)

Aunque en algunas doctrinas ya estaban establecidas (e.g. AJP de US), el debate y la necesidad de CYBMILDEC se ha hecho especialmente visible en el último Summit de la OTAN (NATO, 2021); donde abiertamente se ha planteado y discutido la necesidad de usar MILDEC en operaciones cibernéticas. Esto es prácticamente una llamada a la acción entre los distintos miembros de la Coalición (incluso EU), los que han empezado a valorar y establecer hojas de ruta para el desarrollo de capacidades CD ofensivas. Por ello se crea la necesidad de una metodología que involucre todos los procesos y tareas de una misión en el sector militar.

La Metodología MILCYBDEC es mejor para la tarea de Planificación y Ejecución de Ciberengaño que cada uno de sus rivales MILDEC(JP3-4), FM3-12, dando la visión completa de una Misión de CIberengaño, más que relegando dichos procesos a simples tareas de la Misión Principal en el Sector Militar.

Capítulo 2: Estado del Arte

2.1. Taxonomía del Riesgo

2.1. Introducción

En la literatura de ciberseguridad, demasiadas veces se define a Riesgo, como el producto de dos valores escalares: Probabilidad por Impacto.

(OpenGROUP, 2021) (OpenGROUP, 2021) Ahora bien, Probabilidad e Impacto no son valores escalares en origen, sino que son funciones que se alimentan de otras variables. En Figura 1, se presenta un árbol taxonómico completo que se irá desarrollando y ampliando a lo largo de este capítulo.

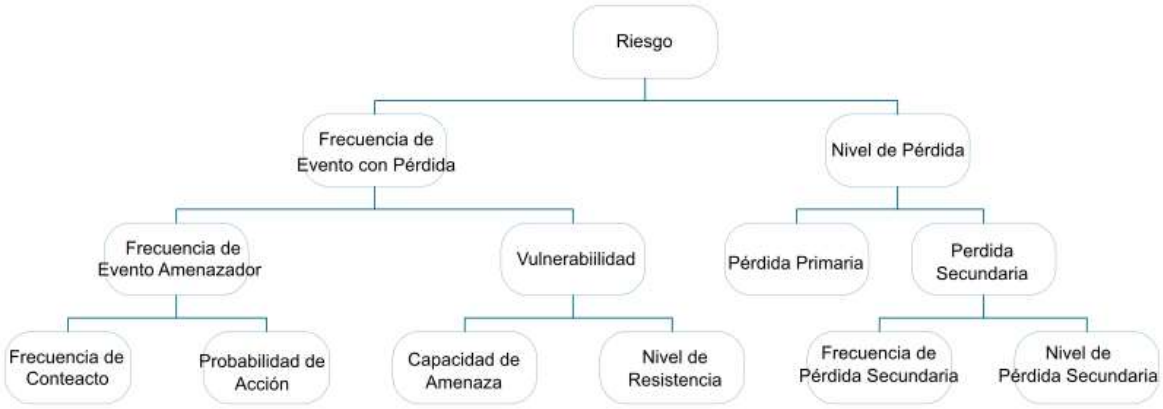


Figura 1: Árbol de Riesgo (OpenGROUP, 2021)

2.1. Riesgo Cibernético

Figura 2: Riesgo: LEF^LM (OpenGROUP, 2021)

En este documento, “riesgo” es definido como la frecuencia probable y el probable grado de perdida futura (también conocido como ‘exposición a perdida’). (NB: No estamos hablando de riesgos especulativos que puedan generar pérdidas o ganancias)

Una medición de riesgo es una estimación de la probabilidad (en inglés “likelihood”) y del impacto de eventos adversos (pérdidas). De hecho, en inglés hay por lo menos dos palabras no-sinónimas que traducidas al castellano significan probabilidad: “likelihood” y “probability”. “Likelihood” se acerca más al concepto de “muy probable, poco probable, etc.”, mientras que “probability”, en general, es la probabilidad estadística como tal, que de hecho muchas veces se mide como frecuencia estadística.

Medir el riesgo NO debe ser en absoluto un proceso de predicción de si algún evento adverso ocurrirá, p.e. que un terremoto destruya un CPD (centro de proceso de datos) causando pérdidas de un millón de euros en el año siguiente; sino más bien, la medición de riesgo es la estimación de la probabilidad (sea likelihood o probability) de que dicho evento adverso ocurra en el año o periodo económico siguiente. Las mediciones de riesgo son precisas si el rango de valores de las medidas reales (cuántos terremotos ocurrieron en el año, p.e.) se encuentran dentro de los rangos previamente estimados. Una medición de riesgo de terremoto sería un análisis razonado y defendible, cuyos resultados sería parecido a “Hay entre 10% a 20% de probabilidad de que un terremoto destruya el CPD causando daños de entre mil euros y cinco millones. Dicha estimación se vería probada correcta o incorrecta en la siguiente ventana de tiempo de la que habla, cuando durante dicho periodo se observen o no daños por terremotos.

Si hablamos de análisis de riesgo, cabe diferenciar entre los conceptos de posibilidad y probabilidad (“probability”). “Posibilidad” puede ser visto como algo binario: posible o imposible. Probabilidad (“probability”), sin embargo, es un rango continuo que vive entre certeza e imposibilidad. Ya que el riesgo forzosamente trata sobre eventos futuros, siempre habrá cierta cantidad de incertidumbre, lo que significa que el personal de gestión no puede priorizar un riesgo sobre otro de manera efectiva sólo basándose en el atribuido de ‘posibilidad’. La toma efectiva de decisiones sólo puede ser llevada a cabo si hay disponible información sobre las probabilidades de los riesgos. Por otro lado, los análisis de riesgo no deberían ser consideras “predicciones de futuro”. La palabra “predicción” implica un nivel de certeza que raramente existe en el mundo real, y no ayuda a las personas a comprender la naturaleza probabilística del análisis. Para el personal de gestión, incluso siendo imposible “adivinar qué número va a dar un dado”, sabiendo que la probabilidad es 1 entre 6, ya de por sí es información muy útil.

Con todo esto en mente, pasamos a detallar los dos componentes más inmediatos de riesgo cibernético. Aquí nos referiremos a ellos como “Frecuencia de Evento con Pérdida” (“Loss Event Frequency” ó LEF) y “Magnitud de pérdida” (“Loss Magnitude” ó LM)

2.1.2.1. Frecuencia de Evento con Perdida (LEF)

Figura 3: LEF: VULN ^ TEF: CF ^ PoA (OpenGROUP, 2021)

La frecuencia de un evento con perdida (LEF) es la frecuencia probabilística, dentro de una ventana de tiempo, con la que el Agente Amenazador causará daños sobre un Activo.

Para que un Evento con Pérdida ocurra, un Agente Amenazador tiene que actuar sobre un tipo de Activo, de tal forma de que se produzca pérdida, lo que nos lleva a los dos subcomponentes de LEF que son: Frecuencia de Evento con Amenaza (TEF) y Vulnerabilidad (VULN).

2.1.2.2. Frecuencia de Evento Amenazador (TEF)

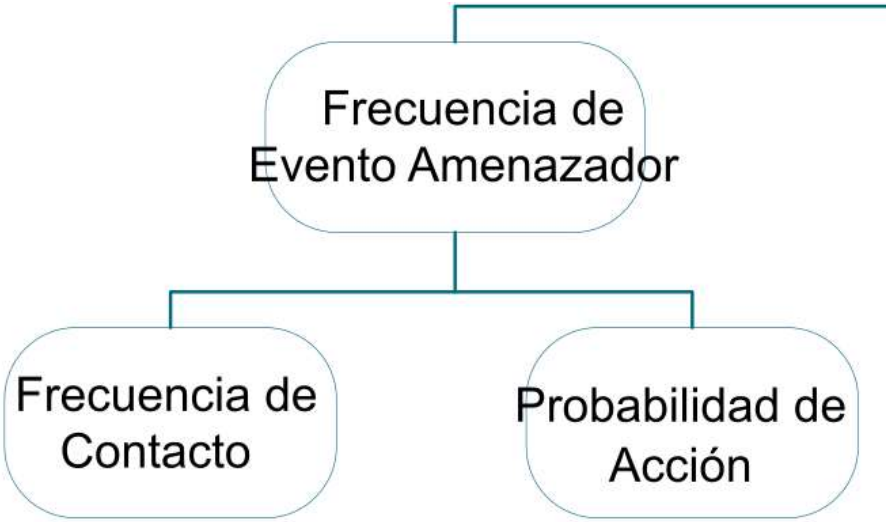


Figura 4: TEF:CF^PoA (OpenGROUP, 2021)

La frecuencia de un Evento Amenazador (TEF) es la frecuencia probabilística, dentro de una ventana de tiempo, con la que el Agente Amenazador actuará en contra de un Activo.

La única diferencia entre esto y la definición de LEF es que la definición de TEF no indica si las acciones del Agente Amenazador han sido exitosas. Dicho de otro modo, los Agentes Amenazadores pueden actuar contra Activos, pero no conseguir dañar parcial o totalmente el Activo. Un ejemplo, muy usado de Evento Amenazador malicioso (que pretende hacer daño) sería un ataque infructuoso de un cracker a un servidor web. Tal ataque puede ser considerado Evento Amenazador, pero no un Evento con Pérdida. Un ejemplo de una Evento Amenazador no-malicioso sería un técnico de CPD tropezando con un cable de corriente. El acto de tropezar se convertiría en Evento con Perdida sólo si el cable se desconecta, o el técnico se hace daño.

Dicho esto, hay que enunciar dos subcomponentes de TEF, que son Frecuencia de Contacto (CF) y Probabilidad de Acción (PoA).

2.1.2.2.1. Frecuencia de Contacto (CF)

La frecuencia de Contacto (CF) es la frecuencia probabilística, dentro de una ventana de tiempo, con la que el Agente Amenazador entra en contacto con un Activo. El hecho de que un Agente Amenazador entre en contacto con un Activo, pasará a llamarse Evento de Contacto. El contacto puede ser físico o lógico (p.e, a través de una red). Independientemente del modo de contacto, tres tipos de contacto pueden producirse:

1. Aleatorio: el Agente Amenazador se topa de manera fortuita con el Activo en el transcurso de actividades que no tienen objetivo en particular. (en algunas metodologías, es también conocido como etapa de reconocimiento)
2. Periódico: el contacto ocurre debido a las acciones periódicas del Agente Amenazador; por ejemplo, si un equipo de limpieza de oficinas suele llegar todos los días a las 17:15

de la tarde, dejar dinero encima de un escritorio y a esta misma hora, establece las condiciones necesarias para un contacto.

3. Intencionado: el Agente Amenazador está buscando unos objetivos muy concretos.

Cada uno de estos tipos de contacto es influido a su vez por otros factores. Una analogía aproximada para describir dicha dinámica sería una Pista de Coches de Choque, en la que el contacto entre los coches obedece a varios factores, entre otros:

1. Tamaño de la Pista
2. Superficie de cada coche prevista para chocar
3. El número de coches
4. Cuán de excitados están los conductores
5. La velocidad y aceleración de los coches
6. La intencionalidad de los conductores, p.e. cuáles son sus preferencias a la hora de chocar: con amigos, enemigos, desconocidos, etc.

2.1.2.2.2. Probabilidad de Acción (PoA)

La probabilidad de Acción es la probabilidad de que un Agente Amenazador actúe contra el Activo, una vez producido el contacto.

Porque, a pesar de que se produzca el contacto, el Agente Amenazador puede o no, actuar en contra del Activo. Para algunos Agentes Amenazadores, la acción siempre toma lugar. Por ejemplo, si una piedra es tirada contra una ventana de una casa residencial, está casi siempre se romperá, ya que la acción implica unas consecuencias inevitables. Sí cabe preguntarse si la acción se realizará o no, en el caso de Agentes Amenazadores pensantes, tales como p.e. humanos u otros animales, o Agentes Amenazadores basados en tecnologías con cierta "inteligencia" programada, tales como programas maliciosos. (que son la extensión de sus creadores u operadores humanos).

La probabilidad de que una acción intencionada tome lugar, en otras palabras, si un Agente Amenazador entrará intencionadamente en contacto con un Activo es influida por tres factores principales:

1. Valor: el valor del Activo que percibe l Agente Amenazador
2. Grado de Esfuerzo: El esfuerzo que el Actor Amenazador prevé que realizará para realizar la acción
3. Riesgo de detección/captura: la probabilidad de que deriven efectos negativos para el Agente Amenazador; por ejemplo, la probabilidad de que el Agente Amenazador sea capturado o de que sufra consecuencias inaceptables, como fruto de su actuación maliciosa

2.1.2.3. Vulnerabilidad (Vuln)

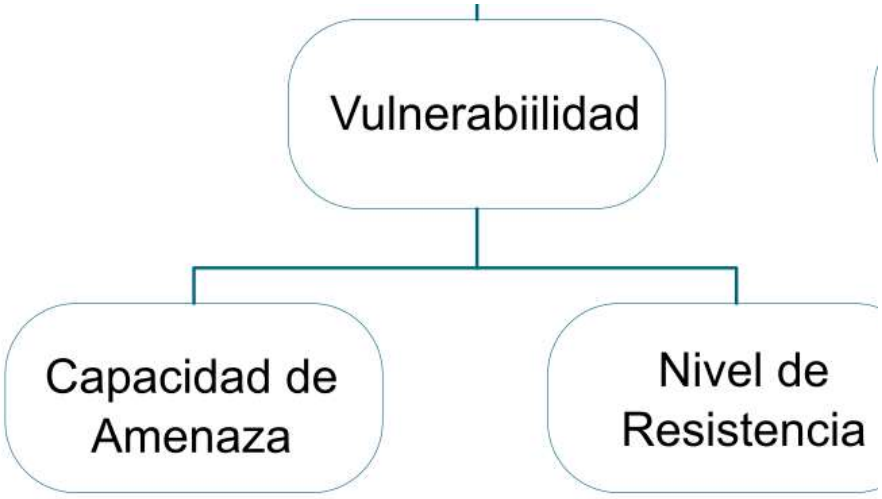


Figura 5: Vuln: TCap ^ RS (OpenGROUP, 2021)

Vulnerabilidad (Vuln), también llamada susceptibilidad, es la probabilidad de que un Evento Amenazador se convierta en un Evento con Perdida. En términos estrictos, Vulnerabilidad es la probabilidad de un Evento con Pérdida, condicionada por la presencia de un Evento Amenazador. Dicho de otra forma, la probabilidad de que, en un Escenario con Perdida, habiendo el Agente Amenazador ejercido fuerza, la Capacidad de Amenaza (TCap) contra el Activo, exceda el Nivel de Resistencia (RS) de los Controles que protegen dicho Activo.

Esto significa que hay por lo menos dos maneras de estimar la Vulnerabilidad, y cada una obtiene el mismo resultado:

Si los datos de Frecuencia de Evento Amenazador y Frecuencia de Evento con Perdida están disponibles o estimados de manera directa, la Vulnerabilidad es estimada como el subconjunto de Eventos Amenazadores que se convierten en Eventos con Perdida

La vulnerabilidad también puede deducirse del valor (estimado o no) de la Capacidad de Amenaza (TCap) y el Nivel de Resistencia del Activo (RS) a dicha Capacidad de Amenaza (TCap) y posteriormente estimar o simular la probabilidad de que la Capacidad de Amenaza (TCap) supere el Nivel de Resistencia del Activo (RS).

La Vulnerabilidad siempre depende del tipo de fuerza y vector de ataque que se utiliza: la Vulnerabilidad de un Activo de Información depende del Escenario con Pérdida que está siendo analizado. A modo de analogía: la resistencia a la tensión mecánica de un cable de acero de un, es relevante, p.e., en caso en que hay un peso colgando de él: dicho peso es la Fuerza del Agente Amenazador. Sin embargo, dicha resistencia no es relevante en un escenario en el que el Agente Amenazador es fuego, erosión, etc. Los analistas de riesgo

evalúan una Vulnerabilidad en el contexto de una amenaza específica a la que se enfrentan el Activo y los Controles que protegen dicho Activo.

Ya que Vulnerabilidad es una probabilidad, un Activo no puede ser vulnerable de más de 100% a cada combinación especifica de Agente Amenazador y vector de amenaza. Se puede dar una Vulnerabilidad que expone el Activo a sufrir daños de múltiples combinaciones de Agentes Amenazadores y vectores de amenaza, representando cada una un posible Evento Amenazador distingo. En palabras simples: un excursionista que pasea por el campo en día de lluvia está expuesto a varios Eventos Amenazadores: ser partido por un rayo, torcerse el tobillo con una raíz, etc. La probabilidad de materialización de cualquiera de estos Eventos Amenazadores siempre es un porcentaje menor o igual que 100%, pero el riesgo de pérdida agregado siempre es mayor debido a los múltiples Escenarios con Perdida que se pueden producir.

2.1.2.3.1. Capacidad de Amenaza (TCap)

Una Capacidad de Amenaza (TCap) es el probable nivel de fuerza (expresada en tiempo, recursos y capacidad tecnológica) que un Agente Amenazador es capaz de aplicar en contra de un Activo. Los atacantes **varían** en habilidades, recursos, habiendo en un extremo atacantes poco habilidosos y motivados, mientras que en el extremo están los atacantes altamente capaces, organizados, experimentados y motivados. El rango de Capacidad de Amenaza clasifica los atacantes en varios percentiles, donde el percentil 25avo de Agentes Amenazadores son menos habilidosos y capaces que el **percentil** 50avo que a su vez son menos habilidosos y capaces que los del percentil 99º de Agentes **Amenazadores**.

Los Agentes Amenazadores que pertenecen a una Comunidad Amenazadora no tiene por qué tener las mismas capacidades. Por lo tanto, la probabilidad de que el Agente Amenazador "más capacitado" actúe en contra de un **Activo** no es precisamente 100%. Dependiendo de la Comunidad Amenazadora analizada, y otras condiciones del **escenario**, la probabilidad de encontrar un Agente Amenazador puede ser pequeña. A menudo a los profesionales de seguridad de información y analistas de riesgo, les cuesta asumir de que la capacidad de un Agente Amenazador pueda ser expresada como un percentil de una Comunidad Amenazadora, cuya distribución hace, a menudo, improbable de que sea el Agente Amenazador más capaz el que ataque. Muchos analistas y gestores, en su lugar, tienden a pensar en el peor caso posible, pero dicho enfoque lleva, erróneamente, a centrarse directamente en Posibilidad (posible/imposible) que en Probabilidad Estadística. Algunos Agentes Amenazadores pueden ser competentes en aplicar ciertos tipos de fuerza, pero ineficaces en aplicar otra. Por ejemplo, un ingeniero de redes puede ser bueno en realizar ataques tecnológicos, pero incapaz de realizar fraude contable complejo.

2.1.2.3.2. Nivel de Resistencia (RS)

Nivel de Resistencia (RS) es la fortaleza de un Control enfrentado al probable nivel de fuerza (expresada en tiempo, recursos y capacidad tecnológica; organizados como un percentil) que un Agente Amenazador es capaz de aplicar en contra de un Activo. Tal como se ha visto en la definición, de TCap, los atacantes varían en habilidades y recursos, y el Nivel de Resistencia mide la fortaleza de un Control respecto de un percentil de atacantes, más precisamente a qué percentiles de atacantes se espera que el Control pueda resistir. Como analogía, un cable de acero de un ascensor está certificado para aguantar esfuerzos desde 0 a 750N/m2, I.e. la unidad de medida de Nivel de Resistencia para un cable de acero es el N/m2. Separemos un intervalo 1000 N/m2 en cuatro percentiles. Eso significa que el cable de acero está certificado para resistir a esfuerzos que incluyen 1º,2 y 3º percentil de dicho intervalo, pero no del 4º (que es mayor que 750N/m2). Los protocolos de seguridad de la información, sin embargo, no tienen una unidad bien definida como el N/m2. Aun así, hay excepciones: p.e en el caso de las contraseñas, la entropía (o tiempo que se tarda en adivinarla por fuerza bruta) se calcula a partir de varios factores, entre ellos longitud, complejidad, etc. Por lo tanto, el Nivel de Resistencia de una contraseña sí puede repartirse en Percentiles. (recordemos que el Nivel de Resistencia depende del tipo de fuerza aplicada; en este caso cracking). Vulnerabilidad (Vuln) se estima comparando RS contra la capacidad de una Comunidad Amenazadora especifica analizada y extrayendo la probabilidad de que la Capacidad de Amenaza (TCap) supere el Nivel de Resistencia (RS).

2.1.2.4. Tabla Resumen de subcomponentes LEF

En resumen, la Frecuencia de Eventos con Pérdida (LEF) es el número probable, expresado como una distribución, de Eventos con Pérdida dentro de un periodo dado. LEF está compuesto por varios subcomponentes que se pueden ver resumidos en la tabla “Resumen LEF”:

Comp. LEF	**Descripción**	**Ud. De Medida**
LEF	Número probable de pérdidas económicas en un periodo dado	• Eventos por unidad de tiempo (eventos por año) • Probabilidad de un único Evento con Pérdida en un periodo dado (20% de probabilidad en el próximo año)

TEF	Número probable de intentos, en periodo dado, de causar pérdidas, por parte de Agentes Amenazadores	• Eventos por unidad de tiempo (eventos por año) • Probabilidad de un único Evento Amenazador en un periodo dado (20% de probabilidad en el próximo año)
Vuln	• Probabilidad de que un Evento Amenazador se convierta en Evento con Perdida • Probabilidad de que Tcap>RS	Probabilidad estadística: entre 0 y 1 o Porcentaje entre 0 y 100%
CF	Número probable de veces en que un Agente Amenazador entra en contacto con un Activo en un periodo de tiempo dado	• Eventos por unidad de tiempo (eventos por año) • Probabilidad de un único Evento de Contacto en un periodo dado (20% de probabilidad en el próximo año)
PoA	Probabilidad de que un Evento de Contacto se convierta en un Evento Amenazador	Probabilidad estadística: entre 0 y 1 o Porcentaje entre 0 y 100%
TCap	La clasificación por posición dentro de una Comunidad Amenazadora de las habilidades de un Agente Amenazador, tiempo, recursos, y tiempo	Percentil Estadístico (0-100)
RS	La habilidad de resistir a una Comunidad Amenazadora, según rangos de habilidades , recursos y tiempo	Percentil Estadístico (0-100)

Tabla 2 : Resumen LEF (OpenGROUP, 2021)

2.1.2.5. Nivel de Pérdida (LM)

La definición de riesgo con la que trabajamos define riesgo como la frecuencia probabilística y nivel de pérdida en el futuro. El apartado anterior introdujo factores que alimentan la probabilidad de que ocurran Eventos con Perdida. Este apartado describe la otra mitad de la ecuación de riesgo: dos factores o subcomponentes que alimentan al Nivel de Pérdida (LM) cuando ocurren eventos. Nivel de Pérdida (LM) es el nivel probable de pérdida económica como consecuencia de un Evento con Pérdida. El Nivel de Pérdida se expresa como una distribución de perdidas, no como un único valor escalar de pérdida, y siempre se evalúa desde la perspectiva del o Interesado o Propietario Principal', que es la parte que soporta la pérdida económica resultante de un Evento con Pérdida. Tradicionalmente, los datos que describen Nivel de Pérdida (LM) siempre han sido escuetos. Muchas organizaciones aún no miden las pérdidas en caso de eventos concretos, y cuando sí se hace, es un análisis bastante sencillo (i.e. persona*mes, coste de nuevo hardware, etc.). Además, la falta de una taxonomía estándar ha hecho difícil de normalizar los datos de manera transversal a varias organizaciones.

Ya que Nivel de Pérdida (LM) puede ser difícil de estimar, los analistas a menudo no lo analizan en absoluto, sino que evalúan sólo los peores casos posibles, escenarios especulativos de caso peor, o modelan las pérdidas con herramientas que son engañosamente precisas. Excluir Nivel de Pérdida (LM) de un análisis significa que el analista no está analizando el riesgo: el riesgo siempre tiene un componente de pérdida. Centrarse en escenarios de 'caso peor' elimina el componente probabilístico del análisis. Las herramientas de modelado de riesgo por computador que presentan los resultados de riesgo con una precisión elevada dan una sensación y peligrosa a los gestores, de que están muy bien informados y preparados. En general la mayoría de las perdidas asociadas con sistema de la información son pequeñas, pero aun así subsiste una remota posibilidad de una pérdida considerable. Dicha topología se puede visualizar mediante una gráfica de 'cola larga':

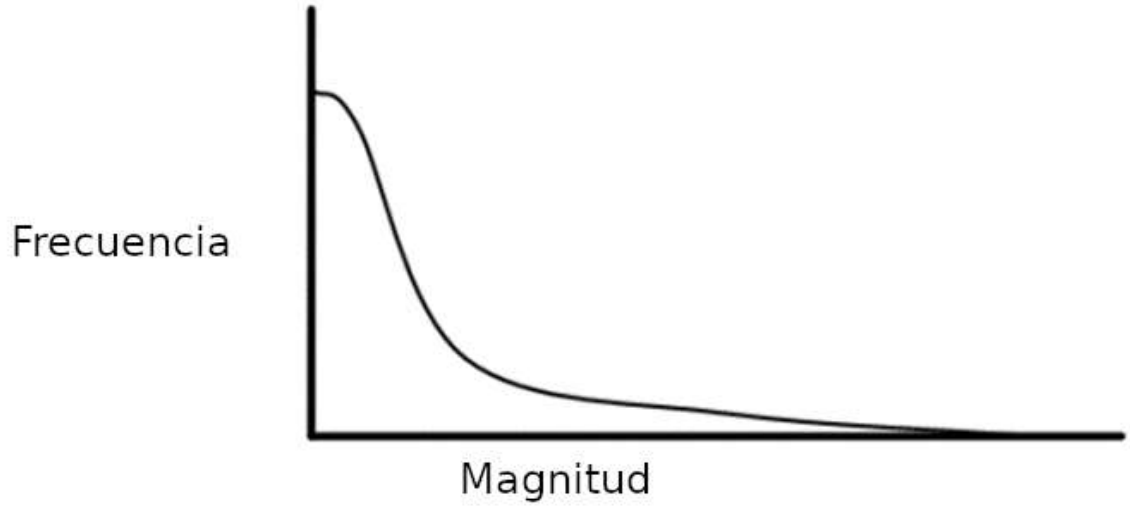


Figura 6: Distribución típica de Nivel de Pérdida (OpenGROUP, 2021)

2.1.2.6. Tipos de Pérdida

El rango de perdida varía su valor según el/los Activos afectados y/o las responsabilidades que conlleva poseer estos Activos para la empresa. Por ejemplo, los datos de potenciales clientes producen valor para una empresa que se dedica a la promoción comercial, pero por otro lado tener dichos datos conlleva responsabilidades en materia de Protección de Datos. De ahí que una degradación de un Activo no sólo puede afectar su valor, sino contravenir compromisos contractuales o legales, lo que puede aumentar aún más las pérdidas económicas.

Definiremos por lo menos seis tipos de pérdida (en varios casos implican gasto económico):

1. Productividad: pérdidas directas asociadas con la reducción en la habilidad de una organización a generar su producto primario de valor (ingresos, bienes, servicios); puede también implicar costes asociados a personal que está “sentado parado sin hacer nada”; toma en cuenta la perdida debido a paradas involuntarias irrecuperables de la cadena de producción/entrega al cliente; también incluye costes asociados con la bajada de productividad de los trabajadores (p.e. por pasar de métodos de producción automáticos a manuales)
    a. Pérdida de Ingresos no es lo mismo que Aplazamiento de Ingreso. P.e. cuando el vendedor de una tienda de barrio cierra con llave a la puerta y pone el cartel de “vuelvo en cinco minutos”, habrá clientes que van a esperar delante, o volverán algo más tarde. Aun así, este tipo de procedimientos, hay que

hacerlos analizar por los gestores de marketing, ya que, si ocurren en rangos de tiempo críticos, puede derivar en una cadena de (ir)responsabilidades.

2. Reacción: gasto directo relacionado con gestionar un Evento con Pérdida(i.e. costes de persona*hora, costes logísticos, costes legales, costes de RRP)
3. Reemplazo: gastos directos asociados a tener que reemplazar un Activo; por regla general gastos para reemplazar un Activo dañado o perdido (i.e. reconstruir un edificio, cambiar un ordenador portátil, reemplazar un empleado despedido, cubrir internamente los costes de un fraude financiero, etc.)
4. Multas y Juicios: gastos directos asociados con procedimientos legales o regulatorios contra la Organización, inclusive contra trabajadores de dicha Organización
5. Ventaja Competitiva: pérdida estimada asociada con una posición menos competitiva, sobre todo cuando hay degradación de Activos que proporcionan diferenciación competitiva (p.e. costes menores de producción, calidad más alta, capacidades avanzadas) frente a la competencia, secretos de negocio, secretos militares, etc.
6. Reputación: perdidas futuras estimadas, relacionada con actores externos que percibirán que el valor de la organización ha disminuido o que podría traer problemas a dicho actor externo. A menudo se materializa en pérdida de cuota de mercado, caída del precio de la acción bursátil, disminución de propuestas para inclusión en Consorcios, etc.

2.1.2.7. Flujo de Pérdida

a Al inicio de un Evento con Pérdida se aprecian por lo menos dos etapas en la pérdida desde el punto de vista de Nivel de Pérdida (LM): Pérdida Primaria y Pérdida Secundaria. El flujo de pérdida es una descomposición estructural de cómo las pérdidas se materializan cuando ocurre un Evento con Pérdida. Un flujo de pérdida se compone como mínimo de los siguientes pasos:

1. Un Agente Amenazador actúa en contra de un Activo (Evento Amenazador)
2. Este Evento Amenazador afecta directamente al Propietario/Interesado Primario en términos de pérdida de productividad, costes de reacción, etc. Esto es llamado Evento con Pérdida Primaria
3. A veces, este Evento con Pérdida Primaria, también afecta directamente Propietarios/Interesados secundarios, tales como clientes, legisladores/reguladores, medios de comunicación, quienes pueden reaccionar contra el Propietario/Interesado Primario.
4. Cuando Propietarios/Interesados Secundarios reaccionan en contra del Propietario/Interesado Primario, estos primeros actúan como como si fuesen Agentes

Amenazadores en contra de ciertos tipos de activos de la organización (tales como reputación, costes legales, etc.), que a su vez afecta al Propietario/Interesado Primario.

A modo de ejemplo, si un Procesador de Pagos (Propietario/Interesado Primario) sufre un incidente de seguridad de la información, debe reaccionar y recuperarse de dicho incidente. Los costes generados durante la recuperación del incidente son Pérdidas Primaria. Sin embargo, clientes que hayan sufrido fraude de tarjetas de crédito en contra de ellos, sufren, en consecuencia, también daño indirecto. Cuando dichos clientes (Propietarios/Interesados Secundarios) piden compensaciones al Procesador del pago, estos clientes se convierten en Agentes Amenazadores que intentan causar daño al Procesador de Pagos, por regla general "atacando" los Activos Financieros del Procesador de Pagos mediante demandas judiciales. En este caso, el Procesador de pagos puede instanciar recursos para proveer monitorización adicional a los movimientos crediticios de sus clientes, a fin de de mitigar este tipo de Pérdidas Secundarias. En resumen, este es un ejemplo de Pérdida Primaria (Reacción y Recuperación del Incidente) seguido, en el tiempo, por una Pérdida Secundaria (gastos por monitorización adicional, y multa judicial).

2.1.2.8. Pérdida Primaria

La primera fase de un Evento con Pérdida, también llamada Pérdida Primaria, ocurre como resultado directo de las acciones del Agente Amenazador sobre el Activo. En la presente metodología de análisis, el propietario de los Activos Afectados es considerado Propietario/Interesado Primerio. De los seis tipos de pérdida descritos en la sección previa, Productividad, Reacción y Reemplazo se producen habitualmente como Pérdida Primaria. Los otros tres tipos de pérdida sólo se producen como Pérdida Primaria cuando el Agente Amenazador es directamente responsable por dichas pérdidas (i.e., multas y pérdida en juicio cuando el Agente Amenazador es el demandante)

2.1.2.9. Pérdida Secundaria

La segunda fase de un Evento con Pérdida, llamada Pérdida Secundaria, se produce como resultado de que los Propietarios/Interesados Secundarios (i.e. clientes, accionistas, reguladores y legisladores) reaccionen de manera negativa a una Perdida Primaria. En palabras sencillas, las Pérdidas Secundarias suelen ser las repercusiones de las Pérdidas Primaria. Un ejemplo sería que los clientes "se lleven su negocio a otra parte" después de que su información personal se haya visto filtrada o p.e. si ha habido cortes frecuentes en el servicio.

La Pérdida Secundaria tiene dos componentes primarios: Frecuencia de Perdida Secundaria (SLEF) y Nivel de Pérdida Secundaria (SLM).

La Frecuencia de Pérdida Secundaria permite a los analistas estimar la probabilidad (% de veces) cuando un escenario es propenso a acarrear efectos secundarios. Aun cuando dicha variable es llamada “frecuencia”, se estima como porcentaje, ya que representa la probabilidad condicional de que una Pérdida Primaria derive en Pérdida Secundaria. El Nivel de Pérdida Secundaria representa las pérdidas que se espera que se materialicen al lidiar con las reacciones de Propietarios/Interesados (i.e. multas y demandas, pérdida de cuota de mercado). De entre los seis tipos de pérdida, Respuesta, Multas y Demandas, Ventaja Competitiva y Reputación son normalmente asociados con Pérdida Secundaria. En el caso de Pérdida de Ventaja Competitiva resultante del robo de una Secreto de Negocio, mientras que el secreto se da por perdido al instante mismo, el impacto de la pérdida se alarga durante un largo periodo de tiempo, e incluso puede no producirse en absoluto. El efecto de la Pérdida Secundaria puede causar un ‘Efecto Cascada’ dentro de una organización. A medida que las pérdidas se acaban produciendo como efecto de la Pérdida Secundaria, Propietarios/Interesados Secundarios pueden reaccionar negativamente, amplificando el efecto hasta que las pérdidas hasta tal punto de que la organización colapsa. (a modo de ejemplo, el “Caso Enron” en 2002)

Factores de Pérdida

Figura 7: Factores de Pérdida (OpenGROUP, 2021)

Los Factores de Pérdida son atributos o propiedades de del Activo, Amenaza, Organización o Entorno que afectan el nivel de pérdida, en un Evento con Pérdida que concierne a un Propietario/Interesado Primario.

Los Factores de Pérdida pueden influir tanto en una Pérdida Primaria como en una Secundaria, por lo que el analista de riesgo debe evaluar factores en cada una de las cuatro categorías. Sin embargo, los factores de pérdida, en Activo y Amenaza, son clasificados como Factores de Pérdida Primaria, mientras que los factores de pérdida de tipo organización y externos son clasificados como Factores de Pérdida Secundaria.

2.1.2.9.1. Factores de Pérdida en Activos

Los Factores de Pérdida en un Activo son, como mínimo, valor/problemas y volumen. Las características de valor/problemas de un Activo juegan un papel clave tanto en la naturaleza como en el nivel de la pérdida. La escala de volumen de un Activo simplemente significa que el riesgo cubre más o menos unidades de un Activo y esto causa más Nivel de Pérdida en caso de Evento con Pérdida (p.e. no es lo mismo que se confisque un camión con 20kg de patatas que uno con 20000kg). Valor/problemas se puede descomponer en componentes más concretos:

1. Criticidad: las características de un Activo relacionadas con el impacto en la productividad de la Organización; p.e. una caída de cierta BBDD puede impactar directamente en los ingresos financieros.
2. Coste: el valor intrínseco del Activo; i.e. el gasto asociado con reemplazarlo si ha quedado indisponible (p.e. robado o destruido);
3. Sensibilidad/daño de la información: el daño producido en caso de una filtración involuntaria de información clasificada. La sensibilidad/daños se puede clasificar a su vez en cuatro subcategorías:
    a. Reputacional: la información expone pruebas de una gestión incompetente, criminal o inmoral, y refiere a daño reputacional causado por la naturaleza de la información en sí (no confundir con el daño reputacional causado cuando por la sola aparición de un Evento con Pérdida)
    b. Ventaja Competitiva: la información proporciona ventaja competitiva (i.e. estrategias clave, secretos de negocio) y, de entre las categorías de Sensibilidad/Daño expresa un valor concreto; en todos los demás, la Sensibilidad/Daño expresa problemas/responsabilidades.
    c. Legal/Regulatoria: la organización está obligada/atada por leyes y/o contratos, a proteger la información
    d. General: la información sensible/confidencial que no encaja en ninguna de las categorías anteriores, pero que produciría algún tipo de pérdida si es revelada públicamente.

2.1.2.9.2. Factores de Perdida en Amenaza

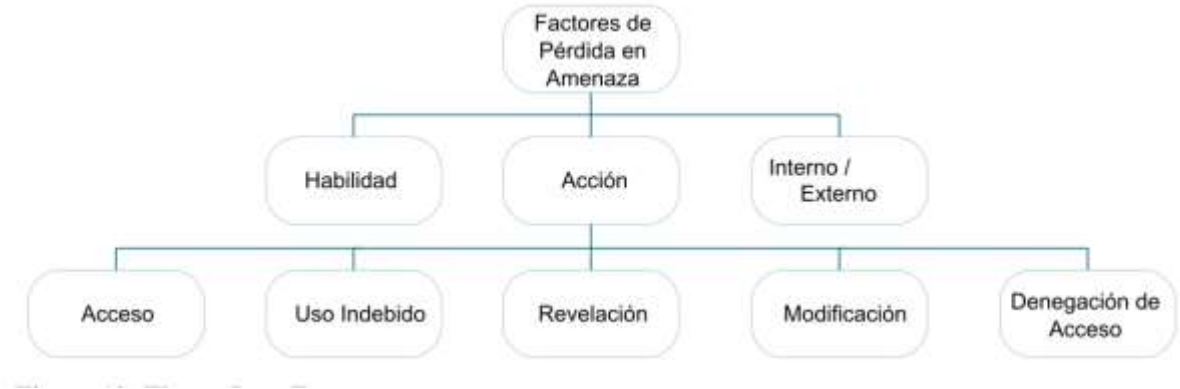


Figura 8: Factores de Pérdida en Amenaza (OpenGROUP, 2021)

Los factores de pérdida en amenaza son, entre otros: actuación, habilidad, y si es el Agente Amenazador es interno o externo de la organización, y cómo el uso por parte del Agente Amenazador de la información comprometida afecta la pérdida sufrida por el Propietario/Interesado Primario. Los Agentes Amenazadores pueden realizar una o múltiples de las siguientes actuaciones contra un Activo:

Acceso: Acceso no autorizado a Activos
Uso indebido: uso no autorizado de los Activos
Revelación: revelación ilícita de información sensible/confidencial
Modificación: cambios no autorizados a los Activos
Denegación de Acceso: impedimento o denegación de accesos autorizados

NB: Cualquiera de estas acciones puede haber tenido éxito en realizar una violación de confidencialidad, integridad o disponibilidad en contra de un Activo del Propietario/Interesado, tal como se puede ver en la siguiente tabla:

Dimensión de la Activo afectada (Brecha)	Explotación Post-Brecha por parte del Agente Amenazador
Confidencialidad	• Acceso: el Agente Amenazador obtiene acceso no autorizado, pero realiza actuaciones adicionales, más allá de 'conservar los datos obtenidos' • Uso Malicioso: el Agente Amenazador realiza un uso no autorizado del Activo y causa a su vez pérdidas tanto al Propietario/Interesado Primario como al Secundario. P.e. realizar robo de identidad, o usar un servidor afectado como almacén para ficheros ilegales. • Filtración: el Agente Amenazador entrega información confidencial/sensible a terceras partes no autorizados
Integridad	Modificación: El Agente Amenazador crea o modifica información que afecta a la credibilidad o exactitud de la información o procesos de tratamiento de información.
Disponibilidad	Denegación de Acceso: El Agente Amenazador previene o impide activamente el acceso autorizado al Activo. Esto incluye borrado de información, apagado de sistemas y eventos de tipo ransomware.

Tabla 3: Acciones del Agente Amenazador tras una Violación de la Seguridad Exitosa (OpenGROUP, 2021)

Al obtener acceso no autorizado a un Activo de Información, los Agentes Amenazadores pueden conseguir persistencia en dicho Activo, para usarla más tarde con fines maliciosos. Si no es detectada, dicha persistencia no es aún una pérdida para el Propietario/Interesado Primario. En cuánto sea detectada, la pérdida será en confidencialidad, integridad o disponibilidad junto con las consecuencias/problemas que acarreen dicha(s) pérdida(s). Los Agentes Amenazadores pueden conseguir persistencia como parte una estrategia a largo plazo a fin de cumplir su misión asignada, p.e. con fines de infiltración y/o inteligencia.

Cada de estas acciones afectan los Activos de manera diferente, lo que diversifica el nivel y la naturaleza de su pérdida. La combinación del Activo, tipo de violación, y tipo de aprovechamiento de dicha violación determinan la naturaleza fundamental y nivel de perdida. Por ejemplo, la potencial pérdida productividad resultante de un Activo perdido o robado, depende de cuán critico es dicho Activo para la Productividad de la Organización. Si un Activo

critico es accedido en modo lectura de manera ilícita, no hay pérdida directa de productividad. De manera parecida, la destrucción de un Activo altamente confidencial/sensible, que por su naturaleza no influye en la productividad, tampoco resultará en una pérdida directa de productividad. Ahora bien, si este mismo Activo es filtrado al exterior, se puede producir una pérdida significante de ventaja competitiva o reputacional, y generar costes legales. Los pasos y actuaciones, que realice un Agente Amenazador, son normalmente guiados por las intenciones del atacante (p.e. motivos financieros, venganza, lúdicos, etc.) y la naturaleza del Activo. [...] Sin embargo, la clasificación no es en blanco y negro, sino en matices de gris. P.e. un ataque de Ransomware puede tener motivaciones económicas, pero ser altamente destructivo aun si la victima paga el rescate[...] Por esta razón, el Analista de Riesgo debe tener una visión clara de la Comunidad Amenazadora y sus intenciones.

La Habilidad es una medida de cuán capaz es el Agente Amenazador en explotar el Activo Comprometido a fin de conseguir alguno de sus fines. Es la cantidad de daño que un Agente Amenazador es capaz de infligir una vez que se compromete un Activo de Información asociado a un Propietario/Interesado Primario o Secundario. Como ejemplo, un Agente Amenazador con baja habilidad no puede causar daños extensos a pesar de tener suficiente Capacidad Amenazadora para superar los Controles sobre el Activo.

NB: La habilidad de amenaza difiere de Capacidad de Amenaza: la Capacidad de Amenaza influye Nivel de Pérdida mientras que Habilidad de Amenaza influye a la Frecuencia de Evento con Perdida.

Que el Agente Amenazador sea externo o interno de la organización, puede hacer toda la diferencia del mundo, respecto de cuánta pérdida se produce. Más específicamente, los Eventos con Pérdida generados por Agentes Amenazadores internos (empleados, subcontratados, etc.) normalmente no han derivado en pérdidas regulatorias o de reputación, ya que se considera de que a los Agentes Internos se les debe conceder cierto nivel de confianza para que la Organización pueda funcionar, por lo que es difícil protegerse contra Agentes Internos.

2.1.2.9.3. Factores Organizacionales de Pérdida

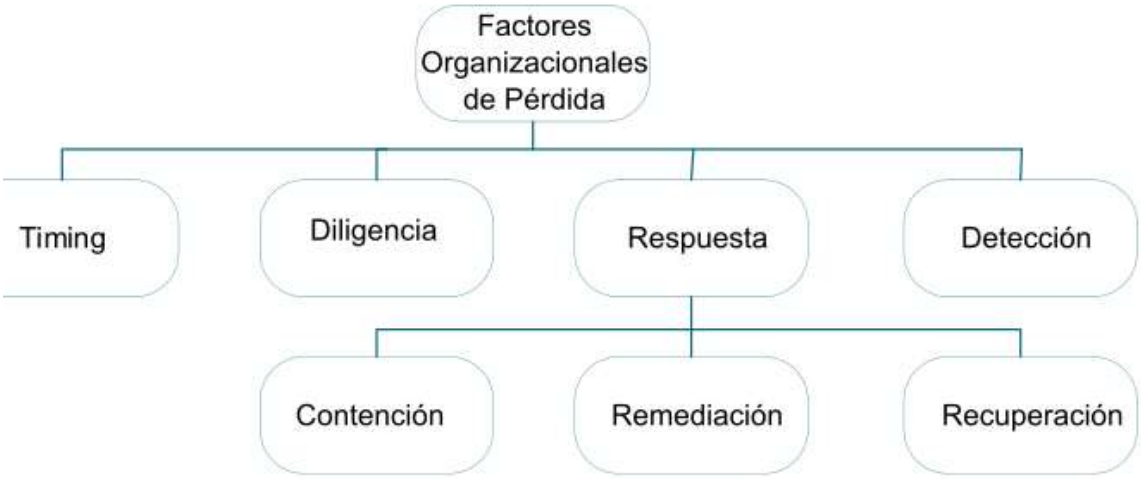


Figura 9: Factores de Pérdida Organizacionales (OpenGROUP, 2021)

Los factores organizaciones de pérdida son aquellos característicos de la organización o del negocio que sufre la pérdida. Son: (cuando) el Evento con Pérdida ocurrió, (si) la organización había tomado suficientes medidas para proteger el Activo de Información dañado, y (cómo) detectó la Organización dicho Evento con Pérdida. Cuando un Evento con Pérdida ocurre, su cronología puede impactar significativamente en el Nivel de Pérdida. Por ejemplo, la filtración de las cuentas de una compañía antes de su publicación, o la filtración de un acuerdo de compra, antes de que sea públicamente anunciado.

Una falta de diligencia de una organización al proteger los Activos puede causar problemas y consecuencias legales en caso de un Evento. El hecho de que se hayan implementado medidas preventivas (según entorno de amenazas, valor del Activo, y requisitos legales y regulatorios), puede influir positiva o negativamente en la severidad de los daños reputacionales o consecuencias de procesos legales.

La manera en que una organización reacciona ante un evento puede marcar la diferencia entre que este Evento sea recordado por el público de manera positiva o negativa. Una reacción tiene por lo menos tres componentes:

1. Contención: la capacidad de la organización de limitar la extensión y profundidad de un Evento. A modo de ejemplo, que la red local de la organización tenga una red segmentada, defensa en profundidad, etc.
2. Remediación: la capacidad de una organización de suprimir el Agente Amenazador (p.e. limpiar un gusano de la red local)
3. Recuperación: la capacidad de devolver los procesos a su funcionamiento normal

Todos estos tres aspectos deben existir, ya que, si cualquiera de ellos tuviese deficiencias, estas influirían de manera significativa en el Nivel de Pérdida.

Las capacidades de Reacción son normalmente analizadas sólo desde el punto de vista de criticidad; Sin embargo, dichas capacidades pueden también influir en pérdidas por filtración de información confidencial/sensible. A modo de ejemplo, una organización que sufre un filtrado de información confidencial de cliente puede reducir sus pérdidas siendo transparente en el proceso de apertura de incidente y colaborando con las autoridades y el cliente. Ahora bien, una organización que niega lo ocurrido, suele sufrir una pérdida reputacional muy considerable

La organización debe detectar el Evento con Pérdida a fin de que pueda reaccionar y mitigarlo. Incidentes pueden pasar desapercibidos por un periodo largo de tiempo. Sin embargo, para que dicho evento derive en pérdida material, debe ser detectado previamente. Por ejemplo, muchas filtraciones y robos de información por espionaje industrial pueden pasar años sin ser detectado. Pero cuando el competidor saca un producto sospechosamente parecido al de la organización afectada, es cuando el evento es detectado y cuando se oficializa.

NB: “Eventos de Pérdida No Detectados” tales como APT (advanced persistent threats) o situaciones donde el Agente Amenazador consigue persistencia, son en su nacimiento Eventos de Amenaza. Es cuando son detectados, cuando se convierten en Eventos con Pérdida.

2.1.2.9.4. Factores externos de pérdida

Figura 10: Factores externos de Pérdida (OpenGROUP, 2021)

Factores de Pérdida Externos se clasifican, entre otros en: detección por parte de actores externos, legal y regulatorio, competencia, medios de comunicación y Propietarios/Interesados Secundarios (p.e. clientes, socios, accionistas, etc.).

Estas cinco categorías tipifican entidades que pueden causar Pérdidas Secundarias a la organización, como consecuencia de un Evento. En otras palabras, los Eventos, a menudo, resultarán en formas directas de pérdida (i.e. de productividad, de reacción, reemplazos) debido a la criticidad y valor inherente de los Activos afectados. Las Pérdidas Secundarias

pueden también producirse, y debido a reacciones externas al Evento con Pérdida (p.e. filtración al público de información confidencial). Asimismo, todos los factores dentro de estas categorías externas pueden describirse como “reacciones a un evento”. Dicho de otra forma, para que un factor externo afecte al Nivel de Pérdida (LM), el actor externo debe primer detectar dicho evento. Por ejemplo, si un empleado utiliza de manera indebida su acceso licito a información de un cliente, a fin de realizar un robo de identidad, el cliente, reguladores y abogados no pueden realizar daño a la organización al menos que el robo de identidad sea asociado a la organización. De manera similar, si una interrupción en la productividad no es detectada por clientes, socios, etc., entonces la organización no se verá sujeta a reacciones negativas por parte de estos actores.

La detección por parte actores externos puede modelizarse como un factor binario que (in)habilita todos los demás factores externos. La detección de un evento por parte de un actor externo puede ocurrir como consecuencia de la severidad del evento, a través de actuaciones intencionadas del Agente Amenazador, a través divulgación no autorizada de un actor interno de la organización conocedor del evento, a través de divulgación intencionada por parte de la organización (por imperativo ético o legal), o por accidente. El marco legal y regulatorio muy posiblemente afecte en mayor o menor medida de que el Propietario/Interesado Primario sufra riesgo de multas, condenas y otras sanciones asociadas a Pérdida Primaria. Los Propietarios/Interesados Primarios pueden ser previsores, buscar asesoramiento legal y actuar para mitigar dicho riesgo, invirtiendo en Cumplimiento Regulatorio y Legal.

Las pérdidas asociadas al marco competitivo normalmente tienen que ver con la habilidad y voluntad de la competencia a aprovechar la pérdida de control sobre Información Clasificada/Sensible por parte del Propietario/Interesado Primario.

La respuesta de los medios de comunicación puede tener efectos significantes sobre cómo actores, abogados, e incluso reguladores y competidores ven el Evento. Si los medios de comunicación eligen afear la Organización y p.e. mantener su nombre en las portadas de los periódicos por un periodo largo, los daños puedes multiplicarse. Al opuesto, si los medios de comunicaciones presentan la Organización como bienintencionada y diligente y que ha sido víctima de actores criminales, entonces el legal y reputacional pueden verse minimizado. Es por eso por lo que las organizaciones deben tener un proceso eficaz de comunicación para gestionar crisis de este tipo.

2.1.2.10. Tabla Resumen de subcomponentes LM

El Nivel de Pérdida es, en esencia, la pérdida económica que sufre, por un Evento con Pérdida, el Propietario/Interesado Primario, medida en dinero o en unidades de algún bien

material. Estos eventos se componen de un impacto directo, llamado Pérdida Primaria, y un posible impacto secundario llamado Perdida Secundaria, que aparece como reacción a la Pérdida Primaria, por parte de los Propietarios/Interesados Secundarios que se convierten en Agentes Amenazadores. Las pérdidas se presentan en seis formas: productividad, reacción, reemplazo, multas y sentencias, ventaja competitiva y reputación. Las pérdidas pueden verse multiplicadas o atenuadas por factores de pérdida, que representan como atributos del Activo, de la Amenaza, de la Organización o del Ambiente Externo, afectan las pérdidas una vez empiezan estas a producirse.

Factor de Nivel de Pérdida	Descripción	Unidad de Medida
Nivel de Pérdida Total	La suma de Niveles de Pérdida Primaria y Secundaria	Dinero, Divisas, Uds. de Bienes
Nivel de Pérdida Primaria	Pérdidas económicas directas relacionadas con la confidencialidad	Dinero, Divisas, Uds. de Bienes
Nivel de Pérdida Secundaria	Pérdidas indirectas condicionales, relacionadas con Propietarios/Interesados Secundarios que se han convertido en Agentes Amenazadores que intentan causar pérdidas al Propietario/Interesado Primario	Dinero, Divisas, Uds. de Bienes
Frecuencia de Evento con Pérdida Secundaria	Probabilidad condicional de que una Pérdida Primaria derive en una Pérdida Secundaria	Probabilidad estadística: entre 0 y 1 o Porcentaje entre 0 y 100%
Tipos de Pérdida	Seis tipos de pérdida que engloban pérdidas posibles, sean primarias o secundarias: de productividad, de reacción, por multas y condenas, de ventaja competitiva, y de reputación	Dinero, Divisas, Uds. de Bienes
Factores de Pérdida	Cuatro factores de pérdida que influyen el nivel de pérdida: de Activo, de Amenaza, Organizacionales, Externos	Escalares: variables y coeficientes

Tabla 4: Factores LM

2.2. Principios operativos y consideraciones operacionales de operaciones OTAN (extracto de Doctrina AJP-03)

2.2. Descripción

(NATO, 2019) Unas infraestructuras de TI, pueden servir a muchos fines. En lo que concierne este documento, habilitan la presencia en el quinto dominio de batalla, que es el Ciberespacio. Dicho eso, conviene señalar unos principios operativos, y consideraciones operacionales contenidos en la doctrina de la OTAN, que facilitan abordar problemas complejos y dinámicos. Dichos principios y consideraciones están armonizados en mayor o menor medida con las doctrinas respectivas de los ejércitos de países miembros de la OTAN, como es el caso de España. (BOE , España, 2020)

La doctrina AJP-03 está estrechamente enlazada con FM3-12, JP3-12, JP3-13.4, que son doctrinas que viven total o parcialmente en el plano cibernético. Por lo que es esencial repasar los principios de AJP-03 que son aplicables en el ciberespacio.

2.2. Unidad de Esfuerzo

La unidad de esfuerzo es un requisito que viene a pedir que todos los medios están orientados a un objetivo final. Conseguir una unidad de esfuerzo es a menudo complicado por la variedad de actores militares y no militares nacionales e internaciones implicados, por la falta de acuerdos C2 (mando y control) entre ellos, y por distintas visiones y definiciones de los objetivos de la operación según qué Estado miembro. La consecución de una armonización del esfuerzo es posible, partiendo desde una buena voluntad, planificación conjunta, acuerdos de repartición de responsabilidades, una comprensión de las capacidades y limitación de los demás miembros, y respecto por la autonomía de los otros miembros. En ausencia de un mecanismo unificador multi-agencia, el jefe de mando, con el apoyo de un equipo, puede asumir un rol de coordinación, tratando de alinear perspectivas y prioridades, a priori, divergentes. Para conseguir unidad de esfuerzo, es esencial planificar, comunicar y coordinar a todos los niveles, y con todos los actores implicados, de una manera integrada. En algunos casos, fuerzas de la OTAN pueden operar en apoyo a otras Organizaciones Internacionales (IO), previa firma de términos de acuerdo y técnicos o de un memorando de referencia. Algunas IO pueden u ONG pueden negarse a colaborar directamente con fuerzas militares. Esto requerirá un enfoque flexible hacia la creación de procesos o cuerpos para compartir NATO información con las IO y ONG implicadas, siempre basándose en los principios de colaboración civil-militar. (CMI)

2.2. Concentración de Fuerza

La fuerza de combate debe ser concentrada en tiempo y espacio, a fin de generar superioridad y conseguir resultados decisivos. Una fuerza superior no es simplemente cuestión de número, pero también de habilidades de combate, cohesión, ánimo, momento adecuado, selección de objetivos y aprovechamiento de ventajas tecnológicas.

2.2. Economía de esfuerzo

Debido a recursos finitos, puede ser necesario asumir riesgo en algunas áreas o disminuir la ambición/alcance. El principio de economía de esfuerzo enuncia de que para que una fuerza concentrada pueda ser aplicada en áreas decisivas, en otras de menor prioridad se deben economizar medios. Esta economía de esfuerzo (o economía de medios) implica, tras un análisis de riesgo, repartir los recursos disponibles según instrucciones del mando.

2.2. Libertad de Actuación

La libertad de actuación habilita a los jefes de mando a proseguir con sus misiones y debería aligerar posibles restricciones de actuación que sufren estos. El jefe de mando de nivel operacional procurará dirigir operaciones, batallas y compromisos. Para tener éxito, y anticipar escenarios o aprovechar oportunidades emergentes, los jefes de mando, deben tener libertad de actuación para desplegar unidades de reserva, establecer prioridades y asignar activos marítimos, terrestres, aeroespaciales, especiales y de apoyo. Sin embargo, el nivel de libertad a nivel operacional variará según la naturaleza del conflicto, según la interacción de líneas de operación, militares y no militares, siempre dentro la estrategia y decisiones colectivas de los líderes de miembros y países satélite de la OTAN. Con dichas restricciones en mente, el jefe de mando debe enunciar claramente sus propósitos de actuación, definiendo, de cara los mandos subordinados, los conceptos de operaciones y estableciendo objetivos a cumplir, a fin de acotar la libertad de acción también para estos mandos subordinados.

2.2. Definición de Objetivos

Las operaciones multinacionales conjuntas deben perseguir objetivos bien definidos y comprendidos por todos los miembros. Un estado de finalización, conciso y claro, permite a los planificadores a mejor identificar objetivos que deben ser alcanzados a fin de llegar a dicho estado. Una planificación conjunta integra actuaciones y capacidades militares con otros instrumentos de poder nacional, dentro de un tiempo, lugar y propósito. Los objetivos y sus efectos auxiliares proveen la base para identificar actuaciones a llevar a cabo. Alcanzar los

objetivos operacionales también obliga a que las tareas tácticas alcancen el estado de finalización. Hay cuatro consideraciones primarias para un objetivo:

1. Cada objetivo establece un único resultado o finalidad.
2. Cada objetivo debería enlazar directamente a objetivos de un nivel más alto, o al estado de finalización
3. Cada objetivo debe ser preciso y no-ambiguo
4. Un objetivo no propone metodología ni medios y no es escrito como si fuese una tarea

2.2. Espíritu Ofensivo

El núcleo de este principio es la noción de un estado mental de proactividad. Además, implica autoconfianza, anima emprendimiento y determinación en no ceder la iniciativa, y promueve una cultura de éxito y compleción de objetivos. Como estado mental, en términos prácticos, el espíritu ofensivo es a menudo decisivo, pero su aplicación más amplia no debería ser priorizada ante una actuación defensiva cuando las circunstancias y la prudencia lo demandan. El espíritu ofensivo implica un enfoque enérgico e incisivo para derrotar los oponentes, aprovechar las oportunidades y aplicar presión constante sobre otras formas de resistencia y fuentes de inestabilidad. La actuación ofensiva es la manera práctica en el que un jefe de mando trata de obtener ventaja, mantener la inercia y tomar la iniciativa. Un espíritu ofensivo proporciona los beneficios que da la acción más que la reacción, y la libertad de forzar una decisión.

2.2. Sencillez

Planes sencillos y claros, ordenes concisas, ayudan a minimizar malentendidos y confusiones. Los planes sencillos son menos propensos a fricciones que los complejos, y son rememorados fácilmente incluso bajo presión. Cuanto más complejo el plan, más maneras hay que vaya mal, aun así, la sencillez no es una excusa para que los planes falten de instrucciones detalladas de coordinación operativa. Instrucciones claras y un entendimiento del propósito del jefe de mando, simplifican la planificación y la dirección de las operaciones.

2.2. Flexibilidad

Los planes deberían ser suficientemente flexibles para responder ante lo inesperado y habilitar a los jefes de mando con la mayor libertad de actuación. Esto requiere: comprensión de los propósitos del mando superior, flexibilidad de pensar, rápida toma de decisiones, organización efectiva y comunicaciones suficientes.

2.2. Iniciativa

La iniciativa debe ser cuidad mediante la confianza y el entendimiento mutuo, y ser desarrollada a través de entrenamientos. La iniciativa trata sobre reconocer y aprovechar oportunidades y resolver problemas de formas originales. Para instaurar un clima de iniciativa, a un jefe de mando se le debe de haber concedido la libertad de usar la iniciativa, y debería, a su vez, animar a sus subordinados a que la aprovechen. Esto requiere un entrenamiento y cultura en operaciones, que promuevan una en enfoque de asumir riesgos calculados de cara a ganar, más que de cara a prevenir la derrota. Las autoridades de mando delegadas al nivel más bajo factible deben animar los individuos bajo su mando a usar la iniciativa que se les ha concedido.

2.2. Sorpresa

Sorpresa consiste en atacar un adversario en un momento, lugar o manera de cara a cuáles este no está preparado. Sorpresa es la consecuencia, o confusión producida por la introducción, deliberada o no, de lo inesperado. La sorpresa es temporal y una sorpresa exitosa requerirá ser aprovechada de manera a prevenir la recuperación del adversario. La sorpresa está basada en velocidad, secretismo y engaño. Si es exitosa, la sorpresa puede conseguir efectos desproporcionados (mayores) de cara al esfuerzo realizado.

2.2. Seguridad

La seguridad mejora la libertad de actuación, al limitar la vulnerabilidad a actividades hostiles y amenazas. Medidas activas y pasivas de seguridad ayudan a negar al adversario información crítica. Ayudan al engaño y habilitan actuaciones contraofensivas.

2.2. Cuidar Estado Anímico

Los jefes de mando deberían dar a sus subordinados una cara e identidad, promover la autoestima, inspirarles con un propósito común y unidad de esfuerzo, y proporcionarles unos fines alcanzables. Un estado anímico correcto, se basa en un buen liderazgo, que insufla coraje, energía, determinación, respeto y unidad entre los subordinados.

2.2. Consideraciones Operacionales

2.2.14.1. Descripción

Los principios de operación, previamente mencionados, toman, a su vez, soporte en las siguientes consideraciones operacionales. Las consideraciones operacionales están siempre vigentes, sin embargo, su nivel importancia varía según el tipo de operación.

2.2.14.2. Credibilidad

Una fuerza dirigida por la OTAN deber tener credibilidad. Un actor fundamental en establecer credibilidad es asegurarse de que, a todos los niveles, las palabras son secundadas por hechos y de que cualquier fuerza desplegada es vista como profesional y capaz de cumplir su misión. Afianzar la credibilidad es esencial para autoconfianza y esto se hace mediante la coordinación de actividades de información y operaciones de información (Info Ops) en concordancia con las directivas y guías de comunicaciones estratégicas (StraCom) (por regla general en la forma de Marco StatCom). Esto puede potenciarse también en desplegar fuerzas con suficiente capacidad en disuadir acciones hostiles o si necesario, de aplicar fuerza de manera juiciosa. En caso de uso de fuerza (o de amenazar de usar la fuerza), será necesario tener una estimación del impacto que dichas acciones pueden causar, no sólo sobre la credibilidad, pero también en la operación entera, a través de implicaciones asociadas en Política, Economía, Sociedad y Medio Ambiente.

Como ejemplo del mundo real, el ciberespacio se ha usado como canal de Operaciones de Información contra países miembros de la OTAN, en contra altos cargos de un gobierno o para llevar campañas de desinformación.

2.2.14.3. Autorización

Promover la autorización y la cooperación de la nación huésped (HN) es prerrequisito para muchas operaciones. Antes de llevarse a cabo cualquier actividad de fuerza militar, que pueda sufrir una retirada de autorización, dicha actividad debería ser sopesada y analizada de cara al estado final de la misión. (entiéndase misión global u operación, no la particular de dicha actividad). Autorización y cooperación son capaces de promover una legitimidad visible si se puede hace entender a las partes (HN) que su estatus y autoridad se verán reforzados si participan en resolver sus disputas por medios propios (entiéndase cooperación). Cuando las personas y partes son participes en el proceso, entonces tienen más motivos para cooperar. En el nivel táctico, dicha vía puede tomarse, al ofrecer incentivos a la HN para cooperar en llevar conjuntamente ciertas tareas.

2.2.14.4. Respeto Mutuo y Entendimiento

El respeto que se le proferirá a una fuerza de la OTAN es consecuencia directa de su actitud profesional y del buen trato que da a la población local y autoridades reconocidas. A través de un mandato de Naciones Unidas (UN), Acuerdo de Estatus de Fuerzas (SOFA), y otros acuerdos especiales, la fuerza de la OTAN puede disfrutar cierta inmunidad en relación con sus deberes. En caso contrario, sus miembros deben respetar las leyes y costumbres de la HM y sobre todo cuando están en público. El jefe de mando debe asegurar de que los mismos principios son reconocidos e implantados en las formaciones que componen la fuerza, independientemente de las nacionalidades, culturas y etnicidades de los integrantes. Todo el personal debe consistentemente demostrar los más altos estándares de disciplina ejercida mediante comportamiento profesional dentro y fuera de las horas de trabajo. Esto también contribuye a mantener una legitimidad visible.

2.2.14.5. Transparencia

La misión y el concepto de operaciones (ConOPS), así como el estado final, deben ser bien entendidos por todos los actores y estar claros a todas las partes implicadas y agencias. Llegar a un entendimiento común ayudará a disminuir las sospechas y desconfianza y mejorará la efectividad operacional. La información debería ser recogida y compartida siempre que sea posible. Aun cuando la transparencia de operaciones, incluido el acceso a la prensa, debería ser normal general, hay que equilibrar dicha transparencia de cara a la seguridad de la misión y de la operación.

2.2.14.6. Libertad de Movimiento

La libertad de movimiento es esencial para cualquier operación. El mandato, SOFA y reglas de combate (ROE) deben permitir a las fuerzas de la OTAN ser libres, en todo momento, para realizar sus deberes sin interferencia de grupos locales y organizaciones. Normalmente, varias facciones intentarán imponer restricciones locales al desplazamiento. Estas restricciones deben ser firme y rápidamente resueltas: al principio mediante negociación, y si es necesario mediante actuaciones contundentes que pueden culminar en uso de fuerza, según el marco legal aplicado y las ROE.

2.2.14.7. Comunicaciones Estratégicas (STRATCOM)

Todos los aspectos de OTAN tienen implicaciones y componentes de información. Por lo tanto, es importante que los efectos relacionados con comunicaciones de la OTAN y la narrativa sean parte integral del Plan de Operaciones. (OPLAN) Tienen que ser tomados en

cuenta en el proceso de planificación, reflejados en el diseño operacional, expresados en los propósitos del jefe de mando, y aplicados durante el proceso de ejecución y selección de objetivos. StratCom es la integración de las capacidades de las capacidades de comunicación y las funciones del personal de información, con otras actividades militares, a fin de dar forma al 'Entorno de Información' para dar apoyo a los fines y objetivos de la OTAN. Los principios de StratCom tienen una importancia particular dentro e las capacidades de comunicación de Asuntos Públicos Militares (Mil PA) y operaciones psicológicas (PsyOP) y el personal de operaciones de información (Info Ops) y requiere de un enfoque centrado en una red de colaboración para dar apoyo a la toma rápida de decisiones, la eficiencia y la unidad de esfuerzo. Como tal, las capacidades de comunicación operacional y las funciones de personal de comunicación deben ir sincronizados. Mediante sincronización, cada personal de comunicación sigue reteniendo sus responsabilidades funcionales y el "Mil PA" conservará un rol activo de consejero con canal directo al jefe de mando. (Ministario de Defensa de España, 2020)Cabe mencionar países como España, que en vez de en vez de usar el concepto de Dominio de la Información, usan el concepto de 'Dominio Cognitivo', cognitivo se refiere a la dimensión humana y social de la información.

2.2.14.8. Operaciones en Ciberespacio

(EEAS, 2021) Desde la perspectiva EU (y en transposición de NATO), el ciberespacio se compone de tres niveles que han de entenderse como conjunto (y no por separado)

1. Físico: geografía, persona, hardware, espectro electromagnético, et al.
2. lógico: sistemas, servicios, software, et al.
3. ciberpersona: interfaces persona-computador, cognitivo (individual, usuario) y social (colectivo, redes sociales)

Muchas facetas de las operaciones conjuntas se basan en el ciberespacio, que va más allá de fronteras geográficas o geopolíticas. El ciberespacio está también integrado en la operación de infraestructuras críticas, así como en el comercio, gobierno, y seguridad nacional. Por lo tanto, los jefes de mando deben tener en cuenta sus dependencias críticas de la información y ciberespacio, así como factores tales como la degradación de la confidencialidad, disponibilidad e integridad da la información y de los sistemas de información, cuando planifican y organizan las operaciones. Los jefes de mando llevan a cabo ciber-operaciones a fin de conservar la libertad de movimiento en el ciberespacio, denegar libertad de actuación a los adversarios, y habilitan otras actividades operacionales. Las ciber-operaciones se realizan sobre todo porque existen enlaces y nodos que residen en el dominio físico, y por lo tanto consisten en actuaciones ciber físicas. De manera análoga, operaciones

en el dominio físico pueden crear efectos en el ciberespacio, mediante, p.e., interferencia electromagnética en infraestructura física. Las operaciones en ciberespacio podrían ser llevados por naciones miembro, de manera individual, en respuesta de un requerimiento formal y de acuerdo con sus respectivas leyes nacionales y ciber-capacidades, siendo la información de las operaciones provista por parte de OTAN de acuerdo con sus respectivas políticas nacionales y guías.

2.2.14.9. Protección del medio ambiente

Una protección efectiva del medio ambiente mejora la protección sanitaria de las fuerzas, también apoya las operaciones al contribuir a una relación positiva con la HN. A fin de alcanzar el objetivo de protección medioambiental, el gasto de energía debería ser optimizado en todas las fases de las actividades militares de la OTAN y en concordancia con requerimientos operacionales. La eficiencia energética ahora dinero y salva vidas al reducir el sobrecoste logístico. Una protección medioambiental efectiva mejora la protección de la salud de las fuerzas, y mejora las relaciones con la HN. Los factores a tener en cuenta son prevención de la contaminación, gestión de residuos, gestión de riesgos NRBQ (químico, biológico, radiológico y nuclear) (o CBRN). Esto último debe incluir prevención, protección y recuperación de incidentes CBRN deliberados o accidentales. Así como protección de patrimonio cultural y protección de la flora y fauna.

2.2.14.10. Protección de civiles

La protección de civiles (PoC) es relevante dentro de cada una de las tres tareas principales de la OTAN. Todas las operaciones dirigidas o propias de OTAN, misiones y otras actividades encomendadas por el concejo, son llevadas en concordancia con las Leyes Internacionales de Derechos Humanos. Un enfoque bien claro en operaciones, basado en imperativos legales, morales y políticos, es importante para la credibilidad de la OTAN y su legitimidad. PoC (personas, objetos y servicios) incluye todos tipo de medidas tomadas para evitar, minimizar y mitigar los efectos negativos que pueden derivar de operaciones propias o dirigidas por OTAN, sobre la población civil, y cuando proceda, proteger los civiles de violencia física derivada del conflicto, o amenazas de violencia física por otros actores, inclusive mediante la creación de un ambiente seguro. Durante la ejecución de operaciones y misiones, el entrenamiento, formación, ejercicios, los análisis en retrospectiva, las actividades de adquisición de capacidades de defensa y seguridad, los jefes de mando deberían incluir una perspectiva PoC que cubra temas transversales: mujer, paz y seguridad; niños y conflictos armados; violencia sexual como parte del conflicto y violencia relacionada con el género; mitigación de bajas civiles; políticas de estabilidad y herencia cultural. Los jefes de mando

deberían esforzarse en compartir buenas prácticas y experiencia en el PoC, sobre todo la mitigación de daños a civiles.

2.3. MILDEC: Compendio de Principios de Engaño Militar

3.3.1. Descripción

(MILDEC JP3-13.4 Military Deception, 2012) MILDEC o Técnicas de Engaño Militar son acciones llevas a cabo para. Intencionadamente, engañar al Mando del adversario para que este realice acciones que favorezcan objetivos de nuestra propia misión.

3.3.2. Alcance

MILDEC es aplicable en todos los ámbitos de guerra, incluyendo todo el abanico de operaciones militares, y puede ser llevado a cabo durante cualquiera o todas las fases de operaciones militares. […] Es el Mando Conjunto es el que tiene la autoridad de elegir el rol que tendrá MILDEC en las operaciones conjuntas. Durante la planificación de una Operación, MILDEC debe ser integrado en las fases tempranas de una operación. El rol de MILDEC en las fases tempranas de una operación, estará basado en un momento especifico de la operación o campaña, con intención de establecer las condiciones que facilitarán la ejecución de fases posteriores.

MILDEC está pensado para disuadir acciones hostiles, aumentar el grado de éxito de acciones defensivas amistosas, o para aumentar el grado de éxito de cualquier posible acción ofensiva amistosa. El uso de MILDEC durante cualquier fase de una operación debería ayudar a engañar los adversarios sobre las fuerzas, capacidades, ubicaciones, y misiones planeadas de fuerzas amistosas. MILDEC como elemento de un Plan Operaciones Integradas (IO), puede ser una opción factible disuasoria flexible. En situaciones de combate, hay un enfoque hacia cumplimiento de objetivos y llevar el adversario a la derrota. En situaciones de no-combate, el jefe de Mando Conjunto busca dominar la situación con operaciones decisivas diseñadas para establecer condiciones para alcanzar una conclusión favorable y temprana. Hay tres categorías de MILDEC que dan apoyo a operaciones conjuntas de MILDEC:

1. MILDEC conjunto: Un MILDEC conjunto es planificado y llevado a cabo en el teatro de operaciones para dar apoyo a campañas y operaciones militares de envergadura. Las actividades de MILDEC son planificadas y ejecutadas por y como apoyo a los mandos de combate, jefes de mando conjuto, y mandos de grupos de opeaciones conjuntas, con la finalidad de llevar el adversario a la toma de ciertas acciones.o inacciones de manera favorable a los objetivos de misión. La mayoría de ordenes planeadas y

ejecutadas de tipo MILDEC de combate son de timpo conjunto con efectos a nivel operacional.

2. Engaño en Apoyo a Operaciones de Seguridad (DISO): DISO es una clase de actividades MILDEC que protegen operaciones amistosas, equipamientos y otros activos, frente a acciones de reconocimiento y recolección de datos por parte de agencias de inteligencia extranjeras y servicios de seguridad. (FISS). El propósito de una DISO es crear múltiples falsos indicios a fin de confundir al adversario, o dificultar la interpretación de los propósitos de fuerzas amistosas. Los DISOs son no-dirigidos por diseño: no están dirigidos específicamente hacia algún adversario en particular, sino más bien para proteger operaciones amistosas al ofuscar sus capacidades, propósitos o vulnerabilidades. El Mando Conjunto puede llevar a cabo ordenes DISOs ya sea pre-misión, o como parte de un plan operacional (OPLAN), plan operacional en formato conceptual (CONPLAN), o como una orden operacional (OPORD)
3. Engaño táctico (TAC-D): TAC-D son actividades planificadas de engaño que son ejecutadas con fines de dar apoyo en batalla y combate. TAC-D es planificado y ejecutado por y en apoyo a mandos del nivel táctico, con la finalidad de llevar el adversario a la toma de ciertas acciones o inacciones de manera favorable a los objetivos de misión. TAC-D es llevado a cabo a fin de ganar una ventaja táctica provisional, para enmascarar vulnerabilidades en fuerzas amistosas, o para aumentar las capacidades defensivas de estas últimas.

Victoria y Estado de Finalización Estratégica: En fases tardías de una operación, antes de victoria, MILDEC debería dar apoyo al traspaso de responsabilidad hacia detentores civiles u otras autoridades. La complejidad de operaciones conjuntas en fases tardías se debe a varios factores: el esfuerzo de retirada de las fuerzas conjuntas; el apoyo a la nación huésped y a agencias gubernamentales mientras dure el traspaso de responsabilidades; la naturaleza no lineal del área de operaciones; y la posible falta de agenda secuencial en el traspaso de responsabilidades de control del área. Por eso, la planificación y ejecución de MILDEC durante las fases tardías de la campaña puede implicar contados miembros no militares, complicando los problemas de seguridad operacional (OPSEC); por eso MILDEC debería tener en cuenta no solo la victoria militar sino también los objetivos nacionales y estado final. Durante dichas fases, el jefe de mando conjunto se centra en la sincronización e integración acciones conjuntas de las fuerzas, con la actividad de otros instrumentos de poder nacional. Con tal de llevar las operaciones a resultados satisfactorios, que por regla general consisten en una paz autosostenida y la implantación del imperio de la ley. MILDEC puede ser ejecutado para: apoyar operaciones de redespliegue o retirada; proteger de revelación a capacidades operativas sensibles; establecer condiciones favorables para operaciones militares posteriores; dar posible apoyo a operaciones de contrainsurgencia; defender o reconstruir

infraestructuras críticas; y ayudar en el traspaso de responsabilidades al control civil u otras autoridades.

3.3.3. Calidad de la Información

Calidad de la información refiere a la exactitud, completitud, relevancia y credibilidad de la información disponible al tomador de decisiones. Se debería proteger con sumo cuidado la calidad de la información disponible, destinada a la toma de decisiones de fuerzas amistosas, o para diseminación pública. Esto ayudará a garantizar de que el jefe de mando conjunto tenga información correcta y evitará que el personal y subordinados perciban erróneamente como información veraz las tareas de MILDEC lanzadas por el jefe de mando.

La calidad de la información también implica asegurarse de que la información hecha pública por el jefe de mando conjunto, no forma parte de ninguna acción MILDEC [...].

MILDEC, por diseño, debería afectar a la calidad de la información utilizada por el adversario para tomar decisiones, de las siguientes formas:

1. Presentar a los adversarios de manera intencionada información engañosa a fin de disminuir la exactitud de la información en sus manos.
2. Procurar dar a los mandos adversarios una falsa sensación de completitud de información sobre fuerzas amistosas y/o propósitos.
3. Hacer que el adversario juzgue mal la importancia de informaciones disponibles y coloque mal recursos operacionales y/o de inteligencia.
4. Hacer dudar al adversario de las capacidades de sus sistemas de recolección de inteligencia.

3.3.4. Objetivos/Blancos

El plan MILDEC debería definir claramente la meta y el objetivo de este último. Esto proporciona al mando un entendimiento sólido de cómo el engaño da apoyo a la operación global y establece una base sólida para planificar y ejecutar operaciones MILDEC.

La meta MILDEC: la meta MILDEC es la declaración de propósito del MILDEC por parte del mando, ya que contribuye a llevar a cabo exitosamente la misión asignada. La meta de un MILDEC, normalmente, está expresada como un resultado positivo. Como toda forma de operación militar, el grado de éxito para MILDEC es su capacidad de contribuir de manera directa al cumplimiento de misión. MILDEC requiere a menudo inversión significativa en esfuerzo, y recursos que de otra manera se gastarían contra el adversario de una manera más directa y tradicional. Por consiguiente, es importante que el mando exprese la ‘meta’ MILDEC en términos de cumplimiento de una cierta misión.

El objetivo MILDEC: el objetivo MILDEC es una expresión de qué es lo que el adversario no hará o dejará de hacer, a causa suya. Se expresa en términos de acciones de adversario o inacciones, que lleven directamente al propósito o condición expresada en la 'meta' MILDEC. Como ejemplo de objetivo MILDEC es "Causar que el adversario […] defienda el sector equivocado […]".

Otros objetivos MILDEC pueden:

1. Causar que el mando adversario emplee fuerzas y activos de formas que sean ventajosas para las fuerzas amistosas.
2. Causar que el adversario revele fortalezas, planes y propósitos.
3. Causar que el adversario retenga sus reservas estratégicas mientras que las fuerzas amistosas terminen la misión de manera exitosa.
4. Condicionar el adversario a ciertos patrones de maniobras amistosas a fin de hacerle percibir erróneamente que son explotables en una ventana temporal elegida por el mando conjunto.
5. Hacer que el adversario despilfarre potencia de combate con acciones no apropiadas y/o retrasos.
6. Condicionar al adversario, que, ante ciertos patrones de información, reacciones de manera determinista, y que las fuerzas conjuntas amistosas puedan explotar dichas reacciones

3.3.5. Cauces hacia los blancos

El blanco del engaño es el mando adversario con autoridad de tomar decisiones que contribuyan al cumplimiento de los objetivos de engaño. El blanco o blancos del engaño son individuos clave en quienes estará enfocada toda la operación de engaño. Varios factores se tomarán en cuenta al elegir el blanco del engaño:

1. El blanco del engaño debe ser capaz de materializar las deseadas acciones o inacciones. El blanco debe tener la autoridad para hacer decisiones que ayudarán a las fuerzas conjuntas en completar el objetivo de engaño deseado.
2. Tiene que haber cauces hacia los blancos del engaño, o debe haber esperanzas razonables de que dichos cauces puedan ser establecidas cuando se necesite.
3. Durante el desarrollo del engaño, hay que poseer suficientes datos de inteligencia para determinar qué conocimientos y qué preconcepciones tiene el blanco sobre las operaciones de las fuerzas conjuntas. La experiencia ha demostrado que las operaciones de engaño que se basan en preconcepciones y prejuicios que tiene el blanco, han tenido mayor éxito.

4. El coordinador de MILDEC debería presentar un requerimiento de información (RFI) a la Comunidad de Inteligencia (IC), pidiendo análisis de influencia comportamental (BIA), datos de análisis de factor humano (HFA) de adversarios militares, paramilitares y personal de mando veterano.

3.3.6. Historia/Escenario/Guion

En MILDEC, los cauces son vías de información o inteligencia, que comunican con el blanco del engaño. Los cauces puedes ser utilizadas para controlar el flujo de información al blanco del engaño. Cabe señalar de que es muy poco común enviar mensajes de engaño directamente al blanco. Más bien, a menudo, los mensajes de engaño son enviados a los recolectores de inteligencia con la esperanza de que el mensaje de engaño seguirá los escalará por los diferentes niveles de recolección de inteligencia, propiedad del adversario.

1. A modo de ejemplo, son cauces: agencias de inteligencia extranjeras y servicios de seguridad. (FISS), plataformas de recolección de inteligencia, e individuos a través de los cuales se puede llegar al blanco del engaño.
2. El desarrollo y uso de cauces debería realizarse de manea metódica. Se debería determinar una ruta bien clara, antes siquiera de empezar a realizar entradas al cauce al blanco. Lo ideal sería que los cauces formasen parte de un sistema con retroalimentación que informe de la recepción del mensaje de engaño y de si el blanco realizará las acciones o inacciones deseadas. Los factores a tener cuenta son entre otros:
    1) ¿Hay puntos de parada o filtros para llegar al blanco?
    2) ¿Hay algún prisma que distorsione la percepción que se quiere dar al blanco?
    3) ¿Hay cauces que puedan, posiblemente, validar o contradecir el mensaje deseado?
    4) En el caso de FISS, ¿podría el cauce servir a su vez como mecanismo de retroalimentación?

3.3.7. Funciones

La piedra angular de cualquier operación de engaño es el guion de engaño. El guion del engaño es un escenario que esboza las acciones amistosas que serán llevadas a cabo a fin de que el blanco del engaño adopte una percepción de las cosas acorde a lo planeado. Es un enunciado conciso o narrativa de exactamente lo que el planificador de MILDEC quiere que el blanco crea que es la situación supuestamente real, para que luego este último (blanco) actúe en consecuencia. En otras palabras, el guion del engaño está en consonancia con lo que el engaño querría que la inteligencia adversaria pensara y dijera sobre las fuerzas

conjuntas amistosas y sus mandos. El guion de engaño considera que estas acciones amistosas, ya sean reales o imaginarias, moldearán la percepción situacional del adversario. El guion del engaño es tanto un proceso analítico como creativo, que implica un amplio abanico de información sobre las capacidades del adversario para adquirir datos inteligencia y procesarla.:

- Un entendimiento correcto de las percepciones e indicios requeridas para que el engaño, asegura una base sólida para fabricar el guion del engaño. El guion del engaño junta estos elementos en una representación coherente de la situación que el blanco va a reconstruir a partir de la información que se le proporcione. De manera ideal, el planificador del engaño quiere que la imagen mental que se forme el blanco a medida que se despliega el engaño, se calcada al guion del engaño. El guion del engaño debería parecerse mucho al output de la inteligencia recolectada por el adversario. El guion del engaño es, en efecto, lo más parecido a las piezas de un puzle que se van juntando. Como tal, sirve como medio para verificar la lógica y la consistencia de los elementos internos del engaño. Esto permite al planificador del engaño identificar elementos deseados, tales como percepciones, indicios y ejecuciones que necesitan mejoras y ajustes, y añadir indicios de apoyo para fortalecer ciertos elementos del guion del engaño o mitigar el impacto de indicios adversos al guion. Cada elemento del guion de engaño debe tener medios a su disposición para escenificar los datos necesarios, además de tener cauces bien determinados para transferir esta información los sistemas de procesamiento de información del adversario. Inevitablemente varios nodos de la línea de comunicación pueden convertirse en filtros, distorsionando la información engañosa o directamente parándola. El planificador MILDEC debe tener esto en cuenta. A medida que el guion se va desplegando y ejecutando, el planificador MILDEC continuamente monitorea cambios situaciones y valida la situación real comparada con el guion y otras acciones amistosas.
- El guion debería ser creíble, verificable, consistente e implementable.
    - Creíble: el guion debe describir la percepción buscada, del blanco hacia la misión de las fuerzas amistosas, propósitos, y capacidades.
    - Verificable: el adversario debería verificar (erróneamente) como verdadero el guion de engaño implementado, a través de varios canales y cauces. El guion de engaño, por lo tanto, debe tener en cuenta todas las fuentes de inteligencia del adversario y ser implementado con todas estas fuentes en mente.
    - Consistente: Los guiones de engaño deberían ser consistente con el concepto que tiene el blanco adversario de la verdadera doctrina amistosa, con el

historial de manejo de fuerzas, con la estrategia de campaña, con las tácticas de campo de batalla, y con la actual situación operacional. Esto lleva a que el planificador MILDEC a tener una representación tan fiel como sea posible del nivel de conocimiento que posee el blanco adversario. […]

- Implementable: Al igual que con cualquier Curso de Acción (CoA), las opciones que proporciona un MILDEC tienen que estar acotadas por las capacidades de las fuerzas amistosas en el grado en que las percibe el blanco adversario. El blanco del engaño tiene que estar convencido que las fuerzas amistosas tienen la capacidad de llevar a cabo las operaciones descritas por el guion de engaño implementado.

3.3.8. Principios

Al igual que los principios de la guerra proporcionan una guía general sobre la realización de operaciones militares, los seis principios de MILDEC proporcionan guías para la planificación y ejecución de operaciones MILDEC:

1) Focalización: MILDEC debería apuntar al mando adversario capaz de la acción o acciones deseadas. El sistema adversario de inteligencia, vigilancia y reconocimiento (ISR) normalmente no es el blanco en sí; más bien es el cauce primario utilizado en MILDEC para encaminar la información seleccionada hacia el mando adversario.
2) Objetivo: el principal objetivo de las operaciones MILDEC es enfocar las acciones y recursos en hacer que el adversario realice (o no realice) acciones específicas, y no sólo a creer o no ciertas cosas.
3) Planificación Centralizada y Control: Las operaciones MILDEC deberían planificarse y dirigidas de manera centralizada. Este enfoque es necesario para evitar confusión y asegurar de que los distintos elementos que formar parte del MILDEC cuentan la misma historia/guion y no entran en conflicto con otros objetivos operacionales. Sin embargo, la ejecución de MILDEC puede ser descentralizada mientras todos los actores amistosos estén adheridos a un plan único
4) Seguridad: Una operación MILDEC exitosa requiere de seguridad estricta. Esta empieza a implementarse desde antes de la ejecución del primer paso de MILDEC, mediante medidas para ocultar los propósitos de fuerzas amistosas de engañar. Hay que aplicar políticas estrictas de seguridad, clasificación, acceso y compartimentalización sobre la información y a cada aspecto de la operación MILDEC. Se debe aplicar activamente OPSEC (seguridad operacional) para prevenir filtraciones de información crítica tanto sobre operaciones verdaderas como sobre actividades MILDEC; el conocimiento de planes y ordenes MILDEC debe ser correctamente clasificado y manejado. […]

5) Pertinencia Temporal: una operación MILDEC requiere de una sincronización cuidadosa. Por eso hay que prever suficiente tiempo para el despliegue del guion MILDEC: que los sistemas ISR del adversario tengan tiempo de recolectar, analizar y reportar, para que los mandos adversarios reaccionen, y para que los sistemas ISR amistosos detecten la acción resultante de la decisión del mando adversario. […] Puede ser necesario la intervención de un mando amistoso para ajustar el curso de la operación.
6) Integración: Integrar plenamente cada operación MILDEC con las operaciones de apoyo. El desarrollo de un concepto MILDEC debe realizarse como parte del desarrollo del Concepto de Operaciones (CONOPS) del mando. MILDEC debe ser tenido en cuenta en las fases tempranas de planificación a todos los niéveles, para asegurar de que los planes de engaño subordinados están bien integrados con los planes de nivel superior.

3.3.9. Medios, Tácticas, Técnicas y Procedimientos

Medios para MILDEC: MILDEC emplea tres grandes grupos de medios: físicos, técnicos y administrativos. Cabe mencionar que MITRE, en su Ontología CTI 'ATT&CK (MITRE, s.f.), ya incluye varias clases de objetos referentes a Engaño Cibernéticos.

1) Medios Físicos: Actividades y recursos utilizados para encaminar la información seleccionada hacia un adversario. Son medios físicos entre otros:
   a) Desplazamiento de fuerzas
   b) Ejercicios y actividades de entrenamiento.
   c) Dispositivos y equipamientos de señuelo
   d) Actuaciones tácticas
   e) Actuaciones logísticas y localización de almacenes y talleres.
   f) Actividades de pruebas y evaluación
   g) Actividades de reconocimiento y vigilancia
2) Medios técnicos: aquellos recursos militares materiales y sus técnicas operativas asociadas, utilizadas para encaminar u ocultar al adversario. información seleccionada. […] Son medios técnicos entre otros:
   a) Emisión, alteración, absorción o reflexión intencionados de energía
   b) Emisión o supresión de olores químicos o biológicos
   c) Multimedia (radio, televisión, difusión de radio, ordenadores, redes de ordenadores, smartphones y PDA's)
3) Medios Administrativos: incluyen recursos, métodos y técnicas para encaminar u ocultar evidencias orales, gráficas, documentales o de otro tipo físico

Tácticas MILDEC: La aplicación de tácticas varía según cada operación dependiendo de variables tales como tiempo, activos, equipamiento y objetivos que también son revisadas en función de su implementación. Son tácticas MILDEC entre otros:

1) Enmascarar un aumento o redespliegue de las fuerzas o sistemas de armamento expuestos al adversario
2) Moldear la percepción del adversario y/o identificación de nuevas fuerzas o armamento introducidos en combate
3) Reforzar las preconcepciones del adversario
4) Desviar la atención del adversario de ciertas actividades
5) Sobrecargar los ISR de recolección y análisis, del adversario.
6) Crear la ilusión de poderío donde en realidad hay debilidad.
7) Insensibilizar el adversario / hacer invisibles ciertos patrones de comportamiento de fuerzas amistosas, a fin de poder explotar las percepciones del adversario en momentos determinados
8) Confundir las expectativas del adversario, a fin de causarle efecto sorpresa, sobre el tamaño de fuerzas amistosas, actividades, emplazamientos, unidades, tiempos, equipamiento, propósito y/o estilo de misión ejecutada
9) Disminuir la habilidad del adversario para percibir claramente y/o gestionar la batalla.

Técnicas MILDEC: las operaciones MILDEC usan cuatro técnicas básicas de engaño: fintas, demostraciones, artimañas y exposición.

10) Fintas: una finta es una acción ofensiva que implica contacto con el adversario, llevada a cabo con el propósito de engañar al adversario en cuanto a la localización y/o momento de la acción ofensiva principal.
11) Demostraciones: una demostración es una muestra de fuerza donde no se persigue una decisión ni contacto con el adversario. El propósito de una demostración es hacer que el adversario elija realizar un CoA favorable a los intereses de las fuerzas conjuntas.
12) Artimaña: una artimaña es un truco elaborado para engañar al adversario con fin de conseguir ventaja amistosa. Se caracteriza por exponer, intencionadamente, información falsa o contradictoria para que la recolecte e interprete el adversario
13) Exposición: la exposición consiste en simular, disfrazar y/o representar objetos amistosos, unidades o capacidades que en realidad son proyecciones del guion MILDEC. Tales capacidades pueden no existir. (simulaciones)
14) Engaños ilegales: algunas técnicas de engaño pueden ser considerados “actos pérfidos” debido a su naturaleza rastrera. Los actos pérfidos están prohibidos bajo la ley de

conflictos armados (LOAC) porque dificultan el cumplimiento de las Leyes de la Guerra y por lo tanto ponen en peligro l seguridad de civiles, no combatientes y/o la inmunidad de estructuras y actividades protegidas. Los actos de perfidia son engaños ideados para hacerle creer que tiene o que tiene que conceder a algún objeto o persona un estatus protegido. Los actos pérfidos aprovechan de que el perjudicado es un agente cumplidor con la LOAC. Los actos de perfidia incluyen entre otros: simular rendición a fin de atraer el enemigo a una trampa, utilizar símbolos y signos, en principio de protección, para inhabilitar o herir al enemigo, utilizar ambulancias o naves médicas con símbolos tales como Cruz Roja, Luna Roja, etc, para transportar combatientes armados, munición y armas, con la finalidad de atacar o evitar fuerzas enemigas. Cabe mencionar que en la legislación de ciberespacio aún existe cierto vacío legal: el derecho internacional parte de la diferenciación de combatientes y no combatientes, focalizándose principalmente en el jus ad bellum y el jus pos bellum. En el ciberespacio esto no tiene cabida, ya que ni siquiera es viable la atribución de la amenaza. En la actualidad no hay acuerdos internacionales al respecto, exceptuando proposiciones como el Manual de Tallin (Ramon Y Cajal Ramo & Maestre Vidal, 2021)

Procedimientos MILDEC: los procedimientos MILDEC varían según cada operación MILDEC y son llevados a cabo en acuerdo con la guía de los mandos, y también en acuerdo con los procesos utilizados para sincronizar en tiempo real tácticas y técnicas.

2.4. Operaciones en el ciberespacio

3.4.1. Descripción

(DOD, CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE , FM3-12, 2021) (DOD, Cyberspace Operations JP3-12, 2018) Aunque es posible que las operaciones en el ciberespacio (CO) produzcan efectos tácticos, operacionales o estratégicos por sí solas y así lograr los objetivos, los comandantes integran la mayor parte del CO con otras operaciones para crear los efectos coordinados y sincronizados necesarios para apoyar el cumplimiento de la misión. La superioridad global permanente en el ciberespacio no es posible debido a la complejidad de este. Incluso la superioridad local puede ser impracticable debido a la forma en que se implementan las tecnologías de la información; al hecho de que los gobiernos de EE.UU. y de otros países no controlan directamente grandes porciones del ciberespacio de propiedad privada; a la amplia gama de actores estatales y no estatales; al bajo coste de entrada; y a la rápida e impredecible proliferación de la tecnología. Por tanto, los mandos deben estar preparados para llevar a cabo operaciones en condiciones degradadas en el ciberespacio. Los mandos pueden gestionar los riesgos resultantes utilizando acciones de mitigación de amenazas; medidas de recuperación tras el impacto;

prioridades defensivas claras; medios de comunicación primarios/secundarios/terciarios; y otras medidas para cumplir su misión y garantizar la fiabilidad de los datos críticos. Una vez que un segmento de una red ha sido explotado o denegado, la percepción de la falta de fiabilidad de los datos puede extenderse inapropiadamente más allá del segmento comprometido debido a la incertidumbre sobre cómo interactúan las redes. Por lo tanto, es imperativo que los comandantes estén bien informados del estado de las partes del ciberespacio de las que dependen y que comprendan el impacto en las operaciones planificadas y en curso. La necesidad expuesta en el anterior párrafo es un subconjunto de necesidades satisfechas por metodologías y/o productos de Ciber conciencia Situacional (o CYSA). (Medenou, y otros, 2020).

3.4.1.1. Ciberespacio

(DOD, CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE , FM3-12, 2021) (Medenou, y otros, 2020) (DOD, Cyberspace Operations JP3-12, 2018)

El ciberespacio es uno de los cinco dominios de la guerra […]. El ciberespacio, aunque forma parte del entorno de la información, depende de los dominios físicos aéreo, terrestre, marítimo y espacial. Al igual que las operaciones en los dominios físicos dependen de la infraestructura física creada para aprovechar las características naturales, las operaciones en el ciberespacio dependen de la infraestructura de TIC en red, independiente e integrada en la plataforma, además de los datos que residen y se transmiten a través de estos componentes para permitir las operaciones militares en un dominio creado por el hombre. Las acciones en el ciberespacio, a través de efectos en cascada cuidadosamente controlados, pueden permitir la libertad de acción de las actividades en los dominios físicos. Del mismo modo, las actividades en los dominios físicos pueden crear efectos en y a través del ciberespacio al afectar al espectro electromagnético (EMS) o a la infraestructura física.

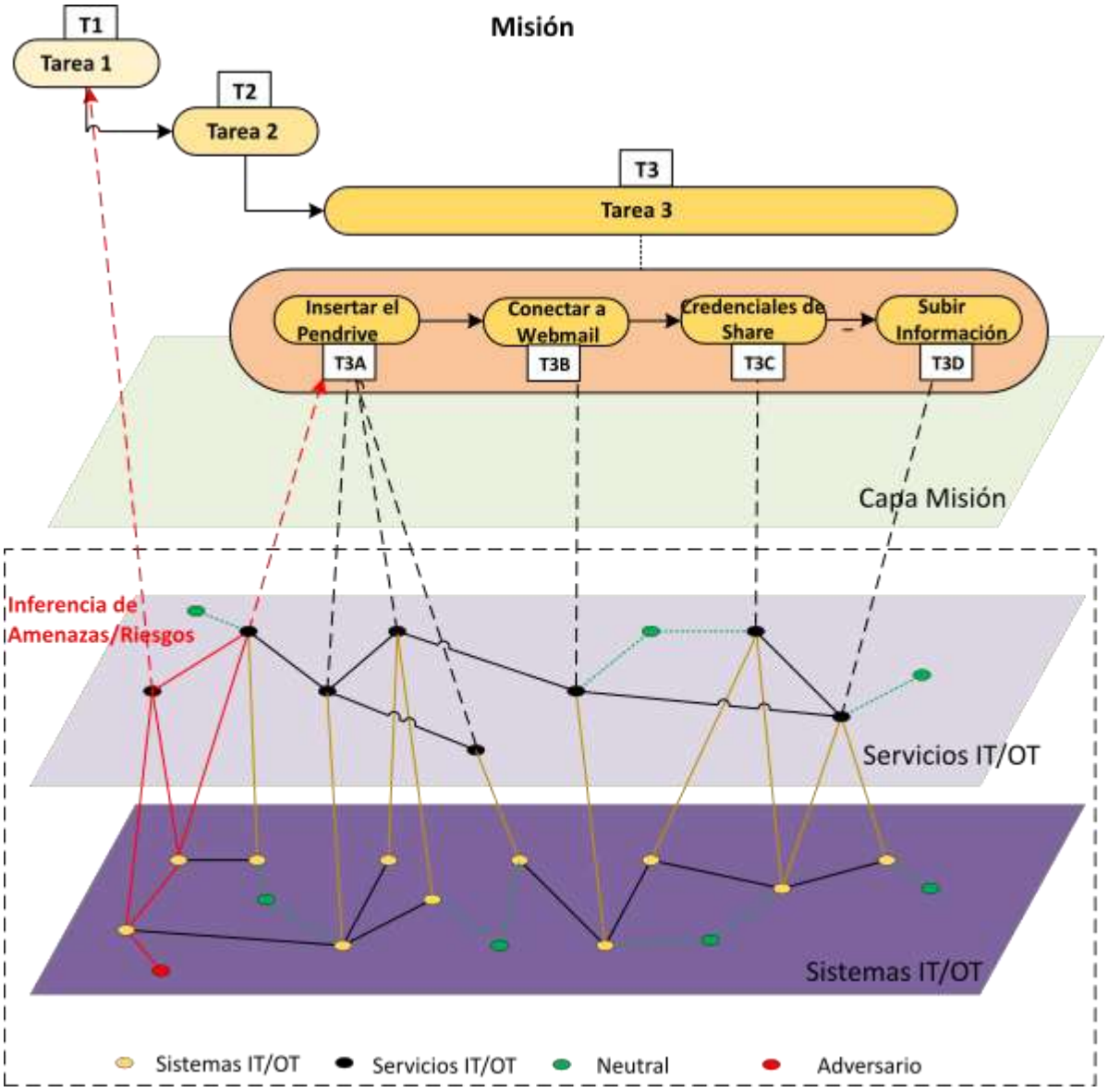


Figura 1: Grafo de Dependencia y de Propagación entre Plano Cibernético y Plano Físico y Misión; Fuente: (Sotelo Monge, Maestre Vidal, & Medenou Choumanof, 2021)

3.4.1.2. Ciber conciencia Situacional (CYSA) enfocada a Misión

(Martínez, Vidal, & González, 2021) La conciencia situacional (CS) es un estado mental humano que se refiere a ser consciente del contexto operacional y del desarrollo de acciones planificadas/en curso con el objetivo de seleccionar y planificar CoAs reactivos/proactivos más efectivos. Este término ha sido revisado activamente por Mica Endsley, que propuso el modelo de CS más adoptado en las últimas décadas. El modelo de Endsley divide la CS en tres fases principales: Percepción del entorno operativo; Comprensión de la información percibida para que sea posible la inferencia de nuevos conocimientos relacionados; y la Proyección de la CS en diferentes horizontes temporales futuros. [...] Una abstracción bien conocida del paradigma

de la CS es el modelo de bucle OODA (Observe Orient Decide Act) propuesto por el ex coronel de la UCSF John Boyd para apoyar la toma rápida de decisiones, que constituye en realidad el pilar central de las soluciones de C2. Siguiendo la filosofía de la CS acuñada, la comunidad investigadora ha realizado un importante esfuerzo para adaptar estos modelos cognitivos al ciberespacio, denominando al estado mental resultante como Ciber conciencia Situacional (CYSA). A nivel europeo, el proyecto más significativo, financiado por EC, EDA y MODS, que desarrolla capacidades de CYSA, es ECYSAP (Prensa, 2021). Como afirmaron Jajodia et al., para proteger las infraestructuras de red y las misiones críticas, debemos entender no sólo las vulnerabilidades de cada sistema individual, sino también sus interdependencias y cómo apoyan las misiones, lo que gana en dificultad cuando se opera en ecosistemas tecnológicos emergentes se combina la percepción de amenazas tanto internas como externas o se enfrenta a tácticas de evasión del adversario. Al mismo tiempo, propusieron un marco para obtener una CS centrada en la misión (Caldero) que combina la fusión de datos, las rutas de red de las vulnerabilidades, la correlación de alertas, el análisis del impacto en la misión y las acciones de mitigación reactivas/proactivas recomendadas. [...]

3.4.1.3. Ciber terreno Clave (KCT)

Según el Field Manual de Operaciones defensivas del JDP, se define el concepto de Terrenos decisivos (DT), aquellos activos y procesos que tienen prioridad máxima para la misión (i.e. su pérdida implica fracaso inmediato de la misión), mientras que los terrenos críticos (KT) como su nombre indica son esenciales para la ejecución de la misión. (Martínez, Vidal, & González, 2021) Las doctrinas militares occidentales definen un Terreno Clave como cualquier localidad o área cuya toma o retención proporciona una marcada ventaja a cualquiera de los combatientes. Esta definición se alinea con el propósito de la CS de conocer el entorno y los actores hostiles con el fin de tomar alguna ventaja para lograr el objetivo de cada misión. En CD, al desarrollar la CYSA, el concepto de terreno clave abarca el dominio cibernético con el objetivo de identificar aquellos componentes dependientes del ciberespacio que desempeñan un papel crucial para el desarrollo de una misión. Se denominan Terrenos Cibernéticos Clave (KCT). Pero a diferencia de los terrenos cinéticos convencionales, los KCT son más difíciles no sólo de defender sino también de identificar debido a su naturaleza de TIC (Tecnología de la Información y la Comunicación), que afecta a la accesibilidad. Por ejemplo, los componentes de geográficos y temporales que caracterizan a los entornos físicos pueden desaparecer por completo en el mundo digital, donde los actores hostiles pueden hacerse con el control de infraestructuras críticas a miles de kilómetros, cambiar las políticas de los sistemas en milisegundos y utilizar técnicas avanzadas de ocultación para evitar ser

descubiertos por los procedimientos convencionales de Inteligencia, Vigilancia y Reconocimiento (ISR).

3.4.1.4. Integración de las operaciones en el ciberespacio con otras operaciones

(DOD, Cyberspace Operations JP3-12, 2018)Durante la planificación conjunta, las capacidades del ciberespacio se integran en los planes de la Mando Conjunto (Mando Conjunto) y se sincronizan con otras operaciones en toda la gama de operaciones militares. Aunque no es la norma, algunos objetivos militares pueden alcanzarse sólo con el CO (Operaciones Cibernéticas). Los comandantes llevan a cabo el CO para obtener o mantener la libertad de maniobra en el ciberespacio, cumplir los objetivos del Mando Conjunto, negar la libertad de acción a la amenaza y permitir otras actividades operativas. La importancia del apoyo del CO a las operaciones militares crece en proporción directa a la creciente dependencia de las fuerzas conjuntas del ciberespacio. Entre las cuestiones que deben abordarse para integrar plenamente el CO en la planificación y ejecución conjuntas figuran la planificación centralizada del CO para las operaciones de defensa y las operaciones de defensa y otras operaciones globales; la necesidad del Mando Conjunto de integrar y sincronizar todas las operaciones y los fuegos en toda el entorno operativo, incluidos los aspectos ciberespaciales de los objetivos conjuntos; los requisitos de des conflicto entre entidades gubernamentales; las relaciones con países amigos; y la amplia variedad de autoridades y cuestiones legales relacionadas con el uso de las capacidades del ciberespacio. Esto requiere que todos los miembros del personal del comandante que realizan la planificación, la ejecución y la evaluación de las operaciones comprendan los procesos y procedimientos fundamentales del CO, incluida la organización y las funciones de las fuerzas del ciberespacio asignadas o de apoyo. La integración efectiva del CO con las operaciones en los dominios físicos requiere la participación de los planificadores y operadores de CO en cada fase de las operaciones conjuntas en cada estado mayor apoyado por las fuerzas del ciberespacio. Los límites físicos y lógicos dentro de los cuales las fuerzas conjuntas ejecutan el CO, así como las prioridades y restricciones de su uso, también deben ser identificados por el Mando Conjunto, en coordinación con otros departamentos y agencias del USG y el liderazgo nacional. En particular, la creación de efectos en el ciberespacio extranjero puede tener el potencial de afectar a otros esfuerzos del Gobierno [...]. Cuando existe la posibilidad de dicho impacto, la política nacional requiere la coordinación del MOD con los socios interinstitucionales.

3.4.1.5. Desafíos para el uso del ciberespacio por parte de la Fuerzas Aliadas

(DOD, Cyberspace Operations JP3-12, 2018) El Mando Conjunto se enfrenta a un conjunto único de desafíos persistentes en la ejecución del CO en un entorno de seguridad global complejo.

1) **Amenazas**. El ciberespacio presenta a las operaciones del JFC muchas amenazas, desde estados-nación hasta actores individuales, pasando por accidentes y peligros naturales.
   a) **Amenaza del Estado-nación**. Esta amenaza es potencialmente la más peligrosa debido al acceso de los estados-nación a recursos, personal y tiempo que pueden no estar disponibles para otros actores. Algunas naciones pueden emplear las capacidades del ciberespacio para atacar o realizar espionaje contra La Nación. Las amenazas de los estados-nación implican a los adversarios tradicionales; a los enemigos; y potencialmente, en el caso del espionaje, incluso a los aliados tradicionales. Los Estados-nación pueden llevar a cabo operaciones directamente o pueden subcontratarlas a terceros, incluyendo empresas de fachada, hackers patrióticos u otros sustitutos, para lograr sus objetivos.
   b) **Amenazas no estatales**. Las amenazas no estatales son organizaciones formales e informales que no están vinculadas por las fronteras nacionales, incluidas las organizaciones no gubernamentales (ONG) legítimas y las organizaciones ilegítimas, como las organizaciones criminales, las organizaciones extremistas violentas u otros enemigos y adversarios. Las amenazas no estatales utilizan el ciberespacio para recaudar fondos, comunicarse con el público objetivo y entre sí, reclutar, planificar operaciones, socavar la confianza en los gobiernos, realizar espionaje y llevar a cabo acciones terroristas directas dentro del ciberespacio. Las organizaciones criminales pueden ser de carácter nacional o transnacional y robar información para su propio uso, incluida su venta para recaudar capital y dirigirse a las instituciones financieras para el fraude y el robo de fondos. También pueden ser utilizadas como sustitutos por estados-nación o amenazas no estatales para llevar a cabo ataques o espionaje a través del ciberespacio.
   c) **Amenaza individual o de grupos pequeños**. Incluso individuos o pequeños grupos de personas pueden atacar o explotar el ciberespacio Nacional, gracias a técnicas y programas maliciosos asequibles y fácilmente disponibles. Sus intenciones son tan variadas como el número de grupos e individuos. Estas amenazas explotan las vulnerabilidades para acceder a descubrir otras vulnerabilidades o datos sensibles o maniobrar para conseguir otros objetivos. Los hackers éticos pueden compartir la

información sobre la vulnerabilidad con los propietarios de la red, pero, con mayor frecuencia, estos accesos se utilizan con fines maliciosos. Algunas amenazas tienen una motivación política y utilizan el ciberespacio para difundir su mensaje. Las actividades de estas amenazas a pequeña escala pueden ser cooptadas por amenazas más sofisticadas, como organizaciones criminales o estados-nación, a menudo sin su conocimiento, para ejecutar operaciones contra objetivos mientras se oculta la identidad de la amenaza/patrocinador y también se crea una negación plausible.

d) **Accidentes y riesgos naturales**. La infraestructura física del ciberespacio se ve interrumpida habitualmente por errores de los operadores, accidentes industriales y desastres naturales. Estos acontecimientos imprevisibles pueden tener un mayor impacto en las operaciones conjuntas que las acciones de los enemigos. La recuperación de accidentes e incidentes peligrosos puede ser complicada por la necesidad de una significativa coordinación ajena al MOD y/o la dependencia temporal de sistemas de respaldo con los que los operadores pueden no ser familiares.

2) **Anonimato y dificultades de atribución**. Para iniciar una respuesta defensiva adecuada, la atribución de las amenazas en el ciberespacio es crucial para cualquier acción externa al ciberespacio defendido más allá de la autorizada como autodefensa. El aspecto más desafiante de la atribución de acciones en el ciberespacio es la conexión de una persona o acción cibernética particular con un individuo, grupo o nación-estado, con suficiente confianza y verificabilidad para hacerlos responsables. Este esfuerzo requiere un análisis importante y, a menudo, la colaboración con agencias u organizaciones ajenas al ciberespacio. La naturaleza del ciberespacio, las políticas gubernamentales y las leyes, tanto nacionales como internacionales, plantean retos para determinar el origen exacto de las amenazas del ciberespacio. La capacidad de ocultar al comendatario y/o la amenaza detrás de un efecto malicioso concreto en el ciberespacio dificulta la determinación de cómo, cuándo y dónde responder. El diseño de Internet propicia al anonimato y, combinado con las aplicaciones destinadas a ocultar la identidad de los usuarios, la atribución seguirá siendo un reto en el futuro próximo.

3) **Desafíos geográficos.** En el ciberespacio no existe un espacio de maniobras no afiliado a un Estado-nación. Por lo tanto, cuando las fuerzas militares aliadas maniobran en el ciberespacio extranjero, los requisitos de la misión y de la política pueden requerir que maniobren clandestinamente sin el conocimiento del estado donde se encuentra la infraestructura. Dado que las OC a menudo pueden ejecutarse a distancia, a través de una presencia virtual posibilitada por vías digitales o analógicas, muchas OC no requieren la proximidad física al objetivo, sino que utilizan acciones remotas para crear efectos, lo que representa un aumento del alcance operativo no disponible en los dominios físicos.

Este uso del alcance global se aplica igualmente a las operaciones externas en el ciberespacio rojo y gris, así como a los efectos de protección interna en el ciberespacio azul. Los efectos propagados de algunas OC pueden extenderse más allá del objetivo inicial, de un área de operaciones conjuntas (JOA), o fuera de una única área de responsabilidad (AOR). Debido a las consideraciones transregionales y a la necesidad de fuerzas y capacidades de alta demanda, algunas OC se coordinan, integran y sincronizan utilizando la ejecución centralizada desde una ubicación remota de soporte al mando.

4) **Desafíos tecnológicos.** El uso de una capacidad cibernética que depende de la explotación de las vulnerabilidades técnicas del objetivo puede revelar su funcionalidad y comprometer la eficacia de la capacidad para futuras misiones. Esto tiene implicaciones para las misiones de operaciones cibernéticas ofensivas (OCO) y defensivas (DCO). Las capacidades del ciberespacio sin componentes de hardware pueden reproducirse por un coste mínimo o nulo. Esto significa que, una vez descubiertas, estas capacidades estarán ampliamente disponibles para los adversarios, en algunos casos antes de que las medidas de seguridad en los Sistemas Informáticos Amigos puedan ser actualizadas para tener en cuenta la nueva amenaza. Además, dado que tecnologías similares en todo el mundo comparten vulnerabilidades similares, un solo adversario puede ser capaz de explotar varios objetivos a la vez utilizando el mismo malware o táctica de explotación. El malware puede modificarse (o estar diseñado para modificarse automáticamente), lo que complica los esfuerzos para detectarlo y erradicarlo.
5) **Colaboración Publico Privada.** Muchas de las funciones y operaciones críticas del MOD dependen de activos comerciales contratados, incluidos los proveedores de servicios de Internet (ISP) y las cadenas de suministro globales, sobre las que el MOD y sus fuerzas no tienen autoridad directa. Esto incluye tanto los servicios de almacenamiento de datos como las aplicaciones proporcionadas desde una arquitectura de computación en nube. La computación en nube permite al MOD consolidar la infraestructura, aprovechar las funciones de TI básicas y eliminar las redundancias funcionales a la vez que mejora la continuidad de las operaciones. Sin embargo, el éxito general de estas iniciativas depende de unas medidas de protección y mitigación de riesgos bien ejecutadas, definidas y compuestas tanto por los componentes del MOD como por la industria. La dependencia de los proveedores comerciales de Internet significa que la coordinación del MOD con el Ministerio de Interior, otros socios interinstitucionales y el sector privado es esencial para establecer y mantener la seguridad de la información del MOD. El MOD apoya al Ministerio de Interior, que lidera los esfuerzos interinstitucionales para identificar y mitigar las vulnerabilidades del ciberespacio en las infraestructuras críticas de la nación. El MOD lidera la mejora de la seguridad del sector de la base industrial de defensa (DIB), que incluye a los principales contratistas del sector y al apoyo de los principales contratistas a

las operaciones, independientemente del país de domicilio de la empresa, y sigue apoyando el desarrollo de enfoques de todo el gobierno para su gestión de riesgos. La cadena global de suministro de tecnología afecta a aspectos de misión crítica de la empresa del MOD, y los riesgos informáticos resultantes sólo pueden mitigarse eficazmente mediante la cooperación entre el sector público y el privado.

6) **Uso proporcional de la fuerza:** cumplimento de RoEs, teoría de guerra justa, etc. sin poder medir efectos, sin poder atribuir acciones, sin poder revertir acciones, etc.

De cara al ciberespacio el Manual de Tallin (Schmitt, 2017), y la naturaleza misma de los riesgos cibernéticos (OpenGROUP, 2021) cabe destacar adicionalmente varias familias de desafíos:

1) **Propagación en cascada:** la propagación de impacto en plano ciber físico, Político, económico, diplomático implica a menudo impactos secundarios difícilmente medibles sin sistemas informáticos explícitamente diseñados para ellos. La presencia de impactos secundarios en guerra de la información dificulta medir la proporcionalidad, y el efecto que ha tenido un fuego en el plano cibernético.
2) **Tiempo de respuesta e incertidumbre:** El ritmo de batalla no siempre permite que un humano pueda realizar decisiones suficientemente rápidas, o por lo menos no lo puede hacer sin herramientas informáticas adecuadas.
3) **Preservar el orden de batalla y cadena de mando:** del punto anterior, hay que encontrar un punto de equilibrio entre la preservación de cadena de mando y la automatización de ciertas CoAs y contramedidas. La atribución de responsabilidad en el caso de sistemas semiautomáticos aún sigue siendo un terreno muy discutido en Derecho Militar y Civil.

3.4.2. Actividades Básicas de las Operaciones Cibernéticas

3.4.2.1. Descripción

(DOD, Cyberspace Operations JP3-12, 2018)

- Las OC son el empleo de las capacidades del ciberespacio cuando el propósito principal es lograr objetivos en o a través del ciberespacio. Las OC engloban las operaciones militares, de inteligencia nacional y de negocios ordinarios del MOD en el ciberespacio. Aunque los comandantes necesitan conocer el impacto potencial de los otros tipos de CO del MOD en sus operaciones, el componente militar de CO es el único guiado por la doctrina conjunta y es el foco de esta publicación. Los Mandos de Campos y los Servicios utilizan el CO para crear efectos en el ciberespacio en apoyo

de los objetivos militares. Las operaciones militares en el ciberespacio se organizan en misiones ejecutadas a través de una combinación de acciones específicas que contribuyen a lograr el objetivo del comandante. Varias agencias y componentes del MOD llevan a cabo actividades de inteligencia nacional, negocios ordinarios y otras actividades en el ciberespacio. Aunque se discuten brevemente aquí para contextualizarlas, estas actividades se rigen por las políticas del MOD relativas al CO. Si bien la doctrina conjunta se aplica a los CSA cuando se relaciona directamente con su misión de apoyo a las fuerzas militares, los CSA y otros organismos y actividades del MOD también realizan diversas actividades de CO que se consideran actividades habilitadas para operar en el ciberespacio.

- **Actividades habilitadas para operar en el ciberespacio**. La mayoría de las acciones del MOD en el ciberespacio utilizan el ciberespacio para permitir otros tipos de actividades, que emplean las capacidades del ciberespacio para completar las tareas, pero no se llevan a cabo como parte de una de las tres misiones CO: Operaciones OCO, DCO o Sistemas Informáticos Aliados. Estos usos incluyen acciones como el funcionamiento de un sistema C2 o logístico, el envío de un correo electrónico para apoyar un objetivo de información, el uso de Internet para completar un curso de formación en línea, o el desarrollo de una sesión informativa. Aparte de ser un usuario autorizado de la red, el personal del MOD no necesita ninguna autoridad especial para utilizar las capacidades del ciberespacio de esta manera. Es a través de estos usos del ciberespacio que la mayoría de las vulnerabilidades de los Sistemas Informáticos Aliados están expuestas a, y son explotadas por, nuestros adversarios. El reto consiste en formar a todos los usuarios del Sistemas Informáticos Aliados para que comprendan la importancia de las amenazas del ciberespacio y reconozcan las tácticas de las amenazas, de modo que estos usos del ciberespacio no creen un riesgo innecesario para la misión. La protección de la Sistemas Informáticos Aliados mediante el establecimiento de una cultura de concienciación sobre la vulnerabilidad, especialmente a través del MOD y las políticas, prácticas y formación interinstitucionales son fundamentales para el éxito de todo tipo de misiones del MOD relacionadas con el ciberespacio.

3.4.2.2. Operaciones militares en el ciberespacio

(DOD, Cyberspace Operations JP3-12, 2018)

1) **Misiones del ciberespacio.** Todas las acciones en el ciberespacio que no son actividades habilitadas para operar en el ciberespacio se realizan como parte de una de las tres misiones del ciberespacio: Operaciones OCO, DCO o Sistemas Informáticos Aliados.

Estos tres tipos de misiones abarcan de forma global las actividades de las fuerzas del ciberespacio. La ejecución con éxito de la OC requiere la integración y sincronización de estas misiones. Las misiones militares en el ciberespacio y las acciones que incluyen se autorizan normalmente mediante una orden militar (por ejemplo, orden de ejecución [EXORD], orden de operación [OPORD], orden de asignación de tareas, orden verbal), denominada en lo sucesivo orden de misión, y por la autoridad derivada del memorando, la directiva o la instrucción de política del MOD. Las misiones en el ciberespacio se clasifican como operaciones OCO, DCO o Sistemas Informáticos Aliados basándose únicamente en la intención u objetivo de la autoridad emisora, y no en las acciones ciberespaciales ejecutadas, el tipo de autoridad militar utilizada, las fuerzas asignadas a la misión o las capacidades ciberespaciales utilizadas. Algunas órdenes pueden abarcar varios tipos de misiones. Por ejemplo, una orden permanente para proteger el Sistemas Informáticos Aliados puede incluir componentes de misión de operaciones de los Sistemas Informáticos Aliados y del DCO, y una orden para una misión externa podría apoyar tanto objetivos ofensivos como defensivos. [...] La ejecución eficaz de todas las misiones en el ciberespacio requiere indicadores de inteligencia y de amenaza oportunos procedentes de sensores tradicionales y del ciberespacio, información sobre la vulnerabilidad procedente de fuentes del MOD y ajenas al mismo, y una evaluación precisa de las misiones anteriores. [...]

a) **Operaciones en Sistemas Informáticos Aliados.** La misión de las operaciones de los Sistemas Informáticos Aliados incluye acciones operativas tomadas para asegurar, configurar, operar, extender, mantener y sostener el ciberespacio del Sistemas Informáticos Aliados y para crear y preservar la confidencialidad, disponibilidad e integridad de los Sistemas Informáticos Aliados. Esto incluye acciones proactivas de seguridad del ciberespacio que abordan las vulnerabilidades de los Sistemas Informáticos Aliados o de segmentos específicos de los Sistemas Informáticos Aliados. También incluye la creación de redes tácticas por parte de las fuerzas desplegadas para ampliar las redes existentes, las acciones de mantenimiento y otras acciones no relacionadas con la seguridad necesarias para el mantenimiento de los Sistemas Informáticos Aliados, y el funcionamiento de los equipos rojos y otras formas de evaluación y pruebas de seguridad. Las operaciones en los Sistemas Informáticos Aliados se centran en la red y son agnósticas en cuanto a las amenazas: las fuerzas y el personal del ciberespacio que llevan a cabo esta misión se esfuerzan por evitar que todas las amenazas afecten negativamente a una red o sistema concreto que se les ha asignado para proteger. Se informan de las amenazas y utilizan toda la inteligencia disponible sobre amenazas específicas para mejorar la postura de seguridad de la red. Las operaciones MOD no incluyen las acciones tomadas bajo la

autoridad estatutaria de un jefe de información (CIO) para proporcionar el ciberespacio para las operaciones, incluyendo el desarrollo de la arquitectura de TIC; el establecimiento de normas; o el diseño, la construcción, o la puesta en marcha de TIC del MOD para su uso por un comandante. Las operaciones MOD son una misión permanente, y aunque muchas de las actividades de las operaciones sobre Sistemas Informáticos Aliado son eventos programados regularmente, no pueden considerarse rutinarias, ya que su efecto agregado establece el marco del que dependen en última instancia la mayoría de las misiones del MOD.

b) **Operaciones Cibernéticas Defensivas (DCO).** Las misiones DCO se ejecutan para defender los Sistemas Informáticos Aliados, u otro ciberespacio que las fuerzas del ciberespacio del MOD hayan recibido la orden de defender, de amenazas activas en el ciberespacio. Específicamente, son misiones destinadas a preservar la capacidad de utilizar las capacidades del ciberespacio azul y proteger los datos, las redes, los dispositivos habilitados para el ciberespacio y otros sistemas designados, derrotando la actividad cibernética maliciosa en curso o inminente. Esto distingue las misiones DCO, que derrotan amenazas específicas que han evadido, violado o amenazan con violar las medidas de seguridad, de las operaciones sobre Sistemas Informáticos Aliados, que se esfuerzan por proteger el ciberespacio del MOD de todas las amenazas antes de cualquier actividad de amenaza específica. Las DCO son específicas para cada amenaza y suelen apoyar los objetivos de aseguramiento de la misión. Las misiones DCO se llevan a cabo en respuesta a amenazas específicas de ataque, explotación u otros efectos de la actividad maliciosa en el ciberespacio y aprovechan la información de maniobra de la colección, de la contrainteligencia (CI), de la aplicación de la ley (LE), y de otras fuentes según sea necesario. Los DCO incluyen la superación o interdicción de adversarios que toman o están a punto de tomar acciones contra elementos defendidos del ciberespacio, o que responden de otra manera a las amenazas inminentes del ciberespacio interno y externo. El objetivo del DCO es derrotar la amenaza de un adversario específico y/o devolver una red comprometida a un estado seguro y funcional.

c) **Operaciones Cibernéticas Ofensivas (OCO).** Las OCO son misiones de CO destinadas a proyectar poder en y a través del ciberespacio extranjero mediante acciones realizadas en apoyo de los objetivos nacionales o de los Mandos de Campo. Las OCO pueden dirigirse exclusivamente a las funciones del ciberespacio del adversario o crear efectos de primer orden en el ciberespacio para iniciar efectos en cascada cuidadosamente controlados en los dominios físicos para afectar a los sistemas de armas, los procesos de C2, los nodos logísticos, los objetivos de alto valor, etc. Todas las misiones de CO llevadas a cabo fuera del ciberespacio azul con la

intención de un comandante que no sea defender el ciberespacio azul de una amenaza cibernética en curso o inminente son misiones de OCO. Al igual que las misiones DCO-RA (DCO reactivas), algunas misiones OCO pueden incluir acciones que alcanzan el nivel de uso de la fuerza, con daños físicos o destrucción de sistemas enemigos. Los efectos específicos creados dependen del contexto operacional más amplio, como la existencia o inminencia de hostilidades abiertas y las consideraciones de política nacional. Las misiones OCO requieren una orden militar debidamente coordinada y una cuidadosa consideración del alcance, las reglas de juego y los objetivos medibles.

2) **Acciones en el ciberespacio**. La ejecución de cualquier misión de operaciones OCO, DCO o sobre Sistemas Informáticos Aliados requiere la realización de acciones o tareas específicas a nivel táctico que emplean las capacidades del ciberespacio para crear efectos en el ciberespacio. Todos los objetivos de la misión del ciberespacio se logran mediante la combinación de una o más de estas acciones, que se definen exclusivamente por los tipos de efectos que crean. Para planificar, autorizar y evaluar estas acciones, es importante que el comandante y el personal entiendan claramente qué acciones han sido autorizadas bajo su orden de misión actual. Por ejemplo, la transición de las operaciones sobre Sistemas Informáticos Aliados a las misiones DCO-IDM (Operaciones Cibernéticas de Medidas Defensivas Internas) puede tener que ocurrir rápidamente siempre que los Sistemas Informáticos Aliados estén amenazados y los operadores del ciberespacio comiencen a tomar acciones de defensa del ciberespacio. Para permitir y sincronizar esta transición y las subsiguientes acciones de defensa del ciberespacio, se necesitan órdenes claras que comuniquen a los operadores del ciberespacio las limitaciones, restricciones y autoridades aplicables. Dado que siempre serán necesarias, las órdenes permanentes para las operaciones Sistemas Informáticos Aliados y las misiones DCO-IDM cubren la mayoría de las acciones de seguridad y defensa inicial del ciberespacio. Sin embargo, las misiones OCO y DCO-RA son episódicas. Pueden requerir acciones clandestinas de maniobra y recolección o pueden requerir acciones abiertas, incluyendo fuegos. Por lo tanto, la aprobación de las acciones CO en el ciberespacio extranjero requiere autoridades de misión OCO o DCO-RA separadas. Las acciones efectuables en el ciberespacio son:

   a) **Protección del ciberespacio.** Las acciones de protección del ciberespacio se llevan a cabo dentro del ciberespacio protegido para derrotar las amenazas específicas que han violado o amenazan con violar las medidas de seguridad del ciberespacio e incluyen acciones para detectar, caracterizar, contrarrestar y mitigar las amenazas, incluyendo el malware o las actividades no autorizadas de los usuarios, y para restaurar el sistema a una configuración segura. El CCMD (Mando de Combate), el Servicio o la agencia del MOD que posee u opera la red está generalmente autorizado a tomar estas acciones defensivas, excepto en los casos en que comprometan las

operaciones de elementos del ciberespacio fuera de la responsabilidad del respectivo CCMD, Servicio o agencia. En algunos casos, se asignará un CPT (equipo de Ciberdefensa) para asistir en las acciones de reaseguramiento y mitigación. El Centro de Mando Conjunto de Sistemas Informáticos Aliados coordina todas las acciones defensivas que afectan a más de un CCMD o que tienen impactos fuera del ámbito del propietario de la red. Las acciones de protección del ciberespacio son las acciones componentes de una misión DCO-IDM. Dado que el mismo personal suele realizar acciones de seguridad y protección del ciberespacio, estas acciones se denominan colectivamente protección.

b) **Explotación del ciberespacio.** Las acciones de explotación del ciberespacio incluyen actividades de inteligencia militar, maniobras, recopilación de información y otras acciones de apoyo necesarias para preparar futuras operaciones militares. Las acciones de explotación del ciberespacio se realizan como parte de una misión OCO o DCO-RA e incluyen todas las acciones en el ciberespacio gris o rojo que no crean efectos de ataque en el ciberespacio. La explotación del ciberespacio incluye actividades para obtener inteligencia y apoyar la preparación operativa del entorno para las operaciones actuales y futuras a través de acciones como la obtención y el mantenimiento del acceso a redes, sistemas y nodos de valor militar; la maniobra hacia posiciones de ventaja; y el posicionamiento de las capacidades del ciberespacio para facilitar las acciones de seguimiento. La explotación del ciberespacio también apoya las operaciones actuales y futuras a través de la recopilación de información, incluyendo el mapeo del ciberespacio rojo y gris para apoyar el conocimiento de la situación; descubriendo vulnerabilidades; permitiendo el desarrollo de objetivos; y apoyando la planificación, ejecución y evaluación de las operaciones militares. Las acciones de explotación del ciberespacio se coordinan con otros departamentos y agencias del Gobierno Nacional de acuerdo con la política nacional.

c) Ataque al ciberespacio. Las acciones de ataque al ciberespacio crean efectos de denegación perceptibles (es decir, degradación, interrupción o destrucción) en el ciberespacio o manipulación que conduce a efectos de denegación en los dominios físicos. A diferencia de las acciones de explotación del ciberespacio, que a menudo pretenden permanecer clandestinas para ser efectivas, las acciones de ataque al ciberespacio serán evidentes para los operadores o usuarios del sistema, ya sea inmediata o eventualmente, ya que eliminan alguna funcionalidad del usuario. Las acciones de ataque al ciberespacio son una forma de fuegos, se toman como parte de una misión OCO o DCO-RA, se coordinan con otros departamentos y agencias del Gobierno de La Nación, y se sincronizan cuidadosamente con los fuegos planificados en los dominios físicos. Incluyen acciones para:

i) **Denegar.** Impedir el acceso, la operación o la disponibilidad de una función de destino por un nivel específico durante un tiempo determinado, por:
   (1) Degradar. Negar el acceso o el funcionamiento de un objetivo hasta un nivel representado como un porcentaje de la capacidad. Se especifica el nivel de degradación. Si se requiere un tiempo específico, se puede especificar.
   (2) Interrumpir. Impedir totalmente pero temporalmente el acceso o el funcionamiento de un objetivo durante un periodo de tiempo. Normalmente se especifica un tiempo de inicio y de finalización deseado. La interrupción puede considerarse un caso especial de degradación en el que el nivel de degradación es del 100%.
   (3) Destruir. Negar completa e irremediablemente el acceso o el funcionamiento de un objetivo. La destrucción maximiza el tiempo y la cantidad de negación. Sin embargo, la destrucción tiene un alcance acorde con la duración de un conflicto, ya que muchos objetivos, con suficiente tiempo y recursos, pueden ser reconstituidos.

ii) **Manipular.** La manipulación, como forma de ataque al ciberespacio, controla o cambia la información, los sistemas de información y/o las redes en el ciberespacio gris o rojo para crear efectos de negación física, utilizando el engaño, el señuelo, el condicionamiento, la suplantación, la falsificación y otras técnicas similares. Utiliza los recursos de información del adversario con fines amistosos, para crear efectos de negación que no son inmediatamente evidentes en el ciberespacio. La red atacada puede parecer que funciona con normalidad hasta que los efectos secundarios o terciarios, incluidos los físicos, revelan la evidencia del efecto lógico de primer orden.

iii) **Contramedidas en el ciberespacio**. Las contramedidas son la forma de la ciencia militar que, mediante el empleo de dispositivos y/o técnicas, tiene como objetivo el menoscabo de la eficacia operativa de la actividad del enemigo. En el ciberespacio, el término se aplica a cualquier acción del CO que se ajuste a la descripción del término, independientemente del lugar en el que se tome la contramedida. Al igual que en los dominios físicos, las acciones de contramedidas pueden tomarse tanto en el interior como en el exterior del terreno defendido y pueden utilizarse de forma preventiva o reactiva. Las contramedidas internas son acciones de defensa del ciberespacio tomadas como parte de una misión DCO-IDM; por ejemplo, cerrar los puertos del router que está utilizando un adversario para el acceso no autorizado o bloquear el malware que está balizando fuera del Sistemas Informáticos Aliados. Las contramedidas externas, que formarían parte de una misión DCO-RA u OCO, se emplean más allá de los límites del Sistemas Informáticos Aliados contra una

actividad cibernética maliciosa específica. En apoyo de una misión OCO, pueden ser acciones de ataque al ciberespacio que falsifican o anulan de otro modo la eficacia de los sensores o defensas del adversario. Como parte de una misión DCO-RA, pueden utilizarse para identificar el origen de una amenaza y/o utilizar técnicas no intrusivas o mínimamente intrusivas para interceptar o mitigar las amenazas. Las contramedidas defensivas externas son normalmente de naturaleza no destructiva/no letal, suelen afectar sólo a la actividad maliciosa pero no a los sistemas de amenaza asociados y terminan cuando la amenaza cesa. Todas las contramedidas externas están sujetas a las mismas directrices de sincronización, desconflicción, legales y políticas que cualquier otro aspecto de una misión OCO o DCO-RA.

iv) Respecto de las **actividades del adversario en el ciberespacio**. Los términos de planificación del CO del DOD pueden no describir con exactitud las acciones de nuestros adversarios y enemigos en el ciberespacio porque sus objetivos de misión y la intención del comandante pueden no conocerse con certeza. Por lo tanto, el término “actividad maliciosa en el ciberespacio” se refiere a todas esas actividades. Si el contexto de la discusión requiere descripciones más específicas de esta actividad, utilice términos genéricos (por ejemplo, ataque, explotación, sabotaje, maniobra), dependiendo de los efectos específicos de las acciones maliciosas.

3.4.2.3. Operaciones de inteligencia nacional en el ciberespacio

Las organizaciones de inteligencia a nivel nacional llevan a cabo actividades de inteligencia en, a través de y sobre el ciberespacio en respuesta a las prioridades nacionales de inteligencia. Esta inteligencia puede apoyar la planificación y preparación de un comandante militar. Aunque las fuerzas del ciberespacio del MOD pueden recopilar información útil desde el punto de vista táctico y operativo mientras maniobran hacia y a través del ciberespacio extranjero, al igual que todas las fuerzas conjuntas, también dependen del apoyo de inteligencia de las fuentes de inteligencia militares y nacionales tradicionales.

3.4.2.4. Operaciones comerciales ordinarias del MOD en el ciberespacio

Las operaciones comerciales ordinarias en y a través del ciberespacio son “actividades habilitadas por el ciberespacio” que comprenden aquellas capacidades, funciones y acciones no relacionadas con la inteligencia y la lucha bélica que se utilizan para apoyar y sostener a

las fuerzas y componentes del MOD. Esto incluye las funciones habilitadas por el ciberespacio de las agencias y actividades civiles del MOD. Dado que la realización de las operaciones comerciales ordinarias del MOD en el ciberespacio se rige por la política del MOD y no, en general, por la doctrina conjunta, no se analiza aquí en detalle. Sin embargo, las vulnerabilidades que pueden existir en las aplicaciones y dispositivos utilizados para las operaciones comerciales ordinarias del MOD podrían ser explotadas de una manera que afecta directamente a la misión de un comandante militar. Dado que las agencias y actividades del MOD utilizan muchas de las mismas redes que los mandos militares, un compromiso en cualquier área de los Sistemas Informáticos Aliados utilizados para las operaciones comerciales podría resultar en una pérdida de la seguridad de la misión en el ciberespacio para las operaciones militares.

3.4.2.5. Las funciones conjuntas y las operaciones en el ciberespacio

1) **Mando y Control (C2).** La discusión sobre el C2 y el ciberespacio requiere una distinción entre el uso de sistemas cibernéticos que implementan el C2 de las operaciones militares y el C2 de las fuerzas que ejecutan el CO. [...] El C2 abarca el ejercicio de la autoridad y la dirección por parte de los comandantes sobre las fuerzas asignadas y adscritas en el cumplimiento de su misión. El uso del ciberespacio como medio de intercambio de comunicaciones es el método más común en los niveles estratégico y operativo de la guerra y es cada vez más importante en la guerra táctica. Los métodos de comunicación digital han suplantado en gran medida a las comunicaciones analógicas, excepto en el nivel táctico, donde se mantienen los métodos de señalización analógica. Es probable que las comunicaciones analógicas persistan indefinidamente en las operaciones tácticas por razones de simplicidad, fiabilidad y seguridad. Sin embargo, los sistemas militares de C2 que funcionan mediante la transmisión de datos digitales forman parte de los Sistemas Informáticos Aliados. El ciberespacio proporciona vías de comunicación, ayudas a la planificación y a la toma de decisiones, e inteligencia relacionada con el ciberespacio para permitir la toma de decisiones y la ejecución de estas en el momento oportuno. Esto proporciona al comandante la ventaja de controlar el tiempo y el ritmo de las operaciones. El ciberespacio ofrece una gama excepcionalmente diversa de circuitos para la emisión de órdenes y señales a las fuerzas y para que éstas transmitan la información operativa a la cadena de mando. Las órdenes militares convertidas a formato digital, incluyendo la voz y el vídeo digitales, pueden viajar por circuitos que transitan por todos los dominios físicos, lo que aumenta significativamente la probabilidad de entrega oportuna. Sin embargo, la confianza de un comandante en el sistema C2 puede verse fácilmente comprometida

cuando la seguridad de los Sistemas Informáticos Aliados se vuelve sospechosa; por lo tanto, cuanto más dependa el comandante del ciberespacio para el C2, más importante es la protección de los activos del ciberespacio de apoyo para esta función conjunta.

2) **Inteligencia.** La comprensión del entorno operativo (OE) es fundamental para todas las operaciones conjuntas, incluyendo el CO. La inteligencia puede derivarse de la información obtenida durante las operaciones militares en el ciberespacio o de otras fuentes. [...] El apoyo de inteligencia de todas las fuentes al CO utiliza el mismo proceso de inteligencia utilizado por todas las demás operaciones militares, con atributos únicos necesarios para el apoyo a la planificación del CO.
   a) Planificación y dirección, para incluir la identificación de las vulnerabilidades de los objetivos para permitir la planificación continua y la dirección de las actividades de CI para proteger contra el espionaje, el sabotaje y los ataques contra los misión MILCYBDEC/instalaciones nacionales y examinar continuamente los criterios de éxito de la misión y las métricas asociadas para evaluar el impacto de la OC e informar las decisiones del comandante.
   b) Sensores de recogida con acceso a información sobre el ciberespacio.
   c) Procesamiento y explotación de los datos recogidos, incluida la identificación de información útil a partir de los datos recogidos, ya sea en tiempo real o a posteriori
   d) Análisis de la información y elaboración de productos de inteligencia.
   e) Difusión e integración de la inteligencia relacionada con el ciberespacio con las operaciones.
   f) Evaluación y retroalimentación sobre la eficacia y la calidad de la inteligencia.
3) **Fuegos**. Las capacidades de ataque al ciberespacio crean Fuegos en el ciberespacio y a menudo se emplean con poca o ninguna destrucción física asociada. Sin embargo, la modificación o destrucción de los ordenadores que controlan los procesos físicos puede provocar efectos en cascada (incluidos los efectos colaterales) en los dominios físicos. Dependiendo del objetivo del comandante, los fuegos en el ciberespacio pueden ser ofensivos o defensivos, de apoyo o de soporte. Al igual que todas las formas de fuego, los fuegos en el ciberespacio deben incluirse en los procesos de planificación y ejecución conjuntos para facilitar la sincronización y la unidad de esfuerzo y deben cumplir con la ley de la guerra y las ROE (Reglas de Enfrentamiento). Los fuegos en y a través del ciberespacio abarcan una serie de tareas, acciones y procesos, incluyendo la selección de objetivos, la coordinación y la desconflicción. Si varias entidades del Gobierno Nacional o aliadas tienen requisitos para crear efectos o recopilar información sobre el mismo objetivo en el ciberespacio, se requerirá la sincronización y la desconflicción de todas las entidades del Gobierno Nacional, ya que, de lo contrario, sus acciones no coordinadas podrían exponerse o interferir entre sí. Incluso si los efectos pueden crearse de forma

independiente y están suficientemente justificados, sigue siendo necesario un análisis técnico para determinar si las capacidades pueden operar según lo previsto en el mismo entorno sin interferir o aumentar las posibilidades de detección no deseada.

4) **Movimiento y Maniobra:** El movimiento y las maniobras implican el despliegue de fuerzas y capacidades en una OA y el posicionamiento dentro de esa zona para obtener una ventaja operativa en apoyo de los objetivos de la misión, incluido el acceso y, en caso necesario, el control del terreno clave. Las operaciones en el ciberespacio permiten la proyección de fuerzas sin necesidad de establecer una presencia física en territorio extranjero. Las maniobras en los Sistemas Informáticos Aliados u otro ciberespacio azul incluyen el posicionamiento de fuerzas, sensores y defensas para asegurar mejor las áreas del ciberespacio o participar en acciones defensivas según sea necesario. La maniobra en el ciberespacio gris y rojo es una acción de explotación del ciberespacio e incluye actividades como la obtención de acceso a los enlaces y nodos adversarios, enemigos o intermediarios y la configuración de este ciberespacio para apoyar futuras acciones. La capacidad de acceder o incluso de controlar este terreno puede cambiar el resultado de un compromiso. Un factor importante en la maniobrabilidad en el ciberespacio es obtener y mantener el acceso lógico al entorno. Esta capacidad de maniobra y alcance operativo puede perderse en cualquier momento si se modifica la configuración de los nodos del ciberespacio correspondientes. La naturaleza ubicua del ciberespacio crea otra consideración importante, porque permite a un adversario o enemigo establecer puntos clave de presencia fuera de la OA física, en terceros países, áreas protegidas o incluso nacionales. Además, los adversarios o enemigos pueden llevar a cabo CO desde conexiones de red físicas nacional, PNs, o naciones de terceros, limitando así el espacio de maniobra del Mando Conjunto basado en la ley y la restricción de la política y creando dependencias en nuestra capacidad de coordinar con la interagencia y otros socios de la misión. Otro componente de la maniobra en el ciberespacio es la capacidad de trasladar los datos a un lugar o proceso en el que tengan la máxima utilidad militar, incluyendo el movimiento de los datos fuera de peligro y hacia un lugar o proceso seguro. Debido a las latencias de la red y a las diferencias de rendimiento entre los modelos de mensajería del sistema, los almacenes de datos remotos suelen ser más lentos que los locales. Esto podría marcar la diferencia entre el éxito y el fracaso en la OC. En este contexto, tener acceso a un ancho de banda seguro por cable o inalámbrico es análogo a mantener las líneas de comunicación (LOC) en los dominios físicos. La capacidad de desviar el flujo de datos de un enlace físico a otro frente a las amenazas, por ejemplo, de los cables terrestres a los enlaces de comunicaciones por satélite (SATCOM), es un ejemplo de libertad de maniobra en el ciberespacio. Por lo tanto, la gestión del EMS (espacio electromagnético) dentro del espacio de batalla es una consideración de planificación clave para el CO. Otro

componente de la maniobra en el ciberespacio es la capacidad de trasladar los datos a un lugar o proceso en el que tengan la máxima utilidad militar, incluyendo el movimiento de los datos fuera de peligro y hacia un lugar o proceso seguro. Debido a las latencias de la red y a las diferencias de rendimiento entre los modelos de mensajería del sistema, los almacenes de datos remotos suelen ser más lentos que los locales. Esto podría marcar la diferencia entre el éxito y el fracaso en la OC. En este contexto, tener acceso a un ancho de banda seguro por cable o inalámbrico es análogo a mantener las LOC en los dominios físicos. La capacidad de desviar el flujo de datos de un enlace físico a otro frente a las amenazas, por ejemplo, de los cables terrestres a los enlaces de comunicaciones por satélite (SATCOM), es un ejemplo de libertad de maniobra en el ciberespacio. Por lo tanto, la gestión del EMS dentro del espacio de batalla es una consideración de planificación clave para las CO.

5) Sostenimiento:

a) El sostenimiento es la provisión de servicios logísticos y de personal para mantener las operaciones hasta el cumplimiento de la misión y el redespliegue de la fuerza. Desde la perspectiva de las actividades habilitadas por el ciberespacio en apoyo de la logística global, el DOD depende de los segmentos protegidos de Sistemas Informáticos Aliados y de la red comercial para coordinar el mantenimiento de las fuerzas.

b) Los rápidos avances en TIC exigen el desarrollo, el despliegue y el mantenimiento de capacidades cibernéticas adaptables a la cambiante OE. Por ejemplo, los dispositivos móviles seguros e inalámbricos proporcionan anonimato a los usuarios de Internet del adversario; un adversario puede actualizar o cambiar los sistemas operativos; o puede pasar a utilizar máquinas virtuales más seguras en su arquitectura de red. Las fuerzas conjuntas necesitan la capacidad de adaptarse incorporando rápidamente nuevas capacidades cibernéticas a su arsenal. Además, la fuerza conjunta puede necesitar la capacidad de actualizar rápidamente su propio ciberespacio para aprovechar estas mismas nuevas tecnologías. Sin embargo, la presión para desplegar la nueva tecnología debe equilibrarse con el potencial de aumento del riesgo y los requisitos de la política de ciberseguridad, y la implementación debe ser cuidadosamente orquestada para evitar la divergencia entre el ciberespacio proporcionado por el Servicio que podría crear vulnerabilidades en la arquitectura de Sistemas Informáticos Aliados.

c) La planificación del mantenimiento debe identificar y abordar los sistemas heredados. Muchos sistemas heredados de misión crítica no fueron diseñados ni configurados para ser fácilmente actualizados. Como resultado, muchas de las vulnerabilidades en las que se incurre en los Sistemas Informáticos Aliados se introducen a través de

sistemas no parcheados (y efectivamente no parcheables). Estas vulnerabilidades pueden mitigarse mediante capas adicionales de protección, que luego deben mantenerse. Además, las capacidades de hardware, incluidos los sensores y otras capacidades cibernéticas desplegadas hacia adelante, pueden deteriorarse con el tiempo debido al desgaste o al descubrimiento por parte del adversario, lo que requiere la reparación o sustitución de componentes para seguir siendo operables. Esto puede ser particularmente problemático cuando los sistemas físicamente inaccesibles (como los desplegados en sitios remotos) requieren ser reemplazados o actualizados. Es vital que los mandos comprendan el riesgo que supone para la misión dejar estas capacidades cibernéticas en funcionamiento durante largos periodos, no sólo para las operaciones actuales, sino para el éxito de futuras misiones del MOD que dependan de dichas capacidades. Por último, las capacidades de software de contingencia a las que se accede con poca frecuencia también pueden requerir una actualización periódica y nuevas pruebas para verificar que siguen siendo seguras y capaces de crear los efectos requeridos, a pesar de los cambios en la OE.

6) **Protección:**

a) La protección de los Sistemas Informáticos Aliados y de otros ciberespacios críticos nacionales incluye la integración continua y sincronizada de la seguridad del ciberespacio y, cuando sea necesario, de las acciones de defensa del ciberespacio. La protección de los activos del ciberespacio se complica por su conectividad lógica que puede permitir a los enemigos crear efectos múltiples y en cascada que pueden no estar restringidos por la geografía física y las fronteras civiles/militares. Las capacidades del ciberespacio que requieren protección incluyen no sólo la infraestructura (ordenadores, cables, antenas y equipos de conmutación y enrutamiento), sino también partes del EMS (frecuencias de enlace de datos para incluir el enlace descendente por satélite, celular e inalámbrico) y el contenido (tanto los datos como las aplicaciones) del que dependen las operaciones militares. La clave de la protección del ciberespacio es el control positivo de todas las conexiones directas entre los Sistemas Informáticos Aliados e Internet y otras partes públicas del ciberespacio, así como la capacidad de supervisar, detectar e impedir la entrada de tráfico de red malicioso y la exfiltración no autorizada de información a través de estas conexiones

b) La protección del ciberespacio azul utiliza una combinación de capacidades de seguridad y defensa del ciberespacio. Debido a la velocidad de los efectos y al número de elementos en el ciberespacio, los procedimientos automatizados para defender el ciberespacio, verificar las configuraciones y descubrir las vulnerabilidades de la red suelen ofrecer más posibilidades de éxito inicial contra un agresor que los equivalentes

manuales. Varios factores van en contra de lograr una seguridad perfecta de un conjunto de redes y sistemas tan complejos como los Sistemas Informáticos Aliados. Por lo tanto, las partes de misión crítica de los Sistemas Informáticos Aliados que proporcionan una ventaja a cualquiera de los combatientes se consideran terreno clave y se les da prioridad para su protección. Incluso el cifrado más potente y los protocolos más seguros no pueden proteger los Sistemas Informáticos Aliados de usuarios mal formados y/o desmotivados que no emplean prácticas de seguridad adecuadas. Por lo tanto, la formación de todos los usuarios de los Sistemas Informáticos Aliados sobre los comportamientos adecuados y la aplicación estricta por parte del comandante de las mejores prácticas de seguridad en el ciberespacio forman parte de un programa general de gestión de riesgos. Los comandantes son responsables de las acciones de su personal en el ciberespacio y deben asegurar una clara comprensión en todos los niveles del comando de las normas de seguridad del ciberespacio, las expectativas y las mejores prácticas para proteger el ciberespacio.

c) La protección de las capacidades del ciberespacio requiere una estricta adherencia a contramedidas de Seguridad de Operaciones (OPSEC) únicas, ya que estas operaciones podrían ser frustradas si se descubren antes de sus efectos. La ocultación de los movimientos en el ciberespacio utiliza técnicas diferentes a las de la ocultación en los dominios físicos. Habilidades como evitar la detección son fundamentales para la mayoría de las misiones externas y, por lo tanto, esenciales para muchas CO militares conjuntas.

7) Información:

a) La función de información abarca la gestión y aplicación de la información y su integración deliberada con otras funciones conjuntas para influir en las percepciones, el comportamiento y/o la acción o inacción de los actores relevantes y apoyar la toma de decisiones humanas y automatizadas. La función de información ayuda a los mandos y al personal a comprender y aprovechar la naturaleza omnipresente de la información, sus usos militares y su aplicación durante todas las operaciones militares. Esta función proporciona al Mando Conjunto la capacidad de integrar la generación y preservación de la información amiga al tiempo que aprovecha los aspectos informativos inherentes a todas las actividades militares para lograr los objetivos del comandante y alcanzar el estado final. Esta función de la fuerza conjunta apoya las acciones que logran los objetivos dentro de los entornos operativos y de información. Dado que el objetivo del CO es alcanzar los objetivos dentro del ciberespacio y que el ciberespacio está totalmente contenido en el entorno de la información, es importante comprender su relación con la función conjunta de información.

b) La fuerza conjunta lleva a cabo el CO en concierto con otras capacidades, para ganar y mantener una ventaja. El ciberespacio es un medio a través del cual se pueden emplear capacidades de información específicas, como MISO (Operaciones Militares de Apoyo a la Información) o MILDEC. Obsérvese que, aunque algunas operaciones en el entorno de la información pueden realizarse utilizando únicamente CO, siguen estando sincronizadas, integradas y libres de conflictos respecto de otras actividades y operaciones que afectan a los objetivos del comandante.
c) Es importante entender que, aunque el OC permite ciertas actividades primarias dentro de la función de información, hay actividades de información que no implican al OC. Por lo tanto, si no se sincroniza el OC con otros planes y ejecuciones de operaciones militares, las fuerzas amigas pueden llevar a cabo actividades de información redundantes o conflictivas, lo que supone una pérdida de tiempo y de recursos y la pérdida de una ventaja operativa.

Planificación, Coordinación, Ejecución y Evaluación de las Operaciones Cibernéticas

3.4.2.6. Consideraciones sobre la planificación de las operaciones en el ciberespacio

(DOD, Cyberspace Operations JP3-12, 2018)

1) **Descripción:** Aunque a los planificadores de OC se les presentan las mismas consideraciones y desafíos de diseño operacional que a los planificadores de operaciones en los dominios físicos, hay algunas consideraciones únicas para la planificación de OC. Por ejemplo, debido a los vínculos imprevistos en el ciberespacio, los efectos de orden superior de algunas OC pueden ser más difíciles de predecir. Esto puede requerir una planificación más ramificada y secuencial. Además, mientras que muchos elementos del ciberespacio pueden ser mapeados geográficamente, una comprensión completa de la disposición de un adversario y la planificación de las capacidades en el ciberespacio implica la comprensión del objetivo, no sólo en la capa de la red física subyacente, sino también en la operativa y de misión, incluyendo los perfiles de los usuarios y administradores del sistema y su relación con los factores críticos del adversario. Para planificar las operaciones internas en el ciberespacio del MOD, los planificadores de operaciones Sistemas Informáticos Aliados y DCO-IDM deben comprender claramente qué fuerzas o capacidades amigas podrían ser el objetivo de un adversario; qué vulnerabilidades en los Sistemas Informáticos Aliados tienen más probabilidades de ser el objetivo y los efectos potenciales de la acción del adversario; los riesgos de seguridad de la misión implicados; y una comprensión de las leyes nacionales, extranjeras e internacionales aplicables y de la política del Gobierno de la Nación. Las amenazas en el ciberespacio pueden ser estados-nación, grupos no estatales o individuos, y las partes del ciberespacio que controlan no están necesariamente dentro de las fronteras geográficas asociadas a la nacionalidad de la amenaza o proporcionales a su influencia geopolítica. Un elemento criminal, un grupo políticamente motivado o incluso un individuo con buenos recursos puede tener una mayor presencia y capacidad en el ciberespacio que muchas naciones. Además, muchos adversarios operan las capacidades del ciberespacio desde porciones del ciberespacio asociadas geográficamente con el Estado-nación o que son

propiedad de una entidad nacional. Cada uno de estos factores complica la planificación del CO.

2) **Plazos de Planificación:** Para las misiones externas, es esencial que los planificadores de la OCO y la DCO-RA contengan las autorizaciones necesarias para ejecutar las acciones específicas de la OCO propuestas. Las autorizaciones aplicables pueden variar dependiendo de la fase de la operación. Esto incluye tener en cuenta el tiempo de espera requerido para obtener la inteligencia necesaria para definir el objetivo correcto; desarrollar el acceso al objetivo; confirmar las autorizaciones apropiadas; completar la coordinación necesaria, incluyendo la coordinación y/o sincronización interinstitucional; y verificar que la capacidad del ciberespacio coincide con el objetivo previsto utilizando los resultados de las evaluaciones de garantía técnica. En el caso de las misiones internas, los plazos de los planificadores de operaciones DCO-IDM y Sistemas Informáticos Aliados se ven afectados por otros factores, como los niveles de automatización disponibles para gestionar la postura de la red, la disponibilidad de soluciones de seguridad de proveedores comerciales y sus requisitos de licencia, y las consideraciones operativas que pueden afectar a las capacidades del defensor para maniobrar o desconectar los sistemas para gestionar mejor su protección. Sin embargo, los fundamentos de la planificación siguen siendo los mismos, y a pesar de las consideraciones adicionales y los retos de la integración de la OC, los planificadores utilizan la mayoría de los elementos de los procesos tradicionales para implementar la intención y la orientación del comandante.

3) Consideraciones de planificación para operar en el ciberespacio rojo y gris

a) Características de las capacidades del ciberespacio. Aunque el ciberespacio es complejo y está en constante cambio, las capacidades del ciberespacio, ya sean dispositivos o programas informáticos, deben crear de forma fiable los efectos previstos. Sin embargo, las capacidades del ciberespacio se desarrollan sobre la base de suposiciones y expectativas del entorno sobre las condiciones de funcionamiento que se encontrarán en el OE. Estas condiciones pueden ser tan sencillas como el tipo de sistema operativo informático que utiliza un adversario o tan complejas como el número de serie exacto del hardware o la versión del software instalado, qué recursos del sistema están disponibles y qué otras aplicaciones se espera que se estén ejecutando (o no) cuando la capacidad ciberespacial se active en el objetivo. Estas condiciones esperadas deben estar bien documentadas por el desarrollador de la capacidad y son importantes para que los planificadores y el personal de selección de objetivos las entiendan como limitaciones de la capacidad. La medida en que las condiciones ambientales esperadas de un objetivo no pueden ser confirmadas a través de fuentes ISR representa un mayor nivel de riesgo asociados al uso de la capacidad.

En igualdad de condiciones, se prefieren las capacidades cibernéticas que tienen menos dependencias del entorno y/o permiten al operador reconfigurar la capacidad.

b) Efectos en cascada, compuestos y colaterales: Los solapamientos entre las actividades militares, gubernamentales, corporativas y privadas en las redes compartidas en el ciberespacio hacen que la evaluación de los probables efectos en cascada, compuestos y colaterales sea especialmente importante cuando se apunta al CO. Los efectos pueden extenderse a través de un sistema objetivo, a veces en cascada a través de enlaces con sistemas relacionados que no eran evidentes para el planificador. Los efectos en cascada se desplazan a veces a través de sistemas subordinados al que es objeto de la acción, pero también pueden desplazarse lateralmente a sistemas afines o a sistemas de nivel superior. Los efectos compuestos son una agregación de varios niveles de efectos que han interactuado de maneras que pueden ser intencionadas o pueden haber sido imprevistas. Los efectos colaterales, incluidos los daños colaterales, son los efectos incidentales de las operaciones militares sobre los no combatientes y los bienes civiles que no eran los objetivos previstos del ataque. Dependiendo de la situación estratégica y operativa, una orden o las reglas de juego aplicables pueden limitar las operaciones de mantenimiento de la paz a las acciones que probablemente no produzcan efectos colaterales o que los produzcan en menor medida. Una estimación de los efectos colaterales para cumplir con las restricciones políticas es independiente del análisis de proporcionalidad requerido por la ley de la guerra. Esta estimación es una herramienta para que el comandante comprenda el riesgo al considerar la aprobación de las operaciones. Por lo tanto, incluso si una OC propuesta es permisible después de un análisis de efectos colaterales, los efectos probables de la OC propuesta también deben ser permisibles según un análisis de proporcionalidad del derecho de la guerra, según corresponda.

c) Reversibilidad de los efectos: Una consideración importante para la planificación de los efectos de ataque y explotación del ciberespacio es el nivel de control sobre la duración del efecto que pueden ejercer las fuerzas amigas. Hay dos formas básicas de clasificar los efectos según el criterio de reversibilidad:

   i) Efectos reversibles por el operador: Efectos que pueden ser retirados, recuperados o terminados por fuerzas amigas. Estos efectos pueden representar un menor riesgo de consecuencias no deseadas, incluyendo el descubrimiento o las represalias.

   ii) Efectos no reversibles por el operador: Efectos que no pueden ser retirados, recuperados o terminados por las fuerzas amigas después de su ejecución. Estos efectos pueden representar un mayor riesgo de respuesta de la amenaza u otras consecuencias no deseadas y pueden requerir más coordinación.

4) Consideraciones sobre **planificación** para la **protección de los Sistemas Informáticos Aliados:**

a) Para planes y operaciones específicas. Las operaciones en Sistemas Informáticos Aliados apuntalan casi todos los aspectos de las operaciones militares, y esta dependencia del ciberespacio es bien comprendida por nuestros adversarios. Sin embargo, la dependencia de un comandante en segmentos específicos de los Sistemas Informáticos Aliados a menudo no se tiene en cuenta durante el desarrollo de los planes, pero la planificación para la resistencia de la Sistemas Informáticos Aliados es esencial. Los estados principales de planificación del Mando Conjunto deberían incorporar ramas de DCO-IDM y consecuencias para cualquier operación que suponga una mayor amenaza para la Sistemas Informáticos Aliados. El personal del CO de los Mandos de Combate coordina y desconflicta las actividades de la misión DCO-IDM con los CO-IPE (Elemento de Planificación de CiberOperación). Si las acciones defensivas planificadas crearán efectos en el ciberespacio fuera del AOR de los Mandos de Combate, el Mando Conjunto respecto de los Sistemas Informáticos Aliados se asegurará de que las acciones de defensa del ciberespacio estén coordinadas y sincronizadas globalmente.

b) Priorización de la protección de Sistemas Informáticos Aliados: Las políticas de ciberseguridad se aplican generalmente a todo el Sistemas Informáticos Aliados, a menos que se concedan excepciones o exenciones específicas. Cada segmento de los Sistemas Informáticos Aliados tiene una organización responsable de su seguridad y de las acciones defensivas de primera línea, incluyendo las redes administrativas y no críticas para la misión, que son protegidas principalmente por sus operadores y su CSSP (proveedor de servicios de ciberseguridad). Algunos de estos servicios de protección pueden ser contratados, especialmente cuando se ha contratado la creación y operación de la propia red. La determinación de si una pieza específica de hardware del contratista o un segmento específico de la red del contratista se considera parte de los Sistemas Informáticos Aliados está determinada por el lenguaje exacto del contrato. Dado el limitado número de CPTs y otras fuerzas del ciberespacio, el importante alcance de los Sistemas Informáticos Aliados significa que no todos los segmentos pueden ser defendidos con la misma profundidad. Principalmente, estas fuerzas especializadas en el ciberespacio se centran en la protección de los segmentos más prioritarios de los Sistemas Informáticos Aliados, incluyendo los de misión crítica, los clasificados y los que apoyan directamente las operaciones. Si los recursos lo permiten, los CPT pueden ayudar a los proveedores de servicios y a los operadores de segmentos de red en la defensa de las redes de menor prioridad.

c) Coordinación de la defensa de los Sistemas Informáticos Aliados: Una respuesta eficaz a las intrusiones u otras actividades maliciosas en los Sistemas Informáticos Aliados requiere una acción coordinada. Aunque el objetivo final de los Sistemas Informáticos Aliados es derrotar la amenaza y restablecer un ciberespacio seguro, la naturaleza de la amenaza determina la respuesta específica a cada incidente. Todos los incidentes de ciberseguridad se reportan de acuerdo con la política del MOD, pero algunas actividades de los adversarios de la amenaza pueden ser remediadas efectivamente por fuerzas locales bien entrenadas en el ciberespacio sin apoyo externo. Las amenazas sofisticadas de estados-nación que penetran nuestras medidas de seguridad requieren un tipo de respuesta diferente. Cada encuentro con un adversario de igual o casi igual nivel en el ciberespacio justifica una cuidadosa consideración de la respuesta. Elegir cuándo, dónde y cómo enfrentarse a la amenaza es tan importante en la ACA (ciber area de actuación) como lo es para la defensa en los dominios físicos. Si las circunstancias lo permiten, incluyendo una consideración de la amenaza a la misión apoyada, las consideraciones de ganancia/pérdida de inteligencia (IGL) pueden sugerir una cuidadosa observación de la amenaza mientras se limitan sus maniobras. Cuando un mando se enfrenta a una amenaza en el ciberespacio, la empresa global se adapta para apoyar a ese mando según las prioridades defensivas. Se proporciona apoyo de retroceso para el análisis, la inteligencia e incluso los fuegos para mantener la continuidad de las operaciones en el comando apoyado. Los mandos locales y de los servicios consultan con el Mando Conjunto del Ciberespacio y sus estados mayores subordinados para crear respuestas adaptadas a amenazas específicas. Algunos incidentes requieren una respuesta remota o in situ por parte de los CPT para ayudar a los operadores de la red y al CSSP asignado a remediar y restaurar el segmento de red afectado.

d) Conocimiento de la situación. El conocimiento de la situación del ciberespacio es el conocimiento actual y predictivo requerido del ciberespacio y de la OE de la que depende el CO, incluyendo todos los factores que afectan a las fuerzas del ciberespacio amigas y adversarias. Un comandante evalúa continuamente la OE a través de una combinación de informes de elementos del Estado Mayor y otros; observación personal; inteligencia, para incluir la advertencia de amenazas; y representaciones de varias actividades que ocurren en la OE usando una imagen operacional común (COP). Los Sistemas Informáticos Aliados son una fuente primaria de información utilizada para apoyar el conocimiento de la situación de la OE por parte del comandante, incluyendo el estado de la propia Sistemas Informáticos Aliados. El mantenimiento de los sensores de los Sistemas Informáticos Aliados, los canales de comunicación, las fuentes de datos y las interfaces de usuario es un resultado clave

de las operaciones de los Sistemas Informáticos Aliados. El conocimiento preciso y completo de la situación es fundamental para la rápida toma de decisiones en una OE en constante cambio y al enfrentarse a un adversario escurridizo y adaptable. El conocimiento de la situación de la actividad del adversario en el ciberespacio gris y rojo se basa en gran medida en la explotación del ciberespacio y la SIGINT, pero las contribuciones pueden provenir de todas las fuentes de inteligencia. El conocimiento de la situación dentro de los Sistemas Informáticos Aliados es proporcionado por los servicios y agencias que operan sus partes de los Sistemas Informáticos Aliados, y el Mando Conjunto de Sistemas Informáticos Aliados a través de los centros de operaciones de red y de seguridad, por el Centro de Operaciones Conjuntas del MCCE[...]. Se coordinan entre sí en función de la eficacia operativa y el conocimiento compartido de la situación. La complejidad y el alcance cada vez mayores del ciberespacio significan que un comandante nunca tiene un conocimiento perfecto o incluso óptimo de la situación de los factores del ciberespacio que podrían afectar a las operaciones y debe considerar los riesgos que representa esta falta de información a la hora de tomar decisiones.

e) Preparación para la evaluación(valoración): La evaluación se utiliza para medir el progreso de la fuerza conjunta hacia el cumplimiento de la misión. Los comandantes evalúan continuamente la OE y el progreso de las operaciones y los comparan con su visión e intención iniciales. El proceso de evaluación comienza durante el proceso de planificación y ayuda al comandante y al personal a decidir qué medir y cómo medirlo, para determinar el progreso hacia el cumplimiento de una tarea, la creación de un efecto o la consecución de un objetivo. Los datos recogidos para apoyar estas medidas pueden ir desde la simple constatación de la incapacidad de llegar a la red del objetivo tras un ataque cibernético hasta la compleja monitorización de la red y el análisis estadístico. Los datos recogidos sobre el estado del objetivo antes de la operación, a través del acceso, la ejecución, y posiblemente su estado a largo plazo después del ataque, pueden facilitar la evaluación posterior de los efectos de orden superior. La evaluación de las misiones internas de protección de los Sistemas Informáticos Aliados requiere una preparación similar. Es difícil determinar el grado en que las medidas de protección reducen el riesgo para la misión sin un conocimiento preciso de las condiciones iniciales de la red. La evaluación del CO no se limita al análisis de los datos del ciberespacio. Por ejemplo, si el efecto deseado de una misión OCO fuera causar un corte de energía, la evaluación podría realizarse utilizando sensores visuales para observar las indicaciones de un corte. Los planificadores presentan las solicitudes de evaluación, con una justificación suficiente, con la antelación necesaria para la adecuada asignación de recursos.

3.4.2.7. Apoyo analítico operativo y de inteligencia a la planificación de operaciones en el ciberespacio

(DOD, Cyberspace Operations JP3-12, 2018)

1) **Requisitos de Inteligencia** (RI): Durante el análisis de la misión, el personal de la fuerza conjunta identifica las lagunas de información significativas sobre el adversario y otros aspectos relevantes de la OE. Tras el análisis de las carencias, el personal formula los requisitos de inteligencia (RI), que son temas generales o específicos sobre los que se necesita recoger información o producir inteligencia. Sobre la base de los RI identificados, el personal desarrolla preguntas más específicas conocidas como Solicitudes de Información (RFI) (aquellos elementos de información que deben ser recolectados y procesados para desarrollar la inteligencia requerida por el comandante). Las Solicitudes de Información (RFI) relacionados con el ciberespacio pueden incluir aspectos como las infraestructuras y el estado de la red, la preparación del equipo y el personal del adversario, y los identificadores únicos de la firma del ciberespacio, como las versiones de hardware/software/firmware y los archivos de configuración. Estas IRs se satisfacen a través de una combinación de fuentes de inteligencia militar y de inteligencia nacional.
   a) Solicitudes de información (RFI). Los planificadores del CO pueden presentar una RFI para generar esfuerzos de recopilación de inteligencia en cualquier parte de la OE o disciplina en apoyo del JPP. Las RFIs son requerimientos específicos, sensibles al tiempo y ad hoc de información de inteligencia para apoyar una crisis u operación en curso y no necesariamente relacionados con requerimientos permanentes o producción de inteligencia programada. Las RFIs cumplen con los requisitos del cliente y van desde la difusión de productos existentes, pasando por la integración o adaptación de la información disponible, hasta la programación de una nueva recopilación y producción. El gestor de la RFI que traduce los requisitos del cliente y el productor principal de inteligencia determinan la mejor manera de satisfacer las necesidades del cliente. Además de la información recopilada durante las operaciones militares, la información necesaria para apoyar la planificación del CO puede provenir de la SIGINT, la inteligencia humana, la CI, la inteligencia de medidas y firmas, la inteligencia geoespacial o la inteligencia de fuente abierta (OSINT). Independientemente de la fuente, la información debe ser oportuna, precisa y en un formato utilizable.
2) **Detección y caracterización de amenazas.** Algunas amenazas en el ciberespacio son detectadas por fuentes de inteligencia y otras durante el curso de las maniobras militares.

a) Detección. Las actividades en el ciberespacio de una amenaza sofisticada pueden ser difíciles de detectar. A diferencia de las acciones en los dominios físicos, que a menudo se detectan por la presencia de equipos militares u otros tipos de observables, las acciones de las amenazas en el ciberespacio pueden no ser fácilmente distinguible de la actividad legítima de la red. La detección de actividades en el ciberespacio es fundamental para permitir un control eficaz.
b) Clasificación. Debido a que las misiones del ciberespacio del DOD se clasifican en base a la intención del comandante y porque las fuerzas amigas a menudo no están seguras de la intención real de una amenaza, las actividades de la amenaza en el ciberespacio se denominan de forma más genérica. Las acciones de amenaza en el ciberespacio se denominan generalmente actividad cibernética maliciosa. Si los detalles conocidos de la actividad del adversario apoyan una clasificación más precisa, las acciones específicas de amenaza pueden calificarse como ataque al ciberespacio si han creado efectos de negación notables o explotación del ciberespacio si el adversario sólo ha maniobrado con fines de recolección o habilitación.
c) Análisis y atribución: Debido a las características de la red física, la red lógica y la capa cibernética, la atribución de una actividad maliciosa en el ciberespacio a una persona específica, una organización criminal, una amenaza no estatal o incluso un Estado-nación responsable puede ser excepcionalmente difícil. Aunque la atribución no es necesariamente necesaria para la autodefensa, la dificultad de la atribución, junto con la posibilidad de que una amenaza aparente pueda ser en realidad un intento de distracción, es una de las principales razones por las que la planificación de la misión DCO-RA puede ser más difícil que la planificación de la respuesta a un ataque convencional. Los riesgos de una respuesta defensiva contra la amenaza equivocada, en particular un Estado-nación o un objetivo dentro de un Estado-nación involuntario donde se originó el ataque, se sopesan con los objetivos estratégicos y las consecuencias de cometer un error de atribución. Trabajar eficazmente dentro de estas limitaciones requiere habilidades únicas por parte de los analistas de inteligencia de todas las fuentes para entender el contexto de la actividad de la amenaza. Utilizan habilidades como el análisis de las técnicas de engaño, las técnicas de anonimato, las representaciones virtuales y los avatares, y otros artefactos de la red lógica y las capas del ciberespacio para caracterizar las actividades con el grado de confianza necesario para permitir una respuesta eficaz.

3) IGL. Otra preocupación de la planificación es que las maniobras y los fuegos en el ciberespacio rojo y gris podrían comprometer potencialmente las fuentes y los métodos de las actividades de recogida de información. En la medida de lo posible, se requiere una evaluación de la IGL antes de ejecutar tales acciones. La evaluación de la IGL puede

complicarse por la variedad de socios multinacionales y del Gobierno Nacional no pertenecientes al MOD que operan en el ciberespacio. Los Mandos Conjuntos utilizan el análisis de la IGL para sopesar los riesgos de llevar a cabo la OC frente a la consecución del objetivo deseado a través de otros métodos.

4) **Inteligencia de Alerta Temprana.** La inteligencia sobre amenazas en el ciberespacio incluye el análisis de todas las fuentes para tener en cuenta la inteligencia de alerta temprana política, militar y técnica. Las acciones de los adversarios en el ciberespacio pueden producirse por separado y con mucha antelación a las actividades relacionadas en los dominios físicos. Además, los sensores de amenazas en el ciberespacio pueden reconocer actividades maliciosas con muy poco tiempo disponible para responder. Estos factores hacen que la inclusión del análisis de inteligencia de todas las fuentes sea muy importante para evaluar eficazmente las intenciones de los adversarios en el ciberespacio.
5) **OSINT.** El análisis de inteligencia de todas las fuentes del ciberespacio debe aprovechar la información disponible de OSINT, incluyendo los medios sociales de Internet y otras fuentes de información no tradicionales. La esfera de la inteligencia abierta, en constante evolución La actividad de las fuentes ofrece la oportunidad de añadir datos útiles al análisis de todas las fuentes. Pero este panorama de medios de comunicación en constante cambio y la baja relación “señal-ruido” de los datos disponibles en el ciberespacio también complican el problema de la recopilación de inteligencia, lo que requiere una gestión activa de la recopilación para estar al tanto de estas fuentes.
6) **ISR en el ciberespacio.** La ISR en el ciberespacio es una actividad que sincroniza e integra la planificación y el funcionamiento de los sensores, los activos y los sistemas de procesamiento, explotación y difusión en apoyo directo de las operaciones actuales y futuras. Se trata de una función integrada de inteligencia y operaciones. La ISR en el ciberespacio se centra en la recopilación de información táctica y operativa y en el mapeo de las redes enemigas y adversarias para apoyar la planificación militar. Para facilitar la utilización óptima de todos los recursos ISR disponibles, debe desarrollarse un concepto de operaciones ISR (CONOPS) junto con el esfuerzo de planificación del mando. El CONOPS de ISR debe basarse en la estrategia de recolección y en la planificación de la ejecución de ISR y debe ser desarrollado conjuntamente por la dirección de inteligencia de la fuerza conjunta de un estado mayor conjunto y la dirección de operaciones de un estado mayor conjunto. El CONOPS ISR documenta la sincronización, integración y operación de los recursos ISR en apoyo directo de las operaciones actuales y futuras. Describe la capacidad de asignar, recopilar, procesar, explotar y difundir información precisa y oportuna que proporcione el conocimiento necesario para planificar y dirigir con éxito las operaciones. Aborda cómo se utilizarán todos los medios de recogida de ISR disponibles y la infraestructura de procesamiento, explotación y difusión asociada,

incluidos los medios multinacionales y comerciales, para satisfacer las tareas de recogida previstas por la fuerza conjunta. También requiere una desconflicción adecuada y personal entrenado y certificado según un estándar común con el CI.

3.4.2.8. Selección de Objetivos

La finalidad de la selección de objetivos es integrar y sincronizar los fuegos (el uso de sistemas de armas u otras acciones para crear un efecto específico letal o no letal sobre un objetivo) en las operaciones conjuntas. La selección de objetivos es el proceso de selección y priorización de estos y la adecuación de la respuesta adecuada a ellos, teniendo en cuenta las necesidades y capacidades operativas. La integración y sincronización de la planificación, la ejecución y la evaluación son fundamentales para el éxito de la selección conjunta de objetivos. El ciclo general de objetivos conjuntos y el proceso de desarrollo de objetivos[...] se aplican en general a los objetivos en apoyo de la OC. Además, la coordinación requerida por el Manual del jefe de Estado Mayor Conjunto (CJCSM) [...] para ciertas misiones OCO y DCO-RA es única para el CO y se aplica a muchos aspectos del ciclo de objetivos conjuntos. Por lo tanto, los planificadores y los responsables de la toma de decisiones en materia de CO suelen utilizar un proceso de fijación de objetivos específicamente adaptado a las circunstancias. Hay tres aspectos fundamentales de la OC que deben tenerse en cuenta en los procesos de fijación de objetivos: reconocer que las capacidades del ciberespacio son una opción viable para atacar algunos objetivos designados; comprender que una opción de OC puede ser preferible en algunos casos, porque puede ofrecer una baja probabilidad de detección y/o ningún daño físico asociado; y que los efectos de orden superior sobre los objetivos en el ciberespacio pueden afectar a elementos de los Sistemas Informáticos Aliados, incluida la represalia por ataques atribuidos a la fuerza conjunta. Además, a continuación, se describen algunas características exclusivas de los componentes cibernéticos de los objetivos y de las capacidades del ciberespacio.

1) **Apuntando en el ciberespacio.** Los estados mayores de planificación y focalización desarrollan y seleccionan objetivos en y a través del ciberespacio basándose en los objetivos del comandante más que en las capacidades disponibles para alcanzarlos. La atención se centra en la creación de efectos que cumplan con las tareas y objetivos relacionados con los objetivos, no en el uso de una capacidad particular del ciberespacio simplemente porque está disponible. Los objetivos a los que se puede acceder en el ciberespacio se desarrollan, examinan y validan dentro del proceso de selección de objetivos establecido. Aunque los objetivos emparejados con las capacidades del ciberespacio a menudo pueden ser atacados sin daños permanentes, debido a la interconexión del ciberespacio, los efectos de la OC pueden cruzar las fronteras

geográficas y, si no se planifica cuidadosamente, pueden tener efectos imprevistos. Como resultado, atacar objetivos en y a través del ciberespacio requiere una estrecha coordinación dentro del DOD y con socios interinstitucionales y multinacionales. Cada objetivo tiene características intrínsecas o adquiridas distintas (es decir, físicas, funcionales, cognitivas, ambientales y temporales) que forman la base para la detección, localización e identificación; para determinar el valor del objetivo dentro del sistema del objetivo; y para la clasificación para la vigilancia, el análisis, el ataque y la evaluación futuros. El reto de la selección de objetivos para el CO es identificar, correlacionar, coordinar y desonfliccionar las múltiples actividades que tienen lugar en la red física, la red lógica y las capas de ciberespacio. Esto requiere una capacidad de C2 que pueda operar al ritmo de la OC y que pueda integrar rápidamente a las partes interesadas.

a) **Características del objetivo de la capa física de la red.** La capa física de la red es el medio por el que viajan los datos. Incluye medios de transmisión alámbricos (por ejemplo, cables terrestres y submarinos) e inalámbricos (por ejemplo, radio, radioenlace, celular, satélite). Es un punto de referencia para determinar la ubicación geográfica y el marco legal aplicable.
b) **Características del objetivo de la capa de red lógica.** La capa de red lógica proporciona una visión alternativa del objetivo, abstraída de su ubicación física, y referenciada desde su posición lógica en el ciberespacio. Esta posición suele representarse a través de una dirección de red (por ejemplo, la dirección IP). Representa cómo los nodos de los dominios físicos se dirigen y se refieren unos a otros para formar entidades en el ciberespacio. La capa lógica de la red es el primer punto donde se puede perder la conexión con los dominios físicos. El ataque en la capa lógica requiere la identidad lógica y el acceso lógico al objetivo para tener un efecto directo.
c) **Características del objetivo de la capa de ciberespacio.** La capa de ciberespacio, el conjunto de la(s) identidad(es) en línea de un individuo o grupo, y una abstracción de los datos de la capa de red lógica, tiene importantes implicaciones para las fuerzas conjuntas en términos de identificación positiva de objetivos y atribución de afiliaciones y actividades. Los servicios se crean para agrupar información sobre los actores objetivo con el fin de organizar el análisis, el compromiso y los informes de inteligencia. Dado que los servicios pueden ser complejas, con elementos en muchas ubicaciones virtuales, pero a menudo no vinculadas a una única ubicación o forma física, se requieren suficientes capacidades de recopilación y análisis de inteligencia para que las fuerzas conjuntas obtengan la información y el conocimiento de la situación necesarios para permitir un ataque eficaz a un activo o servicio en el ciberespacio. En

última instancia, los servicios estarán vinculadas a elementos que se comprometerán en las capas lógicas o físicas de la red.

2) **Vías hacia los objetivos.** Las fuerzas del ciberespacio habilitan las vías a los objetivos o a los elementos del objetivo en el ciberespacio utilizando acciones de explotación del ciberespacio. Este acceso puede ser utilizado para diversos fines, que van desde la recogida de información hasta la maniobra y la designación de objetivos. No todos los accesos son igualmente útiles para las operaciones militares. Por ejemplo, el nivel de acceso requerido para recoger información de una entidad puede no ser suficiente para crear un efecto deseado. El desarrollo del acceso a los objetivos en el ciberespacio o a través de él sigue un proceso que a menudo puede llevar mucho tiempo. En algunos casos, el acceso a distancia no es posible, y puede ser necesaria la proximidad. Todos los esfuerzos de acceso al objetivo en el ciberespacio requieren la coordinación con el CI para la desconflicción conforme a la política nacional y para iluminar los posibles problemas de la IGL. Si el acceso directo al objetivo no está disponible o no es deseado, a veces se puede crear un efecto similar o parcial mediante el acceso indirecto utilizando un objetivo relacionado que tiene efectos de mayor orden en el objetivo deseado. Algunos ataques de denegación de servicio en el ciberespacio aprovechan este tipo de acceso indirecto.
3) **Nominación y sincronización de objetivos.** Nominación y sincronización de objetivos. El CO utiliza procesos estándar de nominación de objetivos, pero los dossiers de objetivos deben incluir aspectos únicos del ciberespacio (por ejemplo, configuraciones de hardware y software, dirección IP, aplicaciones de ciberpersona) del objetivo. El desarrollo de estos datos es imperativo para entender y caracterizar cómo los elementos atacables a través del ciberespacio son relevantes para el objetivo del comandante. Estos datos también permiten al planificador hacer coincidir una capacidad ciberespacial apropiada contra un objetivo concreto. Los mandos de los componentes, las agencias nacionales, los mandos de apoyo y/o el personal de planificación del JFC proponen objetivos al personal de selección para su desarrollo e inclusión en la lista conjunta de objetivos (JTL). Una vez incluidos en la JTL, los JFC que reciban una EXORD con los objetivos y las ROE pertinentes pueden atacar el objetivo con recursos orgánicos (si están dentro del área de operaciones asignada al comandante del componente) o nominar el objetivo al MCCE para que actúen otros componentes de la fuerza conjunta y otras organizaciones.
4) **Objetivos tiempodependientes (TST).**
    a) Un TST es un objetivo validado de tan alta prioridad para las fuerzas amigas que el comandante lo designa para un enfrentamiento inmediato porque supone (o supondrá pronto) una amenaza para las fuerzas amigas o es un objetivo fugaz altamente lucrativo. Los TSTs son normalmente atacados dinámicamente. Sin embargo, para ser atacados con éxito, requieren una considerable planificación y preparación dentro del

ciclo de objetivos conjuntos. En la mayoría de las situaciones es difícil enfrentarse a los TST en el ciberespacio, porque es probable que atraviesen las AOR y requieran una planificación detallada conjunta, interinstitucional y/o multinacional.

b) Estar preparado para enfrentarse a un TST en el ciberespacio requiere la coordinación entre los planificadores del ciberespacio, los operadores y el comandante apoyado en una fase temprana de la planificación, para aumentar la probabilidad de que se disponga de la flexibilidad y el acceso adecuados en caso de que surja una oportunidad fugaz. Además, los JFC deben establecer procedimientos para promulgar rápidamente órdenes de ataque para TST en el ciberespacio. El éxito de la ejecución de los TST en el ciberespacio requiere un proceso bien organizado y ensayado para compartir los datos de los sensores y la información sobre los objetivos, identificar los medios de ataque adecuados, obtener la aprobación de la misión y desconfliccionar rápidamente el empleo de las capacidades en el ciberespacio. Realizar la mayor cantidad de la coordinación y la toma de decisiones en la medida de lo posible, en función de los tipos de TST previstos y de la naturaleza de la misión, es la clave del éxito.

3.4.2.9. Mando y Control (C2) de las fuerzas del Ciberespacio

(DOD, Cyberspace Operations JP3-12, 2018)

Las relaciones de mando claramente establecidas son cruciales para garantizar el empleo oportuno y eficaz de las fuerzas, y las OC requieren unidad de mando y unidad de esfuerzo. Sin embargo, la compleja naturaleza de las operaciones de mantenimiento de la paz, en las que las fuerzas del ciberespacio pueden actuar simultáneamente a nivel global y a nivel del teatro o de la Junta de Acción Conjunta, requiere adaptaciones de las estructuras tradicionales de C2. Las fuerzas conjuntas emplean principalmente una planificación centralizada con una ejecución descentralizada de las operaciones. Las OC requieren una coordinación constante y detallada entre el teatro y las operaciones globales, creando un marco de C2 dinámico que pueda adaptarse a los cambios constantes, las amenazas emergentes y las incógnitas. Ciertas funciones de CO, incluyendo la protección de las redes globales de los Sistemas Informáticos Aliados y la persecución de las amenazas globales del ciberespacio, se prestan a la planificación y ejecución centralizada para satisfacer los múltiples y casi instantáneos requisitos de respuesta. El CO controlado centralmente debería estar integrado y sincronizado con el CO regional o local de la CCDR, llevado a cabo por fuerzas asignadas o adscritas a la CCDR, o en apoyo de la CCDR. Por estas razones, puede haber ocasiones en las que el C2 de las fuerzas que ejecutan simultáneamente el CO global y el CO de teatro se lleve a cabo

utilizando relaciones de mando de apoyo/apoyo bajo cadenas de mando separadas, pero sincronizadas. Las OC son integradas y sincronizadas por el comandante apoyado en sus CONOPS, planes y órdenes detalladas, y operaciones conjuntas específicas.

1) **C2 para CO globales.** C2 para el CO global. El MCCE es el comandante de apoyo para el CO trans regional y global y gestiona el CO global diario incluso cuando es el comandante de apoyo para una o más operaciones geográficas o funcionales de la CCDR. Para una misión específica de CO, las relaciones de mando apoyado/apoyado se establecen en una EXORD, OPORD o directiva de establecimiento. Una relación de apoyo para el CO no exime a ninguno de los mandos de coordinar las opciones de respuesta con los mandos afectados antes de llevar a cabo una operación. Independientemente del enfoque que se emplee para una operación en particular, a menos que el presidente o el secretario de Defensa especifiquen lo contrario, el C2 para la OC se implementa de acuerdo con la EXORD [...] y otras órdenes pertinentes para ayudar a garantizar la coordinación y la sincronización eficaces de las fuerzas conjuntas y para proporcionar una estructura común para que los JFC ejecuten su misión dentro de un contexto global. El MOD coordina y dirige de forma centralizada las operaciones globales del Sistemas Informáticos Aliados y el DCO-IDM cuando estas operaciones tienen el potencial de afectar a la integridad y la preparación operativa de múltiples componentes del MOD. Aunque la ejecución de muchas acciones puede estar descentralizada, el MCCE es el comandante apoyado por el CO para asegurar, operar y defender los Sistemas Informáticos Aliados y, cuando se le ordena, para defender otros activos, sistemas y funciones críticos del ciberespacio nacional. A medida que los Sistemas Informáticos Aliados continúan migrando hacia un estándar de arquitectura común, Las acciones rutinarias de seguridad en el ciberespacio para las redes globales seguirán trasladándose a lugares centralizados, como un centro de operaciones de la empresa global.
2) **C2 para CO de soporte a CCMD.** Los CCDR reciben apoyo para las CO en su AOR o para sus responsabilidades trans regionales, con el apoyo del MCCE según sea necesario. Estas CO comprenden acciones destinadas a tener efectos localizados dentro de la AOR de un CGC o de las responsabilidades trans regionales de un CCMD funcional. Pueden ser acciones de seguridad y defensa del ciberespacio internas a un segmento Sistemas Informáticos Aliados de teatro o acciones externas, como la explotación del ciberespacio o el ataque al ciberespacio contra una capacidad enemiga específica. Además de los segmentos de teatro de las redes globales, las operaciones Sistemas Informáticos Aliados a nivel del CCMD y DCO-IDM incluyen la protección de las redes y ordenadores autónomos y tácticos utilizados exclusivamente por el CCMD. Por ejemplo, las maniobras a nivel del CCMD en el ciberespacio incluyen actividades para reposicionar las

capacidades con el fin de mejorar la detección de amenazas en áreas específicas, centrar la actividad de las fuerzas del ciberespacio en áreas vinculadas a ramas y secuelas operativas específicas para mantener al adversario en riesgo, o activar las capacidades tácticas del ciberespacio de reserva para la transición del C2 amigo a lugares más seguros. Estas maniobras de CO son vitales cuando los sistemas de un CCDR son atacados hasta el punto de que subconjuntos de la Sistemas Informáticos Aliados se degradan, comprometen o pierden. En tales operaciones, el CCDR apoyado coordina, a través de su USCYBERCOM CO-IPE, con su centro de operaciones empresariales asociado, apoyado por MCCE, Sistemas Informáticos Aliados y DISA, para restaurar el ciberespacio afectado. El CCDR apoyado también integra, sincroniza y normalmente dirige las acciones del CO en el ciberespacio rojo y gris, incluidos los fuegos, con otros efectos letales y no letales, para lo cual pueden utilizar fuerzas del ciberespacio asignadas, adjuntas o de apoyo. Los CCDRs desarrollan y coordinan sus requerimientos para tales efectos con el CO-IPE del USCYBERCOM, para la desconflicción y la ejecución prioritaria. Cuando un CCDR establece una fuerza subordinada (por ejemplo, una fuerza de tarea conjunta), la(s) unidad(es) ciberespacial(es) asignada(s) para apoyar esa fuerza se determina(n) por los requisitos de la misión del CCDR en coordinación con el MCCE.

3) **Clases de C2 para misiones internas y externas en el Ciberespacio.** La naturaleza de las relaciones C2 para las OC varía, dependiendo de si son internas a los Sistemas Informáticos Aliados o a otro ciberespacio defendido, o si son misiones externas en el ciberespacio extranjero.
   a) Misiones internas. Misiones internas. El C2 de las fuerzas que llevan a cabo operaciones Sistemas Informáticos Aliados y DCO-IDM puede requerir acciones preplanificadas y preautorizadas basadas en condiciones y activadores particulares, ejecutadas manual o automáticamente, dependiendo de la naturaleza de la amenaza y la urgencia de la respuesta requerida. El personal de operaciones y planificación del comandante debe comprender las interrelaciones del ciberespacio que están protegiendo, cómo se pueden emplear eficazmente las capacidades apropiadas para derrotar las amenazas y, cuando sea necesario, cómo desconfliccionar las acciones de defensa del ciberespacio con las operaciones críticas de la misión que no pueden ser interrumpidas. Las fuerzas del ciberespacio que defienden segmentos del Sistemas Informáticos Aliados del CCMD pueden estar geográficamente separadas del teatro de operaciones apoyado. Por ejemplo, las fuerzas que realizan acciones remotas en apoyo del DCO-IDM a menudo apoyan simultáneamente la defensa del ciberespacio en múltiples ubicaciones geográficas. Esto requiere una amplia coordinación, planificación e integración temprana de los requisitos y capacidades. Estos casos requieren que todos los comandantes involucrados tomen medidas

adicionales para que el comandante apoyado esté continuamente de la situación operativa de las fuerzas de apoyo remotas. En otros casos, los CPTs pueden ser desplegados en lugares específicos donde son colocados en apoyo directo a los comandantes locales para resguardar el ciberespacio comprometido. En otros casos en los que no hay un comandante militar local, por ejemplo, cuando un CPT es desplegado para ayudar a una agencia del MOD, todas las autoridades de C2 permanecen con el comandante del CPT. Los comandantes de apoyo y soporte coordinan el despliegue y el empleo de las fuerzas del ciberespacio necesarias para cumplir la misión asignada.

b) Misiones exteriores. Misiones exteriores. Las relaciones C2 establecidas para ejecutar misiones OCO y DCO-RA, que implican acciones en el ciberespacio extranjero, requieren una cuidadosa consideración de los efectos proyectados y de las fronteras geopolíticas. La dependencia de la población mundial de la interconectividad del ciberespacio requiere un control cuidadoso de los efectos creados durante las misiones OCO y DCO-RA, con una planificación detallada, un apoyo de inteligencia en profundidad y una desconflicción a nivel nacional para garantizar la consideración adecuada de factores no militares, como las implicaciones de la política exterior. Algunas de estas misiones externas requieren una ejecución centralizada por parte de los CMT o NMT para crear un efecto global. Por ejemplo, una misión DCO-RA que emplee contramedidas externas en múltiples AOR para contrarrestar una gran botnet (una red de ordenadores conectados entre sí por un malware) o acciones, hasta e incluyendo el tanteo, para bloquear las señales de mando de ataques al ciberespacio dirigidas desde un AOR a otro. Otras misiones externas pueden tener un enfoque más regional y táctico y utilizar fuerzas ciberespaciales desplegadas regionalmente. Cuando se les ordena, los GCC controlan las operaciones en y a través del ciberespacio cuando existe la confianza de que los efectos se limitan a su AOR geográfica. Tales autoridades requieren que los GCC se mantengan al tanto de la política nacional del ciberespacio y su aplicación a sus planes y operaciones.

c) Basado en la naturaleza del CO, el marco del C2 del ciberespacio se ajusta para un C2 flexible y ágil de las fuerzas del ciberespacio para asegurar la libertad de acción de La Nación en el ciberespacio mientras se niega a los adversarios.

4) Habilitación del C2 de las fuerzas del ciberespacio. Para proporcionar un C2 eficaz a las fuerzas que llevan a cabo el CO, son esenciales varios factores de soporte.

a) COP. A pesar de las dificultades para lograr una conciencia situacional precisa y completa de todos los aspectos del ciberespacio en relación con un comandante, el mejor COP disponible en tiempo real para el ciberespacio es importante para un C2 eficaz de las fuerzas que ejecutan el CO. Un COP de las actividades en el ciberespacio

requiere una rápida fusión, correlación y visualización de los datos de los sensores de la red global para ofrecer una imagen fiable de la actividad de los amigos, neutrales, adversarios y enemigos en todas las capas del ciberespacio. Además, un COP preciso del ciberespacio integra datos de amenazas y eventos en tiempo real procedentes de múltiples fuentes (por ejemplo, los centros de operaciones del MOD y otros proveedores de servicios, los socios interinstitucionales, la industria privada y los socios internacionales) y mejora la capacidad de los comandantes para identificar, supervisar, caracterizar, rastrear, localizar y tomar medidas en respuesta a la actividad maliciosa en el ciberespacio. El MCCE mantiene un conocimiento global de la situación del ciberespacio, y los CCMD mantienen un conocimiento regional/funcional de la situación del ciberespacio junto con un conocimiento de los factores globales en el ciberespacio que pueden afectar a las operaciones en su teatro/área funcional.

b) Alcance. Alcance. La complejidad que presenta el ciberespacio requiere flexibilidad de fuerzas y C2 para contrarrestar la amplia variedad de amenazas. Las unidades de las fuerzas del ciberespacio que operan bajo los Sistemas Informáticos Aliados adscritos al MCCE, que proporcionan apoyo global al CO, pueden necesitar alcanzar el apoyo de múltiples CCMDs simultáneamente. Permitirles apoyar a los CCMD de esta manera permite una adaptación más rápida a las necesidades que cambian rápidamente y permite que las amenazas que inicialmente se manifiestan sólo en un AOR sean mitigadas globalmente en tiempo casi real. Del mismo modo, al sincronizar las misiones de las OC relacionadas con el cumplimiento de los objetivos de las CCDR, algunas capacidades del ciberespacio que apoyan esta actividad pueden necesitar ser desplegadas hacia adelante, o para la velocidad en situaciones de tiempo crítico, estar disponibles a través de reachback. Esto podría implicar el aumento o el despliegue de las capacidades ciberespaciales a las fuerzas que ya están avanzadas o requerir el despliegue de un equipo totalmente equipado de personal y capacidades.

c) Reacción. Al mismo tiempo, los CCMD requieren la libertad y la capacidad de planificar, coordinar y dirigir eficazmente el CO de teatro y funcional. Para permitir estos esfuerzos, el personal que apoya a los CCM y a otros CCDR debe organizar un apoyo de retorno oportuno y efectivo del MCCE y sus unidades subordinadas para aumentar la experiencia y la capacidad del comandante apoyado. […]

5) **C2 de CO multinacional.** Aunque es probable que los militares de La Nación entren en futuros conflictos como parte de una fuerza multinacional (MNF), el nivel de integración de las fuerzas estadounidenses del ciberespacio con las fuerzas extranjeras del ciberespacio variará en función de los acuerdos vigentes con cada socio y puede no reflejar el nivel de integración de otros tipos de fuerzas. La planificación de los elementos específicos de C2 deseados por el comandante estadounidense depende del tipo y la escala a operación, la

presencia en el ciberespacio o la sofisticación del adversario, y los tipos de objetivos identificados. Independientemente de los elementos que se establezcan, los solapamientos entre las misiones globales y de teatro en el ciberespacio, y las limitaciones operativas pertinentes, requieren una estrecha coordinación, y potencialmente, cierto nivel de integración, entre los CCDR que realizan operaciones multinacionales, el MCCE, y otros socios multinacionales e interinstitucionales.

3.4.2.10. Sincronización de las operaciones en el ciberespacio

(DOD, Cyberspace Operations JP3-12, 2018)

1) El ritmo de la OC requiere una importante colaboración preoperativa y una vigilancia constante tras su inicio, para una coordinación y desconflicción eficaces en todo el EO. Las claves de esta sincronización son el mantenimiento del conocimiento de la situación del ciberespacio y la evaluación de los impactos potenciales para la fuerza conjunta de cualquier OC planificada, incluyendo la postura de protección de los Sistemas Informáticos Aliados, los cambios de la configuración normal de la red, o los indicios observados de actividad maliciosa. El calendario de las OC planificadas debe determinarse sobre la base de una evaluación realista de su capacidad para crear efectos y apoyar las operaciones en toda la OE. Esto puede requerir el uso de capacidades cibernéticas en fases anteriores de una operación que el uso de otros tipos de capacidades. Los planificadores y operadores eficaces comprenden cómo otras operaciones dentro de la OE pueden afectar al CO. Por ejemplo, la fuerza conjunta utiliza medidas de coordinación de apoyo de fuego en las operaciones aéreas, terrestres y marítimas para facilitar el compromiso rápido de los objetivos y simultáneamente proporcionar salvaguardias para las fuerzas amigas. Los esfuerzos de desconflicción y coordinación del CO con otras operaciones deben incluir medidas similares.
2) **Desconflicción.** Para el CO, la desconflicción es el acto de coordinar el empleo de las capacidades del ciberespacio para crear efectos con los socios aplicables del MOD, interinstitucionales y multinacionales para garantizar que las operaciones no interfieran, inhiban o entren en conflicto entre sí. Los efectos previstos por el comandante en el ciberespacio, y las capacidades planificadas para crear estos efectos, requieren la desconflicción con otros mandos y organismos que puedan tener intereses en la misma área del ciberespacio. Este paso crítico se gestiona desde múltiples aspectos. Desde una perspectiva puramente técnica, puede demostrarse que dos capacidades del ciberespacio pueden interoperar sin interferencias en el mismo entorno o no pueden hacerlo. Sin embargo, desde el punto de vista del riesgo operativo, incluso si varias capacidades

pueden operar sin interferencias, puede no ser prudente utilizarlas juntas. Por ejemplo, el efecto de una capacidad puede atraer la atención del adversario sobre el sistema objetivo de forma que ponga en peligro otra capacidad estadounidense o de un socio de la misión que antes pasaba desapercibida. La desconflicción técnica utiliza los resultados de las evaluaciones de garantía técnica e incluye un análisis detallado de la interoperabilidad de cada capacidad y de los aspectos ciberespaciales de la OE. El CDRUSCYBERCOM es el punto focal del MOD para la desconflicción interinstitucional de todas las acciones propuestas para las misiones OCO y DCO-RA. El Comandante, Sistemas Informáticos Aliados del MCCE, es el punto focal para la desconflicción interinstitucional de las operaciones globales de los Sistemas Informáticos Aliados y las actividades DCO-IDM que puedan afectar a más de un componente MOD. Los plazos necesarios para el análisis y la coordinación deben ser considerados e incluidos en el plan. La coordinación interinstitucional suele llevar más tiempo que la coordinación concomitante del MOD. El CO también puede requerir la desconflicción y la sincronización con las operaciones técnicas especiales conjuntas integradas (IJSTO). Información y procesos relacionados con IJSTO y su contribución al CO pueden obtenerse de los planificadores de IJSTO en el CCMD o en el cuartel general del componente de servicio.

3) **Integración de los fuegos en el ciberespacio.** Las capacidades de ataque al ciberespacio, aunque pueden utilizarse en un contexto independiente, suelen ser más eficaces cuando se integran con otros fuegos. Algunos ejemplos de la integración de los fuegos del ciberespacio son: la interrupción de los sistemas de defensa aérea del enemigo utilizando el ataque ciberespacial habilitado por EMS, la inserción de mensajes en las comunicaciones de los líderes del enemigo, la degradación/interrupción de los sistemas de navegación y cronometraje de precisión del enemigo basados en el espacio y en tierra, y la interrupción del C2 del enemigo. Los efectos en el ciberespacio pueden crearse a nivel estratégico, operativo o táctico, en cualquier fase de la operación militar, y coordinado con los fuegos letales para crear el máximo efecto sobre el objetivo. Los fuegos integrados no son necesariamente fuegos simultáneos, ya que el momento en que se producen los efectos de los ataques al ciberespacio puede ser más ventajoso cuando se sitúan antes o después de los efectos de los fuegos letales. Cada compromiso presenta consideraciones únicas, dependiendo del nivel y la naturaleza de las dependencias del enemigo en el ciberespacio. Los fuegos de apoyo al ciberespacio pueden utilizarse en un papel menor, o pueden ser un componente crítico de una misión cuando se utilizan para permitir operaciones aéreas, terrestres, marítimas, espaciales y especiales. Las fuerzas que operan con armas letales y otras capacidades en los dominios físicos no pueden utilizar los fuegos del ciberespacio de la mejor manera posible a menos que entiendan claramente el tipo y el momento de los efectos planeados en el ciberespacio. Los fuegos en el

ciberespacio adecuadamente preparados y programados pueden crear efectos que no pueden ser creados de ninguna otra manera. Los fuegos mal programados en el ciberespacio pueden ser inútiles, o peor aún, interferir con una misión que de otro modo sería eficaz.

4) **Preocupación por los riesgos.** Preocupación por los riesgos. Los JFC deben buscar continuamente minimizar los riesgos para la fuerza conjunta, así como para las naciones amigas y neutrales, las sociedades y las economías, causados por el uso del ciberespacio. Las operaciones coordinadas de las fuerzas conjuntas se benefician del uso de varias capacidades del ciberespacio, incluyendo sitios web no clasificados y aplicaciones web utilizadas para los esfuerzos de comunicación con audiencias internas y externas al MOD. Las fuerzas desplegadas en el exterior utilizan Internet, los teléfonos móviles y la mensajería instantánea con fines logísticos y morales, incluida la comunicación con amigos y familiares. Estos usos del ciberespacio son el objetivo de innumerables actores, desde naciones extranjeras hasta personas malintencionadas. El JFC trabaja con el MCCE y los Servicios, así como con las fuerzas del ciberespacio asignadas, para limitar la amenaza al ciberespacio de los Sistemas Informáticos Aliados y de los socios de la misión. Existen varias áreas de riesgo significativo para el JFC:
   a) Las amenazas internas son una preocupación importante para la fuerza conjunta. Dado que los usuarios internos tienen una relación de confianza con acceso a los Sistemas Informáticos Aliados, los efectos de su actividad maliciosa o descuidada pueden ser mucho más graves que los de los actores de amenazas externas. Cualquier usuario que no siga de cerca la política de ciberseguridad puede convertirse en una amenaza interna. Los usuarios internos malintencionados pueden explotar su acceso a instancias de gobiernos extranjeros, grupos terroristas, elementos criminales, socios sin escrúpulos o por iniciativa propia. Ya sea que los iniciados maliciosos estén cometiendo espionaje, haciendo una declaración política o expresando su descontento personal, las consecuencias para el MOD y la seguridad nacional pueden ser devastadoras. Los JFC utilizan medidas de mitigación de riesgos para esta amenaza, como el refuerzo de la formación de la fuerza conjunta para estar alerta ante actividades internas sospechosas y el uso de controles bipersonales en hardware, software o datos especialmente sensibles.
   b) Las capacidades basadas en Internet, como el correo electrónico, las redes sociales, los sitios web y los repositorios basados en la nube, se utilizan tanto con fines oficiales como no oficiales y plantean riesgos de seguridad en continua evolución que no se conocen del todo. Los riesgos de seguridad de las capacidades basadas en Internet a menudo quedan ocultos, y nuestra capacidad para mitigar estos riesgos es limitada debido a la propiedad comercial de la mayoría de los sistemas o sitios de información

de apoyo. Estos problemas de seguridad del ciberespacio y de la información, combinados con los requisitos de ancho de banda de las aplicaciones de Internet, crean un imperativo para que el comandante sea consciente y gestione activamente el impacto del uso oficial y no oficial de las capacidades basadas en Internet.

c) Las soluciones entre dominios (redes) que conectan sistemas que operan a diferentes niveles de clasificación pueden proporcionar un valor operativo significativo al JFC, pero complican las consideraciones criptográficas y de apoyo a la seguridad y deben incluirse como una consideración de planificación. Las soluciones entre dominios suelen ser necesarias en operaciones multinacionales y a nivel táctico. El ritmo de las operaciones y la creciente demanda de información por parte de los mandos y su personal pueden a veces presionar a los usuarios finales para que utilicen prácticas de seguridad deficientes. Del mismo modo, las tareas emergentes para el intercambio de información han provocado a veces que los gestores de redes construyan enlaces ad hoc sobre la infraestructura comercial existente o que conecten el ciberespacio Nacional y de sus socios sin los controles de seguridad adecuados. El riesgo para la seguridad de estos comportamientos es significativo. El MCCE trabaja con los JFC para desarrollar soluciones técnicas apropiadas y políticas de seguridad detalladas que aborden los requisitos operativos sin añadir riesgos innecesarios. Los planificadores deben incluir requisitos de coordinación temprana para que los elementos de seguridad incluidos sean apropiados para las necesidades del comandante.

3.4.2.11. Monitorización (evaluación) de las operaciones en el ciberespacio

(DOD, Cyberspace Operations JP3-12, 2018)

1) La monitorización mide el progreso de la fuerza conjunta hacia el cumplimiento de la misión. Los mandos monitorizan continuamente la OE y el progreso de la CO y los comparan con su visión e intención. La medición de este progreso hacia el estado final, y la entrega de una retroalimentación oportuna, relevante y confiable en el proceso de planeación para ajustar las operaciones durante la ejecución, involucra la comparación deliberada de los efectos pronosticados de la OC con los resultados reales para determinar la efectividad general del empleo de la fuerza en el ciberespacio. Más concretamente, la monitorización ayuda al comandante a determinar el progreso hacia la consecución del estado final deseado, la consecución de los objetivos o la realización de las tareas.

2) El proceso de monitorización de las misiones externas de CO comienza durante la planificación e incluye medidas de rendimiento (MOP) y medidas de eficacia (MOE) de los incendios y otros efectos en el ciberespacio, así como su contribución a la operación u objetivo más amplio. Históricamente, la monitorización del combate ha hecho hincapié en el componente de monitorización de los daños de la batalla (BDA) para medir los daños físicos y funcionales, pero este enfoque no siempre representa el efecto más completo, en particular con respecto al CO. Los efectos del CO suelen crearse fuera del ámbito de la batalla y a menudo no crean daños físicos. La monitorización del impacto de los efectos del CO requiere el típico análisis BDA y la monitorización de los componentes físicos, funcionales y del sistema objetivo. Sin embargo, los efectos de orden superior de las acciones en el ciberespacio son a menudo sutiles, y la monitorización de los efectos de segundo y tercer orden puede ser difícil. Por lo tanto, la monitorización de los incendios en el ciberespacio y a través de él requiere con frecuencia importantes esfuerzos de recopilación y análisis de inteligencia. La incorporación de la predicción previa al ataque y la monitorización posterior al ataque para el CO en los procesos existentes del personal de la fuerza conjunta aumenta la probabilidad de que se cumplan todos los objetivos.
3) **Evaluación del CO a nivel operativo.** El planificador de nivel operativo se ocupa de la acumulación de efectos tácticos en un efecto operativo global. En el nivel operativo, los estados mayores de planificación y operaciones desarrollan objetivos y efectos deseados para que el JFC los asigne a los subordinados. Los estados mayores subordinados utilizan los objetivos operacionales asignados para desarrollar los efectos tácticos, objetivos, tareas y objetivos y efectos subordinados, y para planificar las acciones tácticas y los MOP/MOE para esas acciones. Las acciones tácticas individuales suelen combinarse con otras acciones tácticas para crear efectos a nivel operativo; sin embargo, pueden tener implicaciones operativas o estratégicas. Normalmente, la suma de las acciones tácticas en un teatro de operaciones se utiliza para llevar a cabo una evaluación a nivel operativo, principalmente evaluaciones de operaciones [...] que a su vez apoya la evaluación a nivel estratégico (según sea necesario). Los MOPs/MOE operativos evitan la sobrecarga de información táctica proporcionando a los comandantes un método abreviado de seguimiento de las acciones tácticas y de mantenimiento del conocimiento de la situación. Los MOPs y MOE son claramente definibles y medibles, se seleccionan para apoyar y mejorar el proceso de decisión del comandante, y guían las acciones futuras que logran los objetivos y alcanzan los estados finales.
   a) MDE. Los MOE se utilizan para evaluar los cambios en el comportamiento del sistema objetivo o en el OE. Miden el progreso hacia la consecución de un estado final, el logro de un objetivo o la creación de un efecto. Los datos recogidos sobre el objetivo desde su estado previo a la misión hasta el acceso, la ejecución y, posiblemente, el análisis

posterior a las operaciones a largo plazo, pueden permitir una evaluación posterior más completa, incluida la de los efectos de orden superior. Los MOE generalmente reflejan una tendencia o muestran el progreso hacia o desde un umbral medible. Aunque los MOE pueden ser más difíciles de derivar que los MOP para una tarea discreta, son, sin embargo, esenciales para una evaluación eficaz. Por ejemplo, un MOE para una acción de ataque al ciberespacio podría ser una reducción significativa en el rendimiento del tráfico de datos del enemigo o su cambio a un medio de comunicación más interceptable. La evaluación de la OC tiene lugar tanto dentro como fuera del ciberespacio. Por ejemplo, una misión OCO para interrumpir la energía eléctrica podría ser evaluada a través de la observación visual para determinar que la energía está realmente cortada.

b) MOP. Los MOP son criterios para medir el rendimiento o la realización de una tarea. Los MOP son generalmente cuantitativos y se utilizan en la mayoría de los aspectos de la evaluación del combate, que normalmente busca datos cuantitativos específicos o una observación directa de un evento para determinar el cumplimiento de las tareas tácticas. Un ejemplo de MOP para una acción de explotación del ciberespacio podría ser la obtención de un acceso necesario o el emplazamiento de una capacidad ciberespacial en un sistema objetivo.

El desarrollo de MOPs/MOEs a nivel operativo para el CO es todavía un aspecto emergente del arte operacional. En algunos casos, las actividades en el ciberespacio por sí solas tienen efectos a nivel operacional; por ejemplo, el uso de un ataque en el ciberespacio para derribar o corromper la red del cuartel general del enemigo podría muy bien repercutir en toda la JOA. Una opción de CO puede ser preferible en algunos escenarios si sus efectos son temporales o reversibles. En tales casos, una evaluación precisa requiere la capacidad de rastrear efectivamente el estado actual del efecto potencialmente cambiante utilizando indicadores de MOE. Las operaciones de mantenimiento de la paz suelen implicar a varios mandos. Además, dado que las operaciones de mantenimiento de la paz se suelen llevar a cabo como parte de una operación más amplia, la evaluación de las operaciones de mantenimiento de la paz se suele realizar en el contexto del apoyo a los objetivos generales. Por lo tanto, las evaluaciones de las OC requieren una estrecha coordinación dentro de cada estado mayor y entre múltiples mandos. La coordinación y la federación de los esfuerzos de evaluación pueden requerir acuerdos previos antes de la ejecución. Los planificadores del CO presentan las solicitudes de evaluación con la mayor antelación posible y proporcionan una justificación suficiente para apoyar la asignación prioritaria de las capacidades de recopilación pertinentes, incluidas las que están fuera del ciberespacio.

3.5. CYBDEC: Engaño Cibernético

(Stech, Heckman, & & Strom, 2016)

(Jajodia S. , Subrahmanian, Swarup, & Wang, 2016)

La cadena de engaño es un metamodelo de alto nivel para la gestión de las operaciones de ciber-D&D desde la perspectiva del ciclo de vida De forma análoga al modelo de “cadena de muerte cibernética” de Lockheed Martin, la cadena de engaño es una adaptación del proceso de diez pasos de Barton Whaley para la planificación, preparación y ejecución de operaciones de engaño. La cadena de engaño facilita la integración de tres sistemas -el ciber-D&D, la inteligencia sobre amenazas cibernéticas y la seguridad de las operaciones cibernéticas (OPSEC)- en el sistema de defensa activa más amplio de la empresa para planificar, preparar y ejecutar operaciones de engaño. Las operaciones de engaño son llevadas a cabo por una tríada de socios iguales que trabajan en estos tres sistemas de forma interactiva: planificadores de ciber-D&D, analistas de inteligencia de ciberamenazas y especialistas en ciber-OPSEC. Esta tríada (planificadores, analistas y especialistas) es esencial para una Ciberdefensa activa basada en amenazas. Al igual que la defensa de la red informática (CND) no es una herramienta única, sino un sistema que despliega nuevas tecnologías.

Cuando se disponga de ellas, el ciber-D&D debe considerarse como una campaña operativa defensiva activa, que emplea herramientas, tácticas, técnicas y procedimientos (TTTPs) en evolución. Creemos que la cadena de engaño es un marco flexible para integrar las TTTP avanzadas en las campañas operativas mientras se centran en los objetivos de la misión de una organización. La cadena de engaño consta de ocho fases. Propósito Esta fase inicial ayuda a los gestores de la empresa a definir el objetivo estratégico, operativo o táctico de las operaciones de engaño -en otras palabras, el propósito del engaño- y los criterios que indicarían el éxito del engaño. Dado que las operaciones de engaño tienen como objetivo fundamental influir en el comportamiento del adversario, el propósito de las operaciones de Ciberengaño debe definirse en términos de la influencia deseada en los comportamientos del adversario. Es decir, el objetivo de la operación de engaño es influir en el adversario para que actúe o no en beneficio del defensor. Recopilación de inteligencia En la siguiente fase de la cadena de Ciberengaño, los planificadores de D&D definen cómo se espera que el adversario se comporte en respuesta a la operación de engaño. La definición de los comportamientos esperados se hace en parte a través de la asociación de los planificadores con la inteligencia de amenazas cibernéticas, para determinar lo que el adversario observará, cómo el adversario podría interpretar esas observaciones, cómo el adversario podría reaccionar (o no) a esas observaciones, y cómo los defensores monitorearán el comportamiento del adversario. Esta

inteligencia sobre la amenaza ayudará a los planificadores durante las dos últimas fases (supervisar y reforzar) para determinar si el engaño está teniendo éxito. La inteligencia sobre amenazas cibernéticas puede informar a los planificadores de D&D sobre lo que el adversario ya sabe, cree y, potencialmente, sus expectativas.

Notas sobre Ciberengaño efectivo

(Underbrink, 2016)

Una fuente interna de ciberinteligencia es el análisis de campañas de intrusión. En términos generales, una campaña de intrusión es un marco para agrupar eventos y artefactos de intrusión relacionados en el conocimiento de amenazas particulares para una organización. Las metodologías analíticas, como el Modelo Diamante de Análisis de Intrusiones, también son útiles para agrupar las actividades de forma coherente. Las asociaciones para compartir amenazas son otra fuente de inteligencia sobre ciberamenazas y pueden involucrar al gobierno, a la industria privada o a organizaciones sin ánimo de lucro. La información puede compartirse por diversos medios. Dos ejemplos de esfuerzos creados para el intercambio escalable y seguro de información sobre amenazas son los sistemas Structured Threat Information eXpression (STIX; http://stix.mitre.org) y Trusted Automated eXchange of Indicator Information (TAXII; http://taxii.mitre.org), patrocinados por la Oficina de Ciberseguridad y Comunicaciones del flagging) para ocultar las firmas al adversario. Los planificadores también analizan las características de los eventos y actividades nocionales que deben ser representados y observados para apoyar la historia de encubrimiento, identifican las firmas correspondientes que el adversario observaría, y planifican el uso de tácticas de engaño (como la imitación, la invención, el señuelo, o el doble juego o el doble farol) para engañar al adversario. En resumen, los planificadores de D&D convierten la información de la célula matriz en actividades operativas que revelan u ocultan la información clave que transmite la historia de cobertura. Estos pasos deben coordinarse con las actividades de ciber OPSEC para que los pasos de D&D sean lo más realistas y naturales posible, y el engaño debe permitir al adversario observar eventos operativos reales que apoyen la historia de encubrimiento. Preparar En esta fase, los planificadores de D&D diseñan los efectos perceptivos y cognitivos deseados en el adversario de la operación de engaño y exploran los medios y recursos disponibles para crear estos efectos. Esto implica la coordinación con los especialistas en OPSEC sobre el calendario para desarrollar el equipo teórico y real, el personal, la formación y otros preparativos para apoyar la historia de cobertura del engaño. Ejecutar A medida que los preparativos para el engaño y los preparativos operativos reales se sintetizan y apoyan, los planificadores de D&D y los especialistas en OPSEC deben coordinar y controlar todas las

operaciones relevantes en curso para que puedan apoyar y ejecutar de manera consistente, creíble y efectiva la historia de cobertura del engaño, sin obstaculizar o comprometer las operaciones reales. Departamento de Seguridad Nacional de Estados Unidos. STIX y TAXII proporcionan formatos estructurados para que los defensores compartan indicadores de amenazas de una manera que refleje las relaciones de confianza inherentes a dichas transferencias. STIX es un lenguaje impulsado por la comunidad que se utiliza para representar información estructurada sobre ciberamenazas. Contiene un formato estructurado para la cadena de Ciberengaño. TAXII permite compartir información a través de los límites de la organización y del producto para detectar y mitigar las ciberamenazas. Una amenaza vista por un socio hoy puede ser la amenaza a la que se enfrente otro socio en un futuro próximo. Todas estas fuentes de inteligencia sobre ciberamenazas pueden ayudar a los planificadores de D&D a evaluar la madurez de la capacidad de ciberataque de un adversario, lo que a su vez apoya el desarrollo de una operación de ciber-D&D adecuadamente personalizada. Diseño de la historia de portada La historia de portada es lo que el planificador de ciber-D&D quiere que el adversario perciba y crea. El planificador de D&D considerará los componentes críticos de la operación de D&D, evaluará las capacidades de observación y análisis del adversario, y desarrollará una historia convincente que “explique” los componentes de la operación observables para el adversario, pero que engañe al adversario en cuanto al significado y la importancia de esas observaciones. El planificador de D&D decidirá qué información debe ser ocultada (el EEFI y el NDDI, Tabla 2) y qué información debe ser creada y revelada (el EEDI y el NEFI, Tabla 2). La matriz de métodos de D&D de las Tablas 1 y 2 ayuda a los planificadores al capturar la información verdadera y falsa que debe ser revelada u ocultada para que la operación de engaño sea efectiva. Los planificadores y los operadores de ciberseguridad deben decidir qué información “pertenece” a las cuatro celdas de la matriz y obtener la aprobación de los directivos de la empresa para los objetivos del engaño y la historia de cobertura. Planificar En esta fase, los planificadores de ciber-D&D analizan las características de los eventos y actividades reales que deben ocultarse para apoyar la historia de cobertura del engaño, identifican las firmas correspondientes que serían observadas por el adversario, y planifican el uso de tácticas de negación (como el enmascaramiento, el reempaquetado, el deslumbramiento o el rojo al. Los planificadores del D&D trabajan con los analistas de inteligencia de ciberamenazas y los especialistas en OPSEC para supervisar y controlar el engaño y las operaciones reales. Esto implica supervisar los preparativos operativos tanto de los amigos como del adversario, vigilar cuidadosamente los canales de observación y las fuentes seleccionadas para transmitir el engaño al adversario, y supervisar la reacción del adversario a la “actuación”, es decir, la ejecución de la historia de cobertura. Estos canales seleccionados deben permanecer abiertos al adversario, transmitir el engaño planeado y ser observados por el adversario para transmitir

la historia de cobertura. Lo más importante es que los operadores de ciber-D&D deben monitorear al adversario para determinar si las operaciones de engaño están teniendo el efecto deseado en el comportamiento del adversario. Reforzar Si la inteligencia cibernética sobre el adversario indica que la operación de engaño no parece estar “vendiendo” la historia de encubrimiento al adversario y creando los efectos deseados en el comportamiento del atacante, los planificadores de D&D pueden necesitar reforzar la historia de encubrimiento a través de engaños adicionales, o transmitir la operación de engaño al adversario a través de otros canales o fuentes. Los planificadores pueden tener que revisar la primera fase de la cadena de engaño, ejecutar un engaño de respaldo o planificar otra operación. El engaño se ha utilizado ampliamente en la investigación cibernética, especialmente en el uso de honeypots y honeynets construidos con el propósito de recopilar información sobre los atacantes y sus técnicas. Aunque como herramienta estratégica para defender los activos de información, el engaño ha recibido menos atención. Varios investigadores han investigado las posibilidades, con el resultado de que se han propuesto varias técnicas interesantes. Los primeros trabajos en el área del engaño incluyen la exploración del uso del engaño en la ciberguerra; véase Tirenin y Faatz . Aunque el engaño se ha considerado a veces como una actividad ofensiva, las operaciones de información engañosa pueden utilizarse para apoyar funciones defensivas. Desde el punto de vista de Tirenin y Faatz, el objetivo del engaño en la Ciberdefensa es crear confusión e incertidumbre para los potenciales atacantes respecto al valor y la ubicación de los sistemas y recursos de información críticos. Recomiendan que, para que el engaño sea eficaz, debe ser dinámico, presentando al atacante una imagen de la situación que cambie continuamente. Estos cambios deben producirse rápidamente, impidiendo que el atacante construya un entendimiento válido Ciberengaño eficaz de los sistemas y redes. Sin embargo, estos cambios deben ser transparentes para los usuarios legítimos. Esto requiere un conocimiento considerable de los sistemas y redes amigos, así como un alto grado de cooperación entre los elementos que participan en el engaño; además, es probable que estos elementos estén física y lógicamente dispersos y descentralizados, y que posiblemente pertenezcan a miembros de la coalición de la fuerza amiga total, así como a las infraestructuras comerciales. Desde una perspectiva estratégica, Gerwehr y Anderson propusieron que el engaño podía utilizarse de dos formas generales (1) como medidas de protección y (2) como medidas de recopilación de información contra una serie de ataques a la infraestructura de la información. En opinión de estos investigadores, un engaño eficaz requiere un CONOPS bien definido, y proponen un concepto prototípico de operaciones que los autores denominan engaño en profundidad. En este enfoque, los engaños defensivos se implementan en capas concéntricas, con las más débiles en la periferia y las más fuertes en el núcleo. Esto es similar a los modelos de seguridad de los sistemas operativos. Una consecuencia de esto es que los atacantes son engañados de forma diferencial, dependiendo

de sus capacidades. Esto proporciona a los defensores resultados diferenciales, permitiéndoles evaluar las intenciones y capacidades de los atacantes. Gerwehr y Anderson sostienen que, mediante un marco teórico bien desarrollado, el desarrollo de herramientas, una amplia experimentación y un análisis exhaustivo es posible esperar que se proporcionen orientaciones e instrumentos operativos tanto para emplear como para combatir el engaño en la seguridad de la información. Michael y Wingfield investigaron las implicaciones políticas del potencial de abuso en el uso de ciber señuelos como medio para automatizar las actividades de contrainteligencia y las respuestas a los ciberataques. Observando que no sólo los estados, sino también las entidades no gubernamentales y los individuos pueden emplear ciber señuelos, presentaron un análisis de principios sobre el uso de ciber señuelos, y exploraron los mínimos absolutos en términos de principios consuetudinarios para lo que podría considerarse un uso aceptable del engaño. En su opinión, un señuelo anticipa algún tipo de interacción inapropiada entre un proceso de llamada y una unidad de software protegida, proporcionando por adelantado reglas para conocer y evaluar la naturaleza de la interacción, además de reglas para la respuesta. Se necesitan políticas que pongan límites al alcance y al tipo de engaño que se debe emplear, pero que proporcionen cierto grado de libertad al usuario de los señuelos para inyectar creatividad en los engaños con el fin de aumentar la probabilidad de que éstos sean efectivos. Los límites podrían usarse para delinear los umbrales que, en caso de ser violados, podrían resultar en el uso indebido o ilegal de los señuelos. Yuill investigó los procesos, principios y técnicas que intervienen en las operaciones de engaño para la defensa de la seguridad informática. Las operaciones de engaño para la seguridad informática se definen como las acciones planificadas que se llevan a cabo para engañar a los atacantes y así hacer que tomen (o no tomen) acciones específicas que ayuden a las defensas de la seguridad informática. Uno de los objetivos de esta investigación era modelar y examinar sistemáticamente las operaciones de engaño de seguridad informática. La investigación abordó estas cuestiones centrándose en el engaño para la defensa de la seguridad informática. Las cuatro contribuciones principales de esta investigación fueron: (1) un modelo de proceso para las operaciones de engaño que proporcionaría a los planificadores del engaño un marco para llevar a cabo operaciones de engaño; (2) un modelo de proceso de ocultación engañosa que ayudaría al defensor a desarrollar 118ª.J. Underbrink nuevas técnicas de ocultación y en la evaluación de las técnicas existentes; (3) sistemas de detección de intrusiones basados en el engaño; y (4) experimentos y evaluación. Esta investigación proporciona una evaluación exploratoria y confirmatoria de los modelos de engaño. Yuill et al. definieron un modelo para comprender, comparar y desarrollar métodos de ocultación engañosa. El modelo caracterizó la ocultación engañosa en términos de cómo derrota los procesos subyacentes que un adversario utiliza para descubrir lo oculto. Yuill et al. plantearon que el proceso de descubrimiento de un adversario puede adoptar tres formas: observación

directa, investigación y aprendizaje de otras personas o agentes. La ocultación engañosa funciona derrotando uno o más elementos de estos procesos. Aplicaron su modelo a la seguridad informática. Creen que su modelo de proceso ofrece un marco conceptual para desarrollar nuevas técnicas de ocultación engañosa y para evaluar las técnicas existentes, y que proporciona un marco de referencia común para la colaboración entre los profesionales de la seguridad. Rowe desarrolló una taxonomía de engaños ofensivos y defensivos utilizando un nuevo enfoque derivado de la semántica en la lingüística y calificó la idoneidad de cada uno de los engaños para la ofensiva y la defensa en la ciberguerra. La intención de la taxonomía era la planificación militar, pero esta taxonomía ha recibido poca atención dentro de los círculos de investigación o de la industria. En Rowe, el autor observó que el engaño es una práctica de larga data en la guerra, y sería natural extender la práctica a la guerra dentro del ciberespacio. Estudió el uso del engaño como medio de Ciberdefensa y descubrió que los honeypots han sido la forma de engaño más popular. Otros usos identificados por Rowe son la información falsa, los falsos retrasos, los falsos mensajes de error y el engaño de identidad. Rowe también propuso el uso de engaños estratégicos, como el anuncio de debilidades técnicas en los sistemas propios con la esperanza de inducir un ataque que se sabe que puede ser manejado. Rowe concluye que estos engaños pueden ser difíciles de implementar, ya que suelen requerir la coordinación de un gran número de personas y datos. Rowe et al. desarrollaron un banco de pruebas para llevar a cabo experimentos de engaño defensivo con el fondo aleatorio normal de los ataques de Internet. El objetivo del banco de pruebas no era experimentar la Ciberdefensa engañosa, sino utilizar el engaño como medio para investigar los ciberataques. El banco de pruebas se construyó sobre un honeypot modificado para utilizar varios métodos de engaño para engañar a un atacante. Su banco de pruebas permitía la plena interacción de un atacante con el sistema, permitiendo así una amplia gama de engaños. Sus experimentos indican una serie de conclusiones: (1) los ataques son menos probables los viernes, sábados y domingos; (2) los ataques a una dirección IP recién utilizada son elevados al principio y luego disminuyen significativamente a lo largo de unos meses; esto sugiere que una buena manera de reducir los ataques a un ordenador nuevo es reutilizar una dirección IP existente cuando sea posible; (3) unas pocas vulnerabilidades comunes son atacadas repetidamente. Si se mantienen parches actualizados para estas vulnerabilidades, el tráfico de ataques se reducirá con el tiempo, facilitando la gestión de los ataques asociados a las vulnerabilidades menos comunes; (4) desconectar un sistema aumenta las alertas debidas al tráfico ICMP; dado que hay pocas vulnerabilidades relativamente ICMP y la mayoría son fáciles de solucionar, desconectar un sistema de forma irregular puede animar a los atacantes a perder más tiempo atacando infructuosamente un sistema seguro en lugar de buscar un Ciberengaño eficaz119 objetivo más susceptible; (5) muchas de las vulnerabilidades comúnmente atacadas se refieren a características de la configuración de un

sitio; ajustando estos parámetros a valores poco interesantes o apagando los servicios puede desalentar el interés de los atacantes; (6) el último paquete recibido de una dirección IP particular muestra un rango limitado de banderas, y puede ser posible explotar esto en el engaño defensivo. Neagoe y Bishop analizaron el uso del engaño para la Ciberdefensa y señalaron que, mientras que en el pasado los defensores de los sistemas utilizaban el engaño de forma aleatoria, las investigaciones recientes han empleado métodos de engaño sistemáticos. Mientras que esta investigación ha enfatizado la noción de consistencia interna, Neagoe y Bishop desafiaron esta noción y exploraron los posibles usos de la inconsistencia en el engaño como defensa. Descubrieron que la incoherencia puede ser tan eficaz como los enfoques sistemáticamente coherentes, y tiene la ventaja añadida de ser más fácil de aplicar que la coherencia. Borders et al. desarrollaron un sistema llamado OpenFire que utilizaba el engaño para interferir en la actividad de ciberreconocimiento. A diferencia de los cortafuegos que bloquean el tráfico no deseado, OpenFire aceptaba todo el tráfico y reenviaba los mensajes no deseados a un grupo de máquinas señuelo. Para el exterior, todos los puertos y todas las direcciones IP parecían abiertos en una red OpenFire. Comprobaron que OpenFire reducía el número de ataques a servicios reales en un 65% en comparación con un sistema sin protección y en un 46% en comparación con un sistema protegido por un honeypot. Bowen et al. propusieron el uso de mecanismos de defensa basados en trampas y de una plataforma de despliegue para abordar el problema de los intrusos que intentan exfiltrar y utilizar información sensible. Su objetivo era confundir y desconcertar a un adversario que requiriera más esfuerzo para identificar la información real de la falsa y proporcionar un medio para detectar cuándo se ha producido un intento de explotar información sensible. Según su esquema, el sistema generaría automáticamente “documentos señuelo” y los almacenaría en un sistema de archivos con el objetivo de atraer a un usuario malintencionado. También incorporaron “balizas sigilosas” dentro de los señuelos que harían que se emitiera una señal a un servidor indicando cuándo y dónde se abrió el señuelo concreto. Ryu et al. examinaron un sistema de seguridad de la información que incluía el sistema de engaño desde una perspectiva económica. Desarrollaron un modelo de sistema de engaño para atraer a usuarios no autorizados y restringir su acceso al sistema real. Su modelo representa las acciones defensivas de un diseñador de sistemas contra los intrusos de forma que se maximiza la diferencia entre el coste de los intrusos y el coste de protección del sistema del diseñador. Descubrieron que cuando el contenido de información única del sistema de engaño es alto, el diseñador del sistema debe ser cauteloso. Los intrusos pueden entrar primero en el sistema de engaño y luego, utilizando la información obtenida al piratear el sistema de engaño, pueden entrar en el sistema real. La estrategia de seguridad óptima en este caso es aumentar el nivel de protección total del sistema de engaño lo antes posible. El alto contenido de información única en el sistema real ayuda a los intrusos a penetrar directamente en el sistema real

durante ambos periodos. Por lo tanto, el diseñador del sistema necesita elevar el nivel de protección para el sistema real durante ambos momentos. Por último, cuando el contenido de información común es alto, la estrategia de seguridad óptima es aumentar el nivel de protección para ambos sistemas durante el periodo de tiempo anterior. El modelo propuesto muestra que los intrusos tienen un comportamiento diferente según Underbrink la vulnerabilidad del sistema en el momento de la intrusión, así como en función de sus propios incentivos económicos. Los resultados óptimos del modelo propuesto proporcionan al diseñador del sistema información sobre cómo configurar el nivel de protección de los dos sistemas. Bowen et al. desarrollaron un sistema prototipo para inyectar automáticamente señuelos utilizados para detectar a los atacantes que están espiando el tráfico de la red. Los elementos clave del sistema incluían un generador de tráfico de señuelos automatizado, un emisor de señuelos y señuelos basados en trampas que estaban configurados para exponer al atacante cuando éste intentaba utilizarlos. Utilizaron sujetos humanos y herramientas automatizadas para evaluar la credibilidad de los señuelos y descubrieron que los jueces experimentados no podían distinguirlos del tráfico auténtico. También probaron el sistema en una red inalámbrica y detectaron con éxito las escuchas y los intentos de explotación. Aunque el uso del engaño para la defensa de los activos de información no es habitual, la investigación muestra claramente que tiene su lugar dentro del conjunto de herramientas de las operaciones de información. Sin embargo, ninguna de las investigaciones revisadas pone en práctica la visión introducida por Tirenin y Faatz ; es decir, para ser eficaz, la estrategia de engaño debe ser dinámica, presentando al atacante una imagen de la situación que cambie continuamente, impidiendo que el atacante comprenda los sistemas y redes objetivo.

3.5.1.1.1. Honeypotting incrustado

3.5.1.1.2. Descripción

La pila de engaño Las técnicas de engaño pueden introducirse en diferentes capas de la pila de software. La figura 1 ilustra esta pila de engaño, que detalla diversas capacidades de engaño disponibles en las capas de red, punto final, aplicación y datos. Por ejemplo, las redes informáticas conocidas como honeynets presentan intencionadamente vulnerabilidades que invitan, detectan y controlan a los atacantes; las plataformas de protección de puntos finales engañan al software malicioso emulando diversos entornos de ejecución y creando procesos falsos a nivel de aplicación para manipular el comportamiento del malware; y los datos falsificados pueden plantarse estratégicamente en sistemas de archivos señuelo para desinformar y desviar a los atacantes de objetivos de alto valor . La pila de engaños sugiere que la dificultad de engañar a un adversario avanzado aumenta a medida que los engaños ascienden en la pila. Esto es cierto si comparamos, por ejemplo, el trabajo asociado a la

emulación de un protocolo de red con el reto de elaborar datos falsos que parezcan legítimos para el atacante: Los protocolos tienen especificaciones claras y precisas y, por tanto, son relativamente fáciles de emular, mientras que hay muchos factores humanos complejos que influyen en que un dato específico sea plausible y creíble para un adversario concreto.

En general, las defensas de software engañoso deben emplear una o más formas de engaño, y aprovechar todas las capas de la pila de engaño en cierto grado para ser eficaces contra un adversario persistente y hábil. Este capítulo se centra en las técnicas de engaño a nivel de aplicación, que ofrecen capacidades críticas de mediación entre las capas de engaño de red, punto final y datos. Por ejemplo, un servidor web habilitado para el engaño a nivel de aplicación puede pedir al cortafuegos a nivel de red que permita que ciertas cargas útiles lleguen a la capa de aplicación, donde puede ofrecer respuestas engañosas que desvíen al adversario para que ataque a máquinas señuelo dentro de la capa de punto final. Estos señuelos pueden apelar a la capa de engaño de datos para proporcionar desinformación en forma de falsos secretos o incluso contraataques de malware contra los adversarios. Estos escenarios demuestran la necesidad constante de herramientas y técnicas que permitan a las organizaciones diseñar aplicaciones con capacidades proactivas y engañosas que degraden los métodos de los atacantes y desbaraten sus esfuerzos de reconocimiento. Con este fin, el resto de este capítulo presenta una metodología basada en el lenguaje para dotar al software de servidor heredado en vivo de capacidades engañosas de respuesta al ataque y desinformación. Nos referimos a estas capacidades como honeypots incrustados. Los honeypots embebidos se diferencian de los tradicionales en que residen dentro de los sistemas de software de misión crítica en los que los atacantes intentan penetrar; no son sistemas señuelo independientes. Por lo tanto, los honeypots incrustados ofrecen remedios engañosos avanzados contra adversarios informados que pueden identificar y evitar los honeypots tradicionales. Para que puedan ser adoptados, los honeypots incrustados imbuyen el software del servidor de producción con capacidades engañosas sin degradar su rendimiento o funcionalidad prevista. Estas nuevas capacidades engañan a los adversarios avanzados para que pierdan tiempo y recursos en vulnerabilidades fantasma y sistemas de archivos señuelo, y preparan el camino para una ciencia emergente del engaño que facilita ingeniería de software.[…] Los honeypots incrustados son de máxima interacción en el sentido de que proporcionan servicios genuinos y tienen acceso a datos genuinos, a diferencia de los honeypots tradicionales de baja y alta interacción.

3.5.1. Honeypatching

Cuando se descubre una vulnerabilidad de seguridad del software, la reacción convencional del defensor es parchear rápidamente el software para solucionar el problema. Sin embargo,

esta reacción estándar puede ser contraproducente si el parche tiene el efecto secundario de revelar y resaltar otras debilidades explotables en la red del defensor. Desgraciadamente, estos contratiempos son habituales; los parches suelen comportarse de tal manera que los adversarios pueden deducir con seguridad qué sistemas han sido parcheados y, por tanto, cuáles no están parcheados y son vulnerables. La existencia de al menos algunos sistemas sin parchear es casi inevitable, ya que la adopción de parches rara vez es inmediata; por ejemplo, a menudo se requieren pruebas para garantizar la compatibilidad del parche. Así, la mayoría de los parches de seguridad de los programas informáticos corrigen las vulnerabilidades recién descubiertas a costa de anunciar a los atacantes qué sistemas siguen siendo vulnerables. Esto ha dado lugar a una cultura de adversarios en la que el sondeo de vulnerabilidades es un elemento básico de la cibercadena. Los ciberdelincuentes buscan fácilmente en Internet software vulnerable, lo que les permite centrar sus ataques en objetivos susceptibles, de la siguiente manera. En primer lugar, el atacante envía una entrada maliciosa (una sonda) elaborada para desencadenar un fallo de software concreto y conocido de forma masiva a muchos servidores de la red. Los servidores parcheados responden a la sonda con una salida bien formada, como un mensaje de error; pero los servidores no parcheados se comportan de forma errática, por ejemplo, respondiendo con una cadena basura o colapsando y reiniciándose. Al observar esta última respuesta, el atacante envía una entrada maliciosa más constructiva a los servidores no parcheados, como una que aprovecha el fallo para secuestrar el flujo de control del software de la víctima, haciendo que realice acciones maliciosas en nombre del atacante en lugar de simplemente bloquearse. El Honeypatching es un enfoque alternativo para anticipar y frustrar estos ciberataques dirigidos. El objetivo es parchear los nuevos descubrimientos vulnerabilidades de seguridad del software de tal manera que los futuros intentos de explotación de las vulnerabilidades parcheadas parezcan exitosos para los atacantes, incluso cuando no lo son. Esto enmascara los fallos de parcheo, impidiendo a los atacantes discernir fácilmente qué sistemas son realmente vulnerables y cuáles son en realidad sistemas parcheados que se hacen pasar por sistemas no parcheados. Los ataques detectados se redirigen de forma transparente a entornos señuelo aislados y sin parches que poseen toda la potencia interactiva del servidor víctima objetivo, pero que desinforman a los adversarios con datos miel y supervisan de forma agresiva el comportamiento adversario Modelo de amenaza Los honeypatches añaden una capa de engaño para confundir la explotación de vulnerabilidades conocidas (parcheables), que constituyen la mayoría de las vulnerabilidades explotadas en la naturaleza. Los exploits previamente desconocidos (es decir, de día cero) siguen siendo amenazas potenciales, ya que tales vulnerabilidades no suelen ser parcheadas ni con honeypatches. Sin embargo, incluso los zero-days pueden ser potencialmente mitigados a través de la cooperación de los honeypatches con otras capas de la pila de engaño. Por ejemplo, un parche de miel que

recoge información de identificación sobre un adversario particular que busca explotar una vulnerabilidad conocida puede transmitir esa información recogida a un sistema de detección de intrusos a nivel de red, que puede entonces identificar potencialmente al mismo adversario que busca explotar una vulnerabilidad previamente desconocida. Aunque los parches de miel mitigan principalmente los ataques a vulnerabilidades conocidas, pueden mitigar eficazmente los ataques cuyas cargas útiles pueden ser completamente únicas y, por tanto, desconocidas para los defensores. Dichas cargas útiles pueden eludir los monitores a nivel de red, por lo que es mejor detectarlas a nivel de software en el punto de explotación. Los atacantes también podrían utilizar una carga útil para el reconocimiento, pero reservar otra para el ataque final. Por lo tanto, engañar al atacante para que lance el ataque final es útil para descubrir la carga útil del ataque final, que puede divulgar las estrategias y los objetivos del atacante que no se pueden discernir a partir de la carga útil de reconocimiento solamente. El Honeypatching se suele utilizar junto con las protecciones estándar de control de acceso, como el aislamiento de procesos y el privilegio mínimo. Por lo tanto, las solicitudes de los atacantes suelen ser procesadas por un servidor que posee privilegios estrictamente de usuario, por lo que debe aprovechar los errores del servidor web y los servicios suministrados por el kernel para realizar acciones maliciosas, como corromper el sistema de archivos o acceder a la memoria de otros usuarios para acceder a datos confidenciales. La capacidad del defensor para frustrar estos y futuros ataques se basa en su capacidad para desviar a los atacantes hacia señuelos totalmente aislados y realizar un contra-reconocimiento (por ejemplo, atribución de ataques y recopilación de información). La virtualización a nivel de SO permite que varios nodos invitados (contenedores) compartan el núcleo de su anfitrión de control. Los contenedores Linux (LXC) implementan la virtualización a nivel de SO, con gestión de recursos a través de grupos de control de procesos y aislamiento total de recursos a través de espacios de nombres Linux. Esto garantiza que los procesos, el sistema de archivos, la red y los usuarios de cada contenedor permanezcan mutuamente aislados. El control detallado de la utilización de los recursos evita que cualquier contenedor se muera de hambre en su anfitrión. Además, LXC admite contenedores respaldados por instantáneas de overlayfs, lo que es clave para una gestión eficiente de los contenedores y un rápido despliegue de señuelos. En segundo lugar, la redirección transparente de las sesiones de los atacantes puede lograrse mediante una técnica de migración de procesos ligera y de grano fino basada en el reinicio de puntos de control, que facilita la migración en vivo de las sesiones de los atacantes a los señuelos. Este enfoque se beneficia de la sinergia entre las APIs del kernel de Linux y las herramientas del espacio de usuario, permitiendo un pequeño tiempo de congelación de la aplicación objetivo y un mecanismo especial de reubicación para las conexiones establecidas que permite la migración transparente de sesiones. La migración de procesos a través de checkpoint-restart es el acto de transferir un proceso en ejecución entre dos nodos volcando su estado en el

origen y reanudando su ejecución en el destino. Este problema es especialmente relevante para la computación de alto rendimiento. Como resultado, se han desarrollado varias herramientas para soportar el checkpoint-restart de procesos críticos para el rendimiento El reinicio de procesos juega un papel fundamental a la hora de hacer viable el concepto de honeypatch. Proporciona un mecanismo rápido y sin fisuras para permitir la bifurcación transparente de las sesiones de los atacantes, y escala bien incluso en entornos pequeños debido a su granularidad a nivel de proceso, lo que reduce los recursos generales necesarios para migrar el proceso del atacante. En segundo lugar, la redirección transparente de las sesiones de los atacantes puede lograrse mediante una técnica de migración de procesos ligera y de grano fino basada en el reinicio de puntos de control, que facilita la migración en vivo de las sesiones de los atacantes a los señuelos. Este enfoque se beneficia de la sinergia entre las APIs del kernel de Linux y las herramientas del espacio de usuario, permitiendo un pequeño tiempo de congelación de la aplicación objetivo y un mecanismo especial de reubicación para las conexiones establecidas que permite la migración transparente de sesiones. En tercer lugar, para garantizar que los exploits exitosos no permitan a los atacantes acceder a los datos sensibles almacenados en la memoria de la aplicación, los honeypatches deben implementar un mecanismo dinámico de redacción secreta que redacte la imagen del proceso del atacante durante la bifurcación. Esto censura los datos sensibles de la memoria del proceso antes de que se reanude la sesión bifurcada (no parcheada). Los señuelos bifurcados alojan un sistema de archivos engañoso que omite todos los secretos, y que puede ser aderezado con desinformación para engañar, retrasar y desviar a los atacantes. La arquitectura REDHERRING, incorpora estas decisiones de diseño utilizando la clonación a nivel de proceso y la virtualización a nivel de sistema operativo para lograr una redirección ligera, eficiente en recursos y de grano fino de las sesiones de los atacantes a entornos de señuelo con caja de arena en los que los secretos han sido redactados con datos honey. En este marco, los desarrolladores utilizan los parches de miel para proporcionar el mismo nivel de seguridad que los parches convencionales, pero con la capacidad adicional de engañar a los atacantes. El centro del sistema es un proxy inverso que actúa como un proxy transparente entre los usuarios y los servidores internos desplegados como contenedores LXC. El contenedor de destino aloja la instancia del servidor web con parches de miel, y los n señuelos forman el conjunto de contenedores efímeros gestionados por el controlador LXC. Los señuelos sirven como

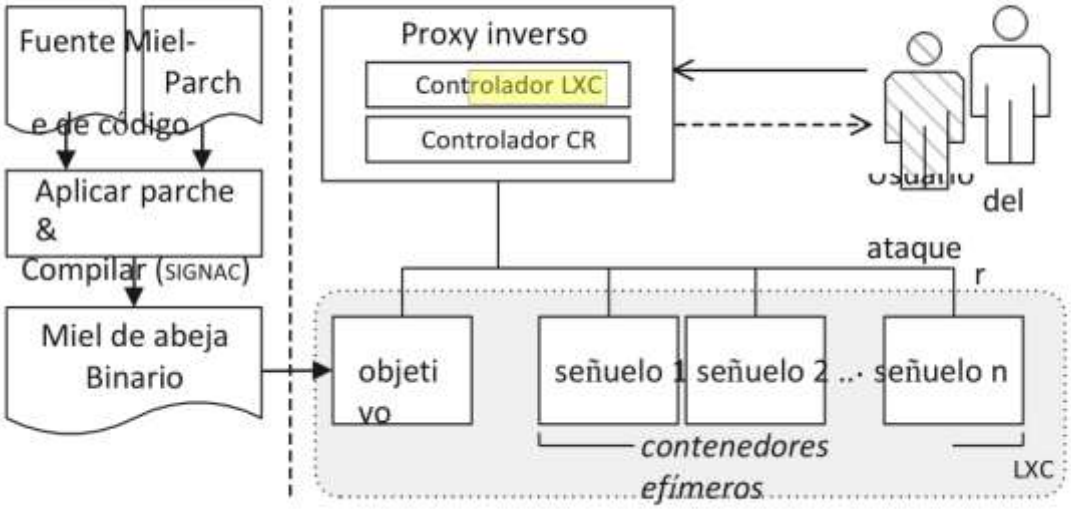


Figura 11: Arquitectura RedHerring. Fuente: (Underbrink, 2016)

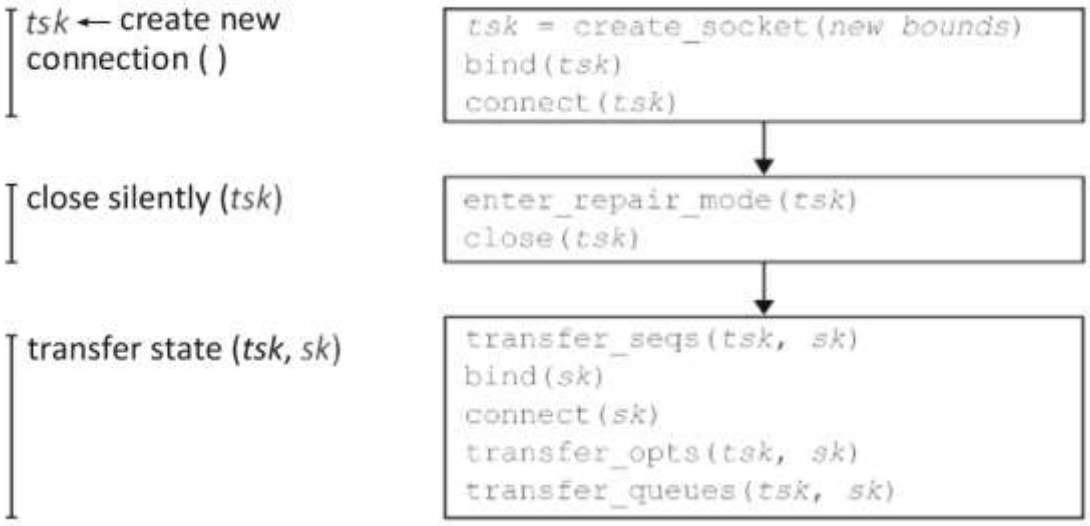


Figura 12: Sockets TCP/IP Sumideros (Fuente: (Underbrink, 2016)):

entornos temporales para las sesiones de los atacantes. Cada contenedor ejecuta un demonio CR-Service (Checkpoint/Restore), que expone una interfaz controlada por el CR-Controller para el checkpoint y la restauración remotos sesión para continuar dentro del mismo señuelo. En el objetivo, se inicia una bifurcación que consta de cuatro pasos: (1) La línea 5 registra el manejador de señales para la terminación y resurrección de la sesión. (2) La línea 6 envía una petición de fork que contiene el pgid, pid y tid de la sesión del atacante al CR- Controller

del proxy. (3) La línea 7 sincroniza el checkpoint y la resurrección de la sesión del atacante en el objetivo y el señuelo, respectivamente, y garantiza que los datos sensibles se redacten de la memoria antes de que se permita la reanudación del clon. (4) Una vez que la bifurcación se ha completado y la sesión del atacante ha sido resucitada, el contexto del parche de miel se guarda y la sesión del atacante se reanuda en el señuelo. La solicitud de bifurcación (paso 2) logra una alta eficiencia al emitir primero una bifurcación del sistema para crear un clon local poco profundo del proceso del servidor web. Esto permite que los servidores web basados en eventos continúen mientras las sesiones de los atacantes se bifurcan en señuelos, sin interrumpir el bucle de eventos principal. También elimina la carga de sincronizar las operaciones de checkpoint concurrentes, ya que CRIU inyecta un objeto binario de gran tamaño (BLOB) en el espacio de memoria del proceso objetivo para extraer los datos de estado durante el checkpoint. La sensibilidad al contexto de este marco permite que el código del parche de miel muestre un comportamiento específico del contexto: En contextos de señuelo, hp_skip elude la ejecución del bloque de código pasado como argumento a la macro, simulando elegantemente el código de la aplicación no parcheada. En un contexto objetivo, normalmente nunca se alcanza debido a la bifurcación. Sin embargo, si la bifurcación falla silenciosamente (por ejemplo, debido al agotamiento de los recursos), abandona el engaño y ejecuta conservadoramente la acción correctiva del parche original por seguridad. LXC Pool Los señuelos en los que se bifurcan las sesiones de los atacantes se gestionan como un pool de contenedores Linux controlados por el controlador LXC. El controlador expone dos operaciones al proxy: adquirir (para adquirir un contenedor del pool), y liberar (para devolver un contenedor al pool). Cada contenedor sigue el ciclo de vida. Al recibir una solicitud de bifurcación, el proxy adquiere el primer contenedor disponible del pool. El contenedor adquirido mantiene la sesión del atacante hasta que (1) la sesión es cerrada deliberadamente por el atacante, (2) el tiempo de espera de la conexión expira, (3) el contenedor efímero se bloquea, o (4) se alcanza el tiempo de espera de la sesión. Las dos últimas condiciones son resultados comunes de explotaciones exitosas. En cualquiera de estos casos, el contenedor se devuelve al pool y se somete a un proceso de reciclaje antes de volver a estar disponible. El reciclaje de un contenedor abarca tres operaciones secuenciales: destruir, clonar (que crea un nuevo contenedor a partir de una plantilla en la que los archivos legítimos se sustituyen por honeyfiles) e iniciar. Estos pasos se realizan rápidamente por dos razones principales. Para reforzar la confidencialidad de los datos y la privacidad en entornos de software engañosos y sensibles a la seguridad, el Honeypatching aprovecha las nuevas técnicas de compilación que dotan al software de capacidades de redacción dinámica de secretos. El software resultante responde a los ciberataques emergentes sustituyendo rápida y exhaustivamente todos los secretos de su espacio de direcciones por honeytokens que desinforman a los atacantes. La redacción segura y eficiente de los secretos de los espacios

de direcciones de los programas tiene muchas aplicaciones, como la liberación segura de los volcados de memoria de los programas para los desarrolladores de software con fines de depuración, la mitigación de los ciberataques a través de la autocensura en tiempo de ejecución en respuesta a las intrusiones, y el engaño de los atacantes a través de honeypotting. La realización de esta redacción secreta de procesos en tiempo de ejecución en la práctica plantea al menos dos retos importantes. En primer lugar, el paso de redacción debe producir un proceso de programa ejecutable. Por lo tanto, los datos no secretos no deben ser redactados de forma conservadora, para que no se borren los datos críticos para continuar la ejecución del programa. La redacción de secretos para procesos en ejecución es, por lo tanto, especialmente sensible a los errores de etiquetado y a la sobrecarga de datos. La proliferación de etiquetas y la sobrecarga son retos clásicos en la literatura sobre el cumplimiento de la confidencialidad de los datos. El primero se refiere a la tendencia a que el nivel de clasificación de un dato sea cada vez más restrictivo a lo largo de su vida, hasta que incluso los propietarios de los datos pueden carecer de privilegios para acceder a ellos. El segundo se refiere a la tendencia de los sistemas de seguridad de la información a clasificar excesivamente como confidenciales incluso los que no son secretos, por ejemplo, debido a que los no secretos entran en breve contacto con los datos confidenciales durante el procesamiento de la información. 3 Proceso de Reducción del Secreto de la Imagen Para reforzar la confidencialidad de los datos y la privacidad en entornos de software engañosos y sensibles a la seguridad, el Honeypatching aprovecha las nuevas técnicas de compilación que dotan al software de capacidades de redacción dinámica de secretos. El software resultante responde a los ciberataques emergentes sustituyendo rápida y exhaustivamente todos los secretos de su espacio de direcciones por honeytokens que desinforman a los atacantes. La redacción segura y eficiente de los secretos de los espacios de direcciones de los programas tiene muchas aplicaciones, como la liberación segura de los volcados de memoria de los programas para los desarrolladores de software con fines de depuración, la mitigación de los ciberataques a través de la autocensura en tiempo de ejecución en respuesta a las intrusiones, y el engaño de los atacantes a través de honeypotting. La realización de esta redacción secreta de procesos en tiempo de ejecución en la práctica plantea al menos dos retos importantes. En primer lugar, el paso de redacción debe producir un proceso de programa ejecutable. Por lo tanto, los datos no secretos no deben ser redactados de forma conservadora, para que no se borren los datos críticos para continuar la ejecución del programa. La redacción de secretos para procesos en ejecución es, por lo tanto, especialmente sensible a los errores de etiquetado y a la sobrecarga de datos. (taint-tracking) En segundo lugar, muchos de los programas del mundo real a los que se dirigen los ciberataques no se diseñaron originalmente con soporte para el seguimiento del flujo de información, y a menudo se expresan en lenguajes de bajo nivel e inseguros desde el punto

de vista tipográfico, como C/C++. Una solución adecuada debe ser Proxy inverso El proxy juega un doble papel en el sistema de Honeypatching, actuando como (1) un proxy transparente de la capa de transporte, y (2) un orquestador para la bifurcación de la sesión del atacante. Como proxy transparente, su principal objetivo es ocultar los servidores web backend y enrutar las peticiones de los clientes. Para atender las peticiones de los clientes, el servidor proxy acepta una conexión de socket descendente del cliente y enlaza una conexión de socket ascendente con el servidor backend, permitiendo adquirir señuelo 1 corriendo señuelo 2 ... señuelo n running running señuelo 1 corriendo que las sesiones de la capa de aplicación se realicen de forma transparente entre el cliente y el servidor backend. Para mantener su tamaño reducido, el proxy no manipula las cargas útiles de los mensajes ni implementa ninguna regla para detectar ataques. Tampoco hay caché de sesión. Esto lo hace extremadamente inocuo y ligero. El proxy se implementa como un proxy inverso de la capa de transporte para reducir la sobrecarga de enrutamiento y soportar la variedad de protocolos que operan por encima de TCP, incluyendo SSL/TLS. Como orquestador, el proxy escucha las solicitudes de bifurcación y coordina la bifurcación de la sesión del atacante. Bajo una carga legítima, el proxy simplemente dirige las peticiones de los usuarios al objetivo y dirige las respuestas del servidor a los usuarios. Sin embargo, las entradas de ataque provocan el siguiente flujo de trabajo alternativo: Paso 1: El atacante sondea el servidor con una solicitud falsa (denominada solicitud GET /malicioso). Paso 2: El proxy inverso enruta de forma transparente la petición al servidor web de destino del backend. Paso 3: La solicitud activa el honeypatch (es decir, cuando el honeypatch detecta un intento de explotación de la vulnerabilidad parcheada) y emite una solicitud de bifurcación al proxy inverso. Paso 4: El CR-Controller del proxy procesa la solicitud, adquiere un señuelo del LXC Pool y emite una solicitud RPC de punto de control al CR-Service del objetivo. El servicio CR 4.1 : comprueba la instancia del servidor web en ejecución en el directorio /imgs; y 4.2 :señala la sesión del atacante con un código de terminación, terminándola elegantemente. Paso 5: Una vez completado el punto de control, el controlador CR ordena al servicio CR del señuelo que restaure las imágenes del servidor web volcadas en el señuelo. A continuación, el servicio CR 5.1: restaura un clon del servidor web a partir de las imágenes de volcado ubicadas en el directorio /imgs; y 5.2 señala la sesión del atacante con un código de reanudación, y limpia el volcar los datos de /imgs. Paso 6: La sesión del atacante se reanuda en el señuelo, y se envía una respuesta al proxy inverso. Paso 7: El proxy inverso dirige la respuesta al atacante. F. Araujo y K.W. Hamlen A lo largo de este flujo de trabajo, la bifurcación de la sesión del atacante es completamente transparente para el atacante. Para evitar cualquier sobrecarga sustancial en la transferencia de archivos entre el objetivo y los señuelos, la carpeta /imgs de cada señuelo está montada en la carpeta del objetivo. directorio /imgs. Una vez que la sesión ha sido bifurcada al señuelo, se comporta como un servidor no parcheado, haciendo parecer

que no se ha producido ninguna redirección y el servidor original sondeado es vulnerable. Reubicación de la conexión TCP establecida El objetivo y los señuelos son contenedores totalmente aislados que se ejecutan en espacios de nombres separados. Como resultado, a cada contenedor se le asigna una IP única en la red interna, lo que afecta a cómo se mueven las conexiones activas desde el objetivo a un señuelo. Para realizar este caso de uso, se implementa una extensión de CRIU como parte del marco de trabajo de Honeypatching para soportar la reubicación de las conexiones TCP durante la restauración del proceso. A continuación, discutiremos detalles importantes de la implementación. El proxy inverso siempre enruta las conexiones legítimas de los usuarios al objetivo; por lo tanto, no hay necesidad de restaurar el estado de las conexiones de estos usuarios cuando se restaura el servidor web en un señuelo. Las conexiones legítimas pueden ser simplemente restauradas a los sockets de drenaje, ya que no tenemos interés en mantener la interacción de los usuarios legítimos con los señuelos. Esto garantiza que las sesiones de usuario asociadas se restauren hasta su finalización sin interrumpir la restauración general de la aplicación. A la inversa, la conexión del atacante debe ser restaurada a su estado de volcado cuando se cambia la sesión del atacante a un señuelo. Esto es importante para evitar la interrupción de la conexión y para permitir la migración transparente de la sesión (desde la perspectiva del atacante). Para conseguirlo, el proxy establece dinámicamente una nueva conexión TCP backend entre los contenedores proxy y señuelo para mantener la comunicación de la sesión del atacante. Además, se emplea un mecanismo basado en las opciones de reparación de TCP para transferir el estado del socket de sesión del atacante original (vinculado a la dirección IP objetivo) al socket recién creado (vinculado a la dirección IP señuelo). La figura 6 describe el mecanismo de reubicación de la conexión, implementado como un paso del proceso de restauración de la sesión del atacante. En el punto de control del proceso, la información de estado del socket sk original se vuelca junto con la imagen del proceso (no se muestra en la figura). Esto incluye los límites de la conexión, las opciones del socket previamente negociadas, los números de secuencia, las colas de recepción y envío, y el estado de la conexión. Durante la restauración del proceso, la conexión se reubica en el señuelo asignado (1) conectando un nuevo socket tsk al proxy $port dado en la solicitud de restauración, (2) poniendo tsk en modo de reparación y cerrando silenciosamente el socket (es decir, no se envían paquetes FIN o RST al extremo remoto), y (3) transfiriendo el estado de la conexión de sk a tsk en modo de reparación. Una vez que el nuevo socket tsk es entregado a la sesión restaurada del atacante, el proceso de reubicación se ha completado y la comunicación se reanuda, a menudo con una respuesta HTTP enviada de vuelta al atacante

3.5.1.1.1. Proceso de Redacción del Secreto de la Imagen

Para reforzar la confidencialidad de los datos y la privacidad en entornos de software engañosos y sensibles a la seguridad, el Honeypatching aprovecha las nuevas técnicas de compilación que dotan al software de capacidades de redacción dinámica de secretos. El software resultante responde a los ciberataques emergentes sustituyendo rápida y exhaustivamente todos los secretos de su espacio de direcciones por honeytokens que desinforman a los atacantes. La redacción segura y eficiente de los secretos de los espacios de direcciones de los programas tiene muchas aplicaciones, como la liberación segura de los volcados de memoria de los programas para los desarrolladores de software con fines de depuración, la mitigación de los ciberataques a través de la autocensura en tiempo de ejecución en respuesta a las intrusiones, y el engaño de los atacantes a través de honeypotting. La realización de esta redacción secreta de procesos en tiempo de ejecución en la práctica plantea al menos dos retos importantes. En primer lugar, el paso de redacción debe producir un proceso de programa ejecutable. Por lo tanto, los datos no secretos no deben ser redactados de forma conservadora, para que no se borren los datos críticos para continuar la ejecución del programa. La redacción de secretos para procesos en ejecución es, por lo tanto, especialmente sensible a los errores de etiquetado y a la sobrecarga de datos La proliferación de etiquetas y la sobrecarga son retos clásicos en la literatura sobre el cumplimiento de la confidencialidad de los datos. El primero se refiere a la tendencia a que el nivel de clasificación de un dato sea cada vez más restrictivo a lo largo de su vida, hasta que incluso los propietarios de los datos pueden carecer de privilegios para acceder a ellos. El segundo se refiere a la tendencia de los sistemas de seguridad de la información a clasificar excesivamente como confidenciales incluso los que no son secretos, por ejemplo, debido a que los no secretos entran en breve contacto con los datos confidenciales durante el procesamiento de la información. Secretos de abastecimiento y seguimiento El rastreo de manchas implica conceptualmente etiquetar cada byte de la memoria del proceso con una etiqueta de seguridad que denota su nivel de clasificación. En el momento de la compilación, un compilador de rastreo de manchas instruye el código objeto resultante con código adicional que propaga estas etiquetas junto con los datos que etiquetan. Extender este seguimiento de manchas al código heredado de bajo nivel que no ha sido diseñado teniendo en cuenta el seguimiento de manchas suele ser difícil. Por ejemplo, el enfoque estándar de especificar las introducciones de taint como entradas de programa anotadas a menudo resulta demasiado tosco para las entradas que comprenden flujos de datos de bajo nivel y no estructurados, como los sockets de red. El listado 2 ejemplifica el problema utilizando un extracto de código del servidor web Apache. El extracto divide un flujo de bytes (almacenado en el búfer s1) en un nombre de usuario no secreto y una contraseña secreta, delimitados por un carácter de

dos puntos. Etiquetar ingenuamente la entrada s1 como secreta para asegurar la contraseña hace que el compilador manche en exceso el nombre de usuario (y el delimitador de dos puntos, y el resto del flujo), llevando a una excesiva sobre-manipulación - todo lo asociado con el flujo se convierte en secreto, con el resultado de que nada puede ser divulgado con seguridad. Una solución correcta debe identificar con mayor precisión el campo de datos uptr->contraseña (pero no uptr->usuario) como secreto después de analizar los datos no estructurados. Esto se consigue en DFSan insertando manualmente una clasificación en tiempo de ejecución A diferencia de la semántica tradicional de introducción de taint, que etiqueta los valores de entrada del programa y las fuentes con taints, reconocer los campos de estructura como fuentes de taint requiere una nueva forma de semántica de taint que interpreta conceptualmente las direcciones de memoria identificadas dinámicamente como fuentes de taint. Por ejemplo, un programa que asigna la dirección &(uptr->password) a la variable de puntero p, y luego asigna una dirección de memoria recién asignada a p, debe identificar automáticamente la memoria recién asignada como una nueva fuente de taint, y a partir de entonces taint cualquier valor almacenado en p[i]. (para todos los índices i). Para conseguirlo, la semántica de combinación de punteros (PCS) de DFSan se amplía para combinar opcionalmente (es decir, unir) las manchas de los punteros y los punteros durante las desreferencias de punteros. Específicamente, cuando se activa la PCS en carga, la operación de lectura p produce un valor manchado con la unión de la mancha del puntero p y la mancha del valor al que apunta p; y cuando se activa la PCS en almacenamiento, la operación de escritura p e mancha el valor almacenado en p con la unión de las manchas de p y e. El uso de PCS conduce a una codificación natural de las anotaciones SECRET como manchas de /* los primeros dos puntos delimitan el nombre de usuario:contraseña */ s1 = memchr(hostinfo, ‘:’, s - hostinfo); si (s1) { uptr-> user = apr_pstrmemdup(p, hostinfo, s1-hostinfo); ++s1; uptr-> contraseña = apr_pstrmemdup(p, s1, s - s1); } typedef struct { NONSECRET apr_pool_t *pool; NONSECRET apr_uuid_t *uuid; SECRET_STR const char *remote_user; apr_tablet *entries; ... } SECRET session_rec; puntero. Continuando con el ejemplo anterior, PCS propaga la mancha de uptr- >contraseña a p, y las subsiguientes asignaciones de desreferencia propagan las manchas de los dos punteros a los secretos almacenados en sus destinos. El PCS funciona bien cuando los secretos están siempre separados de las estructuras que los albergan por un nivel de indirección de punteros, como en el ejemplo anterior (donde uptr-> password es un puntero al secreto en lugar del propio secreto). Sin embargo, las dificultades de deslizamiento de etiquetas surgen cuando las estructuras mezclan valores secretos con punteros no secretos. Para ilustrarlo, considere una lista enlazada ‘de enteros secretos, donde cada entero tiene una mancha diferente. Para que PCS on-store clasifique correctamente los valores almacenados en ‘->secret_int, el puntero ‘debe tener taint y 1, donde y 1es el taint deseado del primer entero. Pero esto hace que los

almacenes a '->next propaguen incorrectamente la mancha y 1al siguiente puntero del nodo, que propaga y 1ª los nodos subsiguientes cuando se dereferencian. En el peor de los casos, todos los nodos se etiquetan con todas las manchas. Estos problemas han puesto de manifiesto que la contaminación efectiva de los punteros es un reto importante en la literatura sobre el seguimiento de la contaminación. Monitorización de señuelos Los señuelos albergan monitores de software que permiten a los defensores recopilar información rica y detallada sobre los ataques. Para minimizar el impacto en el rendimiento de los señuelos, en REDHERRING se implementan dos herramientas de monitorización potentes y muy eficientes: inotifywait (para rastrear las modificaciones realizadas en el sistema de archivos) y tcpdump (para monitorizar la entrada y salida de paquetes de red). Para evitar la posible manipulación de los datos recogidos, todos los registros se almacenan fuera de los entornos de señuelo. Además, ambas herramientas de monitorización están ajustadas para evitar la generación de resultados espurios (por ejemplo, excluyendo ciertos directorios y limitando el tráfico de red monitorizado). Como ejemplos ilustrativos, los datos de ataque recogidos en los señuelos pueden utilizarse para informar a las defensas perimetrales para bloquear los intentos de exploits contra máquinas no parcheadas en la red, y para proporcionar inteligencia de amenazas detallada para ayudar a los analistas en los escenarios de respuesta a la incidencia. Para evaluar el Honeypatching, hay que determinar la sobrecarga de rendimiento impuesta a las sesiones bifurcadas a los señuelos (es decir, el impacto en los usuarios maliciosos), y estimar el impacto del Honeypatching en el rendimiento general del sistema (es decir, su impacto en los usuarios legítimos). Para obtener mediciones de referencia que sean independientes de la sobrecarga de la red, los experimentos de esta sección se ejecutan localmente en un único host utilizando la configuración predeterminada de Apache. El rendimiento se mide en términos de tiempo de ida y vuelta de las peticiones HTTP. Sobrecarga de bifurcación de sesiones Para evaluar el impacto en el rendimiento de los atacantes, se presentan los resultados de las pruebas de referencia para tres implementaciones de Apache con parches de miel: Sobrecarga global del sistema Para completar la evaluación, REDHERRING también se probó en una amplia variedad de perfiles de carga de trabajo que consistían en sesiones de usuarios legítimos y atacantes en un único nodo. En este experimento, los usuarios y los atacantes lanzan peticiones HTTP legítimas y maliciosas, respectivamente. El tamaño de la carga útil de la petición es de 2,4 KB, basado en la mediana de KB por petición medida por las métricas web de Google. Para simular diferentes perfiles de uso, el sistema se prueba tiene un impacto insignificante en el rendimiento de las peticiones legítimas y de los usuarios en comparación con los parches tradicionales, incluso durante los ataques concurrentes. Esto también demuestra que REDHERRING puede hacer frente a grandes cargas de trabajo. Este experimento evalúa su rendimiento de referencia considerando sólo una instancia del servidor de destino que se ejecuta en una máquina virtual

de un solo nodo. En un entorno real, se pueden desplegar varias instancias similares utilizando un esquema de granja web para escalar hasta miles de usuarios, como se presenta a continuación

3.5.1.1.2. ¿Es el Honey-Patching la seguridad a través de la oscuridad?

La “seguridad a través de la oscuridad” se ha convertido en un sinónimo de prácticas de seguridad que se basan en la ignorancia del adversario sobre el diseño del sistema más que en cualquier principio fundamental de seguridad. La historia ha demostrado que tales prácticas ofrecen una seguridad muy débil en el mejor de los casos, y son peligrosamente engañosas en el peor, ofreciendo potencialmente una ilusión de seguridad que puede fomentar una mala toma de decisiones Las defensas de seguridad basadas en el engaño corren el riesgo de caer en la trampa de la “seguridad a través de la oscuridad”. Si el engaño de la defensa se basa en la ignorancia del atacante sobre el diseño del sistema -detalles que los defensores deberían suponer, de forma conservadora, que acabarán siendo conocidos por cualquier actor de amenaza convenientemente persistente-, entonces cualquier seguridad ofrecida por la defensa podría ser ilusoria y, por tanto, poco fiable. Por lo tanto, es importante examinar detenidamente la base subyacente sobre la que se puede considerar que el honeypotting integrado es una tecnología que mejora la seguridad. Al igual que todas las estrategias de engaño, la eficacia de las redes de infiltración se basa en la retención de ciertos secretos para los adversarios (por ejemplo, qué vulnerabilidades de software han sido parcheadas). Sin embargo, el mantenimiento de secretos no descalifica por sí mismo el honeypotting como dependiente de la oscuridad. Por ejemplo, la criptografía moderna es frecuentemente defendida como un sello distintivo de la defensa contra la inseguridad a pesar de su suposición fundacional de que los adversarios carecen de conocimiento de las claves privadas, porque revelar los detalles completos de la implementación de los algoritmos criptográficos no ayuda a los atacantes a romper los criptotextos derivados de las claves no reveladas. Juels define la indistinguibilidad y el secreto como dos propiedades necesarias para el éxito del despliegue de los sistemas de miel. Estas propiedades se formalizan como sigue: Consideremos un sistema simple en el que S s1 ; ::: ; sn denota un conjunto de n objetos de los cuales uno, s* s j, para j 1; :: ; n es el objeto verdadero, mientras que los otros n 1 son objetos miel. Las dos propiedades son entonces: Indistinguibilidad: Para engañar a un atacante, los objetos miel deben ser difíciles de distinguir de los objetos reales. En otras palabras, deben extraerse de una distribución de probabilidad sobre posibles objetos similar a la de los objetos reales. Secreto: En un sistema con objetos miel, j es un secreto. Por supuesto, los objetos miel sólo pueden engañar a un atacante que no conozca j, por lo que j no puede residir junto a S. Por tanto, entra en juego el principio de Kerckhoffs: la seguridad del sistema debe residir en el

secreto, es decir, en la distinción entre los objetos miel y los reales, y no en el mero hecho de utilizar objetos miel. El honeypotting incrustado como paradigma satisface estas dos propiedades por diseño: La Indistinguibilidad se deriva de la incapacidad de un atacante para determinar si un ataque aparentemente exitoso es el resultado de la explotación de una vulnerabilidad sin parches o de un parche de miel que se hace pasar por una vulnerabilidad sin parches. Aunque la Indistinguibilidad absoluta y universal es probablemente imposible de lograr, muchas formas de distinguibilidad pueden, sin embargo, hacerse arbitrariamente difíciles de discernir. Por ejemplo, los servidores-monedas pueden mostrar distribuciones de retardo de respuesta que imitan a las de los servidores sin parches con un grado de precisión arbitrario (por ejemplo, retrasando artificialmente las peticiones legítimas que no se bifurcan para que coincidan con la distribución de las peticiones maliciosas que se bifurcan, como se describe en la Sec. 4). El secreto implica que el conjunto de vulnerabilidades honeypatched debe ser secreto. Sin embargo, el conocimiento completo por parte del atacante de los detalles de diseño e implementación del Honeypatching no revela qué vulnerabilidades ha identificado y parcheado un defensor. Adaptando el principio de Kerckhoffs para el engaño, un honeypatch no es detectable incluso si todo sobre el sistema, excepto el honeypatch, es de conocimiento público. Esto sostiene que el paradigma del honeypotting incrustado (y el engaño cibernético basado en el lenguaje en general) no deriva su valor de seguridad de la oscuridad. Más bien, sus engaños se basan en secretos bien definidos - específicamente, el conjunto de vulnerabilidades parcheadas en las aplicaciones objetivo. Mantener esta distinción de confidencialidad entre el carácter público de los detalles de diseño e implementación de los honeypots, frente al secreto de exactamente qué vulnerabilidades instancian esos detalles, es importante para elaborar engaños robustos y eficaces.

Concepto de honeypatch

Este capítulo introdujo y formuló el concepto de honeypots incrustados como un enfoque a nivel de lenguaje para armar el software de producción con capacidades engañosas que engañan a los adversarios para que pierdan tiempo y recursos en vulnerabilidades fantasmas y sistemas de archivos señuelo incrustados. Los honeypots incrustados emplean parches de miel para ocultar a los atacantes la información de qué vulnerabilidades de seguridad del software están parcheadas, degradando así los métodos de los atacantes y desbaratando sus esfuerzos de reconocimiento. Para realizar un Honeypatching eficiente y preciso de los servidores web de producción, se destaca un nuevo análisis de taint dinámico, estáticamente instrumentado, construido sobre la infraestructura del compilador LLVM. La implementación mejora significativamente la viabilidad del rastreo dinámico de manchas para el código heredado de bajo nivel que almacena secretos en estructuras de datos de gráficos. Para aliviar

la carga de anotación del programador y evitar las explosiones de manchas que sufren los enfoques anteriores, se introduce una nueva semántica de combinación de punteros que

resiste la propagación excesiva de manchas a través de los bordes del gráfico. Los servidores engañosos borran por sí mismos sus espacios de direcciones en respuesta a las intrusiones, lo que ofrece a los defensores una nueva herramienta para el seguimiento y la desinformación de los atacantes. Los honeypots incrustados se diferencian de los tradicionales en que residen

dentro de los sistemas de software reales y de misión crítica en los que los atacantes intentan penetrar, y no como sistemas señuelo independientes. Por lo tanto, los honeypots incrustados ofrecen remedios engañosos avanzados contra adversarios informados que pueden identificar y evitar los honeypots tradicionales. Para que puedan ser adoptados, los honeypots incrustados impregnan el software del servidor de producción con capacidades engañosas sin perjudicar su rendimiento o funcionalidad prevista. Estas nuevas capacidades hacen que los

ciberataques sean significativamente más costosos y arriesgados para sus autores, y dan a los defensores más tiempo y oportunidades para detectar y frustrar los ataques entrantes.

3.5.1.1.3. Infraestructura virtual ágil para el Ciberengaño contra los ataques DDoS sigilosos

(Al-Shaer & Gillani, 2016)

Los ataques DDoS han sido una amenaza persistente para la disponibilidad de la red durante muchos años. La mayoría de las técnicas de mitigación existentes intentan proteger contra los DDoS filtrando el tráfico de ataque. Sin embargo, como los recursos críticos de la red suelen ser estáticos, los adversarios son capaces de eludir el filtrado mediante el envío de tráfico bajo sigiloso de un gran número de bots que imitan el comportamiento del tráfico benigno. Los ataques sigilosos sofisticados a los enlaces críticos pueden causar un efecto devastador, como la partición de dominios y redes. Nuestro enfoque propuesto, llamado MoveNet, defiende contra los ataques DDoS cambiando proactiva y reactivamente la huella de los recursos críticos de forma impredecible para engañar el conocimiento del atacante sobre los recursos críticos de la red. MoveNet emplea redes virtuales (VN) para ofrecer una reasignación constante, dinámica y consciente de las amenazas de los recursos críticos de la red (migración de VN). Nuestro enfoque tiene dos componentes: (1) una planificación de la migración de VNs correcta por construcción que aumenta significativamente la incertidumbre sobre los enlaces críticos de múltiples VNs mientras preserva las propiedades de la VN, y (2) un mecanismo eficiente de migración de VNs que identifica la secuencia de configuración

apropiada para permitir la migración de nodos mientras se mantiene la integridad de la red (por ejemplo, evitando la desconexión de sesiones).[...]

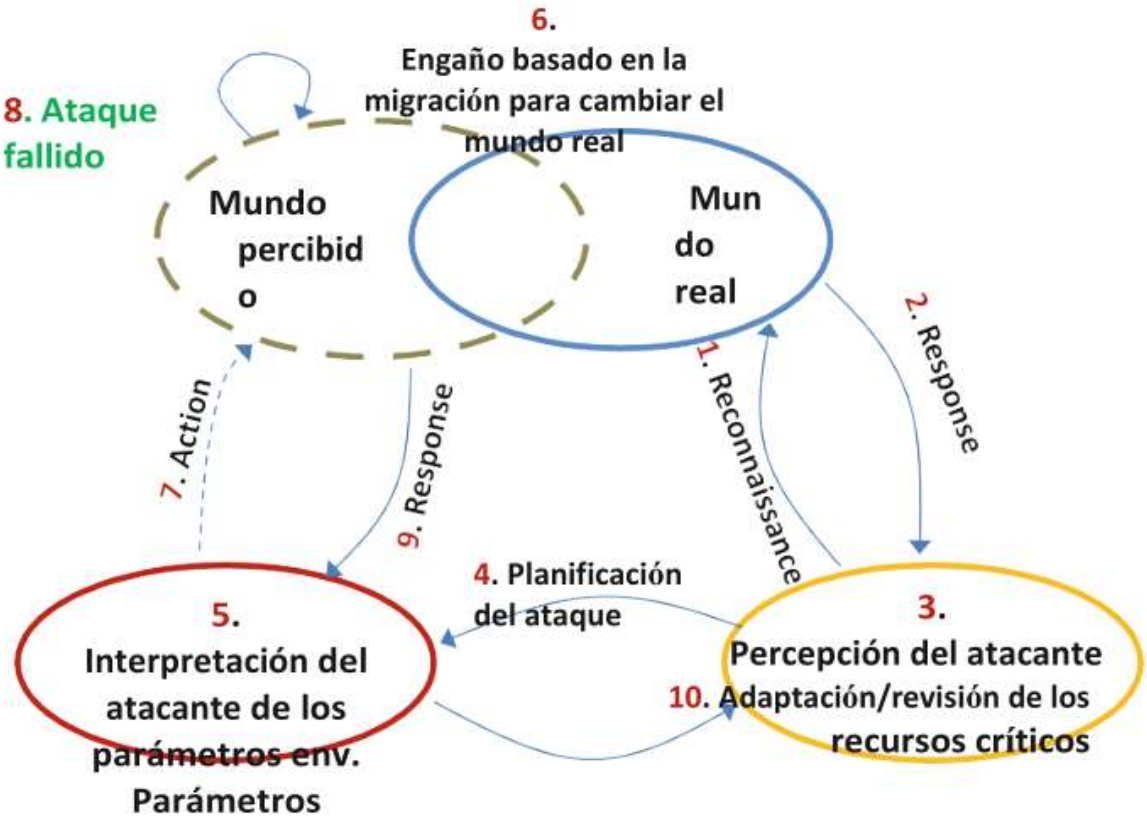


Figura 13: Lógica del Ciberengaño. Fuente: (Underbrink, 2016)

Las ciberamenazas persistentes exigen un movimiento continuo de las VNs, lo que requiere una técnica de colocación de VNs demostrablemente correcta para garantizar la funcionalidad intacta del servicio en todo momento. Formalizamos dicha técnica de colocación de VN como un problema de satisfacción de restricciones utilizando métodos formales basados en la Teoría de la Satisfacción Modular (SMT). Adoptamos los mismos requisitos de colocación de VN utilizados en la literatura y los definimos formalmente como restricciones en el modelo. La defensa proactiva requiere identificar los recursos críticos que pueden ser sustituidos por recursos no críticos para engañar a los atacantes. Nuestro marco VN es genérico para todos los ataques DDoS basados en enlaces y de reconocimiento. Pero para mostrar la eficacia de nuestro enfoque, utilizamos, como caso de estudio, el ataque Crossfire que es el más devastador y sigiloso hasta la fecha. Llamamos a esta defensa proactiva MoveNet Agility. La defensa proactiva, aunque efectiva, puede ser costosa para algunas aplicaciones. Por lo tanto, MoveNet también ofrece un engaño reactivo llamado MoveNet Sensing que investiga activamente los intentos de reconocimiento en la red y utiliza esta información para sustituir los recursos críticos objetivo por recursos no críticos para engañar al adversario. El propósito de la agilidad de la NV es reemplazar con frecuencia el sustrato crítico potencialmente

descubierto por nuevos recursos válidos y seguros para las amenazas, de manera que (1) el proceso de selección de los nuevos recursos sea impredecible para el adversario, y (2) la migración a estos nuevos recursos sea más rápida que el tiempo de reconocimiento del adversario. Esto, por tanto, engañará constantemente a los adversarios invalidando sus suposiciones sobre la colocación de los recursos críticos de la VN, descubiertos en la fase de reconocimiento. Todas estas restricciones se definen formalmente como parte del modelo del marco ágil de la RV utilizando SMT. Los solucionadores SMT avanzados, como Z3 y Yices, pueden resolver decenas de miles de restricciones y millones de variables. Por lo tanto, nuestro enfoque es escalable a grandes redes con múltiples VNs.

3.6. Marco legal y regulatorio

Desarrollar un marco legal y regulatorio que rija MILCYBDEC no está dentro del alcance del presente trabajo, más aún cuando el marco legal de actividades de ciberguerra sigue mutando sustancialmente en la actualidad. Para de cara al presente trabajo, como marco legal y regulatorio, usaremos el Manual de Tallin 2.0 (Schmitt, 2017), que abarca las opiniones de varios expertos legales. El Manual de Tallin contiene recomendaciones de expertos que nos darán indicios sobre el cumplimiento de las Leyes de la Guerra.

En 2007, varios servicios electrónicos públicos y privados de Estonia fueron víctimas de un ataque de operaciones cibernéticas maliciosas. Estos ataques coordinados de la comunidad internacional sobre los graves riesgos que plantea la creciente que plantea la creciente dependencia de los Estados y sus poblaciones del ciberespacio. ciberespacio. En retrospectiva, se trataba de ataques DDoS bastante suaves y sencillos, mucho menos dañinos que los que se produjeron. bastante suaves y sencillos, mucho menos dañinos que los que han seguido. Sin embargo, fue la primera vez que se pudo aplicar el dictado de Clausewitze: La guerra es la continuación de la política por otros medios. Los ataques también aceleraron la creación del Centro de Excelencia de Ciberdefensa de la OTAN (NATO CCD COE) en Tallin. Estonia tiene el honor de acoger y contribuir a este centro de estudios y formación de categoría mundial de clase mundial que es un socio valioso para la OTAN, los aliados y la comunidad internacional. comunidad internacional. Entre las primeras actividades del CCD COE de la OTAN fue encargar un importante estudio sobre la ciberguerra a un grupo internacional de expertos en derecho. Los expertos examinaron el modo en que el derecho El derecho nacional regula el uso de la ciberfuerza por parte de los Estados y el empleo de operaciones cibernéticas durante un conflicto armado. El Manual de Tallin resultante se ha convertido en una guía para que los gobiernos de todo el mundo de todo el mundo a la hora de evaluar la aplicación del derecho internacional en este tipo de situaciones. Tras la publicación del Manual de Tallin en 2013, el CCD COE de la OTAN puso en marcha un esfuerzo de investigación posterior para ampliar el Manual y para que abarque el derecho internacional que rige las actividades cibernéticas que se producen en tiempo de paz. El resultado es, con mucho, uno de los análisis más completos del derecho internacional aplicable a las actividades cibernéticas en tiempo de paz. más completo del derecho internacional aplicable a las operaciones cibernéticas. La publicación que tiene en sus manos abarca temas que van desde el derecho espacial y la jurisdicción hasta derecho internacional de los derechos humanos, así como un análisis del derecho de los conflictos del primer Manual de Tallin. El hecho de que el derecho internacional sea a menudo desestimado como una

fachada de la realpolitik es engañoso. Este enfoque infravalora la importancia de los acuerdos internacionales en el mantenimiento de la paz y la seguridad. Para las democracias liberales que respetan el Estado de Derecho, el derecho internacional sin duda condiciona la actividad de los gobiernos. En un momento en que las acciones de Estados sin escrúpulos y de grupos extremistas violentos siguen amenazando la paz y la seguridad a nivel internacional, es aún más importante que esas acciones se contrarresten con un fuerte compromiso con el derecho internacional vigente y los valores que representa.

3.7. Modelos de Madurez de Ciberseguridad

En el ámbito militar, por razones de Clasificación de la Información, rara vez es posible acceder a la bitácora completa de las Misiones de Ciberengaño. Esto último dificulta poder hacer un análisis pormenorizado del nivel de Ciberseguridad que han alcanzado dichas Misiones. A través de la recolección de evidencias recolectas por Fuentes Abiertas (OSINT) o cedidas por el Mando de dichas misiones, sí es posible medir el Nivel de Madurez en Ciberseguridad, estableciendo una serie de indicadores comunes que habilitan la definición de un Modelo de Madurez elegido. Existe un amplio abanico de Modelos de Madurez. Según un estudio, donde se revisan más de 200 Modelos de Madurez (Rea-Guaman, San Feliu, Calvo-Manzano, & Sanchez-Garcia, 2017), se concluye que

1) La gran mayoría están basados en Cybersecurity Capability Maturity Model C2M2 (US Department Of Energy, 2019)
2) El nivel de Ciberseguridad en una misión MILCYBDEC se puede medir mediante un Modelo de Madurez adaptado de los modelos de capacidad de ciberseguridad del ámbito de TIC.

En los apartados siguientes se discuten varios parámetros, metodología de aplicación y dominios de aplicabilidad de los modelos de madurez de los que derivará la metodología MILCYBDEC.

3.7.1. Cybersecurity Capability Maturity Model (C2M2)

El Cybersecurity Capability Maturity Model C2M2 (US Department Of Energy, 2019) trata sobre la implementación y gestión de la ciberseguridad de procesos y activos TIC, OT y los entornos asociados a su operación. Dicho modelo, entre otros, ayuda a instrumentalizar, planificar, organizar y medir el mejoramiento en capacidades y madurez en Ciberseguridad.

C2M2 es elegido punto de partida de MILCYBDEC, debido a su escalabilidad y su encaje en el NIST Cybersecurity Framework (NIST CSF).

C2M2 considera los siguientes dominios de aplicabilidad:

1) Gestión de Riesgos,
2) Gestión de activos
3) Cambios y configuración
4) Gestión de identidades
5) Gestión de amenazas y vulnerabilidades

6) Conciencia situacional
7) Respuesta a eventos e incidentes
8) Gestión de la cadena de suministro y dependencias externas
9) Gestión de la fuerza de trabajo
10) Gestión de Programas de Ciberseguridad.

3.7.2. NICE Framework WorkForce Framework

NICE Framework (Petersen, Santos, Wetzel, Smith, & Witte, 2020) , publicado por el Instituto NIST, es un marco de trabajo y ontología que se centra en siete categorías que, engloban entre otros roles de personal de seguridad, tareas asociadas, conocimientos y habilidades que deben tener dichos roles. De cara a una organización, el marco de trabajo 'NICE Framework' permite definir de forma completa los conocimientos, tareas y habilidades de los perfiles que deben satisfacer los profesionales de la ciberseguridad que trabajan o trabajarán para dicha organización.

3.7.3. COBIT

COBIT es un metamodelo de gobernanza de la ciberseguridad, publicado por ISACA. ISACA es un colectivo federado mundial, de profesionales expertos en Ciberseguridad y Gobernanza, que han plasmado sus experiencias en dicho modelo. COBIT prevé por lo menos cinco niveles que califican la madurez de los procesos de gobernanza y/o de Ciberseguridad, evaluándolos uno por uno, según el plan de auditoría:

1) Iniciado
2) Repetible
3) Definido
4) Gestionado
5) Optimizado

4. Capítulo 4: Metodología MILCYBDEC

Se procede a presentar el resultado final de la investigación, que es una Metodología de evaluación de la madurez de una Misión de Ciberengaño y la redacción de una serie de mejoras sugeridas a fin de alcanzar un nivel de madurez deseado. Es una metodología adaptable, al valorar primero la aplicabilidad de los dominios de control, antes de comenzar cualquier proceso de valoración y/o auditoría. Dicha metodología está fuertemente derivada de las metodologías mencionadas en el punto 3.

4.1. Metodología de trabajo

La actual investigación se ha basado en una extensa inspección del Estado de Arte (documentación), en entrevistas (derivadas de trabajo desclasificado y autorizado para la diseminación) de colaboradores en proyectos EDIDP y H2020, y algunos inputs de OSINT.

Las etapas de la presente investigación han sido

1. **Investigación** bibliográfica del área de conocimiento referente a MILCYBDEC, Ciberseguridad, Doctrina Militar
2. **Estudiar** los Marcos y Metodologías de Medición de Madurez que satisfagan estructuralmente las necesidades de una Metodología MILCYBDEC y **extraer** los **indicadores** comunes de madurez.
3. **Crear** una metodología junto a un instrumento de medición de capacidad y nivel de madurez
4. **Analizar de resultados** de aplicar la metodología a varios casos experimentales y obtener **conclusiones**

La metodología propuesta asistirá a los planificadores en comprender las carencias de sus procesos de MILCYBDEC y en alcanzar un nivel de madurez superior que el actual, corrigiendo dichas carencias.

En la siguiente figura se ilustra las fases de aplicación de la metodología MILCYBDEC;

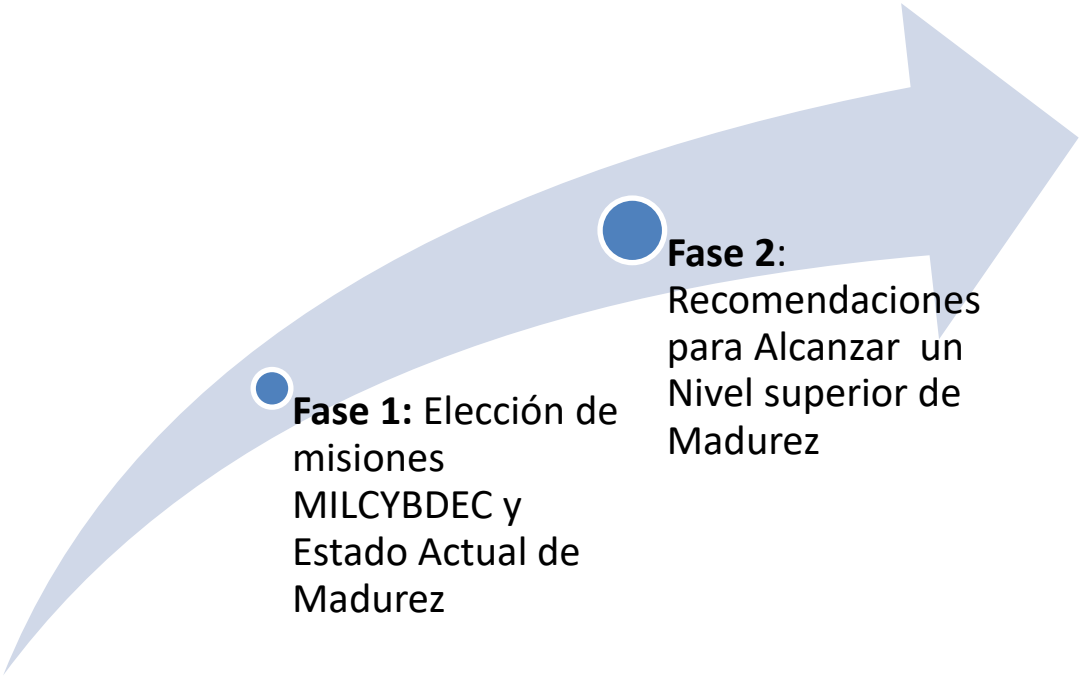


Figura 14: Fases de Madurez de la gestión de MILCYBDEC. Fuente: elaboración propia

4.2. Fase 1: Elección de misiones MILCYBDEC y Estado Actual de Madurez de Seguridad

En Fase 1 se elige la Misión de MILCYBDEC cuyo nivel de madurez de ciberseguridad se quiere medir. En el presente trabajo de investigación, se han escogido misiones sobre las cuales existe suficiente OSINT, ya que las bitácoras de operaciones militares, por regla general, constituyen información reservada, y no es recomendable diseminarlas. Se mide el nivel de madurez de la misión de MILCYBDEC seleccionada, mediante un instrumento de medición 'IMILCYBDEC'. Dicho instrumento analiza el cumplimiento de los dominios de control. Dichos dominios de control vienen extraídos del Análisis del Estado del Arte, de la experiencia personal del experto que realiza la auditoría y del Análisis de Metodologías, hecha en capitulo anterior. Se tienen en cuenta varios dominios, ya sea de Doctrina, de MILDEC, de Seguridad de la Información, de OPSEC, de gestión de personal.

4.3. dominios, subdominios y prácticas

Se define la unidad de medición de madurez en ciberseguridad como estructura de dos componentes más básicos: integridad y alcance. Así mismo la Integridad se define como el grado de implementación sistemática, extendida y más automatizada de dicha medida. El alcance, por su cuenta, mide el grado de ajuste de la medida de ciberseguridad con las necesidades reales del sistema en particular, o con la industria en general. Los dominios de control elegidos para MILCYBDEC, satisfacen dichas dimensiones de alcance e integridad. Dichos dominios han sido extraídos de entre los distintos Modelos de Madurez y Doctrinas Militares Analizados:

1) Misión MILCYBDEC
2) Ciber conciencia Situacional
3) Gestión de Riesgos y Vulnerabilidades
4) Gestión de Identidades
5) Ciclo de Vida, Protección de Activos y Servicios
6) Cumplimiento de Leyes de la Guerra
7) Gestión de Incidentes y Resiliencia

En general, para elegir los dominios aplicables de Ciberseguridad, se ha buscado aquellos que fortalecen los aspectos de Seguridad de la Información, OPSEC, Cumplimiento normativo, Cumplimiento Doctrinal, y que facilitan una mejor Gestión de Riesgos, Continuidad, y de Misión, de cara a una misión MILCYBDEC. Una vez elegidos los dominios, se distinguen por lo menos dos agrupaciones temáticas:

1. Planificación, Misión, Estrategia y Cumplimiento
2. OPSEC y Seguridad de la Información

4.3.1. Planificación, Misión, Estrategia y Cumplimiento

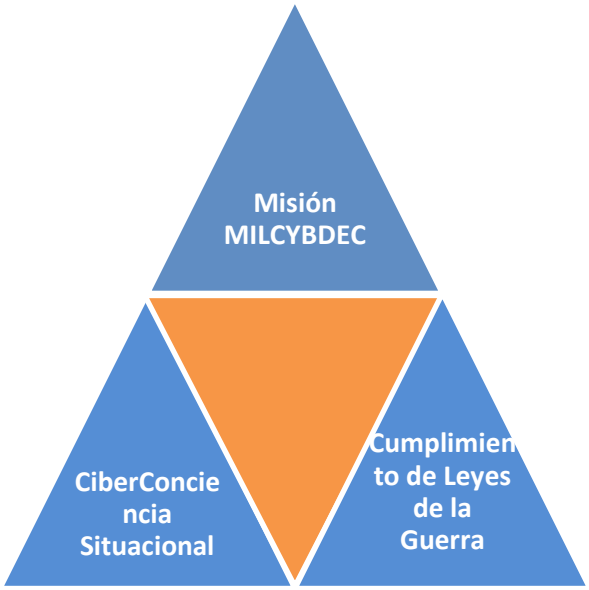


Figura 15: Planificación, Misión, Estrategia y Cumplimiento. Fuente: elaboración propia

Una misión MILCYBDEC es una misión que combina MILDEC y Ciber engaño, ejecutada en el dominio cibernético de batalla. En capítulos anteriores, hemos expuesto el Estado de Arte de dichos dominios de conocimiento. La ciber conciencia situacional, es un concepto explicado en capítulos anteriores, y es esencial para llevar con éxito una misión MILCYBDEC. El cumplimiento de leyes de la guerra sigue de cerca las sugerencias del Manual de Tallin, anteriormente mencionado.

4.3.2. OPSEC y Seguridad de la Información

Figura 16: OPSEC y Seguridad de la Información, Fuente: elaboración propia

Seguridad de Operaciones y Seguridad de la Información es una familia de buenas prácticas y procesos absolutamente esenciales para la buena Gobernanza. La gestión de Riesgos y Vulnerabilidades viene a Mantener, Crear y Alertar sobre Riesgos, para la Misión MILCYBDEC, y Vulnerabilidades técnicas, legales, que pueden afectar a los sistemas (y crear Riesgos). Gestión de identidades, gestión de ciclo de vida y/o Protección de Activos y Servicios son procesos estándar de la buena Gobernanza de todo sistema informático orientado a usuarios finales debe tener. Una vez que se han definido y desarrollado el contexto de cada uno de los dominios y las prácticas que se deben conseguir para establecer el nivel de madurez de una Misión MILCYBDEC, se hace un resumen de todos estos dominios en la Figura 20. Dominios del Modelo de Madurez de Seguridad para MILCYBDEC. La Gestión de Incidentes y Resiliencia, es un dominio necesario para toda buena Gestión de Negocio o de Misión. Principalmente, inspirado en COBIT. (ver capítulos anteriores)

Figura 17: Dominios del Modelo de Madurez de Seguridad para CYBMILDEC, Fuente: elaboración propia

Niveles de Madurez

Mediremos cinco niveles de implementación para cada dominio de prácticas. Desde Nivel 0 hasta Nivel 4. Un número mayor significa una implementación más conseguida. Hay cinco niveles de exhaustividad para cada dominio de seguridad, subdominio y práctica, desde el Nivel 0 hasta el Nivel 4, con un número mayor que indica un mayor grado de exhaustividad. Para el modelo de MILCYBDEC, se toman en cuenta los siguientes principios para los niveles de madurez: (Moreno de Rodríguez, 2020)

1.Los niveles del indicador de madurez se aplican independientemente a cada dominio. Como resultado, una misión MILCYBDEC que usa el modelo puede estar operando en diferentes

clasificaciones o niveles para diferentes dominios. Por ejemplo, una organización podría estar operando en nivel 1 en un dominio, nivel 2 en otro dominio y nivel 3 en un tercer dominio

2.Los niveles son acumulativos dentro de cada dominio; para obtener un nivel en un dominio determinado, una organización debe realizar todas las prácticas en ese nivel y sus niveles predecesores. Por ejemplo, una organización debe realizar todas las prácticas de dominio en nivel 1 y nivel 2 para lograr nivel 2 en el dominio. Del mismo modo, la organización tendría que realizar todas las prácticas en los niveles 1, 2, 3 y 4 para lograr el nivel 4.

Para la metodología MILCYBDEC, cada nivel se define como sigue:

Nivel 0, Inseguro: No hay una comprensión común de cómo se aplica la práctica de seguridad y no se implementan requisitos relacionados.

Nivel 1, Mínimo: Se implementan los requisitos mínimos de la práctica de seguridad. No hay actividades de garantía para la implementación de la práctica de seguridad.

Nivel 2, Ad hoc: Los requisitos para la práctica cubren los principales casos de uso y los incidentes de seguridad conocidos en entornos similares. Los requisitos aumentan la precisión y el nivel de granularidad para el entorno considerado. Las medidas de garantía apoyan las revisiones ad hoc de la aplicación de la práctica para garantizar la mitigación de la línea de base para los riesgos conocidos. Para esta garantía, uno puede aplicar las medidas aprendidas a través de referencias exitosas.

Nivel 3, Consistente: Los requisitos consideran las mejores prácticas, estándares, regulaciones, clasificaciones, software y otras herramientas. Las herramientas establecen un enfoque coherente para practicar la implementación. La garantía valida la implementación con patrones de seguridad, diseños seguros por defecto y enfoques y mecanismos de protección conocidos. Las prácticas están documentadas. Las prácticas en el dominio se realizan de acuerdo con un plan documentado.

En general, las prácticas en el nivel consistente son más completas y ya no se realizan de forma irregular o no son ad hoc en su implementación. Como resultado, el rendimiento de las prácticas de la organización es más estable. En este nivel, la misión MILCYBDEC puede estar más segura de que el rendimiento de las prácticas de dominio se mantendrá con el tiempo.

Nivel 4, Sustentable: Un proceso bien establecido constituye la base para la implementación

de la práctica, proporcionando soporte continuo y mejoras de seguridad. La garantía de la implementación se centra en la cobertura de las necesidades de seguridad y el abordaje oportuno de las cuestiones que parecen amenazar el sistema de interés. En este nivel, las actividades en un dominio se han institucionalizado aún más y ahora se están gestionando. En el nivel sustentable, las prácticas de un dominio se estabilizan aún más y se guían por directivas organizativas de alto nivel, como las políticas. Como resultado, la organización debe tener confianza adicional en su capacidad para mantener el desempeño de las prácticas a lo largo del tiempo y en toda la organización. De acuerdo con lo anteriormente definido, un nivel de madurez de seguridad de la Misión MILCYBDEC, tal como se muestra en la Figura 16. Niveles de Madurez de Seguridad para MILCYBDEC.

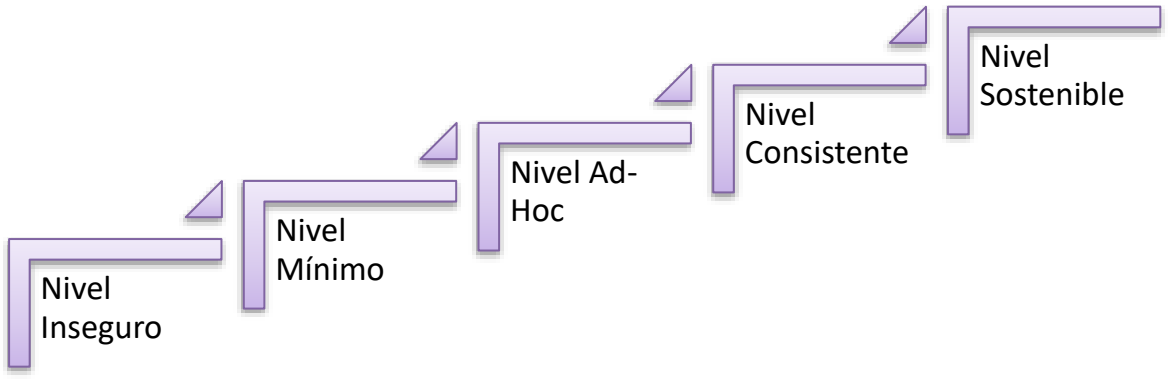


Figura 18: Niveles de Madurez de Seguridad para MILCYBDEC, Fuente: elaboración propia

.

Para determinar estos niveles, es necesario medir el nivel de capacidad en seguridad en las misiones MILCYBDEC, determinar el nivel alcanzado por cada dominio y asignar el valor a la misión MILCYBDEC. Para esto, se desarrolló el Instrumento de Medición de Seguridad en MILCYBDEC (MILCYBDEC).

4.3.3. Instrumento MILCYBDEC

MILCYBDEC está formado por controles, en forma de cuestiones y respuestas simples para constatar si una práctica o proceso está implementado.

1) En figura 22 se muestra un ejemplo de la estructura del instrumento.
2) Los controles están clasificados y agrupados según dominio, y tienen identificador único.
3) El nivel de madurez del dominio de controles se obtiene sumando el peso relativo de los controles multiplicado por el bit de inspección de cada uno. (i.e. la suma de los pesos de todos los controles del dominio es 1 o 100%).
4) SI un control ha sido inspeccionado se pone el bit de 'inspeccionado' y además cumple lo requerido, el bit de inspección se pone a 1, sino a 0
5) Los controles que no sean satisfechos serán tenidos en cuenta para trazar la hoja de ruta para poder alcanzar el Nivel de Madurez siguiente. Las evidencias de dichos controles deben ser referidos al redactar un Plan de Mejora de la Misión MILCYBDEC.
6) Todas las prácticas que no se cumplan o se respondan con 0, serán las prácticas que deberán considerarse como primordiales para aumentar al nivel deseado. Los programas, actividades o evidencias descritos serán las recomendaciones principales para considerar incluir en el Programa de Ciberseguridad que debe gestionarse en la Misión MILCYBDEC para avanzar hacia el siguiente nivel.
7) Según la Misión MILCYBDEC, el ámbito legal, y el tipo de Gobernanza, se aceptan unas evidencias de cumplimiento de controles, u otras, con menor o mayor nivel de flexibilidad.
8) El nivel de madurez de cada dominio y las prácticas que no fueron logradas pasarán a formar parte del informe de deficiencias, indispensables para la Fase 4 de esta Metodología MILCYBDEC

Para consultar la lista completa de controles y dominios cubiertos por MILCYBDEC, consultar ANEXO 1

Controles de Dominio A

	Id. Control	Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
A	A1	Descripción1	1	10%	10%	Evidencia1
	A2	Descripción2	1	10%	20%	Evidencia2
	A3	Descripción3	0	40%	20%	Evidencia3
	A4	Descripción4	1	40%	60%	Evidencia4
					60%	

Figura 19: Sección del instrumento de medición de madurez MILCYBDEC. En este ejemplo, el nivel de madurez acumulado en este dominio es del 60% ; Fuente: elaboración propia

4.3.4. Fase 2: Nivel de Seguridad Objetivo y Pasos para Alcanzar el siguiente nivel

En todos los dominios se marca un nivel objetivo, ver Figura 21, y los controles listados en los dominios vienen a guiar el Stakeholder en la redacción de una guía para alcanzar dicho nivel objetivo.

El nivel objetivo de cumplimiento de cada dominio y práctica viene ponderado por los objetivos estratégicos y de negocio de la Misión MILCYBDEC, sobre todo evitando incurrir en costes excesivos.

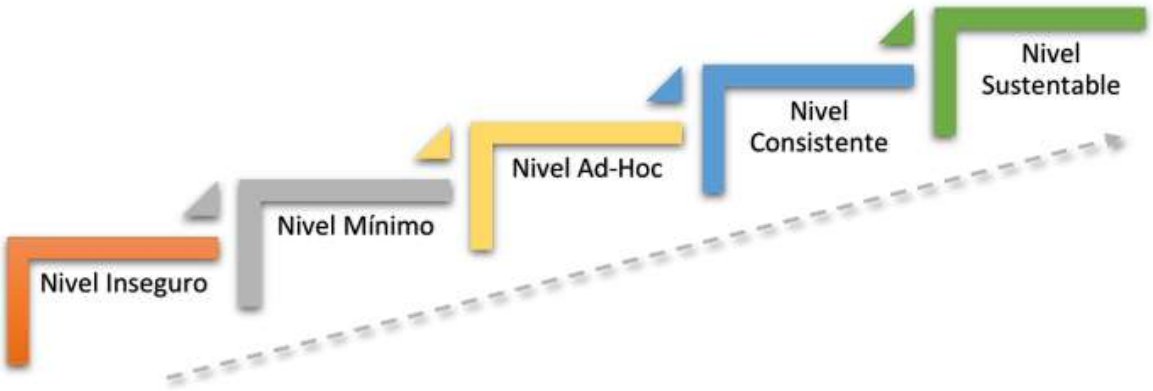


Figura 20: Definir el nivel de seguridad objetivo. Fuente: elaboración propia

Si existen brechas para una práctica en particular, la madurez de esa práctica es inferior a la deseada y debe mejorarse. Si no existen brechas (la puntuación es par o el estado actual es mayor que el objetivo), entonces la madurez de la organización es suficiente o superior respecto a la necesidad. En la Figura 22 se utiliza un gráfico de tipo constelación, que ilustra la brecha entre estado actual y estado objetivo.

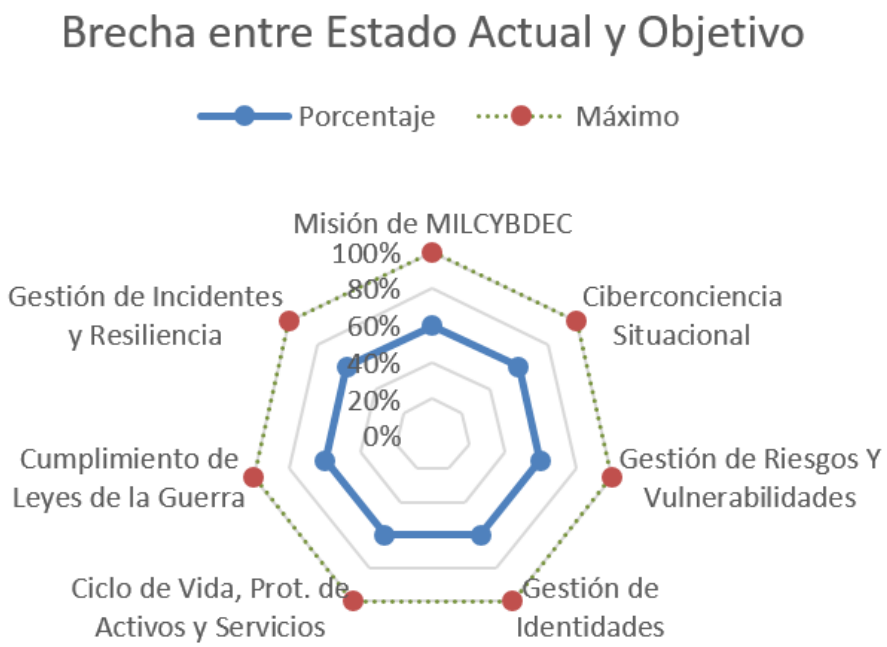


Figura 21: Brechas entre el nivel de madurez actual y el nivel de madurez objetivo, Fuente: elaboración propia

Una vez identificados las prácticas y dominios que están por debajo del nivel objetivo, se debe trazar un plan de mejora, que incluye los controles no satisfechos, entre otros. Dicho plan de mejora debe hacerse según la lista de deficiencias, y las mejoras se priorizan según prioridad del control ponderado con el coste de mejora.

Capítulo 5: Experimentación y Resultados de la metodología MILCYBDEC

En este capítulo se procede a la experimentación de la metodología MILCYBDEC. La metodología MILCYBDEC consiste en elegir Misiones de Ciberdefensa de Países. Esta metodología MILCYBDEC consiste en descubrir los distintos niveles de madurez, con el fin de llegar a un nivel de madurez objetivo. Con ello, en dicho país se analizarán las deficiencias y se trazará un plan de mejora. En esta investigación se ha analizado la madurez de los sistemas informáticos militares utilizando fuentes abiertas OSINT (Geers, 2016) (FireEye, 2014) (Limnéll, 2015) (Oliker, y otros, 2016) (Саприкін, 2015) y fuentes de publicaciones científicas, doctrinas ((NSO), 2020) (DOD, CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE , FM3-12, 2021) (DOD, Cyberspace Operations JP3-12, 2018), y proyectos cuyos entregables son públicos. (Comisión Europea, 2022) Cabe destacar de que, en Ciberdefensa, es habitual que se utilicen soluciones y metodologías de uso dual, i.e de uso civil y militar. Por lo que, en el caso de OSINT sobre Estonia, se usarán evidencias, de libre difusión, provenientes de proyectos H2020 con los que los investigadores, que proponen esta metodología están familiarizados.

5. Elección de Escenarios y Estimación del estado actual de seguridad de Escenarios

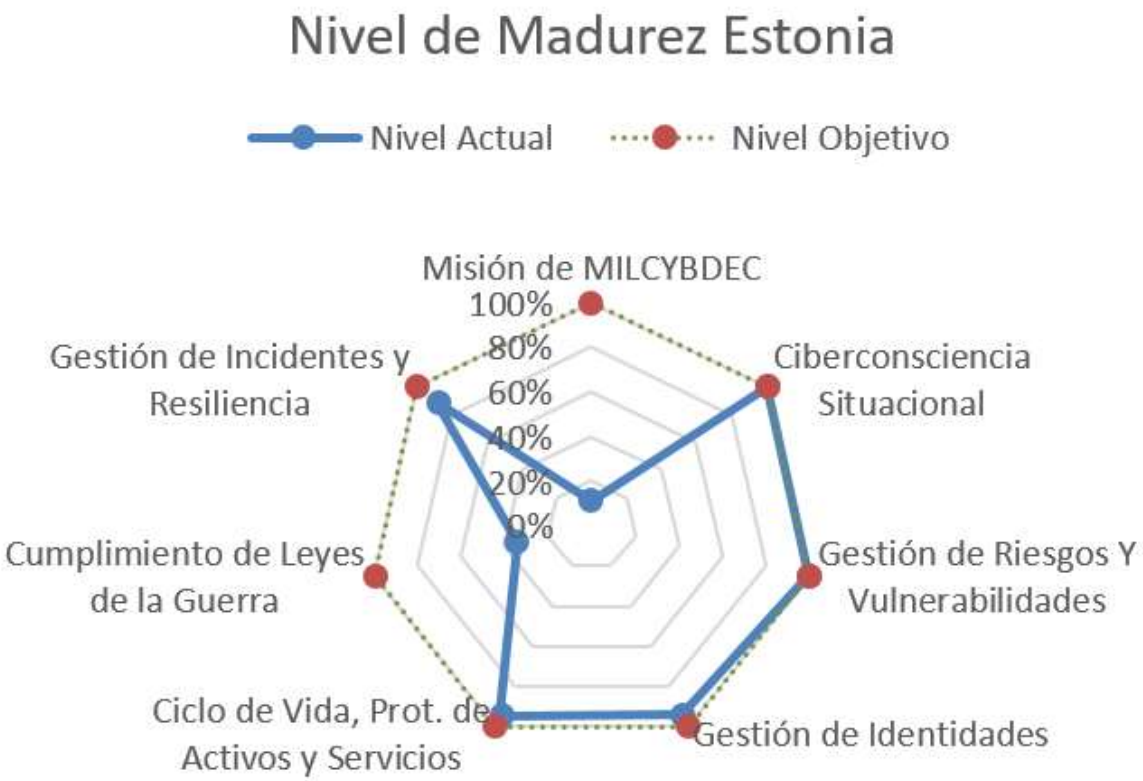
En ciberseguridad, el plano de ciberespacio no tiene fronteras ni tampoco muchas veces localización física ni atribución nacional, ya que los grupos organizados, muchas veces están compuestos de personas de varias nacionalidades. Sin embargo, en el caso de conflictos declarados entre países, es muy común ver operaciones de guerra hibrida, que son ataques no cinéticos por medios no convencionales tales como el ciberespacio. En tales ataques, con determinar el estado atacado es posible intuir el estado atacante. Como estado patrocinador de tales operaciones de guerra hibrida, se encuentra la Federación Rusa, que, en su doctrina de operaciones ofensivas cibernéticas, da mucha importancia a ataques de naturaleza hibrida tales como fakenews, manipulación de opinión pública, o ataque a páginas web estatales. Grupos de BlackHat han atacado una miríada de naciones soberanas, por lo que la lista de posibles Escenarios MILCYBDEC es muy larga. En la historia reciente, hay dos casos significativos diametralmente opuestos, que pueden ser calificados como outliers: Estonia y Ucrania. Estonia, que es miembro de OTAN desde 2004, sufrió una serie de ciberataques de gran envergadura, el primero significativo siendo en 2007. (Traynor, 2007) Estonia y la OTAN reaccionaron de manera espectacular, siendo el primer paso reaccionar a los ataques, en segunda instancia iniciar un proceso de creación de herramientas legales para defenderse

(Schmitt, 2017) (BBC News, 2008), y en tercer lugar fortaleciendo la cultura y organismos civiles y de uso dual: CERT, FIRST, CSIRT, honeynets, honeypots, entre otros. Adicionalmente OTAN ha ubicado el Centro de Excelencia de Ciberdefensa de la OTAN en la propia capital de Estonia, que es Tallin. (The Economist, 2010) En resumen, la reacción ha sido consistente, apoyada por una gran comunidad y sostenible en el tiempo. El Manual de Tallin, que va por su segunda iteración es un referente en relaciones internacionales, en el ámbito de la Ciberdefensa. Con lo que el nivel de madurez esperado es alto. Ucrania es un país que hasta hace poco era satélite de la Federación Rusa, pero con el cambio de régimen, inició su acercamiento a Europa de Oeste y a la OTAN. Dicho acercamiento atrajo ataques cinéticos, cibernéticos e híbridos por parte de la Federación Rusa. El hecho de que Ucrania usara sistemas C3 (C2: Mando y Control) para coordinar sus fuerzas militares no ayudó en absoluto y amplificó el efecto de dichos ataques. Desde que se produjo dicho ataque en 2017 (BBC News, 2017) no está claro que Ucrania haya invertido dinero en Ciberdefensa, tanto como lo ha hecho en armamento convencional. Los ataques cibernéticos de Rusia siguen afectando a sectores críticos. (Holland & Pearson, 2022)Y a diferencia de Estonia, Ucrania no parece haber hecho conexiones con otros CSIRT ni CERT europeos. (European Parliament, 2016) Con lo que el nivel de madurez esperado es bajo. En el caso de Estonia, se elige el nivel de madurez alto como objetivo, mientras que, en el caso de Ucrania, se elige el nivel bajo-medio. En el Anexo 2 y Anexo 3 del presente documento, se pueden consultar los resultados de revisar el cumplimiento de los dominios de control por parte de ambas misiones. En el caso de Estonia, aunque en prácticamente todos los dominios, tiene un nivel de madurez alto, no se puede decir lo mismo del dominio de Misión MILCYBDEC. No es una sorpresa, ya que la OTAN aún no práctica de manera generalizada misiones de MILCYBDEC, más allá de las clásicas misiones de control de la información, honeypots, honeynets. En el caso de Ucrania, prácticamente todos los dominios son en un estado de madurez ‘Ad-Hoc’. Es necesaria una inversión sustancial en Ciberseguridad, MILCYBDEC y mejora. Estonia ha alcanzado ha progresado en nivel de madurez, en los últimos años, ampliando mucho la red de CERT’s e instalando una sólida red de Honeypots, y desarrollando capacidades mes a mes. En cuanto a Ucrania, no queda claro que haya conseguido ningún tipo de soberanía de sus sistemas C2, más allá de la evidente: la física. Es urgente que consiga otros tipos de soberanías de sus sistemas C2, p.e. la de la cadena de suministro: i.e. que jubile los sistemas C2 heredados de la Federación Rusa. Adicionalmente, se recomienda a Ucrania que deslocalice sus activos y procesos informáticos más preciosos a datacenters de países aliados, o si no es posible, que sea a lo largo de embajadas ucranianas a lo largo del mundo.

5.1. Análisis de resultados obtenidos

Aplicar la herramienta ICYBMILDEC se asemeja mucho a un proceso de Auditoría e ISO27K. En caso de tener contacto directo con el MoD, se acuerda el alcance de la auditoría, se analizan los dominios de aplicabilidad, se traza un plan de auditoría, se realizan entrevistas, se recogen evidencias y se realiza un reporte apoyado en los dominios de control. Cada control tiene cierto peso dentro del dominio de aplicabilidad, y según las evidencias recogidas, se marca el control como cumplido o no. Tener acceso a documentos de Defensa Nacional, que por regla general son información clasificada, a menudo no es posible. Aun así, en el mundo cibernético, al utilizarse soluciones de uso dual (civil y militar), se puede inferir de Licitaciones Públicas, de OSINT, y de Incidentes reportados, la estructura de los sistemas y procesos utilizados por las fuerzas. En el Anexo 2 y Anexo 3 del presente documento, se pueden consultar los resultados de revisar el cumplimiento de los dominios de control por parte de ambas misiones.

5.1.1. Análisis de resultados de Estonia



Estonia ha alcanzado ha progresado en nivel de madurez, en los últimos años, ampliando mucho su red de CERT's y CSIRT's incluso conectándolos a una red de CERT's europeos, lo que impacta positivamente en el dominio de Ciberconciencia Situacional, Gestión de Incidentes y Resiliencia y en Gestión de Riesgos y Vulnerabilidades. Respecto de gestión de identidad digital, Estonia es un referente de la llamada 'Democracia Digital' o voto electrónico, lo que lógicamente ha llevado a una transferencia de tecnologías patrias y know-how hacia las operaciones y activos militares. En el dominio de Misión de MILCYBDEC, Estonia no acaba de mantener misiones de Ciberengaño, más allá de los tradicionales honeypots y honeynets, según la información no clasificada a la que ha tenido acceso el autor de este trabajo de fin de máster. En cuanto al cumplimiento de las leyes de la guerra, si bien se ha escrito el Manual de Tallin en Estonia, no acaba de ser totalmente adoptado por los países miembros de la OTAN, por ser muchas de las buenas prácticas sugeridas, consideradas excesivas o sin apoyo legal suficiente.

Figura 22: Nivel de Madurez Estonia; fuente: elaboración propia

5.1.2. Análisis de resultados de Ucrania

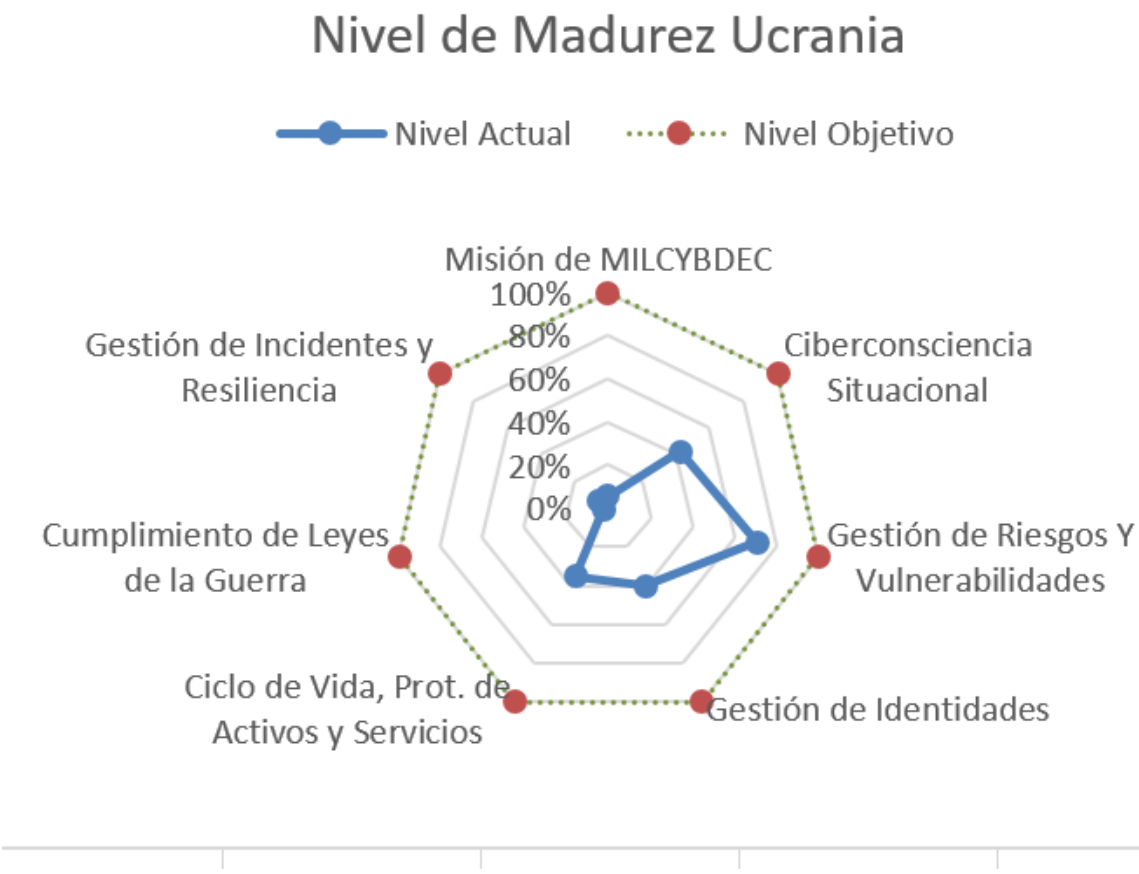


Figura 23: Nivel de Madurez Ucrania; fuente: elaboración propia

En el caso de Ucrania, prácticamente todos los dominios son en un estado de madurez 'Ad-Hoc'. Es necesaria una inversión sustancial en Ciberseguridad, MILCYBDEC y mejora. Desde 2015, Ucrania ha sufrido numerosos ataques cibernéticos 'exitosos' (CSIS, 2022), que paso a listar y que dejan muy mala nota a Ucrania en todos los dominios examinados.

1. Marzo de 2021. El Servicio de Seguridad del Estado ucraniano anuncia que ha evitado un ataque a gran escala por parte de piratas informáticos rusos del FSB que intentaban acceder a datos gubernamentales clasificados.

2. Febrero de 2021. Funcionarios ucranianos informaron de que un ataque de denegación de servicio distribuido de varios días de duración contra el sitio web del Servicio de

Seguridad de Ucrania formaba parte de las operaciones de guerra híbrida de Rusia en el país.

3. Agosto de 2020. Funcionarios ucranianos anunciaron que un grupo de hackers rusos había comenzado a realizar una campaña de phishing en preparación de las operaciones del día de la independencia de Ucrania

4. Abril de 2019. Las organizaciones militares y gubernamentales ucranianas habían sido atacadas era parte de una campaña de hackers de la República Popular de Luhansk, un grupo respaldado por Rusia que declaró la independencia de Ucrania en 2014.

5. Diciembre de 2018. Los investigadores de seguridad descubren una campaña cibernética llevada a cabo por un grupo vinculado a Rusia que tiene como objetivo los organismos gubernamentales de Ucrania, así como múltiples miembros de la OTAN

6. Diciembre de 2018. El Servicio de Seguridad de Ucrania bloqueó un intento de los servicios especiales rusos de interrumpir los sistemas de información de la autoridad judicial de Ucrania

7. Noviembre de 2018. El CERT de Ucrania descubrió un malware en los sistemas informáticos de los organismos estatales de Ucrania que se cree que está implantado como precursor de un futuro ciberataque a gran escala

8. Octubre de 2018. El Servicio de Seguridad de Ucrania anunció que un grupo ruso había llevado a cabo un intento de hackeo de los sistemas de información y telecomunicaciones de los grupos gubernamentales ucranianos

9. Septiembre de 2018. Piratas informáticos rusos atacaron las bandejas de correo electrónico de líderes religiosos relacionados con Ucrania en medio de los esfuerzos por desvincular a la iglesia ortodoxa de Ucrania de su asociación con Rusia.

10. Julio de 2018. Funcionarios de inteligencia ucranianos afirman haber frustrado un ataque ruso a los equipos de red de una planta de cloro en el centro de Ucrania. El virus utilizado en el ataque es el mismo malware responsable de la infección de 500.000 routers en todo el mundo en una campaña que el FBI vinculó a hackers rusos patrocinados por el Estado.

11. Junio de 2018. La policía ucraniana afirma que los hackers rusos han estado atacando sistemáticamente a los bancos ucranianos, las empresas de energía y otras organizaciones para establecer puertas traseras en preparación de un ataque a gran escala contra el país.

12. Diciembre de 2016. Piratas informáticos rusos atacaron la empresa nacional de energía de Ucrania, Ukrenergo, y dejaron sin electricidad al norte de Kiev durante más de una hora.

13. Diciembre de 2015. Piratas informáticos rusos coordinaron ataques contra varias empresas regionales de distribución de energía en el oeste de Ucrania. Los sistemas SCADA y las redes de host del sistema fueron el objetivo y sufrieron daños. Se utilizó software malicioso para buscar vulnerabilidades en la red, establecer el mando y control y borrar los servidores SCADA para retrasar el restablecimiento. Al mismo tiempo, los atacantes lanzaron un ataque de denegación de servicio contra los gestores del sistema para evitar que los clientes informaran de las interrupciones. Aproximadamente 225.000 ucranianos se vieron afectados, pero el servicio se restableció al cabo de 3 a 6 horas.

Conclusión

La hipótesis propuesta para esta investigación fue la siguiente: La Metodología MILCYBDEC es mejor para la tarea de Planificación y Ejecución de Ciberengaño que cada uno de sus rivales MILDEC(JP3-4), FM3-12, dando una visión más centrada en Ciberengaño, más que relegando dichos procesos a tareas de soporte en la Misión Principal. La metodología MILCYBDEC indica métodos de evaluación y evolución de misiones MILDEC en el plano cibernético. MILCYBDEC parte de una premisa diferente que la de las doctrinas militares tradicionales. MILCYBDEC sitúa las acciones cinéticas en segundo plano, y poniendo el foco sobre control de la información, defensa de activos y procesos mediante una Misión de MILDEC de igual envergadura que la misión principal. Adicionalmente la metodología MILCYBDEC aporta herramientas legales para defenderse de ataques cibernéticos de terceros países. En el caso de Estonia, al ser miembro de la OTAN, no se esperan ataques cinéticos por parte de la Federación Rusa, sin embargo, se teme a que se vuelva a repetir la campaña de ataques cibernéticos sobre infraestructuras críticas, bancos, hospitales, y particulares. En su origen, lo que eran recomendaciones del Manual de Tallin, han pasado, por la falta de diligencia de Federación Rusa a limitar ataques futuros, a formar parte de la doctrina de Ciberdefensa de la OTAN. A modo de ejemplo, se acepta una respuesta cinética proporcional a un ataque cibernético. El Manual de Tallin proporciona una guía jurídica sobre cómo justificar respuestas contundentes a ataques cibernéticos originarios de países hostiles a la OTAN.

La presente investigación tuvo los siguientes dos objetivos. Primer objetivo, conectar la Doctrina MILDEC y la Doctrina de Guerra Electrónica exponiendo las necesidades y/o requisitos extendidos. La última iteración de doctrina MILDEC fue publicada años antes que la iteración más reciente de Doctrina de Guerra Electrónica. Dicho acontecimiento creó una brecha entre dichas doctrinas, ya que una estaba más actualizada que la otra. Se espera a que dicha brecha sea cerrada en las próximas publicaciones doctrinales. La presente investigación se adelantó a dicha publicación, tomando en cuenta las necesidades tecnológicas y metodológicas presentes en la metodología MILCYBDEC. Como segundo objetivo se planteó solventar dichas necesidades mediante una propuesta metodológica basada en el Estado del Arte de uso dual. La metodología MILCYBDEC realiza esto conectando el Plano Táctico con el Plano Cibernético, recolectando una serie de tecnologías de Ciberengaño de uso dual, además de proponer un instrumento de medición de la madurez de implementación de dichas tecnologías y su buena gobernanza.

(NATO, 2021)Aunque en algunas doctrinas ya estaba establecido (e.g. AJP de US), el debate y la necesidad de CYBMILDEC se ha hecho especialmente visible en el último Summit de la OTAN (2021); donde abiertamente se ha planteado y discutido la necesidad de usar MILDEC en operaciones cibernéticas. Esto es una llamada a la acción entre los distintos miembros de la Coalición incluyendo a la Unión Europea, los que han empezado a valorar y establecer hojas de ruta para el desarrollo de capacidades de Ciberdefensa ofensivas.

Este trabajo de fin de máster se adelanta a los hechos ocurridos el 24 de febrero 2022 del ataque de la Federación Rusa contra Ucrania. Durante dicho conflicto, Estonia también se ha visto amenazada indirectamente. En el caso de Estonia, este trabajo de fin de máster tiene especial relevancia, ya que unas las pocas vías de ataque a Estonia que se puede permitir la Federación Rusa, es por vía cibernética. En el caso de Ucrania, la guerra se ha convertido en una guerra asimétrica, es decir hay gran desproporcionalidad de fuerzas, siendo Federación Rusa la dominante en fuerzas convencionales. A la fecha del día 1 de marzo 2022, las infraestructuras físicas de comunicaciones de Ucrania se han visto atacadas por la Federación Rusa. (Reuters, 2021).

Trabajo Futuro

Tomando en cuenta que el gobierno de EEUU ya ha iniciado la carrera por la supremacía en tecnologías de Combat Cloud, Europa ha reaccionado y somos testigos de proyectos de la EDA que persiguen los mismos enablers tecnológicos. Sin embargo, dichos proyectos serán confidenciales durante un largo periodo de tiempo. Por ello es importante completar dicho vacío de conocimiento por otros medios, primero la investigación científica y segundo la colaboración tecnológica. Las misiones de Engaño en el CiberEspacio son extremadamente costosas. Las medidas defensivas aplicadas a un sistema deben ser proporcionales al valor de dichos sistemas. A día de hoy, el sector civil puede beneficiarse de una porción del gasto dedicado a material militar: en soluciones de uso dual. A mediano plazo, se pretende publicar esta investigación en una revista indexada. A mediano plazo, el autor quiere incorporar elementos de doctrinas de países no alineados con la OTAN, tales como la de Federación Rusa (Doctrina Gerasimov (Piella, 2018)), o República Popular de China, que tienen planteamientos muy distintos del de la OTAN. Tanto la doctrina de Federación Rusa como de PLA manejan conceptos muy interesantes como guerra de la información, guerra psicológica, y proyecciones de información fuera de las fronteras nacionales, a fin de moldear la opinión pública (ya no sólo las fuerzas hostiles) en países extranjeros.

Bibliografía

(NSO), N. S. (2020). *Allied Joint Doctrine for Cyberspace Operations . AJP-3.20.* NATO STANDARDIZATION OFFICE (NSO).

Al-Shaer, E., & Gillani, S. F. (2016). Agile virtual infrastructure for cyber deception against stealthy DDoS attacks. *Cyber Deception*, 233-257.

Araujo, F., & Hamlen, K. W. (2016). Embedded honeypotting. (C. Springer, Ed.) *Cyber Deception*, 201-231.

BBC News. (23 de 2 de 2008). Estonia fines man for 'cyber war'. *BBC News*. Obtenido de http://news.bbc.co.uk/2/hi/technology/7208511.stm

BBC News. (2017). Ukraine cyber-attack: Software firm MeDoc's servers seized. *BBC News*. Obtenido de https://www.bbc.com/news/technology-40497026

BOE , España. (01 de 09 de 2020). *PDC-01(A) "Doctrina para el empleo de las Fuerzas Armadas"*. (BOE) Recuperado el 01 de 09 de 2020, de http://publicacionesoficiales.boe.es/

Comisión Europea. (2022). *Proyecto SPARTA*. Obtenido de Proyecto SPARTA: https://sparta.eu/

DOD. (2018). *Cyberspace Operations JP3-12.* Departamento de Defensa de EEUU.

DOD. (2021). *CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE , FM3-12.* Departamento de Defensa de EEUU.

EEAS. (2021). Military Vision and Strategy on Cyberspace as a Domain of Operations. Obtenido de https://www.statewatch.org/media/2879/eu-eeas-military-vision-cyberspace-2021-706-rev4.pdf

European Parliament. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Obtenido de http://data.europa.eu/eli/dir/2016/1148/oj

FireEye. (2014). *APT28: A Window Into Russia's Cyber Espionage Operations?* Obtenido de https://www2.fireeye.com/apt28.html

Geers, K. (2016). Tallinn: NATO CCD COE Publications. Obtenido de https://web.archive.org/web/20160816132103/https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html

Holland, S., & Pearson, J. (18 de 1 de 2022). US, UK: Russia responsible for cyberattack against Ukrainian banks. *Reuters*. Obtenido de https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/

Jajodia, S., & Subrahmanian, V. (2016). *Cyber Deception; Building the Scientific Foundation.* Springer.

Jajodia, S., Subrahmanian, V., Swarup, V., & Wang, C. (2016). Cyber deception. Springer.

Limnéll, J. (2015). The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War. *International Journal of Cyber-Security and Digital Forensics*, 521-532.

Martínez, Á. L., Vidal, J. M., & González, V. A. (2021). Understanding and Assessment of Mission-Centric Key Cyber Terrains for joint Military Operations. *Journal of Network and Computer Applications*.

Medenou, R., Mayo, V., Balufo, M., Castrillo, M., Garrido, F., Martínez, Á., . . . & Sánchez, S. (2020). CYSAS-S3: a novel dataset for validating cyber situational awareness related tools for supporting military operations. *15th International Conference on Availability, Reliability and Security (ARES), Proceedings of*, (págs. 1-9).

MILDEC JP3-13.4 Military Deception. (26 de 01 de 2012). Recuperado el 01 de 09 de 2021, de https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdF

Ministario de Defensa de España. (2020). *Implicaciones del ámbito Cognifico en las Operaciones Militares*. Obtenido de Implicaciones del ámbito Cognifico en las Operaciones Militares: https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf

MITRE. (s.f.). *MITRE ATT&CK*. Obtenido de MITRE ATT&CK: https://attack.mitre.org/

Moreno de Rodríguez, D. M. (2020). Título del trabajo: Metodología de ciudades inteligentes seguras (MCIS). *UNIR*.

NATO. (01 de 02 de 2019). *Allied Joint Doctrine for the Conduct of Operations (AJP-3).* Recuperado el 01 de 02 de 2021, de

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf

NATO. (14 de 07 de 2021). *2021 NATO Summit.* Obtenido de 2021 NATO Summit: https://www.nato.int/cps/en/natohq/184620.htm

NATO. (2021). *NATO SUMMIT 2021*. Obtenido de NATO SUMMIT 2021: https://www.nato.int/cps/en/natohq/184620.htm

Oliker, O., Davis, L. E., Crane, K., Radin, A., Gventer, C., Sondergaard, S., . . . Hlavka., J. P. (2016). *Security Sector Reform in Ukraine.* Santa Monica: RAND Corporation. doi:https://dx.doi.org/10.7249%2FRR1475-1

OpenGROUP. (01 de 09 de 2021). *Risk Analysis (O-RA), Version 2.0.* Recuperado el 01 de 09 de 2021, de https://publications.opengroup.org/c20a

OpenGROUP. (01 de 09 de 2021). *Risk Taxonomy (O-RT), Version 3.0.* Recuperado el 01 de 09 de 2021, de https://publications.opengroup.org/c20b

Peñas, J. (2021). El desarrollo de ciberarmas. Un aviso a la industria española. *XV Jornadas CCN.* Madrid.

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). Workforce framework for cybersecurity. *NICE framework*.

Piella, G. C. (2018). La doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo. *Revista Ejército*, 30-37. Obtenido de https://ejercito.defensa.gob.es/Galerias/Descarga_pdf/EjercitoTierra/revista_ejercito/primer_premio_2019.pdf

Prensa. (2021). *Indra lidera el mayor proyecto de ciberconsciencia situacional para la defensa de Europa.* Obtenido de Indra lidera el mayor proyecto de ciberconsciencia situacional para la defensa de Europa: https://actualidadaeroespacial.com/indra-lidera-el-mayor-proyecto-de-ciberconsciencia-situacional-para-la-defensa-de-europa/

Ramon Y Cajal Ramo, P., & Maestre Vidal, J. (2021). Understanding the Ethical and Regulatory boundaries of the Military Actuation on the Cyberspace. *Reliability and Security*, 1-11.

Rea-Guaman, A. M., San Feliu, T., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative study of cybersecurity capability maturity models. *In International Conference on Software Process Improvement and Capability Determination*, 100-113.

Reuters. (2021). *Internet in Ukraine disrupted as Russian troops advance.* Obtenido de Internet in Ukraine disrupted as Russian troops advance: https://www.reuters.com/world/europe/internet-ukraine-disrupted-russian-troops-advance-2022-02-26/

Rico, E. (2021). Has sido tú, te crees que no te he visto. *Jornadas CCN.* Madrid.

Schmitt, M. N. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. *Cambridge University Press*.

Sotelo Monge, M. A., Maestre Vidal, J., & Medenou Choumanof, R. D. (2021). Adaptive Mitigation of Tactical Denial of Sustainability. *In The 16th International Conference on Availability, Reliability and Security*, (págs. 1-9). Dublin.

Stech, F. J., Heckman, K. E., & & Strom, B. E. (2016). Integrating cyber-D&D into adversary modeling for active cyber defense. En *Cyber deception* (págs. 1-22). Springer.

The Economist. (2 de 7 de 2010). War in the fifth domain. Are the mouse and keyboard the new weapons of conflict? *The Economist*.

Traynor, I. (17 de 05 de 2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. Obtenido de https://www.theguardian.com/russia/article/0,,2081438,00.html

Underbrink, A. J. (2016). Effective cyber deception. In Cyber Deception . *Springer-Cham*, 115-147.

US Department Of Energy. (2019). Cybersecurity Capability Maturity Model C2M2. *Cybersecurity Capability Maturity Model C2M2*.

Саприкін, О. (2015). Інтернет-ресурси як інструмент інформаційної війни та інформаційна безпека України. *НАУКОВО-ПОПУЛЯРНИЙ ЖУРНАЛ*. Obtenido de https://web.archive.org/web/20170927155442/http://warhistory.in.ua/1_2015.pdf

Anexo 1: Controles y Dominios de MILCYBDEC

Controles de Misión MILCYBDEC						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
MCC	MCC1	La misión MILCYBDEC apoya la soberanía cibernética del país y/o las fuerzas aliadas	1	10%	10%	Evidencia1
	MCC3	Hay establecidas redundancias de redes, almacenamiento y procesamiento dentro de países aliados	0	10%	10%	Evidencia3
	MCC4	La misión MILCYBDEC garantiza la soberanía física del país y/o las fuerzas aliadas	0	10%	10%	Evidencia4
	MCC5	La misión MILCYBDEC debe definir claramente los cauces hacia los blancos.	0	10%	10%	Evidencia5
	MCC6	El guion de MILCYBDEC es creíble, verificable, consistente, implementable	0	10%	10%	Evidencia6
	MCC7	La misión MILCYBDEC disfruta de planificación y control centralizados	0	10%	10%	Evidencia7
	MCC8	Se ha securizado la información de MILDEC, mediante compartimentalización	0	10%	10%	Evidencia8
	MCC9	Se ha securizado la información de MILDEC, mediante control de accesos e identidad	0	10%	10%	Evidencia9

	MCC10	La misión de MILCYBDEC tiene procesos dedicados a OPSEC	0	10%	10%	Evidencia10
	MCC11	La misión de MILCYBDEC dedica suficiente tiempo y plazo para desplegar el guion y para que el adversario se dé cuenta de él	0	10%	10%	Evidencia11
	MCC12	Las operaciones MILCYBDEC están plenamente integradas con otras Operaciones aliadas	0	10%	10%	Evidencia12
	MCC13	El concepto de MILCYBDEC debe desarrollarse a la vez que CONOPS para la misión principal.	0	10%	10%	Evidencia13

Controles de Dominio CCS						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
CCS	CCS1	Mantiene una conciencia mínima de los eventos relacionados con la seguridad	1	10%	10%	Evidencia1
	CCS2	Atención específica a algunos tipos de eventos de seguridad	0	10%	10%	Evidencia2
	CCS3	Supervisión integral y el intercambio regular de información relacionada con la seguridad	0	40%	10%	Evidencia3
	CCS4	Proporciona y gestiona toda la información relevante para los aspectos de fiabilidad	0	40%	10%	Evidencia4
	CCS5	Obtiene información externa pertinente sobre una base ad hoc	0	40%	10%	Evidencia5
	CCS6	Permite que el personal utilice constantemente fuentes de información externas relevantes	0	40%	10%	Evidencia6
	CCS9	Comprueba los registros del sistema para fines de diagnóstico	0	40%	10%	Evidencia7
	CCS10	Revisa periódicamente los eventos que indican cómo se ejecutan correctamente los procesos críticos	0	40%	10%	Evidencia8
	CCS11	Recopila información relevante para la seguridad	0	40%	10%	Evidencia9
	CCS12	Analiza información relevante para la seguridad, tanto con herramientas construidas como diseñadas específicamente	0	40%	10%	Evidencia10

Comprender las vulnerabilidades del sistema	0	10%	10%	Evidencia3
Comprender las vulnerabilidades de la tecnología	0	10%	10%	Evidencia4
Descripción completa de los riesgos pertinentes	0	10%	10%	Evidencia5

GI	GI1	Se definen las entidades elementales de apoyo para el escenario de uso básico	1	10%	10%	Evidencia1
	GI2	Se emplean las mejores prácticas para apoyar escenarios de acceso sofisticados	0	10%	10%	Evidencia2
	GI3	Protección integral contra los riesgos relacionados con accesos no autorizados	0	10%	10%	Evidencia3
	GI4	Se cuenta con una amplia gama de identidades aprovechando mecanismos automatizados	0	10%	10%	Evidencia3
	GI5	Se gestionan las identidades de varios grupos de personas, sistemas o cosas	0	10%	10%	Evidencia4
	GI6	Se mantiene y controla el uso de identidades de personas, sistemas y cosas a lo largo de su ciclo de vida	0	10%	10%	Evidencia5
	GI7	Se limita la capacidad de los agentes externos para acceder a los sistemas	0	10%	10%	Evidencia6
	GI8	Se considera el perfil del sujeto para controlar los accesos apropiados	0	10%	10%	Evidencia7
	GI9	Utiliza las políticas de control de acceso disponibles con un nivel adecuado de garantía	0	10%	10%	Evidencia8
	GI10	Mantiene un esquema de autorización estrictamente alineado con las necesidades y limitaciones del negocio	0	10%	10%	Evidencia9

Controles de Dominio Ciclo de Vida, Protección de Activos y Servicios						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
CVPAS	CPA1	Definición del uso de activos digitales y físicos	0	10%	0%	Evidencia1
	CPA2	Supervisa los activos sobre la base de un caso de uso	0	10%	0%	Evidencia2
	CPA3	Gestión y protección de los activos de diversos tipos	0	10%	0%	Evidencia3
	CPA4	Se garantiza la aplicación de las políticas de gestión de activos	0	10%	0%	Evidencia4
	CPA5	Se realiza un seguimiento de los cambios poco frecuentes en activos y configuraciones	0	10%	0%	Evidencia5
	CPA6	Siguen algunas reglas específicas para gestionar posibles cambios en el sistema	0	10%	0%	Evidencia6
	CPA7	Existen procedimientos de gestión de cambios para el número de activos y/o configuraciones	0	10%	0%	Evidencia7
	CPA8	Se regula el proceso para el ciclo de vida de los activos, desde el aprovisionamiento hasta la sustitución, incluidos los cambios de emergencia	0	10%	0%	Evidencia8
	CPA9	Se limita el acceso a activos físicos	0	10%	0%	Evidencia9

	CPA10	Definen las restricciones de acceso en cuanto a horarios permitidos	0	10%	0%	Evidencia10
	CPA11	Definen los controles de acceso físico	0	10%	0%	Evidencia11
	CPA12	Automatiza el control de acceso físico utilizando tokens de identidad específicos	0	10%	0%	Evidencia12
	CPA13	Se garantiza un funcionamiento seguro de los controles de acceso físico	0	10%	0%	Evidencia13
	CPA14	Se planifica el mantenimiento general de la confidencialidad e integridad de los datos	0	10%	0%	Evidencia14
	CPA15	Se implementan políticas y métodos para la protección de datos	0	10%	0%	Evidencia15
	CPA16	Se ofrece garantía de la protección de la información comercial crítica en tránsito	0	10%	0%	Evidencia16
	CPA17	Se declara que los datos deben estar protegidos contra el acceso no autorizado	0	10%	0%	Evidencia17
	CPA18	Define el enfoque y los roles/atributos particulares para controlar el acceso a los datos	0	10%	0%	Evidencia18

	CPA19	Se aprovechan los controles de protección integrados (SO, red, servicios)	0	10%	0%	Evidencia19
	CPA20	Apoyar la correcta aplicación de los controles de datos de acuerdo con las normas reconocidas.	0	10%	0%	Evidencia20

LG	LG1	Deben de haber suficientes medidas activas de protección física y legal de los activos/procesos de MILCYBDEC	1	10%	10%
	LG7	El alcance de una misión MILCYBDEC debe estar limitado y bien definido.	0	10%	10%
	LG9	El personal aliado , según nivel de habilitación de seguridad, debe , o no debe, ser consciente de los procesos/activos que componen la misión MILCYBDEC	0	10%	10%
	LG10	La misión de MILCYBDEC debe proveer contramedidas proporcionales a los ataques	0	10%	10%
	LG11	La misión de MILCYBDEC debe tener capacidad de medir la ciber-agresión entrante, a fin de poder equipararla con un ataque cinético (equivalente, y poder, en un futuro, si necesario lanzar una reciprocación proporcional (reciprocidad y proporcionalidad a los ataques)	0	10%	10%
	LG12	La misión de MILCYBDEC debe tener unos objetivos bien definidos.	0	10%	10%
	LG13	La misión de MILCYBDEC debe poder proveer contramedidas de alcance medible de cara a los ataques	0	10%	10%

	LG14	La misión de MILCYBDEC debe poder proveer contramedidas de efectos medibles de cara a los ataques	0	10%	10%
	LG15	La misión de MILCYBDEC tiene que tener procesos/activos en el Espacio Exterior, si dicho dominio afecta a la Misión	0	10%	10%
	LG16	La misión MILCYBDEC debe prever distintos niveles de activación (i.e. nivel de alerta)	0	10%	10%
	LG17	La misión MILCYBDEC debe satisfacer el Principio de Distinción, i.e tener capacidades de reconocer si los objetivos de MILCYBDEC son civiles o militares	0	10%	10%
	LG18	La misión MILCYBDEC garantiza la soberanía física del país y/o las fuerzas aliadas	0	10%	10%
	LG19	La misión MILCYBDEC no debe dañar el entorno natural.	0	10%	10%
	LG20	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de los menores de edad	0	10%	10%
	LG21	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de prisioneros de guerra	0	10%	10%
	LG22	La misión MILCYBDEC no debe interferir con Sistemas de Países Aliados.	0	10%	10%
	LG23	La misión MILCYBDEC no debe interferir con Sistemas de Países Hostiles (adversarios), **(aunque sí puede dificultar operaciones extranjeras no pacificas)**	0	10%	10%
	LG24	La misión MILCYBDEC no debe interferir con Sistemas de Países Neutrales	0	10%	10%

	LG25	La misión MILCYBDEC sólo debe ser activada cuando sea necesario	0	10%	10%
	LG26	La misión no debe provocar acciones ofensivas transfronterizas	0	10%	10%
	LG27	La misión no debe realizar acciones ofensivas transfronterizas	0	10%	10%
	LG28	Las infraestructuras de MILCYBDEC deben ser capaces de detectar los ataques entrantes de fuerzas/países hostiles y alertar a las autoridades competentes , p.e. el Concejo de Seguridad de Naciones Unidas	0	10%	10%
	LG29	Las medidas de MILCYBDEC no deben contravenir los acuerdos internacionales firmados por el País. (p.e. convención de Ginebra, Canadá, Viena)	0	10%	10%
	LG30	Los dominios de batalla afectados por una misión MILCYBDEC deben estar bien definidos	0	10%	10%
	LG31	Los procesos/activos de MILCYBDEC no deben activar fuegos, o en todo caso, si activan fuegos, deben ser fuegos simulados y/o con carga simulada	0	10%	10%
	LG32	Los procesos/activos de MILCYBDEC no deben amenazar con respuesta activa, ya sea cibernética o cinética, en caso de que dicha respuesta no se ajuste a los principios de guerra justa.	0	10%	10%
	LG33	Los procesos/activos de MILCYBDEC no deben causar interferencias dañinas en el ciberespacio	0	10%	10%
	LG34	Los procesos/activos de MILCYBDEC no deben causar interferencias dañinas en el espectro electromagnético	0	10%	10%

	LG35	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de naves aéreas	0	10%	10%
	LG36	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de naves civiles	0	10%	10%
	LG37	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de vehículos terrestres civiles	0	10%	10%
	LG38	Los procesos/activos de MILCYBDEC no deben realizar actos de Perfidia (p.e. hacerse pasar por objetivos civiles, o de primeros auxilios, p.e.)	0	10%	10%
	LG39	Los procesos/activos de MILCYBDEC no deben tener almacenada información secreta verdadera	0	10%	10%
	LG40	Los procesos/activos MILCYBDEC, si son elementos que soportan tráfico de red internacional, deben dar paso libre a dicho tráfico (mientras el origen y el destino sean externos al País)	0	10%	10%
	LG41	Los propietarios de activos y/o procesos de MILCYBDEC deben ser actores legítimos, i.e. autoridades estatales, militares y/o habilitadas para ejercer Ciberdefensa en el ámbito de la misión	0	10%	10%
	LG42	Los sistemas de MILCYBDEC no deben identificarse, sin autorización previa, como actores internacionales, tales como Naciones Unidas (UN)	0	10%	10%
	LG43	MILCYBDEC debe ser necesario y justificable.	0	10%	10%
	LG44	MILCYBDEC debe ser proporcional a las amenazas de las que protege	0	10%	10%

	LG45	MILCYBDEC no debe destruir y/o degradar rutas de datos internacionales, que se encuentren fuera del dominio geográfico y/o lógico de las redes del País	0	10%	10%
	LG46	MILCYBDEC no puede los Derechos Humanos	0	10%	10%
	LG47	MILCYBDEC no va en contra de la Leyes de la Guerra	0	10%	10%
	LG48	Se deben poder lanzar contramedidas simuladas (con un payload inofensivo) en caso de detectar ataques a un Honeypot o Honeynet.	0	10%	10%
	LG49	Según nivel de alerta, la misión MILCYBDEC no debería dirigirse hacia países aliados	0	10%	10%
	LG50	Un proceso/activo de Ciberengaño debe ser 'visitable', i.e. debe poder ser inspeccionado por las autoridades del País.	0	10%	10%

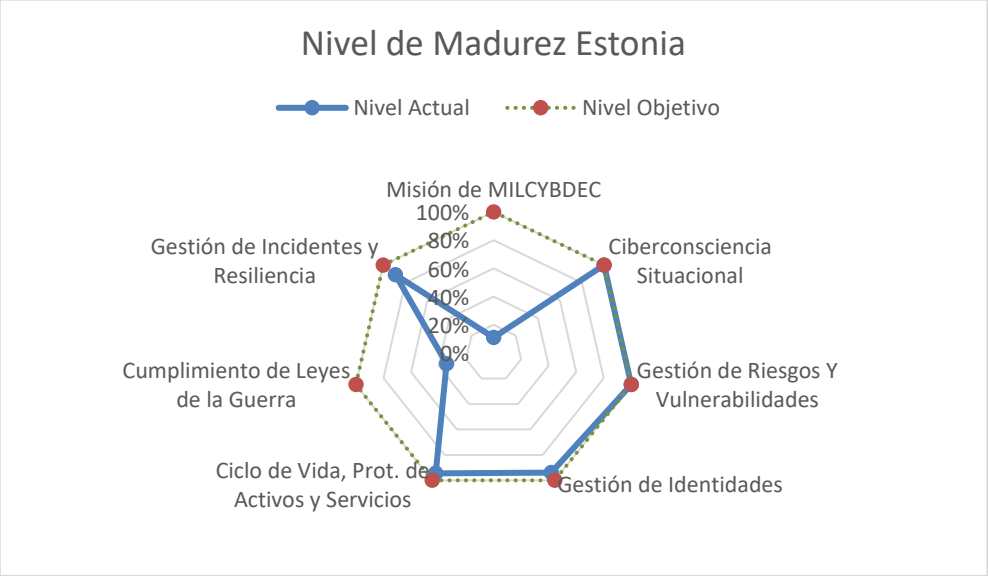
GIR3	Existe un procedimiento de recuperación automática Se generan informes descriptivos sobre los incidentes y sus soluciones Respuesta rápida a incidentes y reducción del daño al negocio tanto por medios técnicos como organizativos	0	10%	10%	Evidencia5
GIR4	Define incidentes específicos y acciones básicas para reaccionar	0	10%	10%	Evidencia6

GIR5	Proporciona orientación para componentes críticos sobre cómo detectar y responder a incidentes	0	10%	10%	Evidencia7
GIR6	Establece la base para la ejecución automática de los procedimientos de respuesta	0	10%	10%	Evidencia8
GIR7	Crear controles para detectar incidentes, asignarlos para la investigación y escalar según sea necesario	0	10%	10%	Evidencia9
GIR8	Posee mecanismos para asignar incidentes para su investigación y escalar según sea necesario	0	10%	10%	Evidencia10
GIR9	Se cuentan con procedimientos con instrucciones básicas para la recuperación del sistema	0	10%	10%	Evidencia11
GIR10	Se manejan todos los incidentes que se detectan	0	10%	10%	Evidencia12
GIR11	Se comprueba si el sistema está completamente recuperado luego de un incidente	0	10%	10%	Evidencia13

GIR12	Se poseen mecanismos para la ejecución automática de procedimientos de corrección y recuperación	0	10%	10%	Evidencia14
GIR13	Se cuenta con una combinación de medidas técnicas y organizativas que faciliten la rápida recuperación del sistema	0	10%	10%	Evidencia15
	La misión de MILCYBDEC debe proveer contramedidas inmediatas a los ataques	0	10%	10%	Evidencia16
	La misión de MILCYBDEC debe poder proveer contramedidas directas de cara a los ataques	0	10%	10%	Evidencia17
	Las infraestructuras de MILCYBDEC deben ser capaces de detectar los ataques entrantes y alertar al propietario de la infraestructura (real) subyacente.	0	10%	10%	Evidencia18

Anexo 2: Resultados MILCYBDEC Estonia

Nombre Dominio	Nivel Actual	Nivel Objetivo
Misión de MILCYBDEC	11%	100%
Ciberconciencia Situacional	100%	100%
Gestión de Riesgos Y Vulnerabilidades	100%	100%
Gestión de Identidades	94%	100%
Ciclo de Vida, Prot. de Activos y Servicios	95%	100%
Cumplimiento de Leyes de la Guerra	34%	100%
Gestión de Incidentes y Resiliencia	89%	100%



Controles de Misión MILCYBDEC						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
MCC	MCC1	La misión MILCYBDEC apoya la soberanía cibernética del país y/o las fuerzas aliadas	1	10%	10%	OSINT, Proyectos H2020, Manual de Tallin

	MCC3	Hay establecidas redundancias de redes, almacenamiento y procesamiento dentro de países aliados	0	10%	10%	OSINT, Proyectos H2020, Manual de Tallin
	MCC4	La misión MILCYBDEC garantiza la soberanía física del país y/o las fuerzas aliadas	0	10%	10%	OSINT, Proyectos H2020, Manual de Tallin
	MCC5	La misión MILCYBDEC debe definir claramente los cauces hacia los blancos.	0	10%	10%	OSINT, Proyectos H2020, Manual de Tallin
	MCC6	El guion de MILCYBDEC es creíble, verificable, consistente, implementable	0	10%	10%	OSINT, Proyectos H2020, Manual de Tallin
	MCC7	La misión MILCYBDEC disfruta de planificación y control centralizados	1	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC8	Se ha securizado la información de MILDEC, mediante compartimentalización	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC9	Se ha securizado la información de MILDEC, mediante control de accesos e identidad	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC10	La misión de MILCYBDEC tiene procesos dedicados a OPSEC	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC11	La misión de MILCYBDEC dedica suficiente tiempo y plazo para desplegar el guion y para que el adversario se dé cuenta de él	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC12	Las operaciones MILCYBDEC están plenamente integradas con otras Operaciones aliadas	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC13	El concepto de MILCYBDEC debe desarrollarse a la vez que CONOPS para la misión principal.	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin

	MCC14	Se posee toda la cadena de suministros de activos/procesos MILCYBDEC	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC15	La misión MILCYBDEC no debe interferir activamente con infraestructuras y servicios de países extranjeros (p.e. publicar 'fake news' en un estado extranjero, aunque sea parte hostil)	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC16	La misión MILCYBDEC debe haber identificado las lagunas de información del adversario	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC17	La misión de MILCYBDEC debe garantizar la inmediatez de reacción, a fin de mantener el 'Uptime' de los activos/procesos protegidos	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC18	El alcance de una misión MILCYBDEC debe estar limitado y bien definido.	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	MCC19	La misión MILCYBDEC no debe interferir con otras misiones aliadas	0	10%	20%	OSINT, Proyectos H2020, Manual de Tallin

Madurez Obtenida
11%

Controles de Dominio CCS						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
CCS	CCS1	Mantiene una conciencia mínima de los eventos relacionados con la seguridad	1	10%	10%	OSINT, Proyectos H2020, Manual de Tallin

	CCS2	Atención específica a algunos tipos de eventos de seguridad	1	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	CCS3	Supervisión integral y el intercambio regular de información relacionada con la seguridad	1	40%	60%	OSINT, Proyectos H2020, Manual de Tallin
	CCS4	Proporciona y gestiona toda la información relevante para los aspectos de fiabilidad	1	40%	100%	OSINT, Proyectos H2020, Manual de Tallin
	CCS5	Obtiene información externa pertinente sobre una base ad hoc	1	40%	140%	OSINT, Proyectos H2020, Manual de Tallin
	CCS6	Permite que el personal utilice constantemente fuentes de información externas relevantes	1	40%	180%	OSINT, Proyectos H2020, Manual de Tallin
	CCS9	Comprueba los registros del sistema para fines de diagnóstico	1	40%	220%	OSINT, Proyectos H2020, Manual de Tallin
	CCS10	Revisa periódicamente los eventos que indican cómo se ejecutan correctamente los procesos críticos	1	40%	260%	OSINT, Proyectos H2020, Manual de Tallin
	CCS11	Recopila información relevante para la seguridad	1	40%	300%	OSINT, Proyectos H2020, Manual de Tallin
	CCS12	Analiza información relevante para la seguridad, tanto con herramientas construidas como diseñadas específicamente	1	40%	340%	OSINT, Proyectos H2020, Manual de Tallin

	CCS13	La misión MILCYBDEC tiene en cuenta KCT (Ciberterrenos clave)	1	40%	380%	OSINT, Proyectos H2020, Manual de Tallin
	CCS14	Monitoreo Y Alerta Continuos de Honeynets	1	40%	420%	OSINT, Proyectos H2020, Manual de Tallin
	CCS15	Monitoreo y Alerta Continuos de Honeypots	1	40%	460%	OSINT, Proyectos H2020, Manual de Tallin
	CCS16	Monitoreo Y Alerta Continuos de Honeywords	1	40%	500%	OSINT, Proyectos H2020, Manual de Tallin

Madurez Obtenida
100%

Controles de Dominio Gestión de Riesgos y Vulnerabilidades						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
GR	GR1	Se ha establecido una estrategia de gestión de riesgos de ciberseguridad	1	10%	10%	OSINT, Proyectos H2020, Manual de Tallin
	GR2	Revisión del panorama actual de amenazas	1	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	GR3	Comprender las vulnerabilidades del sistema	1	10%	30%	OSINT, Proyectos H2020, Manual de Tallin
	GR4	Comprender las vulnerabilidades de la tecnología	1	10%	40%	OSINT, Proyectos H2020, Manual de Tallin

	GR5	Descripción completa de los riesgos pertinentes	1	10%	50%	OSINT, Proyectos H2020, Manual de Tallin
	GR6	Enfoque holístico y sistemático de la gestión de riesgos	1	10%	60%	OSINT, Proyectos H2020, Manual de Tallin
	GR7	Se incluyen temas generales de seguridad de TI como amenazas en el baseline de la ciudad	1	10%	70%	OSINT, Proyectos H2020, Manual de Tallin
	GR8	Se identifican y describen las amenazas de manera intrínseca Se describen los factores de TI que pueden poner el sistema en riesgo Se define la noción de riesgo	1	10%	80%	OSINT, Proyectos H2020, Manual de Tallin
	GR9	Se define la importancia de los riesgos de acuerdo a su probabilidad e impacto	1	10%	90%	OSINT, Proyectos H2020, Manual de Tallin
	GR10	Se miden y gestionan adecuadamente los riesgos	1	10%	100%	OSINT, Proyectos H2020, Manual de Tallin
	GR11	Utiliza un marco y proceso de gestión de riesgos	1	10%	110%	OSINT, Proyectos H2020, Manual de Tallin
	GR12	Mantiene los sistemas actualizados	1	10%	120%	OSINT, Proyectos H2020, Manual de Tallin
	GR13	Aplicar una política de actualización regular para los componentes críticos	1	10%	130%	OSINT, Proyectos H2020, Manual de Tallin

	GR14	Soporte de actualizaciones automatizadas configuradas específicamente para el caso	1	10%	140%	OSINT, Proyectos H2020, Manual de Tallin
	GR15	Planifica un proceso de actualización regular y escenarios de emergencia para los días cero críticos	1	10%	150%	OSINT, Proyectos H2020, Manual de Tallin
	GR16	Considerar si las vulnerabilidades ampliamente conocidas son relevantes para el sistema	1	10%	160%	OSINT, Proyectos H2020, Manual de Tallin
	GR17	Comprueba si los componentes especificados son propensos a ataques	1	10%	170%	OSINT, Proyectos H2020, Manual de Tallin
	GR18	Obtiene una evaluación objetiva de terceros de vulnerabilidades y exposiciones	1	10%	180%	OSINT, Proyectos H2020, Manual de Tallin
	GR19	Realiza inspecciones de seguridad personalizadas periódicas regulares	1	10%	190%	OSINT, Proyectos H2020, Manual de Tallin
	GR20	Considera los avisos de seguridad emitidos por los proveedores e instalar los parches apropiados	1	10%	200%	OSINT, Proyectos H2020, Manual de Tallin
	GR21	Comprueba que los componentes especificados están protegidos contra los ataques más probables	1	10%	210%	OSINT, Proyectos H2020, Manual de Tallin
	GR22	Establece procedimientos de actualización automática siempre que sea posible	1	10%	220%	OSINT, Proyectos H2020, Manual de Tallin

	GR23	Aplica una política del sistema para garantizar la protección continua contra los ataques conocidos	1	10%	230%	OSINT, Proyectos H2020, Manual de Tallin
	GR24	La misión MILCYBDEC debe tener procesos de revisión y automejora	1	10%	240%	OSINT, Proyectos H2020, Manual de Tallin

Madurez Obtenida
100%

Controles de Dominio Gestión de Identidades						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
GI	GI1	Se definen las entidades elementales de apoyo para el escenario de uso básico	1	10%	10%	OSINT, Proyectos H2020, Manual de Tallin
	GI2	Se emplean las mejores prácticas para apoyar escenarios de acceso sofisticados	1	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	GI3	Protección integral contra los riesgos relacionados con accesos no autorizados	1	10%	30%	OSINT, Proyectos H2020, Manual de Tallin
	GI4	Se cuenta con una amplia gama de identidades aprovechando mecanismos automatizados	1	10%	40%	OSINT, Proyectos H2020, Manual de Tallin
	GI5	Se gestionan las identidades de varios grupos de personas, sistemas o cosas	1	10%	30%	OSINT, Proyectos H2020, Manual de Tallin
	GI6	Se mantiene y controla el uso de identidades de personas, sistemas y cosas a lo largo de su ciclo de vida	1	10%	40%	OSINT, Proyectos H2020, Manual de Tallin
	GI7	Se limita la capacidad de los agentes externos para acceder a los sistemas	1	10%	50%	OSINT, Proyectos H2020, Manual de Tallin

	GI8	Se considera el perfil del sujeto para controlar los accesos apropiados	1	10%	60%	OSINT, Proyectos H2020, Manual de Tallin
	GI9	Utiliza las políticas de control de acceso disponibles con un nivel adecuado de garantía	1	10%	70%	OSINT, Proyectos H2020, Manual de Tallin
	GI10	Mantiene un esquema de autorización estrictamente alineado con las necesidades y limitaciones del negocio	1	10%	80%	OSINT, Proyectos H2020, Manual de Tallin
	GI11	Ejecución de MILCYBDEC con la debida cautela. (Due Diligence) El País debe ser cauteloso a fin de evitar que agentes nacionales o externos se apoderen, sin permiso, de la misión a fin de atacar activamente países extranjeros (sean hostiles o no)	1	10%	90%	OSINT, Proyectos H2020, Manual de Tallin
	GI12	Los activos y procesos privados de la misión deben estar bien atribuidos. (atribución)	1	10%	100%	OSINT, Proyectos H2020, Manual de Tallin
	GI13	Los activos y procesos públicos de la misión deben estar bien atribuidos. (atribución)	1	10%	110%	OSINT, Proyectos H2020, Manual de Tallin
	GI14	Los activos de ciberespacio deben encontrarse en instalaciones/infraestructuras físicamente protegidas	1	10%	120%	OSINT, Proyectos H2020, Manual de Tallin
	GI15	Los activos de ciberespacio deben encontrarse en instalaciones/infraestructuras legalmente protegidas	1	10%	130%	OSINT, Proyectos H2020, Manual de Tallin
	GI16	Gestión y protección de los activos de diversos tipos	1	10%	140%	OSINT, Proyectos H2020, Manual de Tallin
	GI17	Se garantiza la aplicación de las políticas de gestión de activos	1	10%	150%	OSINT, Proyectos H2020, Manual de Tallin

	GI18	Se realiza un seguimiento de los cambios poco frecuentes en activos y configuraciones	1	10%	160%	OSINT, Proyectos H2020, Manual de Tallin
	GI19	Siguen algunas reglas específicas para gestionar posibles cambios en el sistema	1	10%	170%	OSINT, Proyectos H2020, Manual de Tallin
	GI20	Existen procedimientos de gestión de cambios para el número de activos y/o configuraciones	1	10%	180%	OSINT, Proyectos H2020, Manual de Tallin
	GI21	Se regula el proceso para el ciclo de vida de los activos, desde el aprovisionamiento hasta la sustitución, incluidos los cambios de emergencia	1	10%	190%	OSINT, Proyectos H2020, Manual de Tallin
	GI22	Se limita el acceso a activos físicos	1	10%	200%	OSINT, Proyectos H2020, Manual de Tallin
	GI23	Definen las restricciones de acceso en cuanto a horarios permitidos	1	10%	210%	OSINT, Proyectos H2020, Manual de Tallin
	GI24	Definen los controles de acceso físico	1	10%	220%	OSINT, Proyectos H2020, Manual de Tallin
	GI25	Automatiza el control de acceso físico utilizando tokens de identidad específicos	1	10%	230%	OSINT, Proyectos H2020, Manual de Tallin
	GI26	Se garantiza un funcionamiento seguro de los controles de acceso físico	1	10%	240%	OSINT, Proyectos H2020, Manual de Tallin
	GI27	Se planifica el mantenimiento general de la confidencialidad e integridad de los datos	1	10%	250%	OSINT, Proyectos H2020, Manual de Tallin
	GI28	Se implementan políticas y métodos para la protección de datos	1	10%	260%	OSINT, Proyectos H2020, Manual de Tallin

	GI29	Se ofrece garantía de la protección de la información comercial crítica en tránsito	1	10%	270%	OSINT, Proyectos H2020, Manual de Tallin
	GI30	Se declara que los datos deben estar protegidos contra el acceso no autorizado	1	10%	280%	OSINT, Proyectos H2020, Manual de Tallin
	GI31	Define el enfoque y los roles/atributos particulares para controlar el acceso a los datos	1	10%	290%	OSINT, Proyectos H2020, Manual de Tallin
	GI32	Se aprovechan los controles de protección integrados (SO, red, servicios)	1	10%	300%	OSINT, Proyectos H2020, Manual de Tallin
	GI33	Apoyar la correcta aplicación de los controles de datos de acuerdo con las normas reconocidas	1	10%	310%	OSINT, Proyectos H2020, Manual de Tallin

Madurez Obtenida
94%

Controles de Dominio Ciclo de Vida, Protección de Activos y Servicios						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
CVPAS	CPA1	Definición del uso de activos digitales y físicos	1	10%	10%	OSINT, Proyectos H2020, Manual de Tallin
	CPA2	Supervisa los activos sobre la base de un caso de uso	1	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
	CPA3	Gestión y protección de los activos de diversos tipos	1	1%	21%	OSINT, Proyectos H2020, Manual de Tallin

	CPA4	Se garantiza la aplicación de las políticas de gestión de activos	1	1%	22%	OSINT, Proyectos H2020, Manual de Tallin
	CPA5	Se realiza un seguimiento de los cambios poco frecuentes en activos y configuraciones	1	10%	32%	OSINT, Proyectos H2020, Manual de Tallin
	CPA6	Siguen algunas reglas específicas para gestionar posibles cambios en el sistema	1	10%	42%	OSINT, Proyectos H2020, Manual de Tallin
	CPA7	Existen procedimientos de gestión de cambios para el número de activos y/o configuraciones	1	10%	52%	OSINT, Proyectos H2020, Manual de Tallin
	CPA8	Se regula el proceso para el ciclo de vida de los activos, desde el aprovisionamiento hasta la sustitución, incluidos los cambios de emergencia	1	10%	62%	OSINT, Proyectos H2020, Manual de Tallin
	CPA9	Se limita el acceso a activos físicos	1	10%	72%	OSINT, Proyectos H2020, Manual de Tallin
	CPA10	Definen las restricciones de acceso en cuanto a horarios permitidos	1	10%	82%	OSINT, Proyectos H2020, Manual de Tallin
	CPA11	Definen los controles de acceso físico	1	10%	92%	OSINT, Proyectos H2020, Manual de Tallin
	CPA12	Automatiza el control de acceso físico utilizando tokens de identidad específicos	1	10%	102%	OSINT, Proyectos H2020, Manual de Tallin

	CPA13	Se garantiza un funcionamiento seguro de los controles de acceso físico	0	10%	102%	OSINT, Proyectos H2020, Manual de Tallin
	CPA14	Se planifica el mantenimiento general de la confidencialidad e integridad de los datos	1	10%	112%	OSINT, Proyectos H2020, Manual de Tallin
	CPA15	Se implementan políticas y métodos para la protección de datos	1	10%	122%	OSINT, Proyectos H2020, Manual de Tallin
	CPA16	Se ofrece garantía de la protección de la información comercial crítica en tránsito	1	10%	132%	OSINT, Proyectos H2020, Manual de Tallin
	CPA17	Se declara que los datos deben estar protegidos contra el acceso no autorizado	1	10%	142%	OSINT, Proyectos H2020, Manual de Tallin
	CPA18	Define el enfoque y los roles/atributos particulares para controlar el acceso a los datos	1	10%	152%	OSINT, Proyectos H2020, Manual de Tallin
	CPA19	Se aprovechan los controles de protección integrados (SO, red, servicios)	1	10%	162%	OSINT, Proyectos H2020, Manual de Tallin
	CPA20	Apoyar la correcta aplicación de los controles de datos de acuerdo con las normas reconocidas	1	10%	172%	OSINT, Proyectos H2020, Manual de Tallin

Madurez Obtenida
95%

Controles de Dominio Leyes de Guerra						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
LG	LG1	Deben de haber suficientes medidas activas de protección física y legal de los activos/procesos de MILCYBDEC	1	10%	10%	OSINT, Proyecto H2020, Manual d Tallin
	LG7	El alcance de una misión MILCYBDEC debe estar limitado y bien definido.	1	10%	20%	OSINT, Proyecto H2020, Manual d Tallin
	LG9	El personal aliado , según nivel de habilitación de seguridad, debe , o no debe, ser consciente de los procesos/activos que componen la misión MILCYBDEC	0	10%	20%	OSINT, Proyecto H2020, Manual d Tallin
	LG10	La misión de MILCYBDEC debe proveer contramedidas proporcionales a los ataques	0	10%	20%	OSINT, Proyecto H2020, Manual d Tallin
	LG11	La misión de MILCYBDEC debe tener capacidad de medir la ciber-agresión entrante, a fin de poder equipararla con un ataque cinético (equivalente, y poder, en un futuro, si necesario lanzar una reciprocación proporcional (reciprocidad y proporcionalidad a los ataques)	0	10%	20%	OSINT, Proyecto H2020, Manual d Tallin
	LG12	La misión de MILCYBDEC debe tener unos objetivos bien definidos.	0	10%	20%	OSINT, Proyecto H2020, Manual d Tallin
	LG13	La misión de MILCYBDEC debe poder proveer contramedidas de alcance medible de cara a los ataques	0	10%	20%	OSINT, Proyecto H2020, Manual d Tallin
	LG14	La misión de MILCYBDEC debe poder proveer contramedidas de efectos medibles de cara a los ataques	0	10%	20%	OSINT, Proyecto H2020, Manual d Tallin
	LG15	La misión de MILCYBDEC tiene que tener procesos/activos en el Espacio Exterior, si dicho dominio afecta a la Misión	0	10%	20%	OSINT, Proyecto H2020, Manual d Tallin
	LG16	La misión MILCYBDEC debe prever distintos niveles de activación (i.e. nivel de alerta)	1	10%	30%	OSINT, Proyecto H2020, Manual d Tallin

	LG17	La misión MILCYBDEC debe satisfacer el Principio de Distinción, i.e tener capacidades de reconocer si los objetivos de MILCYBDEC son civiles o militares	1	10%	40%	OSINT, Proyecto H2020, Manual d Tallin
	LG18	La misión MILCYBDEC garantiza la soberanía física del país y/o las fuerzas aliadas	1	10%	50%	OSINT, Proyecto H2020, Manual d Tallin
	LG19	La misión MILCYBDEC no debe dañar el entorno natural.	0	10%	50%	OSINT, Proyecto H2020, Manual d Tallin
	LG20	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de los menores de edad	0	10%	50%	OSINT, Proyecto H2020, Manual d Tallin
	LG21	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de prisioneros de guerra	0	10%	50%	OSINT, Proyecto H2020, Manual d Tallin
	LG22	La misión MILCYBDEC no debe interferir con Sistemas de Países Aliados.	1	10%	60%	OSINT, Proyecto H2020, Manual d Tallin
	LG23	La misión MILCYBDEC no debe interferir con Sistemas de Países Hostiles (adversarios), **(aunque sí puede dificultar operaciones extranjeras no pacificas)**	0	10%	60%	OSINT, Proyecto H2020, Manual d Tallin
	LG24	La misión MILCYBDEC no debe interferir con Sistemas de Países Neutrales	0	10%	60%	OSINT, Proyecto H2020, Manual d Tallin
	LG25	La misión MILCYBDEC sólo debe ser activada cuando sea necesario	0	10%	60%	OSINT, Proyecto H2020, Manual d Tallin
	LG26	La misión no debe provocar acciones ofensivas transfronterizas	1	10%	70%	OSINT, Proyecto H2020, Manual d Tallin
	LG27	La misión no debe realizar acciones ofensivas transfronterizas	1	10%	80%	OSINT, Proyecto H2020, Manual d Tallin

	LG28	Las infraestructuras de MILCYBDEC deben ser capaces de detectar los ataques entrantes de fuerzas/países hostiles y alertar a las autoridades competentes , p.e. el Concejo de Seguridad de Naciones Unidas	0	10%	80%	OSINT, Proyecto H2020, Manual d Tallin
	LG29	Las medidas de MILCYBDEC no deben contravenir los acuerdos internacionales firmados por el País. (p.e. convención de Ginebra, Canadá, Viena)	1	10%	90%	OSINT, Proyecto H2020, Manual d Tallin
	LG30	Los dominios de batalla afectados por una misión MILCYBDEC deben estar bien definidos	0	10%	90%	OSINT, Proyecto H2020, Manual d Tallin
	LG31	Los procesos/activos de MILCYBDEC no deben activar fuegos, o en todo caso, si activan fuegos, deben ser fuegos simulados y/o con carga simulada	0	10%	90%	OSINT, Proyecto H2020, Manual d Tallin
	LG32	Los procesos/activos de MILCYBDEC no deben amenazar con respuesta activa, ya sea cibernética o cinética, en caso de que dicha respuesta no se ajuste a los principios de guerra justa.	0	10%	90%	OSINT, Proyecto H2020, Manual d Tallin
	LG33	Los procesos/activos de MILCYBDEC no deben causar interferencias dañinas en el ciberespacio	1	10%	100%	OSINT, Proyecto H2020, Manual d Tallin
	LG34	Los procesos/activos de MILCYBDEC no deben causar interferencias dañinas en el espectro electromagnético	1	10%	110%	OSINT, Proyecto H2020, Manual d Tallin
	LG35	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de naves aéreas	1	10%	120%	OSINT, Proyecto H2020, Manual d Tallin
	LG36	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de naves civiles	1	10%	130%	OSINT, Proyecto H2020, Manual d Tallin
	LG37	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de vehículos terrestres civiles	0	10%	130%	OSINT, Proyecto H2020, Manual d Tallin
	LG38	Los procesos/activos de MILCYBDEC no deben realizar actos de Perfidia (p.e. hacerse pasar por objetivos civiles, o de primeros auxilios, p.e.)	0	10%	130%	OSINT, Proyecto H2020, Manual d Tallin

	LG39	Los procesos/activos de MILCYBDEC no deben tener almacenada información secreta verdadera	0	10%	130%	OSINT, Proyecto H2020, Manual d Tallin
	LG40	Los procesos/activos MILCYBDEC, si son elementos que soportan tráfico de red internacional, deben dar paso libre a dicho tráfico (mientras el origen y el destino sean externos al País)	0	10%	130%	OSINT, Proyecto H2020, Manual d Tallin
	LG41	Los propietarios de activos y/o procesos de MILCYBDEC deben ser actores legítimos, i.e. autoridades estatales, militares y/o habilitadas para ejercer Ciberdefensa en el ámbito de la misión	0	10%	130%	OSINT, Proyecto H2020, Manual d Tallin
	LG42	Los sistemas de MILCYBDEC no deben identificarse, sin autorización previa, como actores internacionales, tales como Naciones Unidas (UN)	0	10%	130%	OSINT, Proyecto H2020, Manual d Tallin
	LG43	MILCYBDEC debe ser necesario y justificable.	0	10%	130%	OSINT, Proyecto H2020, Manual d Tallin
	LG44	MILCYBDEC debe ser proporcional a las amenazas de las que protege	0	10%	130%	OSINT, Proyecto H2020, Manual d Tallin
	LG45	MILCYBDEC no debe destruir y/o degradar rutas de datos internacionales, que se encuentren fuera del dominio geográfico y/o lógico de las redes del País	1	10%	140%	OSINT, Proyecto H2020, Manual d Tallin
	LG46	MILCYBDEC no puede los Derechos Humanos	0	10%	140%	OSINT, Proyecto H2020, Manual d Tallin
	LG47	MILCYBDEC no va en contra de la Leyes de la Guerra	0	10%	140%	OSINT, Proyecto H2020, Manual d Tallin
	LG48	Se deben poder lanzar contramedidas simuladas (con un payload inofensivo) en caso de detectar ataques a un Honeypot o Honeynet.	0	10%	140%	OSINT, Proyecto H2020, Manual d Tallin
	LG49	Según nivel de alerta, la misión MILCYBDEC no debería dirigirse hacia países aliados	0	10%	140%	OSINT, Proyecto H2020, Manual d Tallin

	LG50	Un proceso/activo de Ciberengaño debe ser 'visitable', i.e. debe poder ser inspeccionado por las autoridades del País.	1	10%	150%	OSINT, Proyecto H2020, Manual d Tallin

Madurez Obtenida
34%

Controles de Dominio Gestión de Incidentes y Resiliencia						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
GIR	GIR1	Se realiza la comprobación de la recuperación del sistema después de incidentes	1	10%	10%	OSINT, Proyectos H2020, Manual de Tallin
		En la misión MILCYBDEC, hay establecidas redundancias de redes, almacenamiento y procesamiento en el territorio del País	1	10%	20%	OSINT, Proyectos H2020, Manual de Tallin
		Hay establecidas redundancias de redes, almacenamiento y procesamiento dentro de países aliados	1	10%	30%	OSINT, Proyectos H2020, Manual de Tallin
	GIR2	Se garantiza la recuperación de componentes o procesos del sistema separados	1	10%	40%	OSINT, Proyectos H2020, Manual de Tallin
	GIR3	Existe un procedimiento de recuperación automática Se generan informes descriptivos sobre los incidentes y sus soluciones Respuesta rápida a incidentes y reducción del daño al negocio tanto por medios técnicos como organizativos	1	10%	50%	OSINT, Proyectos H2020, Manual de Tallin
	GIR4	Define incidentes específicos y acciones básicas para reaccionar	1	10%	60%	OSINT, Proyectos H2020, Manual de Tallin

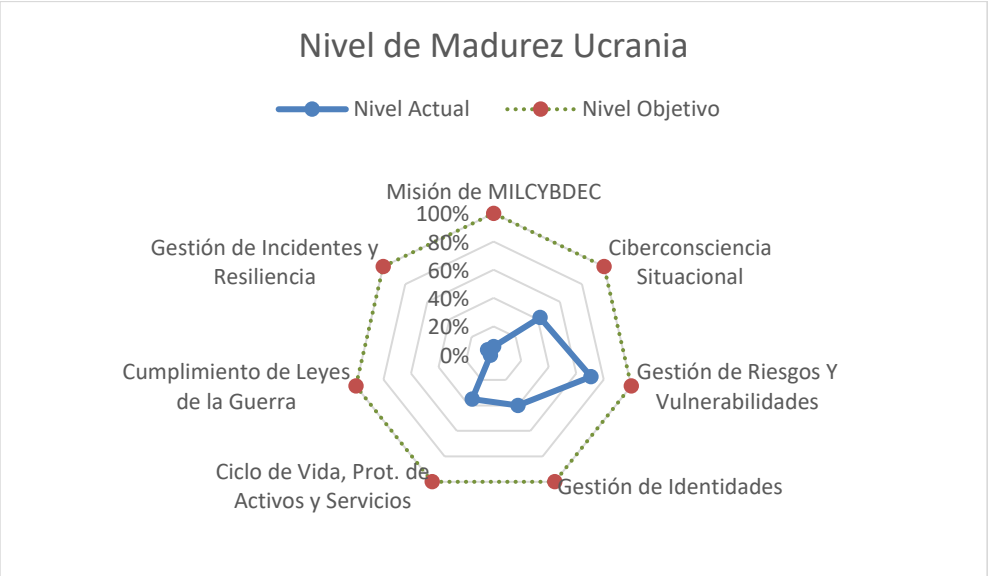
	GIR5	Proporciona orientación para componentes críticos sobre cómo detectar y responder a incidentes	1	10%	70%	OSINT, Proyectos H2020, Manual de Tallin
	GIR6	Establece la base para la ejecución automática de los procedimientos de respuesta	1	10%	80%	OSINT, Proyectos H2020, Manual de Tallin
	GIR7	Crear controles para detectar incidentes, asignarlos para la investigación y escalar según sea necesario	1	10%	90%	OSINT, Proyectos H2020, Manual de Tallin
	GIR8	Posee mecanismos para asignar incidentes para su investigación y escalar según sea necesario	1	10%	100%	OSINT, Proyectos H2020, Manual de Tallin
	GIR9	Se cuentan con procedimientos con instrucciones básicas para la recuperación del sistema	1	10%	110%	OSINT, Proyectos H2020, Manual de Tallin
	GIR10	Se manejan todos los incidentes que se detectan	1	10%	120%	OSINT, Proyectos H2020, Manual de Tallin
	GIR11	Se comprueba si el sistema está completamente recuperado luego de un incidente	1	10%	130%	OSINT, Proyectos H2020, Manual de Tallin
	GIR12	Se poseen mecanismos para la ejecución automática de procedimientos de corrección y recuperación	1	10%	140%	OSINT, Proyectos H2020, Manual de Tallin
	GIR13	Se cuenta con una combinación de medidas técnicas y organizativas que faciliten la rápida recuperación del sistema	1	10%	150%	OSINT, Proyectos H2020, Manual de Tallin
		La misión de MILCYBDEC debe proveer contramedidas inmediatas a los ataques	0	10%	150%	OSINT, Proyectos H2020, Manual de Tallin

		La misión de MILCYBDEC debe poder proveer contramedidas directas de cara a los ataques	0	10%	150%	OSINT, Proyectos H2020, Manual de Tallin
		Las infraestructuras de MILCYBDEC deben ser capaces de detectar los ataques entrantes y alertar al propietario de la infraestructura (real) subyacente.	1	10%	160%	OSINT, Proyectos H2020, Manual de Tallin

Madurez Obtenida
89%

Anexo 3: Resultados MILCYBDEC Ucrania

Nombre Dominio	Nivel Actual	Nivel Objetivo
Misión de MILCYBDEC	6%	100%
Ciberconciencia Situacional	42%	100%
Gestión de Riesgos Y Vulnerabilidades	71%	100%
Gestión de Identidades	40%	100%
Ciclo de Vida, Prot. de Activos y Servicios	35%	100%
Cumplimiento de Leyes de la Guerra	2%	100%
Gestión de Incidentes y Resiliencia	6%	100%



Controles de Misión MILCYBDEC						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
MCC	MCC1	La misión MILCYBDEC apoya la soberanía cibernética del país y/o las fuerzas aliadas	1	10%	10%	OSINT
	MCC3	Hay establecidas redundancias de redes, almacenamiento y procesamiento dentro de países aliados	0	10%	10%	OSINT
	MCC4	La misión MILCYBDEC garantiza la soberanía física del país y/o las fuerzas aliadas	0	10%	10%	OSINT
	MCC5	La misión MILCYBDEC debe definir claramente los cauces hacia los blancos.	0	10%	10%	OSINT
	MCC6	El guion de MILCYBDEC es creíble, verificable, consistente, implementable	0	10%	10%	OSINT
	MCC7	La misión MILCYBDEC disfruta de planificación y control centralizados	0	10%	10%	OSINT

	MCC8	Se ha securizado la información de MILDEC, mediante compartimentalización	0	10%	10%	OSINT
	MCC9	Se ha securizado la información de MILDEC, mediante control de accesos e identidad	0	10%	10%	OSINT
	MCC10	La misión de MILCYBDEC tiene procesos dedicados a OPSEC	0	10%	10%	OSINT0
	MCC11	La misión de MILCYBDEC dedica suficiente tiempo y plazo para desplegar el guion y para que el adversario se dé cuenta de él	0	10%	10%	OSINT1
	MCC12	Las operaciones MILCYBDEC están plenamente integradas con otras Operaciones aliadas	0	10%	10%	OSINT2
	MCC13	El concepto de MILCYBDEC debe desarrollarse a la vez que CONOPS para la misión principal.	0	10%	10%	OSINT3
	MCC14	Se posee toda la cadena de suministros de activos/procesos MILCYBDEC	0	10%	10%	OSINT4
	MCC15	La misión MILCYBDEC no debe interferir activamente con infraestructuras y servicios de países extranjeros (p.e. publicar 'fake news' en un estado extranjero, aunque sea parte hostil)	0	10%	10%	OSINT5
	MCC16	La misión MILCYBDEC debe haber identificado las lagunas de información del adversario	0	10%	10%	OSINT6
	MCC17	La misión de MILCYBDEC debe garantizar la inmediatez de reacción, a fin de mantener el 'Uptime' de los activos/procesos protegidos	0	10%	10%	OSINT7

	MCC18	El alcance de una misión MILCYBDEC debe estar limitado y bien definido.	0	10%	10%	OSINT8
	MCC19	La misión MILCYBDEC no debe interferir con otras misiones aliadas	0	10%	10%	OSINT9

Madurez Obtenida
6%

Controles de Dominio CCS						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
CCS	CCS1	Mantiene una conciencia mínima de los eventos relacionados con la seguridad	1	10%	10%	OSINT
	CCS2	Atención específica a algunos tipos de eventos de seguridad	0	10%	10%	OSINT
	CCS3	Supervisión integral y el intercambio regular de información relacionada con la seguridad	1	40%	50%	OSINT
	CCS4	Proporciona y gestiona toda la información relevante para los aspectos de fiabilidad	0	40%	50%	OSINT
	CCS5	Obtiene información externa pertinente sobre una base ad hoc	1	40%	90%	OSINT
	CCS6	Permite que el personal utilice constantemente fuentes de información externas relevantes	0	40%	90%	OSINT
	CCS9	Comprueba los registros del sistema para fines de diagnóstico	1	40%	130%	OSINT

	CCS10	Revisa periódicamente los eventos que indican cómo se ejecutan correctamente los procesos críticos	0	40%	130%	OSINT
	CCS11	Recopila información relevante para la seguridad	0	40%	130%	OSINT
	CCS12	Analiza información relevante para la seguridad, tanto con herramientas construidas como diseñadas específicamente	0	40%	130%	OSINT0
	CCS13	La misión MILCYBDEC tiene en cuenta KCT (Ciberterrenos clave)	1	40%	170%	OSINT1
	CCS14	Monitoreo Y Alerta Continuos de Honeynets	0	40%	170%	OSINT2
	CCS15	Monitoreo y Alerta Continuos de Honeypots	0	40%	170%	OSINT3
	CCS16	Monitoreo Y Alerta Continuos de Honeywords	1	40%	210%	OSINT4

Madurez Obtenida
42%

Controles de Dominio Gestión de Riesgos y Vulnerabilidades						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
GR	GR1	Se ha establecido una estrategia de gestión de riesgos de ciberseguridad	1	10%	10%	OSINT

	GR2	Revisión del panorama actual de amenazas	1	10%	20%	OSINT
	GR3	Comprender las vulnerabilidades del sistema	1	10%	30%	OSINT
	GR4	Comprender las vulnerabilidades de la tecnología	1	10%	40%	OSINT
	GR5	Descripción completa de los riesgos pertinentes	1	10%	50%	OSINT
	GR6	Enfoque holístico y sistemático de la gestión de riesgos	1	10%	60%	OSINT
	GR7	Se incluyen temas generales de seguridad de TI como amenazas en el baseline de la ciudad	1	10%	70%	OSINT
	GR8	Se identifican y describen las amenazas de manera intrínseca Se describen los factores de TI que pueden poner el sistema en riesgo Se define la noción de riesgo	1	10%	80%	OSINT
	GR9	Se define la importancia de los riesgos de acuerdo a su probabilidad e impacto	1	10%	90%	OSINT
	GR10	Se miden y gestionan adecuadamente los riesgos	1	10%	100%	OSINT0
	GR11	Utiliza un marco y proceso de gestión de riesgos	1	10%	110%	OSINT1
	GR12	Mantiene los sistemas actualizados	1	10%	120%	OSINT2
	GR13	Aplicar una política de actualización regular para los componentes críticos	1	10%	130%	OSINT3
	GR14	Soporte de actualizaciones automatizadas configuradas específicamente para el caso	1	10%	140%	OSINT4

	GR15	Planifica un proceso de actualización regular y escenarios de emergencia para los días cero críticos	0	10%	140%	OSINT5
	GR16	Considerar si las vulnerabilidades ampliamente conocidas son relevantes para el sistema	0	10%	140%	OSINT6
	GR17	Comprueba si los componentes especificados son propensos a ataques	0	10%	140%	OSINT7
	GR18	Obtiene una evaluación objetiva de terceros de vulnerabilidades y exposiciones	0	10%	140%	OSINT8
	GR19	Realiza inspecciones de seguridad personalizadas periódicas regulares	1	10%	150%	OSINT9
	GR20	Considera los avisos de seguridad emitidos por los proveedores e instalar los parches apropiados	0	10%	150%	OSINT0
	GR21	Comprueba que los componentes especificados están protegidos contra los ataques más probables	0	10%	150%	OSINT1
	GR22	Establece procedimientos de actualización automática siempre que sea posible	1	10%	160%	OSINT2
	GR23	Aplica una política del sistema para garantizar la protección continua contra los ataques conocidos	0	10%	160%	OSINT3
	GR24	La misión MILCYBDEC debe tener procesos de revisión y automejora	1	10%	170%	OSINT4

Madurez Obtenida
71%

Controles de Dominio Gestión de Identidades						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
GI	GI1	Se definen las entidades elementales de apoyo para el escenario de uso básico	1	10%	10%	OSINT
	GI2	Se emplean las mejores prácticas para apoyar escenarios de acceso sofisticados	0	10%	10%	OSINT
	GI3	Protección integral contra los riesgos relacionados con accesos no autorizados	1	10%	20%	OSINT
	GI4	Se cuenta con una amplia gama de identidades aprovechando mecanismos automatizados	0	10%	20%	OSINT
	GI5	Se gestionan las identidades de varios grupos de personas, sistemas o cosas	1	10%	20%	OSINT
	GI6	Se mantiene y controla el uso de identidades de personas, sistemas y cosas a lo largo de su ciclo de vida	0	10%	20%	OSINT
	GI7	Se limita la capacidad de los agentes externos para acceder a los sistemas	1	10%	30%	OSINT
	GI8	Se considera el perfil del sujeto para controlar los accesos apropiados	0	10%	30%	OSINT
	GI9	Utiliza las políticas de control de acceso disponibles con un nivel adecuado de garantía	0	10%	30%	OSINT
	GI10	Mantiene un esquema de autorización estrictamente alineado con las necesidades y limitaciones del negocio	1	10%	40%	OSINT
	GI11	Ejecución de MILCYBDEC con la debida cautela. (Due Diligence) El País debe ser cauteloso a fin de evitar que agentes nacionales o externos se apoderen, sin permiso, de la misión a fin de atacar activamente países extranjeros (sean hostiles o no)	0	10%	40%	OSINT0
	GI12	Los activos y procesos privados de la misión deben estar bien atribuidos. (atribución)	0	10%	40%	OSINT1
	GI13	Los activos y procesos públicos de la misión deben estar bien atribuidos. (atribución)	1	10%	50%	OSINT2

	GI14	Los activos de ciberespacio deben encontrarse en instalaciones/infraestructuras físicamente protegidas	0	10%	50%	OSINT3
	GI15	Los activos de ciberespacio deben encontrarse en instalaciones/infraestructuras legalmente protegidas	1	10%	60%	OSINT4

Madurez Obtenida
40%

Controles de Dominio Ciclo de Vida, Protección de Activos y Servicios						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
CVPAS	CPA1	Definición del uso de activos digitales y físicos	1	10%	10%	OSINT
	CPA2	Supervisa los activos sobre la base de un caso de uso	0	10%	10%	OSINT
	CPA3	Gestión y protección de los activos de diversos tipos	1	10%	20%	OSINT
	CPA4	Se garantiza la aplicación de las políticas de gestión de activos	0	10%	20%	OSINT
	CPA5	Se realiza un seguimiento de los cambios poco frecuentes en activos y configuraciones	0	10%	20%	OSINT
	CPA6	Siguen algunas reglas específicas para gestionar posibles cambios en el sistema	0	10%	20%	OSINT
	CPA7	Existen procedimientos de gestión de cambios para el número de activos y/o configuraciones	1	10%	30%	OSINT

	CPA8	Se regula el proceso para el ciclo de vida de los activos, desde el aprovisionamiento hasta la sustitución, incluidos los cambios de emergencia	0	10%	30%	OSINT
	CPA9	Se limita el acceso a activos físicos	0	10%	30%	OSINT
	CPA10	Definen las restricciones de acceso en cuanto a horarios permitidos	0	10%	30%	OSINT
	CPA11	Definen los controles de acceso físico	1	10%	40%	OSINT
	CPA12	Automatiza el control de acceso físico utilizando tokens de identidad específicos	0	10%	40%	OSINT
	CPA13	Se garantiza un funcionamiento seguro de los controles de acceso físico	0	10%	40%	OSINT
	CPA14	Se planifica el mantenimiento general de la confidencialidad e integridad de los datos	1	10%	50%	OSINT
	CPA15	Se implementan políticas y métodos para la protección de datos	0	10%	50%	OSINT
	CPA16	Se ofrece garantía de la protección de la información comercial crítica en tránsito	0	10%	50%	OSINT

	CPA17	Se declara que los datos deben estar protegidos contra el acceso no autorizado	1	10%	60%	OSINT
	CPA18	Define el enfoque y los roles/atributos particulares para controlar el acceso a los datos	0	10%	60%	OSINT
	CPA19	Se aprovechan los controles de protección integrados (SO, red, servicios)	0	10%	60%	OSINT
	CPA20	Apoyar la correcta aplicación de los controles de datos de acuerdo con las normas reconocidas.	1	10%	70%	OSINT

Madurez Obtenida
35%

Controles de Dominio Leyes de Guerra						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
LG	LG1	Deben de haber suficientes medidas activas de protección física y legal de los activos/procesos de MILCYBDEC	1	10%	10%	OSINT
	LG7	El alcance de una misión MILCYBDEC debe estar limitado y bien definido.	0	10%	10%	OSINT
	LG9	El personal aliado , según nivel de habilitación de seguridad, debe , o no debe, ser consciente de los procesos/activos que componen la misión MILCYBDEC	0	10%	10%	OSINT
	LG10	La misión de MILCYBDEC debe proveer contramedidas proporcionales a los ataques	0	10%	10%	OSINT

	LG11	La misión de MILCYBDEC debe tener capacidad de medir la ciber-agresión entrante, a fin de poder equipararla con un ataque cinético (equivalente, y poder, en un futuro, si necesario lanzar una reciprocación proporcional (reciprocidad y proporcionalidad a los ataques)	0	10%	10%	OSINT
	LG12	La misión de MILCYBDEC debe tener unos objetivos bien definidos.	0	10%	10%	OSINT
	LG13	La misión de MILCYBDEC debe poder proveer contramedidas de alcance medible de cara a los ataques	0	10%	10%	OSINT
	LG14	La misión de MILCYBDEC debe poder proveer contramedidas de efectos medibles de cara a los ataques	0	10%	10%	OSINT
	LG15	La misión de MILCYBDEC tiene que tener procesos/activos en el Espacio Exterior, si dicho dominio afecta a la Misión	0	10%	10%	OSINT
	LG16	La misión MILCYBDEC debe prever distintos niveles de activación (i.e. nivel de alerta)	0	10%	10%	OSINT0
	LG17	La misión MILCYBDEC debe satisfacer el Principio de Distinción, i.e tener capacidades de reconocer si los objetivos de MILCYBDEC son civiles o militares	0	10%	10%	OSINT1
	LG18	La misión MILCYBDEC garantiza la soberanía física del país y/o las fuerzas aliadas	0	10%	10%	OSINT2
	LG19	La misión MILCYBDEC no debe dañar el entorno natural.	0	10%	10%	OSINT3
	LG20	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de los menores de edad	0	10%	10%	OSINT4
	LG21	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de prisioneros de guerra	0	10%	10%	OSINT5

	LG22	La misión MILCYBDEC no debe interferir con Sistemas de Países Aliados.	0	10%	10%	OSINT6
	LG23	La misión MILCYBDEC no debe interferir con Sistemas de Países Hostiles (adversarios), **(aunque sí puede dificultar operaciones extranjeras no pacificas)**	0	10%	10%	OSINT7
	LG24	La misión MILCYBDEC no debe interferir con Sistemas de Países Neutrales	0	10%	10%	OSINT8
	LG25	La misión MILCYBDEC sólo debe ser activada cuando sea necesario	0	10%	10%	OSINT9
	LG26	La misión no debe provocar acciones ofensivas transfronterizas	0	10%	10%	OSINT0
	LG27	La misión no debe realizar acciones ofensivas transfronterizas	0	10%	10%	OSINT1
	LG28	Las infraestructuras de MILCYBDEC deben ser capaces de detectar los ataques entrantes de fuerzas/países hostiles y alertar a las autoridades competentes , p.e. el Concejo de Seguridad de Naciones Unidas	0	10%	10%	OSINT2
	LG29	Las medidas de MILCYBDEC no deben contravenir los acuerdos internacionales firmados por el País. (p.e. convención de Ginebra, Canadá, Viena)	0	10%	10%	OSINT3
	LG30	Los dominios de batalla afectados por una misión MILCYBDEC deben estar bien definidos	0	10%	10%	OSINT4
	LG31	Los procesos/activos de MILCYBDEC no deben activar fuegos, o en todo caso, si activan fuegos, deben ser fuegos simulados y/o con carga simulada	0	10%	10%	OSINT5
	LG32	Los procesos/activos de MILCYBDEC no deben amenazar con respuesta activa, ya sea cibernética o cinética, en caso de que dicha respuesta no se ajuste a los principios de guerra justa.	0	10%	10%	OSINT6

	LG33	Los procesos/activos de MILCYBDEC no deben causar interferencias dañinas en el ciberespacio	0	10%	10%	OSINT7
	LG34	Los procesos/activos de MILCYBDEC no deben causar interferencias dañinas en el espectro electromagnético	0	10%	10%	OSINT8
	LG35	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de naves aéreas	0	10%	10%	OSINT9
	LG36	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de naves civiles	0	10%	10%	OSINT0
	LG37	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de vehículos terrestres civiles	0	10%	10%	OSINT1
	LG38	Los procesos/activos de MILCYBDEC no deben realizar actos de Perfidia (p.e. hacerse pasar por objetivos civiles, o de primeros auxilios, p.e.)	0	10%	10%	OSINT2
	LG39	Los procesos/activos de MILCYBDEC no deben tener almacenada información secreta verdadera	0	10%	10%	OSINT3
	LG40	Los procesos/activos MILCYBDEC, si son elementos que soportan tráfico de red internacional, deben dar paso libre a dicho tráfico (mientras el origen y el destino sean externos al País)	0	10%	10%	OSINT4
	LG41	Los propietarios de activos y/o procesos de MILCYBDEC deben ser actores legítimos, i.e. autoridades estatales, militares y/o habilitadas para ejercer Ciberdefensa en el ámbito de la misión	0	10%	10%	OSINT5
	LG42	Los sistemas de MILCYBDEC no deben identificarse, sin autorización previa, como actores internacionales, tales como Naciones Unidas (UN)	0	10%	10%	OSINT6
	LG43	MILCYBDEC debe ser necesario y justificable.	0	10%	10%	OSINT7

	LG44	MILCYBDEC debe ser proporcional a las amenazas de las que protege	0	10%	10%	OSINT8
	LG45	MILCYBDEC no debe destruir y/o degradar rutas de datos internacionales, que se encuentren fuera del dominio geográfico y/o lógico de las redes del País	0	10%	10%	OSINT9
	LG46	MILCYBDEC no puede los Derechos Humanos	0	10%	10%	OSINT0
	LG47	MILCYBDEC no va en contra de la Leyes de la Guerra	0	10%	10%	OSINT1
	LG48	Se deben poder lanzar contramedidas simuladas (con un payload inofensivo) en caso de detectar ataques a un Honeypot o Honeynet.	0	10%	10%	OSINT2
	LG49	Según nivel de alerta, la misión MILCYBDEC no debería dirigirse hacia países aliados	0	10%	10%	OSINT3
	LG50	Un proceso/activo de Ciberengaño debe ser 'visitable', i.e. debe poder ser inspeccionado por las autoridades del País.	0	10%	10%	OSINT4

Madurez Obtenida
2%

Controles de Dominio Gestión de Incidentes y Resiliencia						
Id. Control		Descripción	Visto (1/0)	Peso (%)	Σ	Evidencia
GIR	GIR1	Se realiza la comprobación de la recuperación del sistema después de incidentes	1	10%	10%	OSINT
		En la misión MILCYBDEC, hay establecidas redundancias de redes, almacenamiento y procesamiento en el territorio del País	0	10%	10%	OSINT

		Hay establecidas redundancias de redes, almacenamiento y procesamiento dentro de países aliados	0	10%	10%	OSINT
	GIR2	Se garantiza la recuperación de componentes o procesos del sistema separados	0	10%	10%	OSINT
	GIR3	Existe un procedimiento de recuperación automática Se generan informes descriptivos sobre los incidentes y sus soluciones Respuesta rápida a incidentes y reducción del daño al negocio tanto por medios técnicos como organizativos	0	10%	10%	OSINT
	GIR4	Define incidentes específicos y acciones básicas para reaccionar	0	10%	10%	OSINT
	GIR5	Proporciona orientación para componentes críticos sobre cómo detectar y responder a incidentes	0	10%	10%	OSINT
	GIR6	Establece la base para la ejecución automática de los procedimientos de respuesta	0	10%	10%	OSINT
	GIR7	Crear controles para detectar incidentes, asignarlos para la investigación y escalar según sea necesario	0	10%	10%	OSINT
	GIR8	Posee mecanismos para asignar incidentes para su investigación y escalar según sea necesario	0	10%	10%	OSINT0
	GIR9	Se cuentan con procedimientos con instrucciones básicas para la recuperación del sistema	0	10%	10%	OSINT1

	GIR10	Se manejan todos los incidentes que se detectan	0	10%	10%	OSINT2
	GIR11	Se comprueba si el sistema está completamente recuperado luego de un incidente	0	10%	10%	OSINT3
	GIR12	Se poseen mecanismos para la ejecución automática de procedimientos de corrección y recuperación	0	10%	10%	OSINT4
	GIR13	Se cuenta con una combinación de medidas técnicas y organizativas que faciliten la rápida recuperación del sistema	0	10%	10%	OSINT5
		La misión de MILCYBDEC debe proveer contramedidas inmediatas a los ataques	0	10%	10%	OSINT6
		La misión de MILCYBDEC debe poder proveer contramedidas directas de cara a los ataques	0	10%	10%	OSINT7
		Las infraestructuras de MILCYBDEC deben ser capaces de detectar los ataques entrantes y alertar al propietario de la infraestructura (real) subyacente.	0	10%	10%	OSINT8

Madurez Obtenida
6%

Anexo 4: Deficiencias MILCYBDEC

Deficiencias Ucrania

MCC3	Hay establecidas redundancias de redes, almacenamiento y procesamiento dentro de países aliados
MCC4	La misión MILCYBDEC garantiza la soberanía física del país y/o las fuerzas aliadas
MCC5	La misión MILCYBDEC debe definir claramente los cauces hacia los blancos.
MCC6	El guion de MILCYBDEC es creíble, verificable, consistente, implementable
MCC7	La misión MILCYBDEC disfruta de planificación y control centralizados
MCC8	Se ha securizado la información de MILDEC, mediante compartimentalización
MCC9	Se ha securizado la información de MILDEC, mediante control de accesos e identidad
MCC10	La misión de MILCYBDEC tiene procesos dedicados a OPSEC
MCC11	La misión de MILCYBDEC dedica suficiente tiempo y plazo para desplegar el guion y para que el adversario se dé cuenta de él

MCC12	Las operaciones MILCYBDEC están plenamente integradas con otras Operaciones aliadas
MCC13	El concepto de MILCYBDEC debe desarrollarse a la vez que CONOPS para la misión principal.
MCC14	Se posee toda la cadena de suministros de activos/procesos MILCYBDEC
MCC15	La misión MILCYBDEC no debe interferir activamente con infraestructuras y servicios de países extranjeros (p.e. publicar 'fake news' en un estado extranjero, aunque sea parte hostil)
MCC16	La misión MILCYBDEC debe haber identificado las lagunas de información del adversario
MCC17	La misión de MILCYBDEC debe garantizar la inmediatez de reacción, a fin de mantener el 'Uptime' de los activos/procesos protegidos
MCC18	El alcance de una misión MILCYBDEC debe estar limitado y bien definido.
MCC19	La misión MILCYBDEC no debe interferir con otras misiones aliadas
CCS2	Atención específica a algunos tipos de eventos de seguridad

CCS4	Proporciona y gestiona toda la información relevante para los aspectos de fiabilidad
CCS6	Permite que el personal utilice constantemente fuentes de información externas relevantes
CCS10	Revisa periódicamente los eventos que indican cómo se ejecutan correctamente los procesos críticos
CCS11	Recopila información relevante para la seguridad
CCS12	Analiza información relevante para la seguridad, tanto con herramientas construidas como diseñadas específicamente
CCS14	Monitoreo Y Alerta Continuos de Honeynets
CCS15	Monitoreo y Alerta Continuos de Honeypots
GR15	Planifica un proceso de actualización regular y escenarios de emergencia para los días cero críticos
GR16	Considerar si las vulnerabilidades ampliamente conocidas son relevantes para el sistema

GR17	Comprueba si los componentes especificados son propensos a ataques
GR18	Obtiene una evaluación objetiva de terceros de vulnerabilidades y exposiciones
GR20	Considera los avisos de seguridad emitidos por los proveedores e instalar los parches apropiados
GR21	Comprueba que los componentes especificados están protegidos contra los ataques más probables
GR23	Aplica una política del sistema para garantizar la protección continua contra los ataques conocidos
GI2	Se emplean las mejores prácticas para apoyar escenarios de acceso sofisticados
GI4	Se cuenta con una amplia gama de identidades aprovechando mecanismos automatizados
GI6	Se mantiene y controla el uso de identidades de personas, sistemas y cosas a lo largo de su ciclo de vida
GI8	Se considera el perfil del sujeto para controlar los accesos apropiados

GI9	Utiliza las políticas de control de acceso disponibles con un nivel adecuado de garantía
GI11	Ejecución de MILCYBDEC con la debida cautela. (Due Diligence) El País debe ser cauteloso a fin de evitar que agentes nacionales o externos se apoderen, sin permiso, de la misión a fin de atacar activamente países extranjeros (sean hostiles o no)
GI12	Los activos y procesos privados de la misión deben estar bien atribuidos. (atribución)
GI14	Los activos de ciberespacio deben encontrarse en instalaciones/infraestructuras físicamente protegidas
CPA2	Supervisa los activos sobre la base de un caso de uso
CPA4	Se garantiza la aplicación de las políticas de gestión de activos
CPA5	Se realiza un seguimiento de los cambios poco frecuentes en activos y configuraciones
CPA6	Siguen algunas reglas específicas para gestionar posibles cambios en el sistema
CPA8	Se regula el proceso para el ciclo de vida de los activos, desde el aprovisionamiento hasta la sustitución, incluidos los cambios de emergencia

CPA9	Se limita el acceso a activos físicos
CPA10	Definen las restricciones de acceso en cuanto a horarios permitidos
CPA12	Automatiza el control de acceso físico utilizando tokens de identidad específicos
CPA13	Se garantiza un funcionamiento seguro de los controles de acceso físico
CPA15	Se implementan políticas y métodos para la protección de datos
CPA16	Se ofrece garantía de la protección de la información comercial crítica en tránsito
CPA18	Define el enfoque y los roles/atributos particulares para controlar el acceso a los datos
CPA19	Se aprovechan los controles de protección integrados (SO, red, servicios)
LG7	El alcance de una misión MILCYBDEC debe estar limitado y bien definido.

LG9	El personal aliado , según nivel de habilitación de seguridad, debe , o no debe, ser consciente de los procesos/activos que componen la misión MILCYBDEC
LG10	La misión de MILCYBDEC debe proveer contramedidas proporcionales a los ataques
LG11	La misión de MILCYBDEC debe tener capacidad de medir la ciber-agresión entrante, a fin de poder equipararla con un ataque cinético (equivalente, y poder, en un futuro, si necesario lanzar una reciprocación proporcional (reciprocidad y proporcionalidad a los ataques)
LG12	La misión de MILCYBDEC debe tener unos objetivos bien definidos.
LG13	La misión de MILCYBDEC debe poder proveer contramedidas de alcance medible de cara a los ataques
LG14	La misión de MILCYBDEC debe poder proveer contramedidas de efectos medibles de cara a los ataques
LG15	La misión de MILCYBDEC tiene que tener procesos/activos en el Espacio Exterior, si dicho dominio afecta a la Misión
LG16	La misión MILCYBDEC debe prever distintos niveles de activación (i.e. nivel de alerta)
LG17	La misión MILCYBDEC debe satisfacer el Principio de Distinción, i.e tener capacidades de reconocer si los objetivos de MILCYBDEC son civiles o militares

LG18	La misión MILCYBDEC garantiza la soberanía física del país y/o las fuerzas aliadas
LG19	La misión MILCYBDEC no debe dañar el entorno natural.
LG20	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de los menores de edad
LG21	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de prisioneros de guerra
LG22	La misión MILCYBDEC no debe interferir con Sistemas de Países Aliados.
LG23	La misión MILCYBDEC no debe interferir con Sistemas de Países Hostiles (adversarios), (aunque sí puede dificultar operaciones extranjeras no pacificas)
LG24	La misión MILCYBDEC no debe interferir con Sistemas de Países Neutrales
LG25	La misión MILCYBDEC sólo debe ser activada cuando sea necesario
LG26	La misión no debe provocar acciones ofensivas transfronterizas

LG27	La misión no debe realizar acciones ofensivas transfronterizas
LG28	Las infraestructuras de MILCYBDEC deben ser capaces de detectar los ataques entrantes de fuerzas/países hostiles y alertar a las autoridades competentes , p.e. el Concejo de Seguridad de Naciones Unidas
LG29	Las medidas de MILCYBDEC no deben contravenir los acuerdos internacionales firmados por el País. (p.e. convención de Ginebra, Canadá, Viena)
LG30	Los dominios de batalla afectados por una misión MILCYBDEC deben estar bien definidos
LG31	Los procesos/activos de MILCYBDEC no deben activar fuegos, o en todo caso, si activan fuegos, deben ser fuegos simulados y/o con carga simulada
LG32	Los procesos/activos de MILCYBDEC no deben amenazar con respuesta activa, ya sea cibernética o cinética, en caso de que dicha respuesta no se ajuste a los principios de guerra justa.
LG33	Los procesos/activos de MILCYBDEC no deben causar interferencias dañinas en el ciberespacio
LG34	Los procesos/activos de MILCYBDEC no deben causar interferencias dañinas en el espectro electromagnético
LG35	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de naves aéreas

LG36	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de naves civiles
LG37	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de vehículos terrestres civiles
LG38	Los procesos/activos de MILCYBDEC no deben realizar actos de Perfidia (p.e. hacerse pasar por objetivos civiles, o de primeros auxilios, p.e.)
LG39	Los procesos/activos de MILCYBDEC no deben tener almacenada información secreta verdadera
LG40	Los procesos/activos MILCYBDEC, si son elementos que soportan tráfico de red internacional, deben dar paso libre a dicho tráfico (mientras el origen y el destino sean externos al País)
LG41	Los propietarios de activos y/o procesos de MILCYBDEC deben ser actores legítimos, i.e. autoridades estatales, militares y/o habilitadas para ejercer Ciberdefensa en el ámbito de la misión
LG42	Los sistemas de MILCYBDEC no deben identificarse, sin autorización previa, como actores internacionales, tales como Naciones Unidas (UN)
LG43	MILCYBDEC debe ser necesario y justificable.
LG44	MILCYBDEC debe ser proporcional a las amenazas de las que protege

LG45	MILCYBDEC no debe destruir y/o degradar rutas de datos internacionales, que se encuentren fuera del dominio geográfico y/o lógico de las redes del País
LG46	MILCYBDEC no puede los Derechos Humanos
LG47	MILCYBDEC no va en contra de la Leyes de la Guerra
LG48	Se deben poder lanzar contramedidas simuladas (con un payload inofensivo) en caso de detectar ataques a un Honeypot o Honeynet.
LG49	Según nivel de alerta, la misión MILCYBDEC no debería dirigirse hacia países aliados
LG50	Un proceso/activo de Ciberengaño debe ser 'visitable', i.e. debe poder ser inspeccionado por las autoridades del País.
	En la misión MILCYBDEC, hay establecidas redundancias de redes, almacenamiento y procesamiento en el territorio del País
	Hay establecidas redundancias de redes, almacenamiento y procesamiento dentro de países aliados
GIR2	Se garantiza la recuperación de componentes o procesos del sistema separados

GIR3	Existe un procedimiento de recuperación automática Se generan informes descriptivos sobre los incidentes y sus soluciones Respuesta rápida a incidentes y reducción del daño al negocio tanto por medios técnicos como organizativos
GIR4	Define incidentes específicos y acciones básicas para reaccionar
GIR5	Proporciona orientación para componentes críticos sobre cómo detectar y responder a incidentes
GIR6	Establece la base para la ejecución automática de los procedimientos de respuesta
GIR7	Crear controles para detectar incidentes, asignarlos para la investigación y escalar según sea necesario
GIR8	Posee mecanismos para asignar incidentes para su investigación y escalar según sea necesario
GIR9	Se cuentan con procedimientos con instrucciones básicas para la recuperación del sistema
GIR10	Se manejan todos los incidentes que se detectan
GIR11	Se comprueba si el sistema está completamente recuperado luego de un incidente

GIR12	Se poseen mecanismos para la ejecución automática de procedimientos de corrección y recuperación
GIR13	Se cuenta con una combinación de medidas técnicas y organizativas que faciliten la rápida recuperación del sistema
	La misión de MILCYBDEC debe proveer contramedidas inmediatas a los ataques
	La misión de MILCYBDEC debe poder proveer contramedidas directas de cara a los ataques
	Las infraestructuras de MILCYBDEC deben ser capaces de detectar los ataques entrantes y alertar al propietario de la infraestructura (real) subyacente.

Deficiencias Estonia

MCC3	Hay establecidas redundancias de redes, almacenamiento y procesamiento dentro de países aliados
MCC4	La misión MILCYBDEC garantiza la soberanía física del país y/o las fuerzas aliadas
MCC5	La misión MILCYBDEC debe definir claramente los cauces hacia los blancos.

MCC6	El guion de MILCYBDEC es creíble, verificable, consistente, implementable
MCC8	Se ha securizado la información de MILDEC, mediante compartimentalización
MCC9	Se ha securizado la información de MILDEC, mediante control de accesos e identidad
MCC10	La misión de MILCYBDEC tiene procesos dedicados a OPSEC
MCC11	La misión de MILCYBDEC dedica suficiente tiempo y plazo para desplegar el guion y para que el adversario se dé cuenta de él
MCC12	Las operaciones MILCYBDEC están plenamente integradas con otras Operaciones aliadas
MCC13	El concepto de MILCYBDEC debe desarrollarse a la vez que CONOPS para la misión principal.
MCC14	Se posee toda la cadena de suministros de activos/procesos MILCYBDEC
MCC15	La misión MILCYBDEC no debe interferir activamente con infraestructuras y servicios de países extranjeros (p.e. publicar 'fake news' en un estado extranjero, aunque sea parte hostil)
MCC16	La misión MILCYBDEC debe haber identificado las lagunas de información del adversario

MCC17	La misión de MILCYBDEC debe garantizar la inmediatez de reacción, a fin de mantener el 'Uptime' de los activos/procesos protegidos
MCC18	El alcance de una misión MILCYBDEC debe estar limitado y bien definido.
MCC19	La misión MILCYBDEC no debe interferir con otras misiones aliadas

CPA13	Se garantiza un funcionamiento seguro de los controles de acceso físico
LG9	El personal aliado , según nivel de habilitación de seguridad, debe , o no debe, ser consciente de los procesos/activos que componen la misión MILCYBDEC
LG10	La misión de MILCYBDEC debe proveer contramedidas proporcionales a los ataques
LG11	La misión de MILCYBDEC debe tener capacidad de medir la ciber-agresión entrante, a fin de poder equipararla con un ataque cinético (equivalente, y poder, en un futuro, si necesario lanzar una reciprocación proporcional (reciprocidad y proporcionalidad a los ataques)
LG12	La misión de MILCYBDEC debe tener unos objetivos bien definidos.

LG13	La misión de MILCYBDEC debe poder proveer contramedidas de alcance medible de cara a los ataques
LG14	La misión de MILCYBDEC debe poder proveer contramedidas de efectos medibles de cara a los ataques
LG15	La misión de MILCYBDEC tiene que tener procesos/activos en el Espacio Exterior, si dicho dominio afecta a la Misión
LG19	La misión MILCYBDEC no debe dañar el entorno natural.
LG20	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de los menores de edad
LG21	La misión MILCYBDEC no debe interferir con derechos tales como los de los derechos de prisioneros de guerra
LG23	La misión MILCYBDEC no debe interferir con Sistemas de Países Hostiles (adversarios), (aunque sí puede dificultar operaciones extranjeras no pacificas)
LG24	La misión MILCYBDEC no debe interferir con Sistemas de Países Neutrales
LG25	La misión MILCYBDEC sólo debe ser activada cuando sea necesario

LG28	Las infraestructuras de MILCYBDEC deben ser capaces de detectar los ataques entrantes de fuerzas/países hostiles y alertar a las autoridades competentes , p.e. el Concejo de Seguridad de Naciones Unidas
LG30	Los dominios de batalla afectados por una misión MILCYBDEC deben estar bien definidos
LG31	Los procesos/activos de MILCYBDEC no deben activar fuegos, o en todo caso, si activan fuegos, deben ser fuegos simulados y/o con carga simulada
LG32	Los procesos/activos de MILCYBDEC no deben amenazar con respuesta activa, ya sea cibernética o cinética, en caso de que dicha respuesta no se ajuste a los principios de guerra justa.
LG37	Los procesos/activos de MILCYBDEC no deben dificultar la navegación de vehículos terrestres civiles
LG38	Los procesos/activos de MILCYBDEC no deben realizar actos de Perfidia (p.e. hacerse pasar por objetivos civiles, o de primeros auxilios, p.e.)
LG39	Los procesos/activos de MILCYBDEC no deben tener almacenada información secreta verdadera
LG40	Los procesos/activos MILCYBDEC, si son elementos que soportan tráfico de red internacional, deben dar paso libre a dicho tráfico (mientras el origen y el destino sean externos al País)
LG41	Los propietarios de activos y/o procesos de MILCYBDEC deben ser actores legítimos, i.e. autoridades estatales, militares y/o habilitadas para ejercer Ciberdefensa en el ámbito de la misión

LG42	Los sistemas de MILCYBDEC no deben identificarse, sin autorización previa, como actores internacionales, tales como Naciones Unidas (UN)
LG43	MILCYBDEC debe ser necesario y justificable.
LG44	MILCYBDEC debe ser proporcional a las amenazas de las que protege
LG46	MILCYBDEC no puede los Derechos Humanos
LG47	MILCYBDEC no va en contra de la Leyes de la Guerra
LG48	Se deben poder lanzar contramedidas simuladas (con un payload inofensivo) en caso de detectar ataques a un Honeypot o Honeynet.
LG49	Según nivel de alerta, la misión MILCYBDEC no debería dirigirse hacia países aliados
La misión de MILCYBDEC debe proveer contramedidas inmediatas a los ataques	
La misión de MILCYBDEC debe poder proveer contramedidas directas de cara a los ataques	