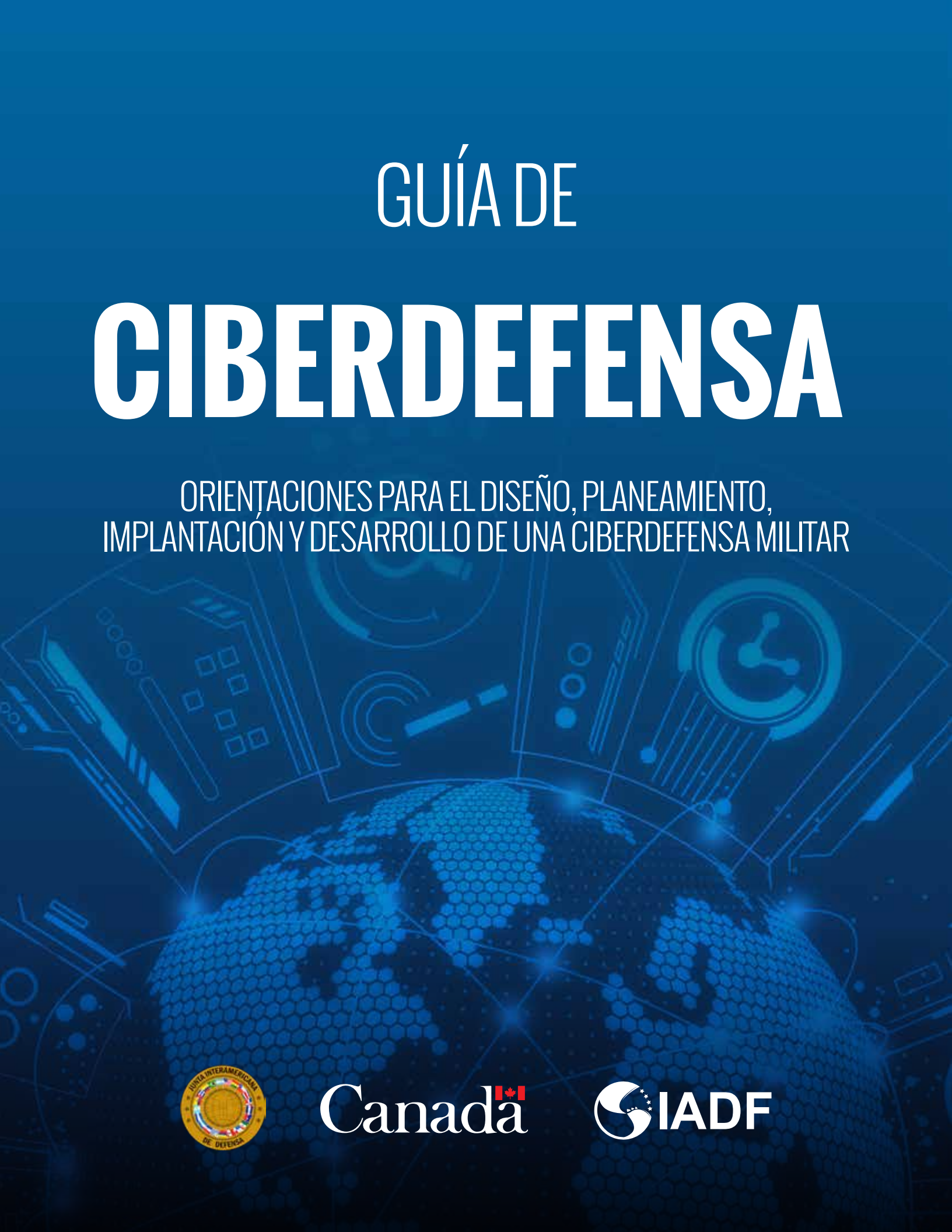
GUÍA DE

CIBERDEFENSA

ORIENTACIONES PARA EL DISEÑO, PLANEAMIENTO, IMPLANTACIÓN Y DESARROLLO DE UNA CIBERDEFENSA MILITAR



JUNTA INTERAMERICANA DE DEFENSA

Canadá

IADF

JUNTA INTERAMERICANA DE DEFENSA

General de División Luciano José Penna
Presidente del Consejo de Delegados

General de Brigada Juan José Gómez Ruiz
Director General de la Secretaría

Coordinación del Proyecto

Isabel Niewola
Directora del Programa de Ciberdefensa de la JID

Autor principal

Néstor Ganuza

Equipo Técnico JID

Gonzalo García-Belenguer
Jossele Monroy
Miguel Rego

ESTE PROGRAMA Y PUBLICACIÓN ES FINANCIADO POR EL GOBIERNO DE

Canada

CONTENIDO

ILUSTRACIONES

PRÓLOGO

Una significativa cooperación regional e internacional ha surgido en torno a la ciberseguridad entre los gobiernos de las Américas durante la última década, sin embargo, gran parte del progreso se ha centrado principalmente en las instituciones civiles. En algunos países, donde las fuerzas armadas y fuerzas de seguridad desempeñan un papel fundamental en la ciberseguridad, el ejército ha participado activamente en el intercambio de información y mejores prácticas con los estados vecinos. Sin embargo, generalmente las fuerzas militares se han mantenido fuera del creciente marco de colaboración regional que ha evolucionado en torno a la ciberseguridad y el cibercrimen en el Hemisferio Occidental.

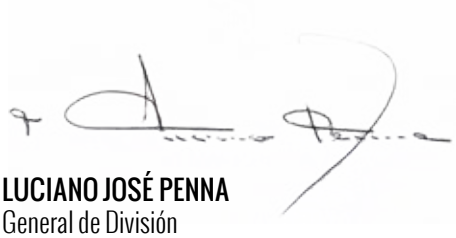
La Junta Interamericana de Defensa (JID), apoyada por la Fundación Interamericana de Defensa (FID), ha recibido ciertos mandatos por parte de la Organización de Estados Americanos (OEA) respecto a ciberdefensa, por lo que hemos dado los primeros pasos para generar progresos significativos con la intención de facilitar la comunicación y la colaboración en ciberdefensa entre la fuerzas armadas y de seguridad del Hemisferio Occidental.

Al ser la organización que encabeza los asuntos militares y de defensa en las Américas, la JID cuenta con la coyuntura ideal para impactar de manera significativa políticas y estrategias, así como, facilitar una mayor cooperación regional. La JID tiene una posición única para reunir a los tomadores de decisiones tanto militares como civiles de América Latina y el Caribe, con la finalidad de mejorar el papel de las instituciones militares y de defensa en el aumento de la ciberseguridad, así como, para mejorar la capacitación y el intercambio de información.

Con el apoyo del Gobierno de Canadá, la JID ha lanzado el Programa de Ciberdefensa, el cual apoya a los 29 países miembros con actividades y ejercicios enfocados a la generación y desarrollo de capacidades individuales y colectivas de ciberdefensa, con la finalidad de fortalecer las políticas y capacidad del Hemisferio a gran velocidad y escala. El Programa de Ciberdefensa de la JID, trabaja con socios tanto regionales como globales con la finalidad de complementar y mejorar las iniciativas existentes, sumando a los esfuerzos en lugar de duplicarlos.

Esta Guía de Ciberdefensa, proporcionará un conjunto de principios para la planificación, diseño, desarrollo y despliegue de capacidades de ciberdefensa. Los militares tienen un interés directo y apremiante en reforzar sus capacidades individuales y colectivas de ciberdefensa para garantizar la seguridad de sistemas militares específicos, infraestructura e información, así como, contribuir en asegurar los más altos intereses nacionales contra las crecientes ciberamenazas.

Finalmente, el Programa de Ciberdefensa de la JID, servirá para apoyar las conversaciones multilaterales, bilaterales y nacionales de ciberdefensa en el Hemisferio Occidental, así como, informar la estrategia y toma de decisiones. La ciberdefensa representa la mayor amenaza y oportunidad compartida para la cooperación en el Hemisferio Occidental, y la JID continuará actuando como un catalizador para fortalecer las relaciones, promover los intereses multilaterales, compartir las mejores prácticas y aprender de los aliados y socios.



LUCIANO JOSÉ PENNA
General de División
Presidente del Consejo de Delegados de la
Junta Interamericana de Defensa.

El ciberespacio ya no es un dominio "emergente", sino un potencial teatro de guerra en el que todas las naciones soberanas podrían participar de manera activa y diaria. En todo el mundo, los actores gubernamentales y no gubernamentales han desarrollado capacidades cibernéticas, tanto ofensivas como defensivas, que han desencadenado una reexaminación de las nociones tradicionales del poder global, la influencia e incluso la guerra.

Hoy en día, existe una dependencia a nivel global de las computadoras y las redes fácilmente disponibles para la mayoría de los aspectos gubernamentales, financieros, comerciales, industriales, así como, para el mando y el control de las operaciones militares - una dependencia que ha generado grandes oportunidades y riesgos significativos.

Las ciberamenazas a la seguridad del Hemisferio Occidental son cada vez más frecuentes, complejas, destructivas y coercitivas. Tenemos que adaptarnos al panorama de ciberamenazas que está en constante evolución. Las Américas requieren ciberdefensas fuertes y resilientes para cumplir tareas críticas como la defensa colectiva, la gestión de crisis y la seguridad cooperativa. Necesitamos estar preparados para defender nuestras redes y operaciones contra la creciente sofisticación de las amenazas y ciberataques que todos enfrentamos.

La ciberdefensa es fundamental para la conducción de las operaciones militares modernas. La infraestructura cibernética militar actual presenta posibles puntos únicos de falla para las operaciones, el entrenamiento y las actividades. La libertad de acción dentro y a través del ciberespacio depende de nuestra capacidad para proteger y defender contra acciones accidentales, maliciosas o adversarias.

La ciberseguridad es el fundamento para preservar la libertad de acción en el ciberespacio. Comprende la aplicación de medidas de seguridad para la protección de la comunicación, la información y otros sistemas electrónicos, así como, la información que se almacena, procesa o transmite en estos sistemas para salvaguardar la confidencialidad, la integridad y la disponibilidad. La buena ciberseguridad establece las condiciones para el comando operativo efectivo y el control de las fuerzas militares.

Dado que el ciberespacio no está limitado a un solo país, proteger nuestros intereses en el ciberespacio es un deporte de equipo. El desarrollar una defensa fuerte contra la actividad cibernética maliciosa requiere una voluntad colectiva para coordinar, colaborar y compartir las mejores prácticas en el desarrollo de las fuerzas cibernéticas y la ejecución de ciber operaciones.

Esta guía es un primer paso para avanzar en el desarrollo de las fuerzas cibernéticas nacionales capaces de operar en este nuevo entorno de manera individual y colectiva en defensa de nuestros objetivos comunes. Exhorto a todas las naciones participantes a revisar y considerar las recomendaciones de esta guía de cerca, esperando cooperar en el ciberespacio para asegurar un futuro próspero y seguro.

STEPHEN M. LACROIX
General de Brigada
Comandante, 3ra División Canadiense
y Fuerza Conjunta (Oeste)
Fuerzas Armadas Canadienses

Canada

INTRODUCCIÓN

La transformación continua de las fuerzas armadas para adaptarse a los escenarios estratégicos del momento es un elemento esencial de la política de defensa de las naciones. Esta transformación y adaptación es especialmente singular en los momentos históricos en los que se reconoce un nuevo ámbito de operaciones. Así ha venido ocurriendo, a lo largo de la historia, en aquellos hitos en los que a las fuerzas terrestres se les han ido añadiendo las fuerzas navales, aéreas, espaciales y ciberespaciales.

La transformación de las fuerzas armadas, para adaptarse al nuevo escenario estratégico actual que contempla el ciberespacio como el quinto ámbito de operaciones, está siendo llevada a cabo por las naciones de manera desigual. A nivel general, se considera que el desarrollo de las fuerzas ciberespaciales y el arte de su empleo (la ciberdefensa militar) se encuentra en un estado de madurez incipiente.

Esta guía tiene la finalidad de proporcionar orientaciones para llevar a cabo esta transformación y desarrollar una capacidad de ciberdefensa militar de una manera integral y organizada, a todos los niveles necesarios.

La guía proporciona un modelo operativo, considerando la ciberdefensa como un elemento componente de las operaciones militares conjuntas y por tanto orientado a la misión operativa y no cediendo a la habitual orientación hacia la seguridad de los sistemas de información y telecomunicaciones.

La guía hace un uso predominante de la terminología militar en vez de la habitual terminología técnica, reforzando así su entendimiento desde la perspectiva operativa militar y facilitando la integración de la ciberdefensa en la acción conjunta con otros ámbitos de operaciones.

El contenido de la guía se organiza en nueve unidades (el ciberespacio, el ámbito de operaciones, la ciberdefensa militar, la fuerza ciberespacial, la ciberamenaza, los principios doctrinales, el ecosistema ciberespacial, los aspectos legales y los estándares) que en su conjunto proporcionan una aproximación integral.

La unidad **"ciberespacio"** analiza el medio en donde se desarrollan las actividades de ciberdefensa, proporciona una representación práctica que facilita su comprensión, estudio y uso, y analiza la parte principal del ciberespacio (internet) incluyendo la internet más oculta.

La unidad **"ámbito de operaciones ciberespacial"** detalla todos aquellos elementos fundamentales de un ámbito de operaciones militares desde la perspectiva ciberespacial, remarcando sus peculiaridades y diferencias con los ámbitos de operaciones convencionales.

La unidad **"ciberdefensa militar"** aproxima la ciberdefensa al arte militar del empleo del ciberespacio y a las operaciones militares en el ciberespacio (ciberoperaciones), y propone una taxonomía que los diferentes tipos de ciberoperaciones.

La unidad **"fuerza ciberespacial"** detalla los aspectos a considerar en el proceso de desarrollo de la fuerza militar responsable del planeamiento y la conducción de las operaciones militares en el ciberespacio y las capacidades básicas que debe tener para llevar a cabo sus cometidos con un mínimo de garantía.

La unidad **"ciberamenaza"** analiza las principales amenazas actuales y las tendencias, y en particular, la principal amenaza asociada a los estados, las amenazas avanzadas persistentes y el modo de combatirlas.

La unidad **"principios doctrinales"** analiza la aplicabilidad al ciberespacio de los principios tradicionales que guían la actuación de las fuerzas militares en las operaciones convencionales (principios fundamentales del arte militar y principios operativos).

La unidad **"ecosistema ciberespacial"** pone en contexto la ciberdefensa militar y analiza las relaciones con sus entornos naturales fundamentales, la ciberseguridad nacional, la ciberseguridad internacional y el sector privado.

La unidad **"aspectos legales"** analiza la situación actual de consenso en la aplicación del derecho internacional a las ciberoperaciones, tanto en tiempo de paz como en periodos de conflicto, zona de operaciones o misiones de paz, y considera aquellos aspectos más relevantes para la ciberdefensa militar.

Finalmente, se detallan y valoran los estándares internacionales de referencia en materia de ciberseguridad.

Para una mayor claridad se incorpora a la guía un convenio de uso del lenguaje especifico del entorno ciberespacial y las definiciones de los términos más relevantes usados en la guía, así como los acrónimos.

CONSENSO EN EL LENGUAJE

Muchos términos relacionados con el dominio "ciber" y el propio término y concepto "ciber" son actualmente controvertidos. No existe un único glosario de definiciones ni una taxonomía globalmente aceptada y como consecuencia, la mayoría de estudios relacionados con el ciberespacio y sus aplicaciones se ven en la obligación de incluir sus propios listados de definiciones.

Esta falta de consenso global de todo lo relacionado con el dominio ciber trae como consecuencia importantes disfunciones:

a Falta de una percepción global común.

La carencia de una percepción global común sobre el dominio "ciber" deriva en diferentes visiones y perspectivas en el análisis y estudio del ciberespacio y, en particular, de las operaciones militares en el ciberespacio, desarrollándose doctrinas, definiciones y taxonomías con diferentes enfoques y en algunos casos de difícil compatibilidad.

b Difícil comprensión del dominio ciber.

La información confusa y, a veces contradictoria, existente acerca de todo lo relacionado con el dominio "ciber" dificulta la labor de las autoridades y directivos en el proceso de toma de decisiones en asuntos relacionados con la ciberdefensa, produciéndose, en muchos casos, resoluciones no idóneas o no adaptadas a la necesidad real.

c Estructuras organizativas diferentes.

La falta de un consenso global repercute en una visión diferente en la forma de organizar las estructuras nacionales de ciberdefensa y consecuentemente dificulta la colaboración nacional e internacional tan necesaria en el ámbito de la ciberdefensa. Mientras algunas naciones han optado por crear mandos componentes específicos subordinados al estado mayor de la defensa otras han optado por crear un servicio propio del ministerio de defensa, otras por la creación de una unidad que lleva conjuntamente la ciberdefensa y los servicios de telecomunicaciones y otras por unidades subordinadas a los servicios de inteligencia.

d Conflicto de responsabilidades.

Diferentes definiciones y taxonomías derivan en conflictos en la asignación de tareas generando dos casos preocupantes: tareas que se quedan sin hacer por no tener especificadas un responsable de manera clara y precisa, y tareas en disputa entre diferentes organizaciones generando conflictos y duplicación de esfuerzos y cómo resultado falta de eficacia y eficiencia.

Por todo ello, es importante llegar a un consenso global en las definiciones de los términos más relevantes relacionados con el entorno del ciberespacio y, en particular, en sus rasgos como ámbito de operaciones.

Además, se necesita un consenso en la forma de escribir los términos relacionados con la ciberdefensa. Actualmente, se dan predominantemente tres casos: uso de la palabra "ciber" o "cibernético" como un adjetivo (ciber arma, arma ciber, arma cibernética), como un prefijo con guion (ciber-arma) o con prefijo sin guion (ciberarma).

Actualmente, se observa la tendencia de usar un número muy reducido de términos con el prefijo "ciber- "(ciberespacio, ciberdefensa, ciberataque) dejando el resto de términos al arbitrio voluntario de cada cual, pudiéndose encontrar los diferentes tipos mencionados (ciberarma, ciber arma, ciber-arma, arma ciber o arma cibernética).

La Real Academia Española (RAE), en su diccionario, contempla un cierto número de términos con prefijo, como ciberarte, ciberartista, cibercafé, cibercultura, ciberespacial, ciberespacio, cibernauta, cibernética, etc. y contempla el prefijo "ciber- "como un elemento compositivo que indica relación con la informática. Cualquier forma sería aceptable, pero es recomendable alcanzar un consenso lo más global posible en el uso de una única forma para todos los términos.

Esta guía adopta el criterio de usar el prefijo **ciber-** (ciberespacio, ciberdefensa, ciberamenaza, ciberarma, ciber terreno clave) de acuerdo a las normas de escritura de los prefijos de la RAE[1], o el adjetivo **ciberespacial** (fuerza ciberespacial, ecosistema ciberespacial) con el significado de **pertenencia o relación con el ciberespacio.**

DEFINICIONES

A los efectos de esta guía se definen los siguientes términos:

Ámbito de operaciones	Entorno de interés e influencia en el que se llevan a cabo actividades, funciones y operaciones para cumplir la misión y ejercer control sobre un oponente con el fin de lograr los efectos deseado. (NATO Bi-SC Initial Assessment of Recognising Cyberspace as a Domain)
Amenaza Persistente Avanzada (APT)	Grupo organizado de expertos, normalmente asociado a un estado, que utiliza sofisticados conocimientos, herramientas y TTPs (técnicas, tácticas y procedimientos) para (de manera anónima, sigilosa y desapercibida) infiltrarse, tomar el control y perpetuarse en una red ajena, con el objeto de tener acceso a la información de su interés y obtener ventajas estratégicas.
Campo de maniobras ciberespacial	Zona restringida del ciberespacio que se usa para entrenar a las unidades de ciberdefensa y practicar ciberoperaciones reales en un entorno seguro y aislado que garantice la inocuidad del ciberespacio.
Caza de ciberamenazas	Proceso dinámico y proactivo de ciberdefensa orientado a la detección y aislamiento de amenazas avanzadas que evaden las soluciones de seguridad tradicionales basadas en SIEM y dispositivos de ciberseguridad perimetral (firewalls, IDS, IPS, sandboxing, etc.).
Ciber-	Prefijo que indica relación con el ciberespacio.
Ciber Terreno Clave (CTC)	Conjunto de elementos del ciberespacio, en cualquiera de sus capas (humana, ciberhumana, cognitiva, lógica, TIC y geográfica) que facilitan las actividades, operaciones o funciones esenciales para la misión y cuya destrucción, interrupción o captura generaría una ventaja operativa para el adversario.
Ciberactivismo	Uso del ciberespacio para desarrollar actividades de desobediencia civil, propaganda o proselitismo para promover un cambio político o social.
Ciberamenaza	Fuente potencial de perjuicio, externa o interna, a algún activo de la organización que se materializa a través del ciberespacio.
Ciberarma	Software específicamente diseñado para causar un daño o efecto perjudicial a un elemento del ciberespacio pudiendo tener consecuencias físicas en los ámbitos de operaciones convencionales.
Ciberataque	Uso deliberado de una ciberarma, por una persona o de manera automática, para causar un daño o efecto perjudicial a un elemento del ciberespacio de un adversario pudiendo tener efectos indirectos en los ámbitos de operaciones convencionales.
Cibercontrol	Grado de dominio del ciberespacio de confrontación de una ciberfuerza sobre la ciberfuerza adversaria.
Ciberdefensa	Capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia.
Ciberespacio	Entorno conceptual en el que se produce la comunicación a través de redes informáticas (Oxford Dictionary).
Ciberfuerza	1. Unidad militar especializada en el combate en el ciberespacio. 2. Capacidad para desarrollar acciones ofensivas en el ciberespacio.

Ciberoperación	Conjunto de acciones militares planificadas, organizadas, coordinadas y llevadas a cabo por unidades de ciberdefensa con la finalidad de lograr efectos en el ciberespacio, así como en los otros ámbitos de operaciones.
Ciberpersona	Identidad que un usuario del ciberespacio establece en comunidades o actividades online.
Ciberriesgo	Probabilidad de que una ciberamenaza aproveche una vulnerabilidad para causar un daño a un activo que tiene un valor y una criticidad determinada.
Ciberseguridad	Conjunto organizado de medidas destinadas a prevenir, evitar y minimizar potenciales daños a redes y sistemas de información propios.
Conciencia Situacional Ciberespacial	Representación de los elementos y eventos del ciberespacio, en un tiempo, lugar y misión determinados, la explicación de su significado y la proyección de su estado futuro.
Ecosistema ciberespacial	Sistema compuesto por todos los elementos que se relacionan entre sí a través del ciberespacio, junto con el propio ciberespacio.
Fuerza ciberespacial	Conjunto de unidades de ciberdefensa de las fuerzas armadas agrupadas bajo un mismo mando.
Sistema de armas ciberespacial	Sistema que integra diferentes ciberarmas, funciones de mando y control y todos los apoyos técnicos necesarios para desarrollar una ciberoperación ofensiva, defensiva o de explotación con un objetivo concreto, estratégico, operacional o táctico.

CIBERESPACIO

001. El *ciberespacio* es el ámbito conceptual en donde se desarrollan las actividades de ciberdefensa, por ello es de vital importancia tener una idea clara y precisa de su naturaleza y peculiaridades.

002. Se adopta la *definición* del diccionario Oxford, *"El entorno conceptual en el que se produce la comunicación a través de redes informáticas."*, debido a que se adapta perfectamente al espíritu del contenido de esta guía.

003. El ciberespacio es un concepto, idea o noción; no es un espacio material, físico, visible ni tangible. Dado que el ciberespacio es una noción, ningún elemento físico o tangible es parte intrínseca de él (infraestructura TIC, personas), tampoco los elementos no tangibles como la información, el software o la energía eléctrica.

004. El concepto "ciberespacio" se materializa gracias a la interrelación de unos *elementos* específicos (*la infraestructura de tecnologías de información y comunicaciones, el software, la información, los protocolos de transporte, la energía eléctrica y las personas*) proporcionándole vitalidad.

005. El conjunto de los elementos, el ciberespacio y sus relaciones conforman el *ecosistema ciberespacial* (párr. 524). En la práctica, se utiliza el término ciberespacio incluyendo los elementos y sus relaciones, asimilándolo al término ecosistema ciberespacial.

ILUSTRACIÓN 1. INTERACCIÓN EN EL CIBERESPACIO

006. Se tiende a identificar al ciberespacio con la *infraestructura de las tecnologías de la información y las telecomunicaciones* (ordenadores, servidores, cableado, todo tipo de dispositivos y material hardware), de esta manera parece más entendible; pero esta identificación ciberespacio-TIC, conlleva el gran peligro de desviar la verdadera finalidad de la ciberdefensa.

007. La *confusión ciberespacio-TIC* es una fuente de conflictos entre las unidades operativas de ciberdefensa, encargadas de planear y conducir operaciones militares en el ciberespacio y las unidades TIC, encargadas de proveer el servicio de telecomunicaciones transversal a todos los ámbitos.

008. La *información* no es una parte intrínseca del ciberespacio, sin embargo, el ciberespacio es un entorno ideal para manejarla (crear, presentar, procesar, almacenar, transportar, compartir y eliminar); pero no es el único entorno donde se puede manejar la información.

009. Las *personas,* individualmente o en todas las formas de grupos organizados (estados, individuos, organizaciones o grupos internacionales o nacionales) no son parte intrínseca del ciberespacio, como no lo son en ningún otro ámbito (tierra, aire, mar, espacio). Las personas crean y modifican el ciberespacio; realizan actividades, funciones y operaciones en el ciberespacio; pero no son parte del ciberespacio.

010. Finalmente, es importante mencionar dos elementos que mantienen vivo el ciberespacio: *software* y *energía eléctrica*. Estos son los dos elementos básicos para mantener los signos vitales del ciberespacio.

011. De una manera práctica, podemos considerar que el ciberespacio está compuesto por dos partes principales: *internet y sistemas aislados* (redes, sistemas y dispositivos de almacenamiento de información no conectados a internet).

012. En el mundo militar las dos partes del ciberespacio (internet y sistemas aislados) son de gran importancia: internet nos proporciona una conectividad global y un acceso masivo a la información; mientras que los sistemas aislados nos proporcionan un entorno eficaz para manejar información clasificada y para realizar actividades que precisan de un alto grado de confidencialidad y aislamiento.

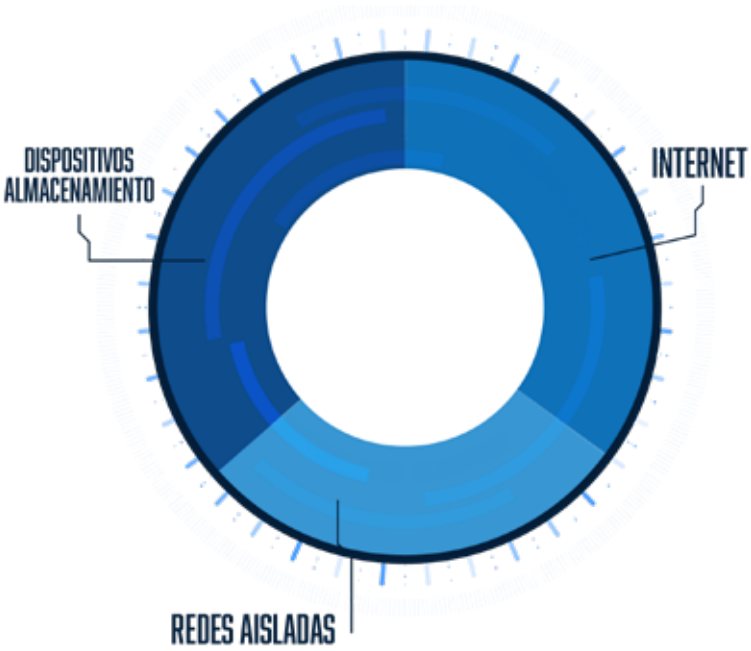


ILUSTRACIÓN 2. CIBERESPACIO. VISIÓN PRÁCTICA

013. Estas dos características, conectividad global y aislamiento, no son privativas de cada una de las partes del ciberespacio. Ya que también se pueden crear entornos confidenciales y aislados en internet y se pueden crear redes aisladas con una conectividad grande; pero no son los entornos naturales.

014. Las dos partes (internet y sistemas aislados) son fundamentales en la ciberdefensa nacional, ya que la conectividad global es imprescindible para un acceso extenso a la información y para la cooperación nacional e internacional y el aislamiento y la confidencialidad son fundamentales en aquellas actividades relacionadas con las operaciones y la investigación y desarrollo.

Capas del ciberespacio

015. Desde un punto de vista práctico y operativo, es de gran ayuda agrupar los elementos que interaccionan en el ciberespacio en diferentes capas *(humana, ciberhumana, cognitiva, lógica, TIC y geográfica)* para facilitar la asignación, organización y distribución de actividades, funciones, servicios y responsabilidades.

ILUSTRACIÓN 3. CAPAS DEL CIBERESPACIO

016. En cada una de estas capas se generan diferentes actividades que se relacionan con unos medios, procesos y cualificación profesional específica.

017. La representación por capas del ciberespacio sigue un proceso lógico en donde las personas generan conocimiento que se procesa en sistemas de información que funcionan a través de redes de telecomunicaciones emplazadas en lugares concretos del terreno.

018. La *capa humana* está compuesta por todas las personas físicas que desarrollan su actividad en el ciberespacio

019. La *capa ciberhumana* está formada por las ciberpersonas o identidades online (identidad que un usuario del ciberespacio establece en comunidades o actividades online). Las personas y las ciberpersonas pueden coincidir o no.

020. La *capa cognitiva* está compuesta por el conocimiento como resultado de la interacción de las personas con los sistemas de información y por el conocimiento específico del ciberespacio y sus actividades reflejadas en doctrina, normas, estándares, procedimientos, guías, etc.

021. En el ciberespacio como ámbito de operaciones, la *conciencia de la situación ciberespacial* (Cyber Situational Awareness, CSA) es un elemento fundamental de esta capa.

022. La *capa lógica* está compuesta fundamentalmente por los sistemas de información; entendiendo sistema de información como un conjunto de recursos lógicos de computación que facilitan el procesado de información con un fin específico (logístico, mando y control, manejo de armas, financiero, recursos humanos, etc.)

023. En la capa lógica se asignan identidades digitales que es la información utilizada por los sistemas de información para representar a una entidad. Esta entidad puede ser una persona, organización, aplicación o dispositivo.

024. La *capa TIC* está compuesta por todos los dispositivos físicos de red que permiten el transporte de datos. Hardware, software de sistemas, redes cableadas o inalámbricas, dispositivos electrónicos de interconexión, conectores, servidores, ordenadores, dispositivos periféricos, dispositivos de seguridad perimetral, etc.

025. La *capa geográfica* está compuesta por las zonas físicas correspondiente a los ámbitos de operaciones convencionales (tierra, mar, aire y espacio) en donde se ubican la infraestructura TIC y las personas que soportan el ciberespacio.

Internet

026. *Internet* es una red de redes, abierta e independiente, que opera en todo el mundo y que está dirigida por organizaciones sin ánimo de lucro (proveedores de servicios, compañías individuales, universidades, gobiernos y otras personas) que trabajan juntas para cubrir sus necesidades.

027. Físicamente, utiliza una parte de los recursos totales de las redes públicas de telecomunicaciones actualmente existentes.

028. Técnicamente, funciona mediante dos protocolos fundamentales (TCP Protocolo de Control de Transmisión / IP Protocolo de Internet).

029. Internet es la parte fundamental del ciberespacio. En toda operación militar en el ciberespacio es fundamental identificar los puntos críticos de Internet que puedan afectar al desarrollo de la misión; en particular, los proveedores de servicio de internet (ISP) y los puntos de intercambio de internet (IXP) también denominados puntos neutros.

030. Los *proveedores de servicio de Internet (ISP)* son organizaciones comerciales (en muchos casos son los propios operadores de telecomunicaciones) con conexión permanente a Internet que venden conexiones temporales a clientes.

031. Los *puntos de intercambio de Internet (IXP)* o puntos neutros son infraestructuras físicas a través de la cuales los proveedores de servicios de Internet (ISP) intercambian tráfico de Internet entre sus redes.

032. La interconexión en internet se realiza a través de una estructura jerarquizada en tres niveles o tiers.

033. En el nivel superior *(nivel 1)* hay un número relativamente pequeño de ISPs de nivel 1 que se conectan directamente a cada uno de los demás ISP de nivel 1 y a un gran número de ISP de nivel 2.

034. Cualquier ISP de nivel 1 tiene una cobertura global; es decir, puede llegar a cualquier punto de internet en el mundo sin necesidad de pagar ninguna tarifa por el intercambio de tráfico.

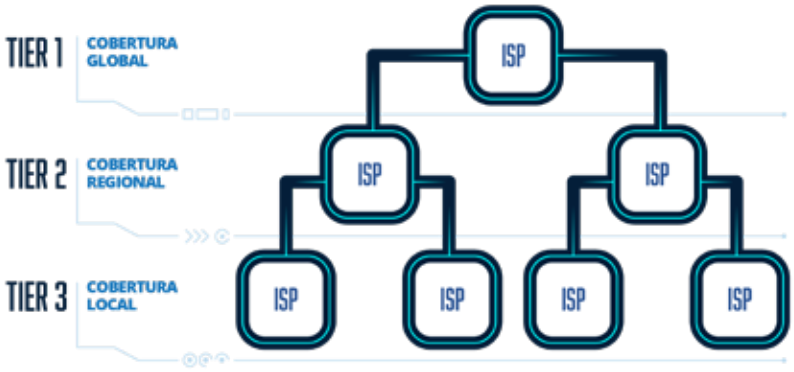


ILUSTRACIÓN 4. JERARQUÍA EN INTERNET

035. Un ISP de *nivel 2* tiene, normalmente, una cobertura regional o nacional, se conecta a sólo a unos pocos ISP de nivel 1 y en algunos casos tienen que pagar una tarifa por el intercambio de tráfico.

036. Los ISP de *nivel 3* tienen una cobertura limitada y se conectan a través de los ISP de nivel 2 y todos deben pagar para transmitir el tráfico en otras redes.

037. Internet es un *sistema distribuido* y por ello no existe un único poder político que pueda causar un impacto significativo a toda la red global de internet. No obstante, el riesgo de que un país pueda quedar desconectado de internet es real. De hecho, existen países que han desarrollado sistemas que permiten aislar la internet de su país de los servidores mundiales y garantizar así su funcionamiento, incluso en caso de conflicto ciberespacial internacional.

038. La *desconexión de un país de internet* es un riesgo potencial estratégico con graves consecuencias. Debido al fenómeno de la globalización, la mayoría de servicios de una nación dependen de conexiones externas, por ello, aun en el caso de existir conectividad total nacional, un aislamiento de internet tendría repercusiones internas graves.

039. El grado de riesgo de que un país pueda quedar aislado de internet depende directamente de la cantidad, robustez y resiliencia de los puntos nacionales de conexión (ISP e IXP).

040. El número de ISP de nivel 1 y de IXP por cada país es muy reducido y por ello son un activo crítico para la ciberdefensa nacional.

041. Además de disponer de un numero de ISP e IXP suficientemente alto para evitar el riesgo de aislamiento, la infraestructura ISP/IXP debe estar bajo el control de diferentes entidades, públicas y privadas, pues el gobierno descentralizado de internet es su mayor robustez.

ILUSTRACIÓN 5. MAPA COBERTURA IXP (TELEGEOGRAPHY)

042. La *internet oculta* (deep web), también llamada internet profunda o internet invisible, es una colección de sitios web y bases de datos que un buscador común (Google, Yahoo, Bing) no puede indexar y por lo tanto es un terreno idóneo para realizar transacciones y actividades sin dejar rastro.

043. A diferencia de la internet convencional o internet superficial la información y el tráfico que corre por la red no puede ser encontrado ni observado libremente por los usuarios. En la práctica, la internet oculta es un conjunto de comunidades cerradas en donde el acceso está restringido a los miembros autorizados de la comunidad. Las comunidades pueden tener intereses lícitos, como comunidades científicas, académicas o gubernamentales o pueden ser de naturaleza maliciosa o delictiva vinculadas a organizaciones criminales.

044. La internet oculta se caracteriza por el anonimato, usando navegadores específicos como TOR (The Onion Router). Nada que se haga en la internet oculta puede ser rastreado o asociado con la identidad del originador, a menos que lo desee.

045. La internet oculta es una parte de internet que debe ser considerada en la ciberdefensa, tanto para la protección frente a actividades maliciosas, como para desempeñar actividades legítimas que por su carácter confidencial o por su potencial peligrosidad precisen un entorno aislado.

ÁMBITO DE OPERACIONES CIBERESPACIAL

046. En la cumbre de la OTAN de Varsovia de 2016, la OTAN reconoce el ciberespacio como otro *ámbito de operaciones*. En concreto, en el punto 70 del comunicado declara: *"ahora, en Varsovia, reafirmamos el mandato defensivo de la OTAN y reconocemos el ciberespacio como un dominio de operaciones en el que la OTAN debe defenderse tan efectivamente como lo hace en el aire, en tierra y en el mar. Esto mejorará la capacidad de la OTAN para proteger y realizar operaciones en estos dominios y mantener nuestra libertad de acción y decisión, en todas las circunstancias. Apoyará la disuasión y defensa más amplias de la OTAN: la ciberdefensa continuará integrada en la planificación operativa y las operaciones y misiones de la Alianza, y trabajaremos juntos para contribuir a su éxito."*

047. La OTAN, en realidad, no hizo más que constatar un hecho, el ciberespacio está siendo usado por fuerzas armadas de muchos países como otra capacidad más en manos del comandante de una operación para generar efectos en el adversario.

Ámbito de operaciones

048. Un *ámbito de operaciones* es el entorno de interés e influencia en el que se llevan a cabo actividades, funciones y operaciones para cumplir la misión y ejercer control sobre un oponente con el fin de lograr los efectos deseado[2].

049. Para que un determinado entorno sea considerado un ámbito de operaciones debe reunir seis *criterios*:
1. Requiere capacidades únicas para operar en ese ámbito.
2. No está totalmente abarcado por ningún otro ámbito (tierra, mar, aire, espacio).
3. Se caracteriza por una presencia compartida de capacidades aliadas y adversarias.
4. Es capaz de ejercer control sobre un oponente a través de la influencia y el dominio.
5. Brinda oportunidades de sinergia con otros ámbitos.
6. Proporciona oportunidades asimétricas entre todos los ámbitos.

050. El ciberespacio reúne, de manera indubitada, los seis criterios y por consiguiente es considerado un ámbito de operaciones.

051. El ciberespacio, en su faceta de ámbito de operaciones, es un entorno en donde se conducen operaciones militares específicas (ciberoperaciones, párr. 206) que pueden producir ciberefectos (párr. 145) directos y efectos físicos indirectos en los ámbitos convencionales.

ILUSTRACIÓN 2. CIBERESPACIO COMO ÁMBITO DE OPERACIONES

052. Para producir los efectos deseados, la fuerza ciberespacial (párr. 221) propia debe disponer de un cierto grado de libertad de acción y poder ejercer un cierto control sobre el oponente (cibercontrol, párr. 168).

053. El fin último de las ciberoperaciones es que los ciberefectos apoyen el cumplimiento de la misión. Por lo tanto, las capacidades de ciberdefensa y sus potenciales efectos deben ser considerados en todo el ciclo de vida de planeamiento y conducción de las operaciones conjuntas.

Naturaleza del ciberespacio

054. El *ciberespacio* goza de unas singularidades *(artificialidad, imperceptibilidad, dinamismo, ubicuidad, inmediatez, transversalidad)* que lo diferencian de los otros ámbitos y por ello, requiere de unas capacidades específicas para operar en él.

055. El ciberespacio es un entorno *artificial*, creado por el hombre y, de la misma manera que lo ha creado, puede modificarlo a voluntad. De hecho, el ciberespacio va adquiriendo una nueva dimensión a medida que se van desarrollando nuevas tecnologías y servicios. Poco tiene que ver la internet original de la web y el correo electrónico a la actual de las redes sociales, las nubes y la internet de las cosas.

056. El ciberespacio es físicamente *imperceptible*, invisible e intangible; esto hace que sea más difícil de entender e interpretar que los ámbitos convencionales. Esta dificultad de comprensión genera una dificultad añadida a la hora de definir y desarrollar capacidades militares y procedimientos para operar en él.

057. El ciberespacio es un entorno *dinámico* y cambiante que obliga a una monitorización continua, a una actualización rápida de la conciencia de la situación ciberespacial (cyber situational awareness) y a una planificación flexible que admita cambios con facilidad.

058. El ciberespacio es *ubicuo* e inmediato. Una acción puede tener unos efectos casi inmediatos en cualquier parte del mundo. Esto, a diferencia de los otros ámbitos, hace que no sea necesario, en la mayoría de los casos, desplegar las unidades de ciberdefensa en los entornos geográficos donde se quiere generar los efectos.

059. El ciberespacio *tiene fronteras* (a diferencia de la percepción extendida que propugna lo contrario), es decir, un perímetro que separa un área interna de una externa y que permite a un propietario o autoridad controlar los movimientos entre las áreas.

060. La protección eficaz de las fronteras en el ciberespacio escala de manera deficiente en comparación con los otros ámbitos. Si bien, en el ciberespacio se puede establecer un control de accesos eficaz para identificar las entidades autorizadas a acceder a una zona del ciberespacio determinada, a medida que esta zona se hace más extensa el control de acceso pierde eficacia.

061. Un país tiene mecanismos eficaces para realizar un control selectivo de acceso a sus espacios soberanos terrestres, marítimos y aéreos; en cambio, realizar un control de eficacia similar en el ciberespacio de soberanía nacional es, actualmente, inviable, a pesar de los intentos de algunos países de crear su propia internet soberana.

ILUSTRACIÓN 7. CIBERESPACIO TRANSVERSAL

062. El ciberespacio es *transversal* a los otros ámbitos. En realidad, se comporta como un supraespacio con gran presencia e influencia en el resto de ámbitos. Esta transversalidad hace que el ciberespacio deba ser considerado de manera especial en todos los aspectos conjuntos (doctrina, planeamiento y conducción de operaciones, orgánica, etc.)

Ciber Terreno Clave

063. El *Ciber Terreno Clave* (CTC) es el conjunto de elementos del ciberespacio, en cualquiera de sus capas (humana, ciberhumana, cognitiva, lógica, TIC y geográfica), que facilitan las actividades, operaciones o funciones esenciales para la misión y cuya destrucción, interrupción o captura generaría una ventaja operativa para el adversario.

064. En cualquier ciberoperación, así como, en cualquier operación conjunta es necesario identificar los elementos del CTC y analizar y valorar sus vulnerabilidades, probabilidad de ser atacados e impacto a la misión en caso de ser afectados por un ataque.

065. Intentar defender simultáneamente todos los elementos del CTC no es práctico y en la mayoría de los casos no es viable, por ello la lista de activos CTC debe ser priorizada, actualizada con cierta periodicidad para, posteriormente, realizar un plan de protección acorde a la priorización.

066. El proceso de identificación y protección del CTC se debe hacer de la misma manera que se hacen la identificación y protección del terreno clave de los ámbitos convencionales de tierra, mar y aire.

067. El modelo de capas del ciberespacio facilita la labor de identificación de los elementos del CTC.

068. Los elementos del *CTC en la capa humana* son aquellas personas cuyo conocimiento se considera esencial para el funcionamiento y la protección de todos los elementos de la lista CTC.

069. Los elementos del *CTC en la capa cognitiva* son aquellos datos, información o conocimiento cuya revelación al adversario pondría en grave riesgo la misión o cuya manipulación por el adversario crearía un estado desconfianza en los sistemas de información esenciales para la misión.

070. Los elementos del *CTC en la capa lógica* son aquellos sistemas de información (incluidos los sistemas de mando y control, sistemas de armas y sistemas de navegación) susceptibles de ser controlados o interferidos por el adversario, en cuyo caso se pondría en grave riesgo la misión.

071. Los elementos del *CTC en la capa TIC* son aquellos componentes de las redes de telecomunicaciones susceptibles de ser controlados o interferidos por el adversario, en cuyo caso se podrían generar denegaciones de servicio o funcionamientos degradados de servicios críticos para la misión.

072. Los elementos del *CTC en la capa geográfica* son aquellos emplazamientos en donde se ubican componentes TIC críticos (centros de procesamiento de datos, centros de control de redes, centros de operaciones de seguridad TIC, puntos de intercambio de internet, proveedores de servicio de internet críticos, infraestructura de cable submarino, etc.) y que su destrucción física pudiera afectar al cumplimiento de la misión.

073. La protección de la infraestructura nacional de *cable submarino* y sus puntos de conexión terrestre (puntos de presencia, estaciones de aterrizaje, estaciones terrestres, etc.) debe ser considerada una necesidad estratégica en el marco de la ciberseguridad nacional, debido a que son el principal soporte de comunicaciones global. En concreto, se estima que más del 95% de todas las comunicaciones digitales transoceánicas se realizan a través de la infraestructura de cables submarinos ya que son un soporte más rápido y más barato que la infraestructura satelital.

074. Sabotear un cable submarino es una operación compleja; no obstante, se cree que, en la actualidad, sabotear cables submarinos de comunicaciones es un procedimiento operativo estándar para los servicios de espionaje de algunas naciones; así como, realizar sospechosas maniobras navales cerca de las rutas y puntos de conexión de cables submarinos estratégicos, lo cual genera inquietud entre los países potencialmente afectados por un sabotaje a dichos cables.

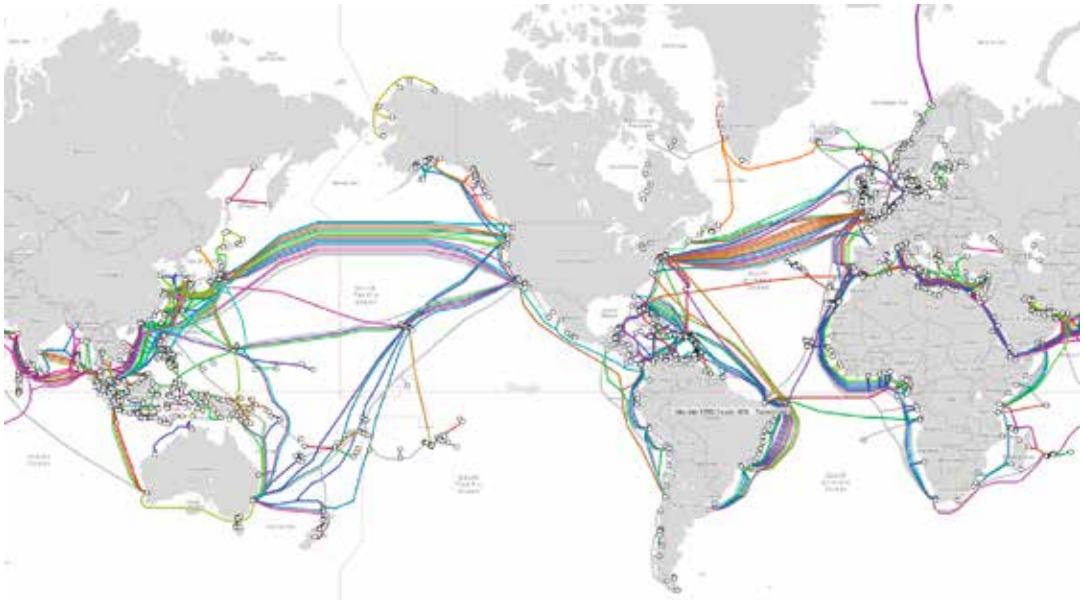


ILUSTRACIÓN 8. MAPA DE COBERTURA DE CABLES SUBMARINOS (TELEGEOGRAPHY)

Ciberriesgo

075. La *gestión del riesgo* es una parte fundamental de la ciberdefensa y se encuentra presente, de manera intencionada o involuntaria, en todas las fases de la toma de decisión. Una decisión, en la mayoría de los casos, es el resultado de la comparación de riesgos asociados a las diferentes opciones factibles.

076. El *ciberriesgo* es la probabilidad de que una ciberamenaza aproveche una vulnerabilidad para causar un impacto (daño) a un activo que tiene un valor y una criticidad determinada. En definitiva, es un indicador que se obtiene de dos factores: la probabilidad y el impacto.

077. La *probabilidad* de sufrir un ciberataque es mayor cuanto mayor sea la capacidad de la amenaza y su interés en los activos de la potencial víctima.

078. La probabilidad de sufrir un ciberataque es mayor cuantas más vulnerabilidades tengan los sistemas objetivos pues le hacen el trabajo más fácil y rentable a la amenaza.

ILUSTRACIÓN 9. CIBERRIESGO

079. El *impacto* es mayor cuanto mayor sea el valor, para la organización, de los activos atacados.

080. El impacto es mayor cuanto mayor es la criticidad de los activos atacados. Es decir, cuando otros activos importantes para la organización dependen de los activos atacados.

081. En el contexto de la ciberdefensa, el riesgo que hay que considerar, por encima de todo, es el riesgo a la misión por ciberamenazas. Es decir, como puede afectar a la misión una materialización exitosa de una ciberamenaza.

082. Es necesario minimizar los riesgos de los elementos del ciberespacio cuyo funcionamiento es esencial para el cumplimiento de la misión. Estos elementos críticos son los componentes del ciber terreno clave.

ILUSTRACIÓN 10. CIBERRIESGO A LA MISIÓN

083. El ciberriesgo se gestiona a través de un proceso sistemático que conlleva las fases siguientes:

1. Identificar y priorizar los elementos del ciber terreno clave por su mayor potencial impacto a la misión en el caso de que su funcionamiento se vea afectado.
2. Identificar y evaluar las vulnerabilidades de los elementos del CTC.
3. Identificar las potenciales ciberamenazas que pueden afectar a la misión y valorar su capacidad.
4. Identificar los activos de mayor interés para la amenaza, bien porque son de mayor valor o utilidad para la amenaza o bien porque son los de mayor impacto a la organización y esto es lo que la amenaza busca.
5. Determinar los riesgos mediante la realización de un análisis metodológico a través de una herramienta y metodología especializada (MAGERIT[3]/PILAR[4], CRAMM[5], OCTAVE[6], etc.).
6. Definir y priorizar las medidas de mitigación de los riesgos determinados.
7. Elaborar e implementar un plan de gestión del riesgo.

084. La gestión del ciberriesgo es un *proceso dinámico*, de tal manera que la identificación y valoración de nuevas amenazas, vulnerabilidades y activos debe ser continua y cuando se produce un cambio significativo, estos deben alimentar el proceso, generándose un nuevo análisis.

085. Las formas tradicionales de mitigación del riesgo son cuatro: evitación, reducción, compartición y retención.

086. La *evitación del ciberriesgo* implica no realizar una actividad que pueda conllevar ciberriesgos.

ILUSTRACIÓN 11. GESTIÓN DEL CIBERRIESGO

087. Aunque parece una medida algo burda, en realidad, en el ciberespacio es una medida bastante habitual. Por ejemplo, la implementación de listas negras o listas blancas en el acceso a determinadas páginas web, la restricción selectiva para el acceso a la información (necesidad de conocer), etc.

088. La *reducción del ciberriesgo* implica reducir la gravedad de la pérdida o la probabilidad de que ocurra la pérdida mediante, por ejemplo, la implementación de medidas de ciberseguridad, la contratación de servicios de ciberseguridad, la inversión en ciberdisuasión o la implementación de planes de contingencia.

ILUSTRACIÓN 12. MITIGACIÓN DEL RIESGO

089. La *compartición o transferencia de ciberriesgo* implica compartir con otra parte la carga de la pérdida o las medidas para reducir los ciberriesgos mediante, por ejemplo, la contratación de un seguro como un mecanismo compensatorio posterior al evento o el establecimiento de un acuerdo de colaboración con otras organizaciones potencialmente afectadas por los mismos ciberriesgos.

090. La *retención del ciberriesgo* implica aceptar la pérdida de un ciberriesgo cuando ocurre. Es decir, significa, no hacer nada para reducir la probabilidad o el impacto. En la práctica, se retienen todos aquellos ciberriesgos que no se evitan, reducen o comparten.

091. La retención de ciberriesgos es una estrategia viable para los ciberriesgos extremos; es decir si la probabilidad de una pérdida muy severa es pequeña o si el coste de asegurarse es tan grande que dificultaría demasiado los objetivos de la organización. Por ejemplo, el riesgo de que un centro de proceso de datos sea destruido por un terremoto en una zona de poca actividad sísmica.

Cibertácticas

092. El uso militar del ciberespacio es un ámbito nuevo que tiene, todavía, mucho por definir y explorar, pero eso no significa que haya que empezar desde cero; las formas tradicionales de defensa y empleo de la fuerza, en su esencia, no varían; solo hay que buscar el modo de realizarlas con medios y procedimientos especialmente adaptados.

093. Las *tácticas militares tradicionales de los otros ámbitos como el reconocimiento del terreno, la concentración de fuerzas, la infiltración, la vigilancia, la emboscada y el fuego y movimiento* son, también, de aplicación en el ciberespacio.

094. El *reconocimiento del ciberterreno* es una actividad indispensable previa al planeamiento y conducción de una ciberoperación con la finalidad principal de identificar la topología y vulnerabilidades del ciberespacio adversario en todas sus capas.

095. La *concentración de ciberfuerzas* en el ciberespacio se puede hacer de dos maneras, cuantitativa o cualitativamente.

096. La *concentración cuantitativa* de ciberfuerzas se refiere a la concentración de numerosos recursos humanos (recursos públicos, universidades, población), la mayoría sin una cualificación técnica o profesional elevada, enfocados a un mismo objetivo o cometido.

097. Un ejemplo de concentración cuantitativa es cuando un estado utiliza un gran número de personas en plantilla (unidades de las fuerzas armadas, estudiantes de universidades, etc.), sin necesariamente una cualificación profesional de alto nivel en el ámbito de la ciberdefensa, para seguir unas instrucciones sistematizadas desarrolladas por un grupo de expertos enfocados a unos objetivos concretos. Es una estrategia rentable para estados donde el recurso humano es de dimensiones generosas y que se pueden permitir el lujo de gastar el esfuerzo de muchas personas en un solo objetivo (pe. muchas personas intentando encontrar un punto de acceso en un sistema hasta que una de ellas lo consiga).

098. Otra variante de la concentración cuantitativa es cuando un estado aprovecha una situación social o política caliente o inestable para convencer y animar a un grupo de población descontento a realizar actividades maliciosas en el ciberespacio, concurrentes en el tiempo y contra un mismo objetivo, siguiendo unas instrucciones claras, sencillas y precisas, buscando, generalmente, efectos de denegación de servicio.

099. La *concentración cualitativa* es cuando se concentran, de manera organizada y coordinada, un gran número de expertos y recursos tecnológicos y económicos generando una unidad especial de ciberdefensa.

100. La concentración cualitativa es una estrategia más común que la cuantitativa y es llevada a cabo, generalmente, por grupos (APTs) asociados a estados, bien de manera orgánica o encubierta.

101. La *infiltración* se refiere al acceso clandestino a redes de adversarios con la finalidad de afectar a sus sistemas o información o con la intención de tomar control subrepticio de ellos. Es una táctica fundamental en APTs.

102. La *vigilancia* se refiere a la monitorización de las redes propias, internamente y en su perímetro, con la finalidad de detectar acciones maliciosas o comportamientos sospechosos. Es una de las actividades principales de los centros de operaciones de seguridad (COS, CERTs, párr.340/341)

103. La *emboscada* en el ciberespacio se realiza, principalmente, mediante señuelos (honey pots), redes trampa (honey nets), plataformas de ciberdecepción (cyber deception platform) o señuelos armados (weaponized tokens).

104. Los *señuelos* son dispositivos de red virtualmente aislados (aunque simulan conectividad) con actividad ficticia (aunque simulan actividad real), deliberadamente vulnerables (no excesivamente para que parezcan reales), orientados a llamar la atención de los atacantes (de modo que los atacantes creen que se han infiltrado con éxito en la red, en cambio, en realidad están siendo analizados en un entorno aislado) con la finalidad de analizar sus tácticas, técnicas y procedimientos (TTPs), así como de intentar infundirles frustración que les lleve al abandono del ataque.

105. Las *redes trampa* son redes de señuelos. Actualmente, la implementación de medidas de ciberseguridad basadas en tecnologías de redes trampa no son protección suficiente frente a ciberatacantes experimentados (APTs), siendo necesario recurrir a otras tecnologías más avanzadas y proactivas como las plataformas de ciberdecepción.

106. Las *plataformas de ciberdecepción* son redes trampa sofisticadas, dinámicas y automatizadas que se ubican en entornos lógicos reales, con capacidad para detectar, analizar y hacer frente, en tiempo real, a ciberataques de día cero[7] y ciberataques avanzados.

107. La tecnología de ciberdecepción considera las TTPs del ciberatacante y se integra con otras tecnologías de ciberseguridad para proporcionar la conciencia de la situación ciberespacial y alertas e inteligencia de ciberamenazas. Es de espacial utilidad para los servicios de caza de amenazas.

108. Las plataformas de decepción tienen más riesgo de interferir en la operatividad de las redes reales por ello la solución tecnológica elegida deber ser cuidadosamente seleccionada y probada antes de implementarse.

109. Los *señuelos armados* son documentos electrónicos o códigos software que simulan información de interés para un potencial ciberatacante y que llevan un malware preinstalado diseñado para activarse en la red del ciberatacante en caso de que haya llevado a cabo su exfiltración.

110. El *fuego y movimiento* en el ciberespacio se refieren a la necesidad de diseñar los ciberataques para que una vez hayan causado el efecto deseado no dejen rastro ni del atacante ni de las TTPs usadas, de tal manera que no puedan ser atribuibles ni reutilizables.

Factor humano

111. En el *ciberespacio*, a diferencia de los otros ámbitos, conviven dos tipos de personas: la persona física (identidad real) y las ciberpersonas (identidad online).

112. La *ciberpersona* o identidad online es la persona tal cual se muestra en el ciberespacio o la identidad que un usuario del ciberespacio establece en comunidades o actividades online. Puede ser creada y gestionada por una persona física o automáticamente por herramientas diseñadas ad hoc.

113. Una ciberpersona puede tener asociada una o varias identidades reales o ficticias y, a su vez, una persona puede tener asociada o controlar una o varias ciberpersonas; siendo, en muchos casos, difícil de identificar si una ciberpersona corresponde a la persona, grupo o entidad que dice que es.

Ciberarmas

114. Una *ciberarma* es un software específicamente diseñado para causar un daño a un elemento del ciberespacio pudiendo tener consecuencias físicas en los ámbitos de operaciones convencionales.

115. A semejanza de las armas convencionales, una ciberarma son los medios (vectores de ciberataque) que permiten transferir la munición o carga explosiva (malware, exploits[8]) a los objetivos (redes y sistemas del adversario). De manera práctica y por extensión, se considera una ciberarma al conjunto de vector de ciberataque y carga explosiva.

ILUSTRACIÓN 13. CIBERARMA

116. Los *vectores de ciberataque* son numerosos, algunos de los más habituales son el phishing[9], spear phishing[10], spoofing[11] , pharming[12,] sniffing[13], watering hole[14], DoS[15], DDoS[16], MitM[17] y SQL injection[18].

117. En el ciberespacio, con frecuencia, se confunden conceptos que en los ámbitos convencionales no generan tal confusión. Este es el caso de los ciberataques y las ciberarmas que suelen asimilarse. Por ejemplo, en el mundo físico nadie duda de que una pistola es un arma y que un ataque se produce cuando una persona hace un uso concreto de la pistola. En el ciberespacio es lo mismo, una ciberarma es un medio y un *ciberataque* es el uso deliberado de ese medio por una persona o de manera automática.

118. Las ciberarmas se diseñan para causar daños de diferente severidad (destrucción, denegación, degradación, interrupción y exfiltración) a objetivos del ciberespacio o de otros ámbitos de operaciones.

119. Los *blancos* habituales de una ciberarma son la información (destrucción, denegación, degradación, interrupción y exfiltración), la funcionalidad de redes y sistemas de información (destrucción, denegación, degradación, interrupción), la reputación (destrucción, degradación), el material (destrucción, degradación), las instalaciones (destrucción, degradación) y las personas (destrucción, degradación)

120. La *información* suele ser el objetivo principal de grupos organizados de alto nivel (APTs) de tal manera que, aun teniendo la capacidad de inutilizar el sistema infectado, prefieren no afectar de ninguna manera a su funcionalidad para así pasar desapercibido la mayor parte del tiempo posible para exfiltrar información. Ciberarmas tipo Flame[19] han sido diseñadas, especialmente, para el ciberespionaje.

121. Está demostrada la existencia de ciberarmas cuyos efectos se extienden más allá del ciberespacio pudiendo afectar a material, instalaciones y personas. Ejemplos de estas ciberarmas son Stuxnet[20], Duqu[21] o Black Energy[22].

122. Una fuerza ciberespacial (párr.221) debe disponer de un arsenal (párr. 409) apropiado que le permita hacer un uso legítimo de la fuerza en el momento y en las condiciones legalmente reconocidas.

123. Hay que resaltar que una ciberarma, en realidad, puede tener múltiples usos y puede ser usada para múltiples objetivos diferentes. Es el conjunto de diferentes ciberarmas junto con procedimientos ad hoc, herramientas de mando y control y personal específicamente cualificado lo que posibilita el desarrollo de un determinado tipo de ciberataque con un objetivo concreto.

124. Un *sistema de armas ciberespacial* es un sistema que integra diferentes ciberarmas, funciones de mando y control y todos los apoyos técnicos necesarios para desarrollar una ciberoperación ofensiva, defensiva o de explotación con un objetivo concreto.

125. El sistema de armas ciberespacial, dependiendo del alcance de sus efectos, puede ser estratégico, operacional o táctico.

Ciberataques

126. Un *ciberataque* es el uso deliberado de una ciberarma, por una persona o de manera automática, para generar un daño o efecto perjudicial en las redes y sistemas de información de un adversario pudiendo tener efectos indirectos en los ámbitos de operaciones convencionales.

127. El comandante de una operación debe considerar todas las capacidades en su mano para conseguir los efectos deseados, para ello debe considerar ataques convencionales y ciberataques y efectos físicos y ciberefectos.

128. No hay una correspondencia biunívoca entre ciberataques y ciberefectos y entre ataques físicos y efectos físicos ya que un ciberataque puede producir efectos físicos y un ataque físico puede producir efectos en el ciberespacio.

129. En una *operación conjunta* se debe considerar todas las combinaciones posibles de ataques: ataques procedentes de un ámbito y con un objetivo en el mismo ámbito (Tierra-Tierra, Mar-Mar, Aire-Aire, Espacio-Espacio, Ciberespacio-Ciberespacio) y ataques procedentes de un ámbito y con un objetivo en otro ámbito (Tierra-Mar, Tierra-Aire, Tierra-Espacio, Tierra-Ciberespacio. Mar-Tierra, Mar-Aire, Mar-Espacio, Mar-Ciberespacio. Aire-Tierra, Aire-Mar, Aire-Espacio, Aire-Ciberespacio. Espacio-Tierra, Espacio-Mar, Espacio-Aire, Espacio-Ciberespacio. Ciberespacio-Tierra, Ciberespacio-Mar, Ciberespacio-Aire, Ciberespacio-Ciberespacio).

ILUSTRACIÓN 14. TIPOS DE ATAQUES

130. Para detectar y repeler un ciberataque es necesario conocer cómo es su funcionamiento y su proceso de desarrollo.

131. La *cadena de ciberexterminio*[23] es un modelo basado en siete fases (*reconocimiento, preparación, distribución, explotación, instalación, mando y control y ejecución*) con la finalidad de sistematizar la identificación y prevención de la actividad de ciberintrusiones y así facilitar la detección de un ataque y la comprensión de las TTPs (tácticas, técnicas y procedimientos) de un adversario. Evidentemente, puede ser usada, a la vez, para coordinar y organizar ciberataques.

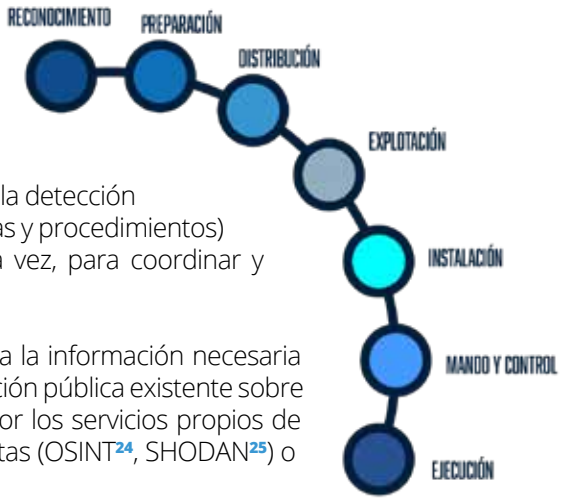


ILUSTRACIÓN 15. CYBER KILL CHAIN (LOCKHEED MARTIN)

132. En la *fase de reconocimiento* se elige el objetivo y se analiza la información necesaria para planificar y ejecutar el ciberataque; esto es, la información pública existente sobre el objetivo (en webs, redes sociales, etc.) y la disponible por los servicios propios de ciberinteligencia, utilizando herramientas de fuentes abiertas (OSINT[24], SHODAN[25]) o herramientas comerciales.

133. El reconocimiento incluye actividades pasivas (monitorización en redes públicas, obtención de información de fuentes abiertas, etc.) y activas (por ejemplo, técnicas de ingenierías social para forzar a un objetivo a proporcionar información) orientadas a conseguir información sobre el objetivo (capacidad de ciberdefensa, vulnerabilidades, topología de la red, credenciales, correos electrónicos asociados al objetivo, etc.).

134. En esta fase inicial, el atacante realiza una huella digital (fingerprinting) del objetivo para crear un esquema o mapa de sus redes y sistemas TIC, estructura organizativa, relaciones, comunicaciones y afiliaciones e identificar sus vulnerabilidades, tanto técnicas como humanas, para posteriormente poder infiltrarse y explotar la red.

135. Esta fase puede prolongarse mucho tiempo, pero vale la pena el tiempo gastado en esta fase ya que cuanto más y mejor conocimiento se tenga sobre el adversario, mayor será la probabilidad de éxito del ciberataque.

136. En la *fase de preparación*, en base a la información obtenida en la fase de reconocimiento, el conocimiento detallado de los recursos propios y los tipos de efectos deseados, se planifica el ciberataque, se seleccionan las herramientas más eficaces y se produce el armado de la carga útil (malware y exploits idóneos para explotar las vulnerabilidades conocidas o desconocidas) en los vectores de ataque (documentos pdf o word, dominios web comprometidos, emails suplantados, dispositivos de memorias usb, etc.).

137. Es necesario usar malware nuevo, modificado o rediseñado para reducir la probabilidad de detección por soluciones de seguridad tradicionales que identifican firmas conocidas.

138. En la *fase de distribución* se produce la transmisión y entrega de las cargas útiles al entorno del objetivo. Es un momento crítico puesto que es el momento en el que se establece contacto con el objetivo y algunos de los intentos pueden ser detectados y rechazados, por lo que es muy importante diseñar el ataque para que deje el menor rastro (huella digital) posible.

139. Es necesario, además, hacer un seguimiento de la efectividad de los intentos de intrusión para enfocarse en los más rentables.

140. En la *fase de explotación* se produce la activación de la carga útil explotando una vulnerabilidad del entorno del objetivo (una aplicación, el sistema operativo o los propios usuarios) y ejecutándose el malware en su sistema. La instalación de malware en entorno del objetivo requiere la participación del usuario final habilitando involuntariamente el código malicioso (carga útil).

141. En la *fase de instalación* se consolida el malware en el sistema del objetivo y se establece una conexión con el exterior, a través de la instalación de un troyano de acceso remoto o una puerta trasera y así, mantener la persistencia dentro del entorno.

142. En la *fase de mando y control,* el atacante aprovechando el canal de comunicación externa y el malware consolidado en el entorno del objetivo toma control subrepticio de parte del sistema para generar nuevos ataques, dirigidos desde un centro de coordinación de las operaciones (centro de mando y control) establecido al efecto.

143. Llegados a este punto, las ciberdefensas tradicionales basadas en cortafuegos, sistemas de detección de intrusos (IDS), sandbox y sistemas de seguridad de eventos (SIEM[26]) no son eficaces. Solo sería eficaz una ciberdefensa basada en un sistema de caza de ciberamenazas (párr. 478) junto con un grupo de expertos bien organizados y con la autoridad necesaria para llevar a cabo medidas de mitigación y reacción.

144. En la *fase de ejecución* el atacante, una vez tomado el control del sistema del objetivo, ejecuta acciones para conseguir los efectos deseados (ciberefectos, párr. 145) y aprovecha el control del sistema para extenderse a otros sistemas y objetivos lo cual implicaría realizar de nuevo la cadena de ciberexterminio.

Ciberefectos

145. Los *ciberefectos* son los daños o impactos producidos por ciberataques. Se pueden agrupar en dos grandes grupos, ruidosos y silenciosos. Cada uno de ellos tienen unas ventajas y unos inconvenientes tanto para el atacante como para las víctimas. En cualquier ciberoperación, tanto de defensa como de ataque, es necesario considerarlos todos.

146. Los *ciberefectos ruidosos* son aquellos impactos claramente perceptibles por la víctima, como la denegación o degradación de un servicio, la falta de disponibilidad de una determinada información a usuarios autorizados, la modificación perceptible de contenidos web, el secuestro de información mediante cifrado con la finalidad de impedir su acceso (en algunos casos solicitando un rescate) e incluso, la destrucción física de algún dispositivo o instalación.

147. Suelen producir perdidas de operatividad, económicas y de reputación importantes, aunque limitadas en el tiempo, ya que en la mayoría de los casos los efectos son reversibles si se dispone de un plan de continuidad de las operaciones (párr. 290) eficaz.

148. Los impactos suelen ser bastante llamativos generando alarma y consecuentemente desencadenando una reacción en la víctima que puede derivar en una inversión de recursos adicionales de ciberdefensa para revertir la situación y prevenir la repetición.

149. La cadena de ciberexterminio de ciberataques ruidoso suele ser de corta duración. Las fases de reconocimiento y preparación suelen ser cortas porque los ciberataques de efectos ruidosos no suelen ser muy sofisticados. Las fases de distribución, explotación e instalación suelen ser cortas porque no necesitan evitar la detección temprana ya que los propios efectos dan la alarma. La fase de mando y control suele ser corta porque no necesita una comunicación externa. La fase de ejecución es corta porque el tiempo que transcurre desde el primer ciberataque hasta que la víctima detecta que está sufriendo un ciberataque es inmediato.

150. Los *ciberefectos silenciosos* son aquellos impactos que pasan desapercibidos para la víctima, como le exfiltración de la información, la modificación no llamativa de información y contenidos web, la suplantación de identidad, la sustracción de credenciales, la monitorización de la red, etc.

151. Los ciberataques de efecto silencioso buscan la persistencia, es decir, mantener el control el mayor tiempo posible y para ello cuidan mucho no dejar rastro (huella digital) y combinan periodos de actividad con periodos (en muchos casos muy largos) de inactividad. Además, camuflan su actividad bajo los parámetros habituales de la actividad de la víctima para no llamar la atención.

152. Suelen producir perdidas de operatividad, competitividad y económicas muy grandes, aunque la organización, en muchos casos, no sea consciente de ello.

153. En la mayoría de los casos, no son detectables por medios de ciberdefensa convencionales y se precisa de sistemas avanzados de ciberdefensa tipo "caza de ciberamenazas".

154. La cadena de ciberexterminio de ciberataques silenciosos suele ser de larga duración. Las fases de reconocimiento y preparación suelen ser largas porque los ciberataques de efectos silenciosos son muy sofisticados y requieren una concienzuda preparación. Las fases de distribución, explotación, instalación y mando y control suelen ser largas porque hay que evitar, por todos los medios, la detección temprana. La fase de ejecución, en particular, suele ser muy larga; es decir, el tiempo que transcurre desde el primer ciberataque hasta

que la víctima detecta que está sufriendo un ciberataque suele ser de años y, en muchos casos, el tiempo que transcurre desde la detección hasta que la víctima logra erradicar totalmente la acción del atacante puede ser también de años.

155. Los ciberataques silenciosos son tremendamente peligrosos porque, durante años, la víctima no percibe la pérdida de operatividad y competitividad.

ILUSTRACIÓN 16. CIBEREFECTOS

Ciberdisuasión militar

156. La disuasión militar es una de las principales líneas estratégicas de las fuerzas armadas; se trata, como dijo Sun Tzu (544 -496 ac), de ganar sin llegar al enfrentamiento.

157. Una capacidad de *disuasión militar* efectiva debe reunir tres requisitos: *capacidad, determinación y declaración*.

158. La disuasión se basa en la *capacidad* de una potencial víctima, de causar a una potencial amenaza, un daño mayor a los beneficios esperados por la amenaza en caso de iniciar un ataque.

159. La capacidad militar debe estar preparada para ser empleada en el momento y lugar necesario, para ello es necesario una formación, entrenamiento y evaluación continua.

160. La *determinación* es la firme voluntad de hacer uso de la fuerza, en caso necesario, para anticipar, prevenir o responder a un ataque.

161. La *declaración* es la expresión pública de la capacidad y la determinación para que sean claramente conocidas por los potenciales adversarios.

ILUSTRACIÓN 17. DISUASIÓN

162. No es necesario, ni aconsejable, detallar más de lo necesario sobre la capacidad; bastaría con hacer ostentación de la dimensión de los efectos que la capacidad podría desencadenar (publicación de estudios, realización de ejercicios, maniobras, etc.).

163. En el ciberespacio, la disuasión no se percibe de una manera tan clara como en los ámbitos convencionales por la dificultad en la atribución del origen del ciberataque. Es decir, la represalia debe ejercerse contra un atacante conocido y cuya autoría es atribuible sin ningún género de dudas, y esto, actualmente, es un asunto complejo ya que los ciberatacantes suelen conducir sus ataques a través de redes secuestradas de terceros, sin que estos sean conscientes de ello.

164. La complejidad en la atribución en el ciberespacio hace que la *disuasión pasiva* (disponer de una ciberdefensa lo suficientemente robusta que no haga rentable el esfuerzo y los recursos consumidos a una potencial ciberamenaza) adquiera una relevancia singular.

165. La disuasión militar se entiende desde una perspectiva integral en donde la represalia a un ciberataque no tiene porque, necesariamente, realizarse a través de una capacidad de ciberdefensa, sino que la represalia puede ser llevada a cabo a través de cualquier otro tipo de ataque convencional; en definitiva, el objetivo es mantenerse libre de ataques de cualquier tipo.

166. Por tanto, se entiende la *disuasión militar integral* como la determinación declarada de hacer uso de todas las capacidades militares disponibles (convencional, nuclear y ciber) en caso necesario.

ILUSTRACIÓN 18. DISUASIÓN MILITAR INTEGRAL

Control del ciberespacio

167. El control de los espacios de influencia en el combate, tanto en tierra como mar y aire, es uno de los requisitos fundamentales para disponer de la necesaria libertad de acción y evitar las interferencias de los adversarios. En el ciberespacio, como ámbito de operaciones, esta necesidad (el cibercontrol) es igualmente necesario.

168. El *cibercontrol* es el grado de dominio del ciberespacio de confrontación de una ciberfuerza sobre la ciberfuerza adversaria.

169. Se distinguen 5 niveles de control del ciberespacio: *cibersupremacía, cibersuperioridad, ciberparidad, ciberdegradación, ciberincapacidad*.

ILUSTRACIÓN 19. CIBERCONTROL

170. El nivel 1 (*cibersupremacía*) se alcanza cuando se tiene control absoluto del ciberespacio de confrontación. Las ciberfuerzas adversarias son incapaces de ejercer ninguna interferencia efectiva sobre el ciberespacio de confrontación. La libertad de acción propia es total mientras que la del adversario es mínima.

171. El nivel 2 (*cibersuperioridad*) se alcanza cuando se dispone de una posición más favorable sobre el adversario en el ciberespacio de confrontación. La libertad de acción propia es mayor que la del adversario.

172. El nivel 3 (*ciberparidad*) se adquiere cuando se dispone, exclusivamente, de control sobre las redes y sistemas propios. Las dos ciberfuerzas disponen de similar libertad de acción y capacidad de interferencia sobre el otro.

173. En el nivel 4 (*ciberdegradación*) el adversario está en una posición más favorable en el ciberespacio de confrontación. La ciberfuerza propia puede seguir funcionando, pero en modo degradado. La libertad de acción propia es menor que la del adversario.

174. En el nivel 5 (*ciberincapacidad*) el adversario tiene control absoluto del ciberespacio de confrontación. Las ciberfuerzas adversarias pueden ejercer interferencia máxima en el ciberespacio de confrontación. La libertad de acción propia es mínima mientras que la del adversario es total.

175. Alcanzar el nivel 1 y 2 requiere disponer de capacidades defensivas y ofensivas. Con capacidades exclusivamente defensivas (capacidades de acción en redes propias) una ciberfuerza solo podrá aspirar al nivel 3 de control (ciberparidad) si la ciberfuerza contraria tampoco dispone de capacidades ofensivas, en caso contrario solo se podrá aspirar al nivel 4 o 5.

Opciones en el enfrentamiento

176. Para realizar una valoración idónea de la mejor opción a usar en el combate para conseguir unos efectos determinados, el comandante debe valorar, de entre todas las capacidades en su mano (convencionales y ciberespaciales) la que mejor reúna, como mínimo, los criterios de eficacia, eficiencia, menor riesgo a fuerzas propias y a terceros.

177. El criterio de *eficacia* se refiere a la acción que genere con exactitud los efectos deseados.

178. El criterio de *eficiencia* se refiere a la acción que precise del menor número de recursos económicos, humanos y materiales.

179. El criterio de *riesgo a fuerzas propias* se refiere a la acción que ponga en menor riesgo a las personas, medios e instalaciones de la propia unidad.

180. El criterio de *riesgo a terceros* se refiere a la acción que produzca menos daños colaterales, principalmente víctimas civiles y aquellas no implicadas en el conflicto.

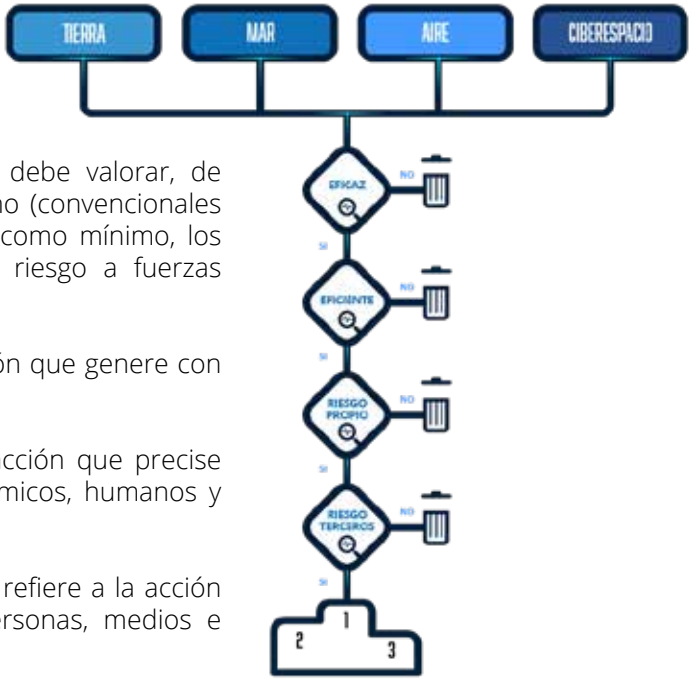


ILUSTRACIÓN 20.
OPCIONES EN EL ENFRENTAMIENTO

181. El peso que cada criterio tiene en la valoración es fijado por el comandante de la operación, aunque, evidentemente, el primer criterio es la eficacia, pues no tiene sentido elegir una opción que no genere los efectos deseados. Una vez elegidas todas las opciones que, en mayor o menor medida, son eficaces se seleccionaría la acción que mejor reúna las condiciones restantes en base a criterios operativos, económicos o por imposición legal (caso de riesgo a terceros o fuerzas propias).

182. En muchos casos, la opción que cumple las cuatro condiciones en mejor medida es una acción en el ciberespacio. Si un comandante de una operación, dispusiera de capacidades de ciberdefensa y la opción que mejor cumple los cuatro requisitos fuera una acción en el ciberespacio, entonces sería difícilmente entendible desde un punto de vista operativo, ético y legal que no eligiera la opción ciberespacial por delante de las convencionales (párr. 645)

Asimetría en el enfrentamiento

183. La *asimetría en el enfrentamiento* en el ciberespacio es la disparidad o desproporción entre los recursos necesarios para ciberatacar y los necesarios para ciberdefender que hace que, en muchos casos, los recursos necesarios para planificar y conducir un ciberataque sean menores que los necesarios para defenderse de ese ciberataque.

184. La asimetría en el enfrentamiento es más agudizada en el ciberespacio que en los otros dominios debido a motivos relacionados con la *superficie de exposición, recursos, marco legal, tecnología, personal e identidad*.

185. La *superficie de exposición* del defensor es mayor que la superficie usada en el ataque. El defensor debe preparar su defensa contra cualquier tipo de ataque a cualquier parte o componente de su red, mientras que el atacante se limitará a aquellos elementos que hacen posible el ataque centrándose en explotar un número reducido de vulnerabilidades.

186. En la mayoría de los casos, una organización invierte más *recursos* (económicos, materiales, técnicos y humanos) en la defensa de sus redes y sistemas que los que deben invertir los atacantes para causar una interrupción o malfuncionamiento de ellos. Esto es así habitualmente, pero no en todos los casos; por ejemplo, para desarrollar un ciberataque tipo STUXNET se necesita la inversión de una cantidad enorme de recursos, solo al alcance de estados o grandes corporaciones.

187. El *marco legal* favorece a los atacantes. El ciberatacante puede eludir las legislaciones nacionales mediante la ejecución de ciberataques desde redes secuestradas ubicadas en terceros países mientras que, el defensor está sujeto al cumplimiento de la legislación nacional en donde se ubica su infraestructura.

188. La falta de acuerdos internacionales y bilaterales y la falta de un marco jurídico internacional consensuado y vinculante en materia de ciberdefensa dificulta la imputación y persecución de los ciberatacantes.

189. El defensor, en la mayoría de las ocasiones, no puede hacer uso de la *tecnología de vanguardia* disponible en el mercado, bien por razones de limitación presupuestaria, o bien por razones técnicas, ya que una organización no puede exponer sus defensas con tecnologías nuevas que todavía no han sido ampliamente probadas. Por el contrario, el atacante puede correr el riesgo de utilizar una tecnología emergente que no está probada y descartarla en caso de que no produzca los efectos deseados (método de prueba y error).

190. Las *tecnologías* y herramientas de defensa suelen ser más conocidas por el atacante que las tecnologías y herramientas de ataque por un defensor; debido a que las tecnologías

y herramientas de defensa tienden a perdurar en el tiempo para rentabilizar la inversión económica, mientras que un atacante prueba continuamente nuevas tecnologías y herramientas para sorprender al defensor.

191. La defensa de redes y sistemas precisan, habitualmente, de un *personal especialmente cualificado* en numerosos aspectos y materias de ciberseguridad; por el contrario, en la mayoría de los ciberataques, se necesita un grupo limitado de expertos que desarrollen instrucciones y coordinen la acción de un grupo más amplio de individuos con poca cualificación en ciberdefensa.

192. El atacante, generalmente, conoce la *identidad* del defensor y su entorno (organización, sistema, actividad, funciones, ubicación, etc.) mientras que el defensor suele desconocer al atacante.

193. En el proceso de planeamiento de una ciberoperación se debe tener en consideración que la rentabilidad de una acción ofensiva puede ser mayor que la de una defensiva, como la máxima en algunos deportes "la mejor defensa es un buen ataque".

CIBERDEFENSA MILITAR

194. La *ciberdefensa militar* es la capacidad de las fuerzas armadas organizada y preparada para combatir en el ciberespacio. Es la base y fundamento de la ciberdefensa nacional que también puede apoyarse en otros poderes estatales (político, económico, diplomático, etc.) cuando la ocasión lo requiera. Comprende actividades defensivas, de inteligencia y ofensivas.

Ciberdefensa y disciplinas asociadas

195. El concepto de ciberdefensa es, a menudo, malinterpretado y confundido con o asimilado a otras disciplinas que tienen áreas de solape con ella y esto dificulta la definición, desarrollo y evolución de la ciberfuerza y su integración fluida y eficaz en las fuerzas armadas y en la ciberdefensa nacional.

196. Las disciplinas especialmente asociadas con la ciberdefensa son las *ciberoperaciones, las operaciones sobre redes TIC (CNO[27]), la ciberseguridad, las operaciones de información, la guerra electrónica, las operaciones psicológicas y la comunicación estratégica.* La mejor manera de diferenciar estos conceptos es fijarse en el objeto que las mueve.

197. Las *ciberoperaciones* se centran, fundamentalmente, en la misión; en causar unos efectos que faciliten los objetivos de la misión. La ciberdefensa es un concepto más amplio que incluye a las ciberoperaciones, como eje central, junto con todas las capacidades de mando, técnicas, logísticas y administrativas necesarias para la planificación y conducción de ellas.

198. Las *operaciones en redes* (CNO, Computer Network Operations) es un concepto en desuso que se puede asimilar a las ciberoperaciones, pero enfocadas, exclusivamente, en los ciberefectos, no considerando los efectos físicos a personas o instalaciones.

199. La *ciberseguridad* se centra en la protección y recuperación de los sistemas TIC propios.

200. Las *operaciones de información* se centran en la información, fundamentalmente en conseguir la superioridad de la información y la influencia. Uno de los objetivos de la ciberdefensa es proteger la información propia y afectar a la del adversario, pero la ciberdefensa tiene muchos más objetivos.

201. La *guerra electrónica* se enfoca exclusivamente en el espectro electromagnético, en cualquier actividad que implique el uso del espectro electromagnético o la energía dirigida para controlar el espectro, atacar a un adversario o protegerse frente a ataques a través del espectro.

202. Las *operaciones psicológicas* se centran en las personas y son, en muchas ocasiones, de gran ayuda y apoyo en la conducción de ciberoperaciones.

203. La *comunicación estratégica* se centra en la comunicación y, evidentemente, el ciberespacio es posiblemente el medio más idóneo para gestionar la comunicación, pero no el único.

204. Todas estas disciplinas asociadas tienen aspectos que encajan en o sirven de apoyo a la ciberdefensa, aunque usando medios y cualificación profesional diferente, por ello es necesario considerarlas en la ciberdefensa y establecer unas líneas de coordinación y colaboración.

205. La ciberdefensa es una disciplina especializada en el uso del ciberespacio y por ello puede servir de gran ayuda para logar los objetivos de las disciplinas asociadas y, viceversa, las disciplinas asociadas pueden ser de gran ayuda a la ciberdefensa.

ILUSTRACIÓN 21.
CIBERDEFENSA Y DISCIPLINAS ASOCIADAS

Ciberoperaciones

206. Las *ciberoperaciones* son acciones militares planificadas, organizadas, coordinadas y llevadas a cabo por unidades de ciberdefensa con la finalidad de lograr efectos en el ciberespacio, así como en los otros ámbitos de operaciones.

207. Se distinguen seis tipos de ciberoperaciones, de acuerdo a su naturaleza, objetivo y entorno en donde se desarrollan: defensivas pasivas, defensivas activas, de explotación pasivas, de explotación activas, de respuesta y ofensivas.

208. Las *ciberoperaciones defensivas* pasivas son aquellas ciberoperaciones ejecutadas en las redes propias, orientadas exclusivamente a la prevención, protección y resiliencia del ciberespacio propio. No se toman acciones específicas contra un adversario o un tercero.

209. Las *ciberoperaciones defensivas activas* son aquellas ciberoperaciones intrusivas u ofensivas (hacking ético, test de penetración, etc.) ejecutadas en las redes propias, autorizadas por los responsables de las redes, orientadas a la búsqueda de vulnerabilidades y riesgos y a la evaluación del estado de seguridad del ciberespacio propio.

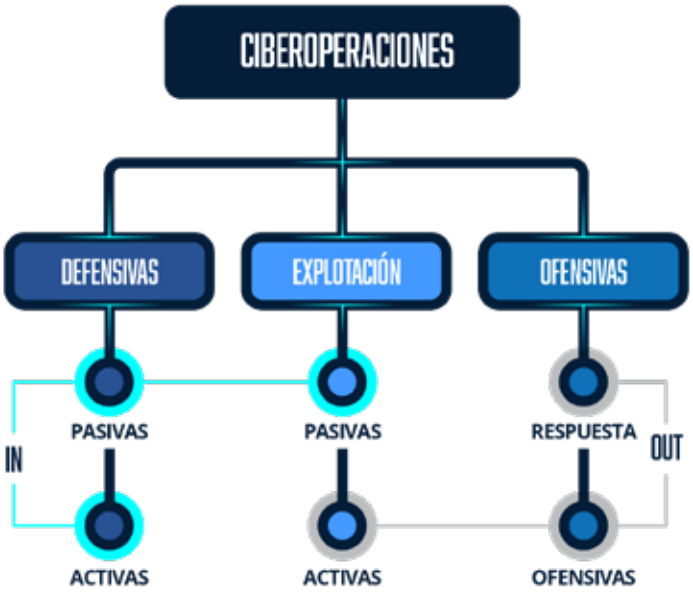


ILUSTRACIÓN 22. CIBEROPERACIONES

210. Las *ciberoperaciones de explotación pasivas* son aquellas ciberoperaciones no intrusivas, ejecutadas en las redes propias o redes públicas abiertas, orientadas a la obtención de la información necesaria para la planificación y conducción de ciberoperaciones defensivas y ofensivas u otras operaciones convencionales.

211. Las *ciberoperaciones de explotación activas* son ciberoperaciones intrusivas, ejecutadas en las redes de adversarios o de terceros, orientadas a la obtención de la información necesaria para la planificación y conducción de ciberoperaciones defensivas y ofensivas u otras operaciones convencionales.

212. Las *ciberoperaciones de respuesta* son aquellas ciberoperaciones ofensivas, ejecutadas en las redes de adversarios o de terceros, con la finalidad prevenir, anticipar o reaccionar ante ciberataques a las redes propias.

213. Dependiendo del momento en el que se ejecutan en relación con las intenciones del adversario, las ciberoperaciones de respuesta pueden ser de tres tipos, preventivas, anticipativas y reactivas.

ILUSTRACIÓN 23.
CIBEROPERACIONES DE RESPUESTA

214. Las *ciberoperaciones preventivas* de respuesta son aquellas ciberoperaciones ofensivas dirigidas contra un adversario para evitar un ciberataque que, por la información obtenida de la inteligencia propia o de aliados, se tiene constancia que está planeado y va a ocurrir en un futuro próximo indeterminado.

215. Las *ciberoperaciones anticipativas* de respuesta son aquellas ciberoperaciones ofensivas dirigidas contra un adversario para evitar un ciberataque que, por la información obtenida de la inteligencia propia o de aliados, se considera inminente.

216. Las *ciberoperaciones reactivas* de respuesta son aquellas ciberoperaciones ofensivas dirigidas contra un adversario para repeler un ciberataque en curso.

217. Algunos estudios contemporáneos equiparan los ataques preventivos con la agresión, y por tanto los califican de ilegítimos. Mientras que otros estudios consideran que cuando un supuesto adversario parece comenzar los preparativos confirmables para un posible ataque en un futuro próximo se puede considerar que el ataque de hecho ya ha comenzado.

218. Las *ciberoperaciones ofensivas* son aquellas ejecutadas, en el marco de un conflicto declarado, en las redes de adversarios o de terceros con la finalidad de causar un ciberefecto o un efecto físico.

219. Las *ciberoperaciones de falsa bandera* son aquellas ciberoperaciones ofensivas que se ejecutan de manera encubierta con la intención de culpabilizar a un tercero.

FUERZA CIBERESPACIAL

220. Las fuerzas armadas de un país para poder cumplir su misión de proteger los intereses nacionales deben de tener la capacidad de hacer frente a la amenaza allá donde se produzca, en tierra, mar, aire, espacio o ciberespacio. Para ello deben de disponer de unas capacidades militares idóneas para combatir en todos los ámbitos de operaciones, adaptadas a la naturaleza del ámbito, formadas y preparadas para ser usadas en el momento y lugar que se necesiten y organizadas adecuadamente para efectuar sus actividades, funciones y operaciones en coordinación con los otros ámbitos.

221. La *fuerza ciberespacial* es el conjunto de unidades de las fuerzas armadas, organizadas bajo un mismo mandó único, responsables del planeamiento y la conducción de las operaciones militares en el ciberespacio.

222. El escenario estratégico global actual incluye la ciberamenaza no solo como una amenaza más presente en cualquier conflicto declarado sino, además, como una amenaza persistente presente también en tiempo de paz o en conflictos no declarados. Por esta razón las fuerzas armadas deben disponer de una fuerza ciberespacial que esté diseñada, organizada y preparada no solo para ser activadas en momentos puntuales en caso de conflicto sino para estar en actividad permanente de combate; lo que imprime a la fuerza ciberespacial una relevancia especial y diferenciadora de la fuerza terrestre, marítima y área.

223. Desarrollar una fuerza para su empleo eficaz en un entorno emergente cuyo nivel de madurez doctrinal es muy bajo requiere una *planificación* cuidadosa, compleja y flexible; un *marco legal* que avale sus misiones y cometidos, una *doctrina* que sirva de referencia para su organización, preparación y empleo, una *organización* adaptada a sus funciones y cometidos, un *personal* especializado, una *formación* continua, unas *capacidades de mando, operativas y técnicas* adecuadas para el combate en el ciberespacio, unas *instalaciones* seguras especialmente adaptadas a los cometidos de la ciberfuerza y todo ello subordinado a un *mando único* que garantice la máxima eficacia y eficiencia.

224. Los términos "ciberfuerza" y "fuerza ciberespacial" son equivalentes y se pueden usar indistintamente; no obstante, se emplea, preferentemente, el término "*fuerza ciberespacial*" cuando nos referimos al conjunto de unidades de ciberdefensa de las fuerzas armadas agrupadas bajo un mismo mando (a imagen y semejanza de los términos fuerza terrestre, fuerza naval y fuerza aérea) y, preferentemente, el término "*ciberfuerza*" cuando nos referimos, de manera genérica, a una unidad militar de ciberdefensa o a la capacidad de desarrollar acciones ofensivas en el ciberespacio.

Planificación del desarrollo

225. La *planificación para el desarrollo de una fuerza ciberespacial* debe ser realizada con cuidado y cautela ya que la falta de conocimiento y experiencia del entorno puede llevar a decisiones erróneas que una vez establecidas y consolidadas pueden ser muy difíciles de erradicar o modificar; por ello debe tomarse en consideración lecciones aprendidas de otros países y adaptarlas a las circunstancias nacionales.

226. En la planificación hay que considerar todos los aspectos (político, orgánico, operativo, técnico, logístico, administrativo y jurídico) de una manera *integral* ya que las decisiones sobre un aspecto pueden afectar a otros aspectos.

227. La planificación debe ser *flexible* porque la falta de madurez del nuevo entorno obliga a tomar decisiones de compromiso que una vez establecidas se descubren como poco idóneas; por ello, la propia planificación tiene que tener previsto mecanismos que faciliten cambios de dirección, procedimientos y objetivos.

228. Cuando se desarrolla una fuerza para su empleo en un entorno en estado de madurez incipiente no se debe considerar definitiva la primera planificación, sino que el desarrollo debe realzarse a través de un *proceso cíclico*, de tal manera que después de implementarse las acciones derivadas del plan se realice una evaluación para valorar la alineación con los objetivos prefijados y de acuerdo a esta valoración se modifique la planificación acordemente e iniciar el ciclo de nuevo.

229. En los primeros años de creación de la fuerza ciberespacial se pueden establecer *planes de desarrollo* anuales o bienales que detallen objetivos estratégicos, líneas de acción y recursos para lograr los objetivos. Una vez que se haya consolidado se pueden establecer planes de desarrollo de mayor duración, aunque dada la naturaleza dinámica del ciberespacio no es conveniente establecer planes de desarrollo con una duración mayor a cinco años.

Marco legal

230. Para garantizar la legitimidad de las misiones, responsabilidades, cometidos, actividades y acciones de la fuerza ciberespacial, su creación deber ser amparada por una norma legal del más alto rango posible, no menor de orden ministerial.

231. La norma debe incluir, como mínimo, el ámbito de actuación, la misión, los cometidos, la organización y la dependencia de la fuerza ciberespacial.

Doctrina

232. Las fuerzas armadas disponen de un *marco doctrinal tradicional* que establecen los principios, conceptos y directrices fundamentales para su organización, preparación y empleo en los ámbitos de tierra, mar y aire, así como en el ámbito conjunto. La fuerza ciberespacial como parte de las fuerzas armadas precisa también de una doctrina específica que guie su organización, preparación y empleo en el ciberespacio.

233. Debido a la naturaleza dinámica del ciberespacio y al bajo nivel de madurez del ámbito de operaciones ciberespacial, la *doctrina del empleo de la fuerza ciberespacial* podría requerir revisiones y modificaciones con más periodicidad que las doctrinas tradicionales y las directrices en ella establecidas podrían requerir un grado mayor de flexibilidad.

234. El ciberespacio es *transversal* al resto de ámbitos de operaciones estando presente en ellos e influyendo en su acción, por ello es necesario también que las capacidades de ciberdefensa sean consideradas en las doctrinas de los ámbitos convencionales, así como en la de doctrina conjunta.

235. La doctrina es necesaria para establecer criterios, referencias, principios y procedimientos relativos a todos los aspectos operativos de la ciberdefensa tanto a nivel interno de la fuerza ciberespacial como a nivel de las fuerzas armadas y a nivel nacional e internacional.

236. La doctrina ha de entenderse como un *conjunto completo* de documentos que faciliten la organización, preparación y empleo de las fuerzas armadas en el ciberespacio. Este conjunto debe incluir como mínimo, la visión sobre la ciberdefensa militar por parte de la más alta autoridad de las fuerzas armadas, el concepto de ciberdefensa, la doctrina de empleo de la fuerza ciberespacial, los procedimientos operativos de cada tipo de ciberoperación, las instrucciones

técnicas, guías, recomendaciones y buenas prácticas de las actividades de ciberdefensa y la integración de la ciberdefensa en otras doctrinas consolidadas.

237. Organizaciones de defensa colectiva de referencia internacional, como la OTAN, tienen una responsabilidad significativa en la elaboración de doctrina que sirve de referencia a las naciones de su entorno. No obstante, el nivel de madurez de la OTAN en relación con la doctrina de ciberdefensa es insuficiente para las necesidades actuales, lo que obliga a las naciones a generar su propia doctrina, lo cual podría llevar, en un futuro, a la convivencia de dotrinas con diferente enfoque que dificultaría la cooperación multinacional e internacional en ciberdefensa.

238. La propia fuerza ciberespacial debe impulsar la elaboración de la doctrina específica de ciberdefensa necesaria para la eficacia de su funcionamiento y para el necesario entendimiento de la ciberdefensa por parte de otros actores implicados eliminando zonas de conflicto o incertidumbre.

Organización

239. La forma tradicional de organizar las capacidades militares para combatir en un determinado ámbito de operaciones convencional es a través de una unidad superior que aglutina todas las capacidades específicas de cada ámbito, esto es, el ejército de tierra, la armada y el ejército del aire. El *ejército*, a su vez, se divide en tres elementos principales: el estado mayor, encargado del asesoramiento al mando y el planeamiento de las operaciones; la fuerza, encargada de ejecutar las operaciones y el apoyo a la fuerza, encargada de prestar todo el auxilio (operativo, logístico y técnico) necesario para llevar a cabo las operaciones.

240. Cuando se crea una unidad de ciberdefensa por primera vez, la falta de doctrina consolidada del ámbito ciberespacial y la reducida dimensión de la unidad (la creación de unidades nuevas suele empezarse por unidades pequeñas) hace que se tienda a incluirla en la orgánica de otro ámbito ya establecido. Esto, a la larga, crea confusión y malos entendidos, llegando a considerar las unidades de ciberdefensa como unas unidades que llevan a cabo una función más (ciberdefensa) dentro de los ámbitos de tierra, mar y aire, como cualquier otra de las funciones tradicionales (mando y control, inteligencia, maniobra, fuegos, información, cooperación cívico-militar, protección y apoyo logístico) y obviar su verdadera naturaleza de fuerza responsable de las acciones militares en todo un completo ámbito de operaciones, el ciberespacio. Por ello, es aconsejable, independientemente del tamaño de la unidad, centralizar todas las unidades de ciberdefensa en una unidad superior a modo de ejército (*ciberejército*) articulado en sus tres elementos principales (estado mayor, fuerza y apoyo a la fuerza) lo cual facilitará la evolución natural de la fuerza ciberespacial.

ILUSTRACIÓN 24. FUERZA CIBERESPACIAL

241. El grado de *conocimientos* técnicos que precisa el personal de la fuerza ciberespacial es elevado, pero esto, no es exclusivo de ella, también en otros ámbitos esto es

una realidad. No obstante, la plantilla orgánica militar (parte superficial del iceberg) debe orientarse, predominantemente, a responsabilidades de mando, organización, gestión y coordinación que requieren un conocimiento fundamentalmente operativo y dejar las responsabilidades de carácter más técnico a los organismos asociados (parte sumergida del iceberg) como consultoras públicas y privadas, servicios profesionales de empresas del sector de ciberseguridad y TIC y sector académico.

242. Estos organismos asociados deben de sentirse parte de la fuerza ciberespacial también y para ello hay que definir las estructuras orgánicas, los acuerdos de colaboración y los contratos que faciliten esta fidelización.

Personal

243. El personal de ciberdefensa debe considerarse como *crítico, operativo, permanente, de dedicación exclusiva y de larga amortización.* Además, se debe prestar especial atención, por su gran potencial, a la reserva voluntaria en el campo de la ciberdefensa.

244. El personal de ciberdefensa es un *recurso crítico*. La base técnica del conocimiento que requiere las tareas de ciberdefensa es de utilidad también en muchas actividades del sector privado. Una parte significativa del personal clave de ciberdefensa, una vez adquirido un nivel de experiencia y conocimientos elevado, va a ser tentado para abandonar las fuerzas armadas e incorporarse a un puesto mejor remunerado en el sector privado.

245. La probable salida de parte del personal más experto obliga a las unidades de ciberdefensa a ser extremadamente cuidadosas y vigilantes con el conocimiento, garantizando que quede siempre documentado y compartido, de tal manera que, si no se puede evitar la fuga de talentos, al menos hay que *evitar la fuga de conocimiento*.

246. El personal de ciberdefensa debe tener, a todos los efectos, la consideración de *personal combatiente*. Todas las tareas y responsabilidades relacionadas con las ciberoperaciones en sus tres facetas, defensivas, de explotación y ofensivas, son acciones de combate, a imagen y semejanza de las acciones defensivas, de explotación y ofensivas en los otros ámbitos.

247. La ciberamenaza actúa no solo en periodos de conflicto declarado sino, también, en tiempo de paz y de conflictos no declarados; si a esto añadimos que los ciberataques proceden de cualquier parte del mundo esto significa que no se puede considerar una disminución de la actividad debido a husos horarios, jornadas laborales o periodos de noche o vacaciones, obligando a disponer de una capacidad para hacer frente a una actividad durante las 24 horas del día, los siete días de la semana y los 365 días del año; por lo que las responsabilidades del personal de ciberdefensa se deben organizar en base a un *servicio permanente* (24x7x365).

248. El personal de ciberdefensa debe considerarse de *dedicación exclusiva*. La ciberdefensa es una disciplina de una gran complejidad técnica y operativa, que se relaciona con un ámbito de operaciones, por lo tanto, el personal de ciberdefensa debe permanecer toda su carrera militar en el ámbito ciberespacial para garantizar su eficacia, de la misma forma que el personal del ámbito terrestre, naval o aéreo. Debe evitarse por todos los medios considerar al personal de ciberdefensa como un personal de otros ámbitos (tierra, mar y aire) que con algún tipo de formación pueda ejercer responsabilidades temporales de ciberdefensa.

249. El personal de ciberdefensa es de *larga amortización*. El personal de ciberdefensa precisa, para alcanzar el nivel de operatividad requerido por su puesto, de unos conocimientos operativos y técnicos elevados que se adquieren a través de una inversión cuantiosa en

formación y tiempo. Por ello, para amortizar lo invertido y poder sacar un rendimiento óptimo del personal, los puestos de ciberdefensa se deben definir de tal manera que garanticen una ocupación mínima de cinco años.

250. Un *reservista voluntario* es un ciudadano que desea aportar, de forma voluntaria y temporal, sus capacidades y conocimientos, en las diferentes misiones que llevan a cabo las fuerzas armadas. Esta aportación se materializa mediante la adquisición de un vínculo con el ministerio de defensa firmando un compromiso que conlleva un determinado tiempo de activación en unidades militares.

251. En los ámbitos tradicionales de tierra, mar y aire, habitualmente, los reservistas voluntarios desempeñan su actividad en las instalaciones de la unidad asignada, por un tiempo limitado continuo al año (normalmente entre 1 y 3 meses) y son las propias unidades las que dotan al reservista del uniforme, material y armamento necesario para el desempeño de la actividad asignada.

252. El ciberespacio goza de unas peculiaridades que lo convierten en idóneo para que la reserva pueda ser de mayor utilidad que en los otros ámbitos, pero para ello es necesario pasar de un modelo presencial a un *modelo online de ciberreserva* que maximice las características del ciberespacio y la ciberdefensa para ganar en eficacia, eficiencia, agilizar la activación, mejorar las prestaciones del personal reservista y aligerar la carga logística y administrativa de las unidades receptoras.

253. El modelo online de ciberreserva goza de las siguientes ventajas:

- El ciberreservista no tiene, necesariamente, que desempeñar su actividad en las instalaciones de la unidad asignada, pudiendo acogerse al *teletrabajo* desde su casa o lugar de trabajo.
- El ciberreservista puede desempeñar su trabajo con sus *propios medios*, sin necesidad del uso de un uniforme y medios oficiales, liberando así a la unidad de la dotación reglamentaria.
- La unidad puede acordar con el ciberreservista unas tareas y unos plazos de *tiempo* determinados, siendo el propio ciberreservista quien elija los momentos de desempeño.
- El ciberreservista puede ser asignado, por el organismo de ciberreserva del ministerio, a un *proyecto* determinado (en base a su experiencia profesional) y no una unidad.

254. No obstante, a pesar de que el proceso se base en un modelo online no se debe olvidar el *vínculo físico* con la unidad y se deben realizar también, actividades de corta duración (reuniones, actos, eventos, ejercicios, etc.) que precisen de la presencia física del reservista en las instalaciones de la unidad y el contacto físico con sus compañeros para conseguir una mejor fidelización con la unidad.

255. Las actividades y tareas asignadas deben ser cuidadosamente seleccionadas de tal manera que sean percibidas por el reservista como una *contribución a la Defensa Nacional*.

Formación

256. Para hacer frente a la complejidad de las actividades relacionadas con la ciberdefensa y a la rápida evolución tecnológica asociada con ella, el personal de la fuerza ciberespacial debe recibir una formación especial y permanente.

257. La formación en ciberdefensa se basa en una actividad periódica, de *formación individual, adiestramiento colectivo de las unidades de ciberdefensa y concienciación* a todos los niveles (personal de ciberdefensa, usuarios finales y autoridades), definida y desarrollada mediante programas específicos de carácter anual y basados en las necesidades formativas de cada puesto y unidad.

258. La *formación individual* se dirige a todos los individuos pertenecientes de las unidades de la fuerza ciberespacial con la finalidad de proporcionarles los conocimientos adecuados que les capaciten para realizar con eficacia las tareas asignadas a su puesto.

259. La fuerza ciberespacial debe definir la *ruta formativa* de cada puesto, en la que se establezca el grado de conocimiento y certificación de acceso (nivel requerido para poder ser asignado a un puesto) y los diferentes grados de conocimiento y certificación de perfeccionamiento (nivel que indica el grado de preparación, "combat ready") que debe ir alcanzando en un periodo de tiempo determinado.

260. La fuerza ciberespacial debe estudiar el porcentaje de tiempo que cada individuo debe dedicar a formación regulada durante su jornada laboral. Dependiendo del tipo actividad que se desempeñe en cada puesto, el porcentaje de tiempo dedicado a formación es diferente, pero se puede tomar como ejemplo una horquilla de 20-60, es decir, todo el personal de ciberdefensa debe dedicar, al menos un veinte por ciento de su tiempo a formación y nadie puede superar un sesenta por ciento. En periodos puntuales estos márgenes pueden ser superados, pero al final de un cómputo global (generalmente relacionado con la duración del plan de desarrollo, anual, bienal o quinquenal) los márgenes deben permanecer estables.

261. El *programa de formación individual* debe detallar, por cada puesto de la fuerza ciberespacial, la ruta formativa considerando todos los aspectos (operativos, técnicos y administrativos) y todos los niveles (táctico, operacional, estratégico y político) y debe reservar los recursos necesarios para su materialización. Además, debe definir los criterios de evaluación y certificación asociados a cada puesto.

262. El *adiestramiento colectivo* se dirige a las unidades y subunidades de ciberdefensa con la finalidad de formar y practicar el uso compartido, coordinado y organizado de capacidades individuales diferentes y complementarias para la consecución de un mismo efecto u objetivo.

263. Los *ciberejercicios* es una práctica habitual, tanto a nivel interno de la propia unidad como a nivel nacional e internacional. Los ciberejercicios tienen dos finalidades fundamentales, adiestrar a los individuos en tareas colectivas y evaluar y, en su caso, certificar el grado de preparación de las unidades.

264. Hay que destacar que las dos finalidades, *adiestramiento y evaluación* son, a menudo, incompatibles; es decir la audiencia objetivo de un ciberejercicio orientado al adiestramiento debe estar compuesta por aquellos individuos (no expertos) idóneos para aprender y sacar rendimiento a las prácticas; mientras que la audiencia objetivo de un ciberejercicio orientado a la evaluación y certificación debe estar compuesta por la plantilla regular de la unidad a evaluar.

265. El *programa de adiestramiento colectivo* comprende ciberejercicios, de carácter técnico y procedimental, a todos los niveles de mando, en todas sus facetas (defensiva, explotación y ofensiva) para todas las unidades de ciberdefensa; y la definición de los criterios de evaluación y certificación asociados a cada unidad.

266. El programa de adiestramiento colectivo debe considerar, además, la integración de la ciberdefensa en ejercicios militares conjuntos y de otros ámbitos y debe prever y fomentar la participación en ciberejercicios de nivel nacional e internacional.

267. Los ciberejercicios más habituales son los *técnico-defensivos, los técnico-ofensivos y los procedimentales*.

268. Los *ciberejercicios técnico-defensivos* se orientan al adiestramiento en técnicas defensivas frente a ciberataques complejos en tiempo real; a la adquisición de experiencias que no se suelen adquirir en el trabajo habitual; a la evaluación o comparación de unidades; al testeo de nuevas tecnologías; a la coordinación y cooperación entre unidades de diferente procedencia (por ejemplo equipos de la fuerza espacial, de los ejércitos, de los cuerpos de seguridad del estado, de protección de infraestructuras críticas, etc.) y a la captura de talento. Se desarrollan en un campo de maniobras ciberespacial, en el cual se configuran redes y sistemas reales y se aplican técnicas y herramientas reales; y todo ello enmarcado en situaciones y escenarios ficticios basados en casos reales probables.

269. La organización más habitual de un ejercicio técnico-defensivo se basa en modelo de cinco tipos de equipos: *equipo blanco, equipo verde, equipo amarillo, equipo rojo y varios equipos azules.*

270. El *equipo blanco* se encarga de la dirección y gestión del ciberejercicio, de la panificación e introducción en el sistema de las situaciones y acciones concretas (injects), de la evaluación, valoración y clasificación de los participantes, de las comunicaciones entre los equipos, de la recepción y valoración de los informes de los equipos azul y rojo y de la simulación de usuarios y medios de comunicación.

271. El *equipo verde* se encarga del diseño e implementación de la infraestructura TIC del ciberejercicio y la gestión del campo de maniobras.

272. El *equipo amarillo* se encarga de elaborar y distribuir apropiadamente la conciencia de la situación ciberespacial.

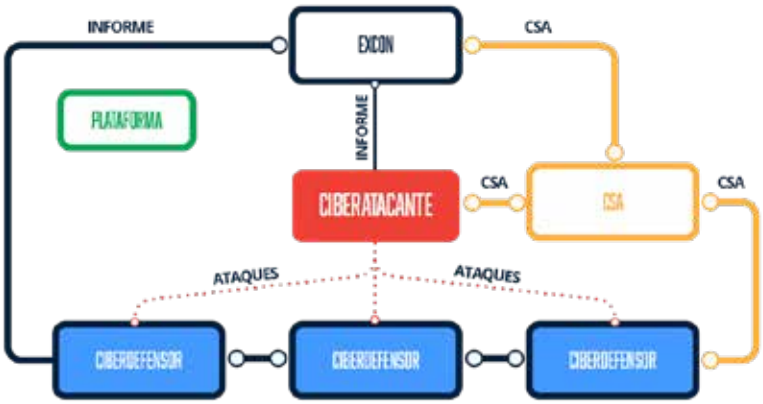


ILUSTRACIÓN 25. CIBEREJERCICIO

273. El *equipo rojo* se encarga de planificar y ejecutar los ciberataques a los equipos azules y de proveer datos al equipo amarillo para la elaboración de la CSA En aquellos ciberejercicios en los que se valoren, clasifiquen o comparen a los diferentes equipos azules, los ciberataques deben ser planificados de tal manera que cada equipo azul reciba ciberataques en la misma cantidad y tiempo y de igual tipo y complejidad.

274. El *equipo azul* es la audiencia objetivo; se encarga de planificar y ejecutar la defensa frente a los ciberataques del equipo rojo, coordinar y cooperar con otros equipos azules, proveer datos al equipo amarillo para la elaboración de la CSA y elaborar los informes y documentos que correspondan (técnicos, legales, forense, medios de comunicación, etc.).

275. En organizaciones pequeñas que no se pueden permitir un ciberejercicio completo con cinco equipos, pueden optar por el desarrollo de un *modelo azul-rojo-morado* (ciberejercicio sencillo en el que participan un equipo rojo, un equipo azul y un equipo morado que se encarga de forzar y facilitar la cooperación entre el equipo rojo y el azul) o por un *modelo*

morado (un mismo equipo realiza las funciones del equipo rojo y azul). Estos modelos no son propiamente ciberejercicios ya que su finalidad no es el adiestramiento sino el análisis y la valoración del estado de ciberseguridad de la organización.

276. Los *ciberejercicios técnico-ofensivos* se orientan al adiestramiento en técnicas ofensivas frente a defensas robustas y dinámicas; a la adquisición de experiencias que no se suelen adquirir en el trabajo habitual; al testeo de nuevas tecnologías y a la captura de talento. Se desarrollan en un campo de maniobras ciberespacial, en el cual se configuran redes y sistemas reales y se aplican técnicas y herramientas reales; y todo ello enmarcado en situaciones y escenarios ficticios basados en casos reales probables.

277. Los *ciberejercicios procedimentales* se dirigen, fundamentalmente, a concienciar y adiestrar en la toma de decisiones de altas autoridades; a la coordinación y colaboración de organismos responsables de la ciberseguridad nacional y gestión de crisis; y a la validación y verificación de la eficacia de los procedimientos y normas. Se desarrollan mediante debates donde los miembros de los diferentes equipos discuten sus roles y responsabilidades durante situaciones de crisis, con la ayuda de un facilitador que guía a los participantes a través de uno o varios escenarios o casos.

278. Las actividades de *concienciación* se dirigen a tres tipos de audiencias, audiencia directiva (autoridades y personal que maneja información sensible y de especial interés para las ciberamenazas), audiencia general (usuarios finales de sistemas de información) y audiencia específica (personal de ciberdefensa) con la finalidad de alertar sobre ciberamenazas y ciberriesgos y fomentar un comportamiento responsable en el ciberespacio.

279. Una concienciación eficaz debe considerar cuatro aspectos, el mensaje, la retención del mensaje, la aplicación de las medidas y la valoración del grado de cumplimiento.

280. El *mensaje* debe ser claro, adecuado a la audiencia objetivo y debe de poder ser distribuido de manera sencilla a cada individuo de la audiencia objetivo.

281. El mensaje debe ser diseñado de tal manera que una vez llegue al destinatario, este sea capaz de asimilarlo, comprender la utilidad para la organización, entender cómo ponerlo en práctica y recordar los momentos y las situaciones que requieren ponerlo en práctica.

282. El *programa de concienciación* debe dirigirse de manera diferenciada a los tres tipos principales de audiencia (directiva, general y específica), debe definir los mecanismos para la monitorización y valoración del grado de cumplimiento de las medidas de concienciación y establecer los criterios de medición de la eficacia de las medidas implementadas.

Capacidades de mando

283. La fuerza ciberespacial debe disponer de unas capacidades orientadas a facilitar la toma de decisiones; como el *planeamiento y asesoramiento, cooperación, representación, gestión del conocimiento, lecciones aprendidas, servicio financiero y servicio jurídico.*

Planeamiento y asesoramiento

284. Como en toda unidad militar, la fuerza ciberespacial debe disponer de un grupo de personal experto en los aspectos operativos fundamentales de la ciberdefensa (personal, inteligencia,

operaciones, logística, planes, sistemas TIC, formación, recursos y finanzas, influencia y cooperación) agrupados en un estado mayor o cuartel general. Este *estado mayor* tiene la responsabilidad de asesorar al mando para facilitar su toma de decisiones, planear todas las actividades relacionadas con los aspectos operativos fundamentales y distribuir y vigilar el cumplimiento de los planes, directrices y órdenes del comandante.

285. El estado mayor debe desarrollar los *planes específicos para cada operación,* así como el *plan de desarrollo* de la unidad, el *plan de continuidad de las operaciones,* el *plan de comunicaciones* y todos los *planes sectoriales* necesarios (formación, adiestramiento y concienciación; captación, reclutamiento, motivación y fidelización; financiero y obtención de recursos; obtención de inteligencia, cooperación, etc.)

286. El *planeamiento de las ciberoperaciones* se debe realizar siguiendo la metodología estándar de planeamiento militar para facilitar el apoyo a operaciones de otros ámbitos y el apoyo y la integración en operaciones conjuntas y combinadas.

287. El *plan de desarrollo* es el plan principal de la unidad. En él, el comandante de la fuerza ciberespacial establece el propósito (la razón permanente de la existencia de la unidad), la misión (el objetivo principal a alcanzar durante el tiempo que dura el plan) y la visión estratégica de la unidad (el modo y condiciones para alcanzar la misión); además de todos los detalles necesarios para conseguir la intención del comandante, como los objetivos específicos, las líneas de acción, los recursos, los roles y responsabilidades y los plazos de tiempo esperados.

288. En los periodos de inmadurez de la unidad, cuando todavía no se ha alcanzado la capacidad operativa final (FOC), el pan de desarrollo debe ser de corta duración (anual o bienal). Una vez alcanzada la FOC lo habitual es que el plan de desarrollo dure 4 o 5 años. Se pueden considerar tres FOCs diferentes a alcanzar de manera progresiva (primero, la FOC de defensa, a continuación, la FOC de explotación y finalmente, la FOC de respuesta) para administrar eficientemente los recursos limitados.

289. El plan de desarrollo es el documento fundamental de la fuerza ciberespacial, es la referencia y guía que orienta todas las actividades, tareas, responsabilidades y cometidos y es la forma más eficaz de cohesionar al personal, converger esfuerzos y alinear resultados.

290. El *plan de continuidad de las operaciones* contiene las medidas técnicas, humanas, procedimentales y organizativas para recuperar y restaurar las funciones críticas inutilizadas o interrumpidas a causa de un ciberataque.

291. El proceso habitual para la elaboración de un plan de continuidad se basa en tres fases: *identificación de la amenaza, identificación de las funciones críticas y definición de las medidas de ciberdefensa.*

292. En la fase de *identificación de las ciberamenazas* se analizan los cuatros casos generales (amenaza y respuesta conocidas; amenaza conocida y respuesta desconocida; amenaza desconocida y respuesta conocida; y amenaza y respuesta desconocidas) y se identifican y clasifican las amenazas más probables y las más peligrosas.

293. En el caso de *amenaza y respuesta conocidas,* se conocen las medidas de ciberdefensa necesarias para hacer frente a una ciberamenaza concreta de la cual se sabe su forma de actuar y sus potenciales impactos.

294. En el caso de *amenaza conocida y respuesta desconocida,* se conoce la forma de actuar de la ciberamenaza y sus potenciales impactos, pero no se conocen las medidas de ciberdefensa idóneas para hacer frente a ellas. Es necesario experimentar posibles soluciones y establecer colaboraciones con organismos que puedan disponer de soluciones.

295. En el caso de *amenaza desconocida y respuesta conocida* se analizan situaciones de contingencia previendo probables impactos cuyas medidas para recuperarse de ellos son conocidas, pero se desconocen las causas que los producen.

296. En el caso de *amenaza y respuesta desconocidas* se establece un mecanismo para organizar, de manera expeditiva, un grupo de expertos que puedan aconsejar en tiempo real sobre las medidas de reacción apropiadas ante situaciones totalmente imprevistas en las que se desconoce la forma de actuar de la amenaza y no se han previsto en el plan medidas de reacción.

297. En la fase de *identificación de funciones críticas* se identifican aquellas funciones, servicios, sistemas, etc. cuya interrupción, total o parcial, pueda derivar en una falta de operatividad inaceptable para la organización y hay que establecer criterios de medición del impacto (indicadores) que deben desencadenar una respuesta automática o humana.

298. En la fase de *definición de medidas de ciberdefensa* se describen todas las medidas de prevención (sistemas de respaldo de datos, COS de respaldo, etc.) y reacción necesarias para recuperarse de los impactos previstos, para reaccionar ante los impactos imprevistos y para prevenirse de amenazas desconocidas (caza de ciberamenazas).

299. El *plan de comunicaciones* establece la postura oficial de la fuerza ciberespacial en todas aquellas materias de especial sensibilidad (operaciones ofensivas, operaciones de inteligencia, organización, recursos, capacidades, misiones, etc.), identificando las situaciones en las que la información se puede hacer pública y como y quien puede llevar a cabo las comunicaciones.

300. El plan de comunicación, además, establece la forma, el modo y el organismo responsable de informar sobre incidentes en curso de especial gravedad.

Cooperación.

301. La *cooperación* en todas sus facetas, internacional, nacional, con el sector industrial y académico, con los ciudadanos y la cooperación interna dentro de la propia fuerza ciberespacial, es una actividad esencial para alcanzar y mantener una ciberdefensa sólida.

302. La *cooperación internacional* es de especial relevancia en la ciberdefensa debido al carácter ubicuo (ataques desde cualquier parte del mundo a través de redes secuestradas) y anónimo (sin firma reconocida) de los ciberataques haciendo necesaria la participación de otros países para la identificación del origen de la ciberamenaza y para la respuesta eficaz.

ILUSTRACIÓN 26. COOPERACIÓN

303. Para alcanzar una sólida cooperación internacional es necesario establecer acuerdos bilaterales con otras fuerzas ciberespaciales del entorno geoestratégico y participar activamente en la ciberdefensa colectiva de las alianzas internacionales de defensa.

304. Para alcanzar *acuerdos de cooperación bilaterales* eficaces es necesario, en primer lugar, crear entornos de confianza mutua que faciliten un intercambio equilibrado de información, de tal manera que ninguna parte se sienta en desventaja con respecto a la otra en cuanto a la cantidad y calidad de la información recibida respecto a la aportada.

305. La ciberdefensa militar constituye la capacidad principal a través del cual el gobierno de una nación implementa la ciberdefensa nacional como parte de la política de defensa, que en coordinación con el resto de instrumentos del poder nacional, contribuye a la seguridad nacional. Pero no siempre es evidente si una amenaza o un ciberataque son responsabilidad de la *ciberdefensa militar*, la *ciberdefensa* nacional o la ciberseguridad nacional. Por ejemplo, hacer frente a un ciberataque cuyo objetivo es la exfiltración de patentes y propiedad intelectual de la industria de defensa, podría ser considerado una responsabilidad de la fuerza ciberespacial o una responsabilidad de los cuerpos de seguridad del estado, dependiendo de si se prioriza como delito o como ataque a la defensa nacional.

306. La información y la inteligencia que la fuerza ciberespacial obtiene en el desempeño de sus funciones (monitorización, caza de ciberamenazas, ciberinteligencia) puede ser de utilidad para los organismos estatales responsables de la ciberseguridad nacional y viceversa. Por lo que la cooperación entre la fuerza ciberespacial, las unidades de ciberdelincuencia de los cuerpos de seguridad del estado, las unidades de ciberseguridad de otros ministerios, los servicios nacionales de inteligencia, las agencias nacionales de ciberseguridad, los centros de ciberseguridad de la infraestructura critica nacional y el gobierno es necesaria para, entre todos, logar el mayor nivel posible de *ciberseguridad nacional.*

307. El *sector industrial* es uno de los pilares principales para el desarrollo de tecnologías de utilidad para la ciberdefensa. Por ello la fuerza ciberespacial debe impulsar acuerdos de cooperación con las empresas para impulsar la investigación, innovación y desarrollo de tecnologías de ciberdefensa.

308. En muchos casos, podría ser suficiente la adquisición de productos comerciales adaptados a los requisitos operativos de la fuerza ciberespacial o la contratación de desarrollos o servicios a empresas comerciales (sector TIC, ciberseguridad, videojuegos, etc.). No obstante, para el desarrollo, sostenimiento y supervivencia de las capacidades críticas de la fuerza ciberespacial es imprescindible *evitar la dependencia* total de la industria comercial, siendo necesario establecer mecanismos que garanticen la continuidad de la operatividad de capacidades críticas de la fuerza ciberespacial, en los casos en los que la empresa proveedora quiebre o exija condiciones inaceptables.

309. Es necesario que se establezcan entornos o acuerdos específicos de *cooperación con la industria* que permita a la fuerza ciberespacial el acceso a la propiedad intelectual y a los conocimientos básicos de los productos, herramientas o sistemas críticos adquiridos, para que, en caso de desaparición o mala relación con la empresa proveedora la fuerza ciberespacial pueda seguir manteniendo su operatividad.

310. El *sector académico* es otro de los pilares para el desarrollo de tecnologías de utilidad para la ciberdefensa, por ello la fuerza ciberespacial debe impulsar acuerdos de cooperación con las universidades, centros de investigación y desarrollo, fundaciones y think-tanks que favorezcan la innovación y el desarrollo de tecnologías de ciberdefensa.

311. La *cooperación interna* es la cooperación establecida entre todos los organismos y unidades de la fuerza ciberespacial; entre las capacidades de mando, las operativas y las técnicas. Todas las unidades de la fuerza ciberespacial deben cooperar entre sí para lograr los objetivos estratégicos que el comandante fija a través del plan de desarrollo. Es la cooperación más necesaria, sin embargo, es a menudo, la más olvidada.

312. La cooperación interna es compleja debido a la necesidad de conciliar el intercambio de información entre unidades y la *confidencialidad* de ciertas actividades. Tanto la cooperación como la confidencialidad son dos aspectos fundamentales que deben ser considerados conjuntamente, estableciendo mecanismos que fomenten el intercambio de información dentro de entornos seguros. Se debe evitar, por todos los medios, que la confidencialidad sea utilizada como excusa para generar compartimientos estancos que no permiten el flujo de información entre las partes necesitadas.

Representación.

313. Existen numerosos foros de información y decisión, a nivel nacional e internacional, en los que se tratan y deciden asuntos de importancia e interés para la ciberdefensa. La fuerza ciberespacial debe identificar aquellos más relevantes y participar en ello de manera activa para conocer de primera mano la situación nacional o internacional de la ciberdefensa e influir en la toma de decisiones para encaminarlas, en la medida de lo posible, a sus objetivos estratégicos.

314. La fuerza ciberespacial debe hacer valer su rol de responsable principal de la ciberdefensa nacional para representar al país en asuntos de ciberdefensa en los foros internacionales y nacionales, por delante de otros implicados (agencias nacionales de seguridad, servicios de inteligencia, cuerpos de seguridad del estado, etc.) que tienen un papel de menor responsabilidad en la ciberdefensa nacional. Para ello, la diferencia entre los conceptos de ciberseguridad nacional y ciberdefensa nacional tienen que quedar explícitamente claros en todos los documentos de nivel nacional pertinentes, como la política de defensa nacional o la estrategia de ciberseguridad nacional.

Gestión del conocimiento

315. La *gestión del conocimiento* es una de las capacidades fundamentales para la operatividad de la fuerza ciberespacial; tiene la finalidad de distribuir el conocimiento entre las partes interesadas y facilitar su acceso de acuerdo a los criterios de necesidad y autorización.

316. La gestión del conocimiento es una capacidad basada en dos áreas, funcional y técnica; siendo el área funcional la parte fundamental y más compleja debido a que precisa de un planteamiento y procedimientos personalizados adaptados a las peculiaridades y necesidades de la unidad; mientras que la parte técnica se puede resolver mediante la utilización de herramientas y procedimientos comerciales de uso generalizado.

317. El *área funcional de la gestión del conocimiento* se encarga del análisis de las necesidades de intercambio y acceso a la información de todas las unidades de la fuerza ciberespacial, el diseño del mapa de flujos de información, la elaboración de los procedimientos y normas para el acceso a la información, la evaluación de la eficacia de los procedimientos y herramientas y la vigilancia del cumplimiento de las normas.

318. El *área técnica de la gestión del conocimiento* se encarga de la identificación, testeo, implementación, administración y sostenimiento de las herramientas informáticas de gestión e intercambio de información adecuadas para el desempeño eficaz de todas las tareas y actividades de la fuerza ciberespacial. Lo habitual es que esta área sea apoyada por unidades técnicas del apoyo a la fuerza.

319. La gestión del conocimiento es una disciplina de tal influencia en la operatividad de la fuerza ciberespacial y de tal complejidad que es necesario establecer una unidad específica responsable, con *cualificación especial y dedicación exclusiva,* dentro de la orgánica de la unidad (normalmente en el estado mayor de la fuerza ciberespacial, destacando así su carácter funcional sobre el técnico).

320. La gestión del conocimiento comprende cuatro grupos de actividades principales: *la gestión interna de la información, la gestión del intercambio de información con entidades externas, la elaboración y actualización del catálogo de expertos y la elaboración y actualización del catálogo de servicios críticos.*

321. La *gestión interna de la información* comprende el diseño, desarrollo, implementación, administración y sostenimiento de la conciencia de la situación ciberespacial (cyber situational awareness, CSA), de las bases de datos y thin-tank internos, de las plataformas internas de intercambio de vulnerabilidades y amenazas (MISP) y todo ello diferenciando información clasificada, sin clasificar y pública.

322. La *gestión externa de la información* se encarga del intercambio de información con los colaboradores de la fuerza ciberespacial (otras unidades de las fuerzas armadas, otros organismos del ministerio, organismos públicos, industria, sector académico, ciudadanos, fuerzas ciberespaciales de otras naciones, organizaciones de defensa colectiva asociadas, organizaciones internacionales de ciberseguridad, etc.) y de la gestión de la estrategia de la comunicación pública.

323. La *catalogación de expertos* es una actividad orientada a la identificación y clasificación de personas y empresas especialmente cualificadas en un área de conocimiento o tecnologías de especial interés y criticidad para la fuerza ciberespacial. El catálogo de expertos debe ser actualizado periódicamente incluyendo áreas de conocimiento y tecnologías emergentes, nuevos expertos y nuevos datos de contacto. Esta actividad tiene una relación estrecha con la unidad encargada de la gestión de la ciberreserva.

324. La *catalogación de servicios críticos* es una actividad orientada a la identificación y clasificación de servicios y sistemas de información críticos para la operatividad de la fuerza ciberespacial de acuerdo con los criterios establecidos, al efecto, por el comandante. Esta actividad tiene una relación estrecha con la unidad encargada de la gestión del plan de continuidad de las operaciones.

325. La gestión del conocimiento es una capacidad esencial de la fuerza ciberespacial; no obstante, a menudo no se le presta la atención debida; por ello, es muy importante que el comandante de la fuerza ciberespacial destaque explícitamente su importancia y necesidad (en particular del área funcional) y establezca los mecanismos y recursos necesarios para su diseño, desarrollo, implementación y sostenimiento en el plan de desarrollo de la unidad.

Análisis y lecciones aprendidas

326. La capacidad de *análisis y lecciones aprendidas* se basa en la implementación de un proceso sistemático con la finalidad de considerar, documentar, analizar y valorar las experiencias adquiridas en proyectos, actividades y situaciones pasadas que deben tenerse en cuenta activamente en futuros proyectos, actividades y situaciones similares, por los mismos o por nuevos actores.

327. Esta capacidad, a menudo olvidada o despreciada, es imprescindible para la fuerza ciberespacial dado el estado de madurez incipiente del ámbito de operaciones ciberespacial; ya que la falta de experiencia y conocimientos va a llevar a la fuerza ciberespacial, no en pocas ocasiones, a tomar decisiones con poco respaldo, que pudieran derivar en resultados erróneos, inapropiadas o poco eficaces y que deben ser evitados o modificados en situaciones similares futuras, o por el contrario, en resultados óptimos que deben ser considerados en situaciones similares futuras.

328. Esta capacidad debe ser apoyada especialmente por la capacidad de gestión del conocimiento, debe alimentar a los procesos de elaboración del cuerpo doctrinal de la ciberdefensa y debe servir al comandante de la fuerza ciberespacial para valorar la eficacia de la organización, medios y procedimientos implementados y su adecuación a los objetivos establecidos en el plan de desarrollo.

Servicio financiero

329. La fuerza ciberespacial necesita unos *recursos económicos ordinarios* que garanticen la obtención de las capacidades planeadas, su sostenimiento y su evolución.

330. La naturaleza dinámica del ciberespacio obliga al establecimiento de mecanismos ágiles de contratación y a una planificación financiera flexible; de lo contrario se corre el riesgo de colapsar los procesos de adquisición de nuevas capacidades.

331. La fuerza ciberespacial necesita, adicionalmente, la dotación de *recursos económicos atípicos* con los que poder hacer frente a adquisiciones de urgencia, adquisiciones de productos de alta confidencialidad o adquisiciones de productos que no se encuentran a través de medios o mercados ordinarios.

Servicio jurídico

332. La fuerza ciberespacial necesita un *servicio jurídico* propio con dedicación exclusiva a los asuntos de la fuerza ciberespacial y la ciberdefensa.

333. El servicio jurídico de la fuerza ciberespacial debe estar formado por juristas especializados en derecho informático y, en particular, en la aplicación del derecho internacional a las ciberoperaciones tanto en tiempo de conflicto o guerra, como en tiempo de paz.

334. El rol fundamental del servicio jurídico de la fuerza ciberespacial es el asesoramiento al mando en asuntos legales ordinarios y operativos y la aplicación de la justicia en el ámbito de la fuerza ciberespacial y la ciberdefensa.

335. Los *asuntos legales ordinarios* son los relacionados con la vida ordinaria de la unidad como contratos, acuerdos de colaboración, acuerdos técnicos, acuerdos de confidencialidad (NDA), asuntos legales relativos al personal y a la discriminación, etc.

336. Los *asuntos legales operativos* son los relacionados con la aplicación del derecho nacional e internacional en ciberconflictos, zona de operaciones y ejercicios; y en particular la aplicación del *ius in bello* (prácticas aceptables durante la guerra) e *ius ad bellum* (legítimas razones de un Estado para entrar en guerra) en el ciberespacio. El servicio jurídico, además, debe tener una participación activa relevante en la elaboración de las reglas de enfrentamiento en el ciberespacio (ROES ciberespaciales).

Capacidades operativas

337. La fuerza ciberespacial debe disponer de unas capacidades orientadas a la conducción de ciberoperaciones, en sus tres facetas (defensiva, explotación y ofensiva); como la *gestión de eventos de seguridad, la inteligencia operativa, la respuesta, la investigación forense digital y la ciberdefensa desplegable.*

Gestión de eventos de seguridad

338. En la actualidad, existe un uso poco claro de diversas nomenclaturas (COR/NOC, COS/SOC, CERT/CSIRT, CCO/CyOC, etc.) para designar organizaciones con responsabilidades en ciberseguridad, generando situaciones confusas y percepciones contradictorias que dificultan el entendimiento y la colaboración frente a ciberamenazas.

339. El *Centro de Operaciones de Red* (COR o NOC en sus siglas en inglés) es un centro operativo que monitoriza la red y sistemas propios con la finalidad de garantizar el funcionamiento y la disponibilidad de los servicios. Debe de tener capacidad para detectar fallos de funcionamiento e interrupciones parciales o totales de servicios. Su capacidad de reacción está limitada a las tareas de prevención de fallos y recuperación del servicio dentro de la propia red.

340. El *Centro de Operaciones de Seguridad* (COS o SOC en sus siglas en inglés) es un centro operativo que monitoriza la red y sistemas propios con la finalidad de garantizar la seguridad de la propia red. Debe de tener capacidad para detectar acciones maliciosas contra las redes y la información. Su capacidad de reacción está limitada a tareas de detección y eliminación de actividades maliciosas con acciones dentro de la propia red.

341. *CERT*[28] es un término registrado por la Universidad de Carnegie Mellon que hace alusión a una entidad, normalmente asociada a un sector concreto (gobierno, defensa, universidad, banca, empresas, infraestructura critica, etc.) establecida con la finalidad de prevenir, minimizar o eliminar eventos o incidentes de seguridad informática. Para usar del término CERT se necesita la autorización expresa de la Universidad de Carnegie Mellon.

342. *CSIRT*[29] es un término genérico con funciones similares al CERT, pero de uso libre y por tanto no necesita ninguna autorización para su uso.

343. Los términos CERT y CSIRT se usan habitualmente para dotar a un COS de una entidad oficial, reconocida y registrada por organismos internacionales (FIRST[30], TERENA[31], EGC Group[32]) que coordinan a todos los CERT/CSIRT asociados y facilitan el intercambio de información sobre vulnerabilidades, amenazas y medidas de mitigación.

344. El *Centro de Ciberoperaciones* (CCO o CyOC en sus siglas en inglés) es un centro de coordinación de operaciones militares en el ciberespacio, incluye operaciones defensivas, de explotación y ofensivas, dentro y fuera de la propia red, de acuerdo a los principios legales de uso de la fuerza.

345. La fuerza ciberespacial, como responsable principal de la ciberdefensa nacional, debe disponer de, al menos, un centro de ciberoperaciones (CCO) que coordine la acción de todos los COS que se establezcan dentro de su ámbito de actuación.

346. Es muy importante definir y detallar claramente las responsabilidades y tareas del CCO y de los diferentes COSs y CORs y generar entornos de confianza y colaboración para gestionar las tareas de responsabilidad compartida, incierta o controvertida.

347. Cada tipo de centro (COS, CCO, COR) está compuesto por personal con diferente cualificación profesional, operan con diferentes herramientas y tienen una finalidad y alcance diferentes. Un COS precisa, fundamentalmente, de herramientas de gestión de eventos de seguridad convencionales (SIEM); un CCO precisa de orquestadores que permitan la gestión de varios SIEMs, herramientas de caza de amenazas, plataformas avanzadas de decepción y sistemas de mando y control; mientras que un COR precisa de herramientas de control y monitorización de las operaciones TIC.

348. Las ciberoperaciones defensivas se pueden agrupar en tres niveles: el primer nivel que comprende actividades de prevención frente a fallos y ciberataques; el segundo nivel que comprende actividades de mitigación de ciberataques en curso convencionales (monitorización en tiempo real, correlación de eventos, notificación de compromisos, visualización de la situación, gestión dinámica de riesgos, alerta temprana y help desk); el tercer nivel comprende actividades de análisis a posteriori y de mitigación de amenazas avanzadas (análisis forense, equipos de reacción rápida, análisis de malware y alarma temprana de APTs).

Inteligencia operativa

349. La Inteligencia relacionada con el ciberespacio se puede entender de dos modos, la inteligencia de la ciberamenaza, fundamental para la fuerza ciberespacial y el ciberapoyo a servicios de inteligencia que la fuerza ciberespacial puede prestar por su especial preparación.

350. La *inteligencia de la ciberamenaza* es la actividad realizada, preferentemente a través del ciberespacio y ocasionalmente a través de otros medios, para obtener información y conocimiento de una ciberamenaza o de potenciales ciberamenazas conocidas o desconocidas.

351. La *inteligencia de la ciberamenaza* se usa para predecir situaciones futuras; para evaluar y valorar vulnerabilidades propias y de adversarios; para evaluar y valorar la capacidad de ciberdefensa de adversarios; para localizar objetivos; para preparar ciberataques propios y anticipar ciberataques de adversarios; para identificar servicios críticos propios y del adversario; para preparar operaciones de ciberespionaje y exfiltración de información; y para generar influencia.

352. La *inteligencia con ciberapoyo* es la actividad realizada a través del ciberespacio para obtener información y conocimiento de cualquier materia o asunto y que la fuerza ciberespacial, como fuerza especializada en la utilización del ciberespacio, puede realizar en apoyo a los servicios de inteligencia o de cualquier otra unidad que lo requiera, normalmente a través de un requerimiento de información (RFI).

353. La fuerza ciberespacial debe participar activamente en los foros nacionales e internacionales de intercambio de información sobre vulnerabilidades y amenazas y debe fomentar acuerdos bilaterales con otras fuerzas ciberespaciales extranjeras para complementar su producción interna de inteligencia de la ciberamenaza.

Respuesta

354. La *respuesta* es la capacidad de la fuerza ciberespacial relacionada con las ciberoperaciones ofensivas.

355. Las *ciberoperaciones ofensivas* en redes ajenas y sin autorización son operaciones muy complejas que requieren una cualificación y unos conocimientos muy sofisticados y que solo se realizarán en ocasiones extraordinarias cuando el uso de la fuerza sea legalmente permitido. Por ello, la unidad de respuesta de la fuerza ciberespacial dedicará, la mayor parte de su tiempo, a su propia formación, a realizar prácticas en entornos aislados (campo de maniobras ciberespacial) y a participar en ciberejercicios; con la finalidad de estar preparada para actuar en el momento necesario.

356. La *complejidad* de las ciberoperaciones ofensivas reside en la dificultad de generar los efectos deseados y a la vez evitar todo rastro (huella digital) para impedir la atribución técnica y legal y evitar la reutilización de la ciberarma por parte del adversario.

357. En la práctica, la *colaboración* con otras fuerzas ciberespaciales extranjeras en materia de ciberoperaciones ofensivas es muy difícil de conseguir; por lo que en esta materia la fuerza ciberespacial debe buscar la autosuficiencia a través de desarrollos propios y acuerdos de colaboración confidenciales con la industria y la universidad.

358. En organizaciones internacionales de defensa colectiva, como la OTAN, la organización en si misma carece de fuerzas de combate, salvo en casos muy particulares, generándose las fuerzas para misiones y operaciones concretas con la aportación voluntaria de las naciones (*generación de fuerzas*).

359. En el caso de la ciberdefensa, en la mayoría de las situaciones no es necesario el despliegue de unidades de la fuerza ciberespacial para generar los efectos deseados por el comandante de la misión, por lo que la generación de ciberfuerzas no es un mecanismo eficiente; pasándose de un modelo de generación de fuerzas a un *modelo de generación de efectos* que establece un mecanismo mediante el cual se genera una capacidad colectiva de ciberefectos, para misiones y operaciones concretas, con la aportación voluntaria de las naciones.

360. Para la ejecución de las acciones de respuesta se debe considerar, además de las instalaciones permanentes regulares de la fuerza ciberespacial, otras instalaciones no regulares que no puedan ser asociadas a organismos estatales.

Investigación forense digital

361. Por muy sólida defensa que se tenga de las redes propias, en ningún caso es posible repeler la totalidad de los ciberataques. En estos casos, es necesario disponer de un servicio que tenga la capacidad de estudiar en detalle la naturaleza del ciberataque, una vez que se ha producido, analizando el malware y las TTPs utilizadas e identificando el origen.

362. La *investigación forense digital* usa técnicas especiales que permitan extraer información cifrada, dañada e incluso aparentemente eliminada preservando la información original, en la medida de lo posible. La fuerza ciberespacial debe considerar dos contextos en la investigación forense digital, el contexto ordinario o regular y el contexto de campaña.

363. La *investigación forense digital regular* es el servicio permanente de la fuerza ciberespacial, compuesto por un equipo humano especializado en técnicas y ciencia forense digital, orientado a la obtención detallada de información sobre ciberataques a redes propias.

364. El equipo de investigación forense digital regular desempeña su trabajo, normalmente, en unas condiciones óptimas de tiempo, lugar y recursos y por ello debe esmerarse en utilizar las técnicas y procedimientos forenses de una manera muy cuidadosa y cautelosa para extraer toda la información posible sin dañar la original, de tal manera que pueda ser usada como evidencia en procesos judiciales.

365. La *investigación forense digital de campaña* es un servicio específico de cada misión u operación orientado a la extracción detallada de información en las redes de adversarios. Se presta, normalmente, en tres escalones: el primer escalón compuesto por el equipo de extracción de información, el segundo por el equipo forense de campaña y el tercero por el servicio forense regular.

366. El equipo de extracción se compone de personal de fuerzas no especializadas en técnicas forenses (normalmente fuerzas de operaciones especiales) que con una formación básica forense y en el menor tiempo posible, debe extraer información y dispositivos de información de redes adversarias, en territorio hostil, de la mejor manera posible para que esa información pueda ser analizada por un equipo forense de campaña o por el servicio forense regular de la fuerza ciberespacial.

367. El equipo forense de campaña realiza el análisis rápido de la información extraída por el equipo de extracción, con la finalidad de extraer información de valor para las operaciones en curso.

368. El servicio regular se encarga de realizar un análisis más en detalle con la información disponible, con la finalidad de obtener inteligencia de valor para futuras operaciones.

369. En el contexto de campaña el equipo de extracción se esmerará en obtener información y dispositivos, de la mejor y más rápida manera posible, para que sea útil al segundo escalón sin considerar el potencial daño a la información original que pudiera afectar a un proceso judicial posterior. En este caso prima la rapidez y la información sobre el adversario que las evidencias legales en un potencial proceso judicial posterior.

370. Uno de los problemas con los que se encuentra, habitualmente, el servicio regular de investigación forense digital es la *ofuscación*[33] de los códigos maliciosos con la finalidad de dificultar la ingeniería inversa de software[34] y la identificación por parte de antivirus o revisores humanos.

371. La unidad responsable de la investigación forense digital debe tener una relación estrecha con la unidad responsable del servicio de caza de amenazas.

Ciberdefensa desplegable

372. Por razones técnicas, operativas o procedimentales, en algunas ocasiones, las acciones de ciberdefensa no pueden realizarse en remoto desde las instalaciones principales de la fuerza ciberespacial siendo necesario desplegar parte de sus capacidades para hacer frente a situaciones concretas de defensa, explotación o ataque.

373. La fuerza ciberespacial debe disponer de unos *equipos desplegables de ciberdefensa* compuestos por personal, medios y procedimientos personalizables (de acuerdo a la misión) y transportables (por medios de transporte militares o civiles ordinarios), adiestrados y preparados para desplegar allá donde se requiera (zonas de operaciones, ejercicios, instalaciones o plataformas de otros ámbitos de operaciones, instalaciones de infraestructura crítica, etc.), en el menor tiempo posible, con la finalidad de reforzar la ciberdefensa existente o hacer frente a situaciones críticas urgentes.

374. Los equipos desplegables de ciberdefensa deben ser capaces, en un tiempo breve, de configurarse en un modo específico de operación, tanto en herramientas como en personal, de acuerdo a la misión. Los modos específicos de operación más habituales son de defensa (monitorización y gestión de eventos, auditorías, investigación forense digital y protección frente a amenazas avanzadas), pudiéndose dar, ocasionalmente, modos relacionados con las ciberoperaciones de explotación y ofensivas.

Capacidades técnicas

375. La fuerza ciberespacial debe disponer de unas capacidades orientadas al apoyo técnico al mando y a las ciberoperaciones, como las *auditorías de seguridad TIC, el campo de maniobras, la observación tecnológica, la investigación y desarrollo, el arsenal, la seguridad de la información y la criptografía.*

Auditorías de seguridad TIC

376. En relación con los sistemas de las tecnologías de la información y las comunicaciones (sistemas TIC) debemos distinguir tres figuras principales: el propietario o autoridad operativa del sistema, el administrador o autoridad técnica del sistema y el responsable de seguridad o autoridad de seguridad del sistema.

377. La *autoridad operativa* del sistema es la más alta autoridad responsable de las unidades, funciones o servicios a las que el sistema sirve, las que usan el sistema y a las que les afecta un fallo o interrupción del sistema para el desempeño de sus cometidos. El propietario del sistema es el responsable de definir los requisitos operativos y de designar y autorizar sus usuarios.

378. La *autoridad técnica* del sistema es la más alta autoridad responsable de las unidades TIC encargadas del diseño, desarrollo, administración y sostenimiento del sistema de acuerdo a los requisitos operativos establecidos por la autoridad operativa y de los requisitos de seguridad establecidos por la autoridad de seguridad.

379. La *autoridad de seguridad* del sistema es la más alta autoridad de las unidades de ciberdefensa y la encargada de definir los requisitos de seguridad del sistema y de vigilar su cumplimiento.

380. El establecimiento de las tres autoridades (operativa, técnica y de seguridad) proporciona equilibrio y estabilidad a los sistemas y, por ello, sus responsabilidades no deben ser traspasadas ni delegadas entre ellas.

381. Las *auditorias de seguridad* de los sistemas TIC es una herramienta que la autoridad operativa tiene en sus manos para conocer de manera fidedigna el nivel de seguridad de los sistemas TIC bajo su responsabilidad.

382. En una auditoria de seguridad de un sistema TIC, el auditado es la unidad TIC (subordinada a la autoridad técnica) que administra el sistema a auditar y conforme con el *principio de independencia* de las auditorías (auditado y auditor no pueden recaer bajo la misma autoridad), el auditor debe ser una unidad subordinada a la autoridad operativa o a la autoridad de seguridad, siendo esta última la más recomendable por disponer del personal y los medios adecuados.

383. Las auditorías de seguridad TIC tienen que considerar todos los aspectos (técnicos, físicos, humanos y procedimentales) que afecten de alguna manera a la seguridad de los sistemas que manejan información clasificada o sin clasificar.

384. Las auditorías deben analizar y valorar el nivel de cumplimento o alineamiento del software, hardware, instalaciones, documentación y personal con las medidas de seguridad establecidas en las normas de referencia correspondientes.

385. El *proceso* habitual en una auditoría es el siguiente:

1. El equipo auditor (normalmente una unidad subordinada a la autoridad de seguridad) planifica y propone un calendario a la autoridad técnica (auditado) y a la autoridad operativa (propietario del sistema).
2. El equipo auditor estudia, prueba y evalúa los controles idóneos de acuerdo con la información proporcionada por la autoridad técnica del sistema.
3. El equipo auditor ejecuta la auditoría.
4. El equipo auditor realiza el informe de la auditoría y lo distribuye a la unidad auditada para que subsane las deficiencias en un periodo determinado.
5. El equipo auditor eleva a la autoridad de seguridad el informe que, a su vez, lo eleva a la autoridad operativa.

ILUSTRACIÓN 27. CICLO AUDITORÍAS

386. En el caso de *sistemas clasificados*, lo habitual es que necesiten ser previamente acreditados por la autoridad operativa antes de que se les permita entrar en operación o reacreditados para que pueden seguir funcionando. En este caso, el informe del equipo auditor llevaría no solo los resultados de la auditoría, sino una propuesta positiva (el sistema está libre de deficiencias graves que le impiden entrar en operación) o negativa (el sistema tiene deficiencias graves que le impiden entrar en operación).

387. La acreditación se suele otorgar por periodos de tres años, aunque, en la medida que la tecnología y la clasificación del sistema lo permitan, lo ideal es realizar auditorías dinámicas online que sean capaces de evaluar la seguridad de los sistemas en tiempo real.

Campo de maniobras

388. Un *campo de maniobras convencional* es una zona restringida de un ámbito de operaciones convencional (tierra, mar, aire) que se usa para entrenar a las unidades militares y practicar operaciones de fuego real en un entorno seguro y aislado que garantice la inocuidad del ámbito.

389. Para una mayor eficacia, el campo de maniobras debe ser ambientado a imagen y semejanza del terreno más probable en donde se produciría la operación que se quiere entrenar o probar y se debería incluir una fuerza adversaria.

390. Un *campo de maniobras ciberespacial,* también llamado cyber range, es exactamente lo mismo que un campo de maniobras convencional; es decir, una zona restringida del ciberespacio que se usa para entrenar a las unidades de ciberdefensa y practicar ciberoperaciones reales en un entorno seguro y aislado que garantice la inocuidad del ciberespacio.

391. El campo de maniobras ciberespacial es en realidad más eficaz que los convencionales, ya que puede simular, con bastante exactitud, el entorno en donde se desarrollaría la ciberoperación, incluyendo topología y actividad de la red, comportamientos de usuarios y un enemigo con fuego real.

392. La fuerza ciberespacial necesita el campo de maniobras ciberespacial para, entre otras actividades, realizar formación y adiestramiento individual y de unidades; modelar y simular entornos, escenarios, redes, efectos y comportamientos para su análisis, valoración o uso en prácticas; análisis de malware y desarrollo de ciberarmas; prueba, evaluación y validación de conceptos, productos, tecnologías y TTPs propias o capturadas.

393. El campo de maniobras de la fuerza ciberespacial debe ser *seguro* (debe permitir el acceso selectivo exclusivamente a los usuarios autorizados), *aislado* (debe impedir que los efectos de las actividades realizadas en él no puedan expandirse al exterior), *confiable* (debe reproducir las actividades tal cual son requeridos por los usuarios), *accesible* (in situ y online), *escalable* (debe permitir fácilmente su incremento en capacidades y potencia), *dinámico* (debe evolucionar conforme a la aparición de nuevas tecnologías), *completo* (debe poder simular cualquier entorno TIC necesario incluidos sistemas de control *industrial* y SCADA), *resiliente* (robusto frente a fallos, incluyendo un campo de maniobras de respaldo) y lo más importante, debe de estar operado por un *equipo multidisciplinar* experto en tecnologías de virtualización y herramientas de modelado y simulación y con una alto grado de conocimiento de los entornos técnicos y operativos de la ciberdefensa.

394. El caso ideal para la ciberdefensa nacional es el desarrollo e implementación de un *campo de maniobras nacional* en el que se pueda modelar internet para la realización de prácticas de respuesta frente a ciberincidentes de gran escala, con la participación de la fuerza ciberespacial y el resto de actores, públicos o privados, implicados en la ciberdefensa nacional.

Observación tecnológica

395. Las tecnologías, productos, herramientas y empresas de interés y utilidad para la ciberdefensa, actual y futura, existente en el mercado global son innumerables.

396. El personal de la fuerza ciberespacial, en su gran mayoría, no dispone de tiempo para estudiar e investigar las tecnologías, productos o herramientas de potencial interés para su ámbito de actuación, ni para asistir a la multitud de eventos que son organizados continuamente, ni para atender a las empresas que prometen soluciones ideales e innovadoras. Por ello, es necesario establecer una unidad de la fuerza ciberespacial (*observatorio tecnológico*) con dedicación exclusiva a la observación tecnológica y de esta manera, liberar al resto de personal de una sobrecarga de trabajo eludible.

397. Las responsabilidades del observatorio tecnológico son: analizar y probar las tecnologías, productos y herramientas del mercado y valorar su madurez y potencial utilidad para la fuerza ciberespacial; recibir a las empresas del sector y valorar la potencial utilidad de las soluciones que proponen; asistir a los eventos más relevantes relacionados con la ciberdefensa y valorar e informar sobre productos y tendencias; informar a potenciales beneficiarios de los resultados de sus análisis y valoraciones; elaborar un catálogo (normalmente con carácter anual) clasificando todos las tecnologías, productos y herramientas consideradas de potencial utilidad para la fuerza ciberespacial y la ciberdefensa nacional; e identificar e informar de fuentes de obtención de exploits y vulnerabilidades de día cero.

Investigación y desarrollo

398. Para mantener un nivel de competitividad aceptable, en el entorno global de la ciberdefensa en el que la fuerza ciberespacial se mueve, es necesario disponer de una capacidad de investigación y desarrollo permanente y estable.

399. La investigación y desarrollo de nuevas tecnologías de ciberdefensa y la adaptación de tecnologías de otros sectores para su uso en la ciberdefensa es una labor de tal magnitud que la fuerza ciberespacial no puede desempeñarla en solitario y necesita gestionarla conjuntamente con la unidad responsable de I+D+i del ministerio de defensa y con colaboraciones con los centros de I+D+i públicos, con la industria y con la universidad.

400. El estudio de la aplicación a la ciberdefensa de tecnologías emergentes (inteligencia artificial, machine learning[35], blockchain[36], big data[37], 5G[38]) o el uso de medios novedosos (drones, UAV, RPAS) es necesario para mantener un nivel de operatividad de las capacidades de la fuerza ciberespacial equivalente a otras fuerzas ciberespaciales de un mismo entorno geoestratégico.

401. La *investigación* es una necesidad para mejorar la ciberdefensa futura y muchos de los resultados que se obtienen de ella no son de aplicación inmediata en las distintas capacidades de la fuerza ciberespacial; pero si se hace una programación adecuada, los resultados deben de ser aplicables en el medio o largo plazo. Por ello, es muy importante mantener programas plurianuales y gestionar, controlar y evaluar la eficacia de los resultados a medio y largo plazo.

402. La aplicación de los resultados de la investigación es muy diversa, pudiendo servir para crear herramientas o productos nuevos, para mejorar tecnologías existentes, para servir de base a nuevos desarrollos, para impulsar o mejorar desarrollos existentes o para descartar otras líneas de investigación menos eficientes o no apropiadas a las necesidades de ciberdefensa.

403. La fuerza ciberespacial, habitualmente, necesita llevar a cabo tres tipos de *desarrollo* (propio, ajeno y mixto) para mantener su nivel operativo.

404. El *desarrollo propio* es aquel desarrollo que la fuerza ciberespacial realiza con sus propios recursos humanos, materiales, cognitivos y financieros. Podría incluir la adquisición de productos comerciales para dar solución a partes específicas del conjunto del desarrollo, pero la dirección, el diseño, la integración de todas las partes, la implementación y la evaluación y validación siempre corre a cargo de la fuerza ciberespacial. En un desarrollo propio solo la fuerza ciberespacial tiene el conocimiento completo del desarrollo y sus funcionalidades.

405. El desarrollo propio puede ser necesario, entre otras cosas, por razones de insuficiencia (no hay posibilidad de acuerdos para su desarrollo), financieras (no se dispone de financiación externa para el producto deseado), seguridad (el producto, su desarrollo y su función exigen un grado elevado de clasificación y la colaboración con terceros pondría en riesgo la salvaguarda de la debida confidencialidad), tiempo (los procesos públicos de contratación y desarrollo pueden ser demasiado lentos para dar respuesta a necesidades urgentes), rentabilidad (opción menos costosa) e idoneidad (la fuerza ciberespacial dispone de los mejores conocimientos en la materia a desarrollar).

406. El *desarrollo ajeno* es aquel desarrollo llevado a cabo por una entidad ajena de acuerdo con los requisitos operativos y, en ocasiones técnicos, establecidos por la fuerza ciberespacial a través de un contrato.

407. El *desarrollo mixto* es aquel desarrollo que es llevado a cabo conjuntamente por la fuerza ciberespacial y otras entidades a través de un acuerdo de colaboración.

408. Habitualmente, la fuerza ciberespacial necesitará llevar a cabo los tres tipos de desarrollo, los propios para desarrollos sensibles o urgentes, los ajenos para desarrollos a largo plazo y los mixtos para desarrollos complejos.

Ciberarsenal

409. La fuerza ciberespacial, como toda unidad militar, necesita un armamento especialmente diseñado para causar unos determinados efectos en el ciberespacio cuyas consecuencias pueden transcender a los otros ámbitos convencionales.

410. Para disponer de una capacidad armamentística adecuada a sus misiones, la fuerza ciberespacial debe desarrollar mecanismos y procedimientos que le permitan adquirir y desarrollar ciberarmas y cargas explosivas y configurar su arsenal.

411. La adquisición de ciberarmas y sus cargas explosivas se puede realizar a través del mercado global, regular o irregular, a través de la industria armamentística nacional, o través de desarrollo propio o en colaboración.

412. La ciberdefensa nacional necesita una *industria ciberarmamentística* nacional robusta para evitar una dependencia externa que pueda poner en riesgo su operatividad actual y futura; de la misma manera que sucede con los ámbitos convencionales.

413. La fuerza ciberespacial necesita adquirir ciberarmas con periodicidad y, además, desarrollar sus propias ciberarmas (a través de sus propios conocimientos, de la personalización de ciberarmas conocidas o mediante la reutilización de ciberarmas capturadas de ciberataques a redes propias) y probarlas en el campo de maniobras.

414. La configuración del ciberarsenal es una de las tareas más delicadas de la fuerza ciberespacial y debe ser llevada a cabo de manera que se garantice que el ciberarsenal es *seguro* (debe permitir el acceso exclusivamente al personal autorizados), *confiable* (las ciberarmas deben ser probadas y actualizadas con frecuencia garantizando que hacen los que se espera de ellas), *registrable* (debe registrar los usos que se hacen de las ciberarmas para evitar su repetición en los mismos objetivos), *escalable* (debe permitir fácilmente su incremento) y *completo* (debe incluir las ciberarmas necesarias para desarrollar los ciberataques que las operaciones y las misiones de la fuerza ciberespacial requieren).

415. En comparación con los ámbitos convencionales, el arsenal de la fuerza ciberespacial es más dinámico, incorporando continuamente nuevas ciberarmas y rediseñando antiguas, con la finalidad de que las ciberarmas empleadas en un ciberataque no puedan ser detectadas a través de huella conocida y si son detectadas que no pueden ser reutilizadas por la víctima. Por ello, las ciberarmas en muchos casos son de un solo uso y se diseñan para que puedan destruirse a sí mismo bajo ciertas condiciones.

Seguridad de la información y criptografía

416. La *seguridad de la información* es un servicio fundamental en la fuerza ciberespacial, dada la naturaleza sensible de la mayoría de sus actividades, tanto operativas como técnicas, contractuales y procedimentales.

417. La seguridad de la información es un servicio transversal a todos los ámbitos de operaciones, orientado a preservar la disponibilidad, integridad y confidencialidad de la información. Es uno de los muchos servicios que la fuerza ciberespacial necesita, no debe, en ningún caso confundirse ni asimilarse a la ciberdefensa.

418. La seguridad de la información debe considerar todos aquellos elementos que, de alguna manera, interactúan con la información, como las personas, los documentos, las instalaciones, los sistemas TIC y las empresas.

419. El servicio de seguridad de la información de la fuerza ciberespacial tiene la responsabilidad de elaborar las normas y procedimientos de seguridad de la información de la fuerza ciberespacial y vigilar y fomentar su cumplimiento.

420. La *criptografía* es una materia que de una u otra manera se encuentra presente en la mayoría de los servicios y medidas de ciberseguridad, siendo fundamental no solo en los aspectos evidentes de confidencialidad sino en muchos otros servicios sensibles como el control de acceso, la firma electrónica, la integridad, etc. Además, muchos ciberataques incluyen criptografía en alguna de sus fases. Por ello, se considera necesario que la fuerza ciberespacial disponga de un gabinete criptográfico adecuado para gestionar los asuntos de criptografía relacionados con la ciberdefensa.

Instalaciones

421. Las *instalaciones* de todas las unidades de la fuerza ciberespacial deben estar debidamente acondicionadas para albergar al material y personal en las debidas condiciones de seguridad, operatividad y ambientales.

422. Las ciberoperaciones, en gran medida, se desenvuelven en entornos confidenciales; por ello, las instalaciones deben estar acondicionadas para proteger la confidencialidad de la información y las actividades hasta el grado que se requiera.

423. Además de las instalaciones regulares, la fuerza ciberespacial debe considerar el uso, permanente o temporal, de *instalaciones encubiertas* necesarias para proteger el anonimato de ciberoperaciones sensibles y desvincularlas de instalaciones asociadas a organismos públicos, estatales o territorio nacional.

Mando

424. La ciberdefensa no es una función de los ámbitos de operaciones convencionales; sino una capacidad de combate especializada en el ámbito de operaciones ciberespacial, por ello debe de estar comandada por un *mando independiente* de los otros ámbitos, aun cuando la dimensión de la unidad de ciberdefensa sea muy reducida.

425. La complejidad de la organización y coordinación de la ciberdefensa, así como su capacidad para generar efectos estratégicos inmediatos obliga a disponer de un *mando único* dependiente de los niveles de conducción de operaciones más altos: el comandante de la fuerza conjunta, el jefe del estado mayor de la defensa y el ministro, cada uno en su ámbito de actuación.

CIBERAMENAZA

426. La ciberamenaza es una fuente potencial de perjuicio, externa o interna, a algún activo de la organización, que se materializa a través del ciberespacio. Aprovecha una vulnerabilidad en algún elemento, técnico o humano, del ciberespacio propio y afecta a activos de valor para la organización o para la propia fuente de la ciberamenaza.

427. Para que una fuente sea considerada una ciberamenaza debe cumplir tres requisitos: *capacidad, interés y animosidad.*

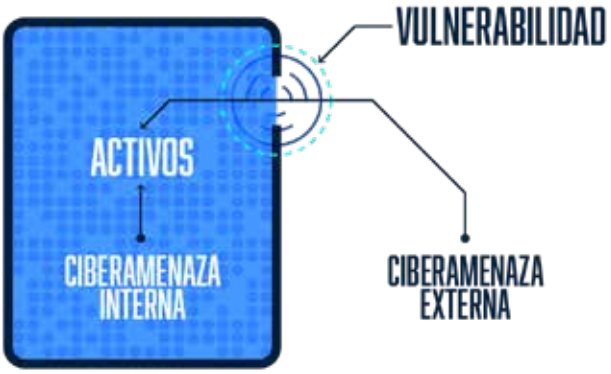


ILUSTRACIÓN 28. CIBERAMENAZA

428. La ciberamenaza debe tener la *capacidad* de identificar y aprovecharse de las vulnerabilidades de las redes y sistemas TIC de la víctima y de llegar a causarles un efecto pernicioso.

429. La capacidad puede configurarse a través de una capacidad técnica y humana propia; a través del secuestro subrepticio de las capacidades técnicas de terceros (botnets), mediante la contratación o subcontratación de una capacidad ajena (universidades, compañías comerciales o grupos criminales) o mediante acciones de influencia sobre terceros para que generen las acciones maliciosas deseadas (aprovechando situaciones sociales, económicas o políticas inestables o conflictivas).

430. La capacidad de la ciberamenaza debe ser considerada en relación con sus potenciales objetivos, dado que no es lo mismo la capacidad necesaria para generar un ciberataque tipo STUXNET que un ransomware[39] o un website defacement[40].

431. La ciberamenaza debe tener *interés* en los activos de la víctima. Dicho de otra manera, los activos de la potencial víctima, en especial la información, deben de tener un valor rentable para la fuente de amenaza, de tal manera, que los beneficios esperados compensen el gasto de los recursos necesarios para realizar el ciberataque.

432. Por último, la ciberamenaza debe tener *animosidad* contra la potencial víctima, es decir, interés en causar un perjuicio a sus redes y sistemas TIC, aunque no le aporte un beneficio directo, sino una ventaja operativa en el marco de un conflicto o una ventaja competitiva en un entorno comercial.

433. La *identificación* de las ciberamenazas es un proceso en tres fases; primero se seleccionan las fuentes (estados, organizaciones o entidades) que tienen un interés en los activos de la potencial victima; segundo, de entre las fuentes con interés se seleccionan las que tienen capacidad; y tercero, se pueden descartar aquellas fuentes que, aun disponiendo de capacidad e interés, guardan una relación de alianza con la potencial víctima.

434. En algunos casos, la pertenencia a una misma *alianza política, económica o de defensa* no es suficiente para descartar a la fuente como una potencial ciberamenaza, ya que, si el interés es lo suficientemente grande, podrían intentar ciberataques extremando el cuidado en el anonimato o realizando ciberataques de falsa bandera.

435. Las ciberamenazas a intereses nacionales y militares son cada vez más comunes, sofisticadas y perjudiciales. Por ello, la ciberdefensa debe incorporarse a la planificación militar en todos los niveles de mando y las ciberamenazas y los ciberriesgos deben tenerse en cuenta a lo largo del ciclo completo de la planificación de las operaciones conjuntas.

436. Se distinguen dos tipos de fuentes de ciberamenazas, las fuentes internas y las fuentes externas.

437. Las *fuentes internas de ciberamenaza* son aquellos individuos o entidades que pertenecen a la organización de la potencial víctima y que, por ello, están autorizados a acceder a los datos, información o sistemas de los objetivos; o aquellos individuos o entidades que no perteneciendo a la unidad actúan desde dentro por que han conseguido, de manera maliciosa, credenciales de acceso. Las causas de ciberamenaza interna suelen ser por ignorancia, accidente, negligencia o deliberadas.

438. Para prevenir la ciberamenaza interna por *ignorancia* es necesario la formación, sensibilización y concienciación a todos los niveles de la organización en ciberseguridad; la vigilancia de la aplicación de las normas, medidas y procedimientos de ciberseguridad y la valoración de su eficacia.

439. Para prevenir la ciberamenaza interna por *accidente* es necesario el desarrollo de planes de continuidad de las operaciones e implementar un modelo de ciberseguridad transparente al usuario, en el que se reducen al mínimo posible las decisiones en materia de ciberseguridad por parte de usuarios finales.

440. Para prevenir la ciberamenaza interna por *negligencia* es necesario la monitorización interna convencional (basada en SIEM) y establecer un modelo de ciberseguridad sencillo donde las medidas de seguridad a aplicar por los usuarios finales sean fáciles de entender y de poner en práctica.

441. Para prevenir la ciberamenaza interna *deliberada* es necesario establecer modelos avanzados de monitorización basados en servicios de caza de ciberamenazas (párr. 478) y la realización de auditorías internas de seguridad TIC.

442. Las *fuentes externas de ciberamenaza* son aquellos individuos o entidades que no pertenecen a la organización de la potencial víctima y que, por ello, no están autorizados a acceder a los datos, información o sistemas de los objetivos. De una manera práctica se agrupan en tres tipos: estados, grupos organizados e individuos.

443. Para combatir la *ciberamenaza de estado* es necesario el desarrollo y establecimiento de una fuerza ciberespacial y la participación en alianzas de defensa colectiva a través de organizaciones internacionales como la OTAN y acuerdos multinacionales y bilaterales de ciberdefensa.

444. Para combatir la ciberamenaza procedente de fuentes no atribuibles a estados (grupos organizados o individuos) es necesario el fortalecimiento de los *tres pilares de la ciberseguridad nacional (ciberresiliencia, ciberprotección y ciberdefensa*, párr. 530), una estrecha cooperación entre ellos y el fortalecimiento del derecho internacional relacionado.

445. Los objetivos más habituales de las ciberamenazas son la información, las redes y sistemas TIC, los dispositivos móviles de comunicación (smartphones, tabletas) y los sistemas de información y de control de infraestructuras críticas; aunque no se pueden descartar las consecuencias indirectas físicas a instalaciones y personas de los ciberataques.

446. La ciberamenaza a los *dispositivos móviles* de comunicación (smartphones y tabletas) debe ser considerada de manera especial debido a que adolecen de ciberriesgos adicionales.

447. A pesar de que un dispositivo móvil actual es un sistema TIC completo, la necesidad de protegerlos frente a ciberataques no se percibe en la misma medida que en los sistemas TIC convencionales (ordenadores, redes de ordenadores, etc.). Esta falta de concienciación hace especialmente vulnerables a estos dispositivos.

448. Los dispositivos móviles son especialmente atractivos para las ciberamenazas, debido a que son *multiformato* (datos, voz y video) y multipropósito (uso personal y profesional conjuntamente, ByOD[41]), son una *extensión* del propietario con cámara y micrófono (salvo restricciones específicas suelen acompañar al propietario permanentemente, atienden a sus reuniones y discusiones y ven y escuchan lo mismo que los asistentes) y son un elemento de geolocalización del propietario.

449. Los ataques a los dispositivos móviles con la finalidad de controlar sus aplicaciones y su cámara y micrófono no son complicados para ciberatacantes expertos, incluso con el dispositivo apagado.

450. Otros objetivos de ciberamenazas a considerar especialmente son las *infraestructuras críticas nacionales* debido a que un impacto en ellas podría tener consecuencias devastadoras a nivel nacional.

451. Los *sectores estratégicos* globalmente aceptados son energía, salud, agua, alimentación, tecnologías de la información y las comunicaciones, transporte, industria química, industria nuclear, espacio, investigación y administración pública

ILUSTRACIÓN 29. INFRAESTRUCTURA CRÍTICA

452. Existe la falsa idea o percepción de que las infraestructuras críticas no se conectan a Internet y por ello no corren riesgo de ciberataque. No solo, la mayoría de los sistemas de información que controlan y gobiernan las infraestructuras críticas se conectan a internet, sino que aquellos pocos que están aislados también son susceptibles de ciberataques.

453. Todos los sectores estratégicos están compuestos por numerosas instalaciones ubicadas en distintos emplazamientos geográficos a gran distancia entre sí; por lo que la gestión y el mantenimiento descentralizado significaría una multiplicación de recursos inasumible para los operadores críticos que, en su mayoría, son empresas privadas orientadas a beneficio económico. Por ello, todos los sistemas que controlan y gobiernan las infraestructuras críticas, en mayor o menor medida, se conectan a internet para disponer de un *sistema centralizado de gestión y mantenimiento.*

454. La criticidad nacional de los sectores estratégicos junto con su conectividad global obliga a extremar la protección frente a ciberamenazas a la infraestructura crítica nacional y en particular el sector eléctrico, puesto que el resto de sectores dependen de él para operar.

Panorama y tendencias de la ciberamenaza global

455. Anualmente, se publican estudios e informes que analizan el panorama global de las ciberamenazas y sus tendencias (CCN/CERT[42], ENISA[43], Gartner[44], CheckPoint[45], FireEye[46], Kaspersky[47], entre otros muchos). En estos estudios se mezclan fuentes de ciberamenazas (estados, terroristas, ciberactivistas, etc.) con tipos de ciberataques (phishing, ataque DNS, etc.) y objetivos (dispositivos móviles, cadena de suministro, informaciones falsas, robos de credenciales, etc.) y se analiza la información desde diferentes puntos de vista.

456. De acuerdo con el informe de "ciberamenazas y tendencias del CERT Gubernamental español (CCN-CERT)" de 2019, las ciberamenazas más significativas del panorama internacional son los Estados y los grupos patrocinados por ellos; siendo otras ciberamenazas relevantes los ataques a la cadena de suministros, las acciones en el ciberespacio de grupos terroristas, yihadistas y ciberactivistas, las noticias falsas, así como los ataques contra los datos personales (con el fin último de cometer ciertos delitos, robar credenciales, suplantación de identidad o espionaje).

457. El informe de CheckPoint (cyber attack trends: 2019 mid-year report) refleja un panorama diferente, o con otro punto de vista, haciendo hincapié en el aumento de cuatro tipos de ataques con respecto al año anterior (ataques a la cadena de suministro de software, estafas cada vez más sofisticadas a través de emails, ciberataques a recursos en la nube y ciberataques a dispositivos móviles) y en la persistencia de otros tres tipos de ataques (ransomware, criptominado[48] y ataques DNS[49]).

458. Todos los informes son útiles, pero hay que analizarlos con la perspectiva adecuada. Por ello, es recomendable que en cada nivel de actuación en la ciberseguridad nacional (fuerza ciberespacial, seguridad nacional, infraestructuras críticas) se elabore un informe propio de panorama y tendencias de ciberamenazas basándose en la inteligencia propia, en los potenciales objetivos y en el análisis de los informes de fuentes contrastadas de diverso origen y posicionamiento geoestratégico.

459. En cualquier caso, se puede confirmar que, actualmente, la *ciberamenaza de estado*, a través de unidades especiales de ciberdefensa ofensiva (APTs), es la principal amenaza a considerar a nivel nacional, como así ha sido públicamente reconocido por la OTAN y las naciones de su entorno.

Amenaza Persistente Avanzada

460. La *amenaza persistente avanzada (APT)* es un grupo organizado de expertos, normalmente asociado a un Estado, que utiliza sofisticados conocimientos, herramientas y TTPs (técnicas, tácticas y procedimientos) para (de manera anónima, sigilosa y desapercibida) infiltrarse, tomar el control y perpetuarse en una red ajena, con el objeto de tener acceso a la información de su interés y obtener ventajas estratégicas.

461. Una APT opera, habitualmente, conforme a un proceso cíclico de 5 fases: *preparación, acceso, persistencia, ejecución y anonimización.*

462. En la fase de *preparación* se procede a la identificación de potenciales objetivos, la valoración de sus activos y la rentabilidad del ciberataque comparando los recursos propios necesarios para el desarrollo del ciberataque y los beneficios esperados.

463. A continuación, se recopila inteligencia de la potencial víctima, su organización, capacidad de ciberdefensa, vulnerabilidades, cualquier información que pudiera ser utilizada como vector de ataque (emails, sitios web) y cualquier información de apoyo a los ciberataques (nombres, cargos, organización, roles, responsabilidades, comportamientos esperados, actividad habitual en la red, etc.) a través de ciberoperaciones de explotación tanto pasivas como activas.

464. Una vez seleccionado el objetivo y con toda la inteligencia disponible se seleccionan del arsenal las ciberarmas, las cargas explosivas (pay load) y las TTPs más idóneas, se diseñan los ciberataques y se prueban en el campo de maniobras propio para verificar su eficacia y anonimización.

465. En la fase de *acceso* se procede a la infiltración en la red objetivo y el establecimiento de un canal de comunicación externo.

466. La infiltración se realiza aprovechando vulnerabilidades previamente detectadas y probadas (habitualmente a través de spear phishing o watering hole) y una vez dentro, se instala un código malicioso que crea una puesta trasera (acceso remoto oculto) a través de herramientas de administración remota (remote administration tool, RAT).

467. Una vez creada la puerta trasera se produce un canal de comunicación oculto entre la red objetivo y el centro de mando y control de la APT estableciéndose el primer punto de presencia.

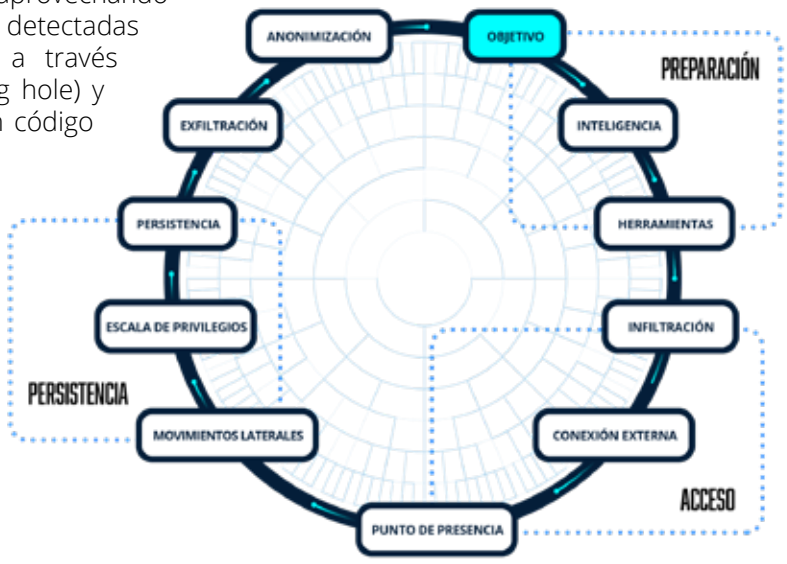


ILUSTRACIÓN 30. CICLO APT

468. En la fase de *persistencia* se emplea el primer punto de presencia para realizar, desde dentro, un reconocimiento detallado de la red que aporte la información necesaria para realizar (de manera segura y silenciosa) movimientos laterales (movimientos dentro de la red) con la finalidad de establecer otros puntos de presencia y escalar privilegios para obtener un grado de control mayor y duradero y alcanzar objetivos más complejos.

469. La fase de *ejecución* empieza cuando se tiene un grado de control y persistencia suficientemente alto para garantizar el ataque a los objetivos estratégicos sin ser descubiertos. En esta fase, se procede, de manera cautelosa, a la selección, recolección, cifrado y exfiltración de la información de interés para el organismo asociado a la APT.

470. En la fase de *anonimización*, a medida que se van logrando los objetivos específicos se procede a implementar las medidas orientadas a eliminar los posibles rastros dejados (huella digital) y a dificultar una potencial atribución futura destruyendo las posibles evidencias de su actividad y de sus técnicas, tácticas y procedimientos.

471. Una premisa fundamental en los ciberataques procedentes de APTs es mantener el control de la red sin ser detectados el mayor tiempo posible, por ello, en todas las fases se extrema las medidas orientadas a no dejar rastro y se mantiene una actividad que pueda ser percibida como habitual en la red, incluyendo periodos largos de inactividad si fuera necesario.

472. Los ciberataques procedentes de APTs son de tal magnitud, sofisticación y complejidad y sus objetivos son de tal criticidad que la acción para combatirlos debe ser planificada, coordinada y desarrollada mediante una *ciberoperación militar específica*.

473. El combate contra APTs que amenazan objetivos militares precisa de una acción liderada por la fuerza ciberespacial en donde la coordinación y la colaboración con las unidades TIC y su centro de operaciones de red (COR) y con las fuerzas y cuerpos de seguridad del estado es esencial.

474. La colaboración con las unidades TIC y su COR es necesaria porque muchas medidas de defensa tienen que ser implementadas por las unidades TIC o el COR y, en algunas ocasiones, las medidas van a afectar a la operatividad de la red, incluyendo desconexiones temporales de servicios críticos.

475. En la toma de decisiones que afectan a la operatividad de la red, la autoridad operativa de los sistemas afectados deberá decidir considerando los argumentos de la fuerza ciberespacial centrados en la erradicación total de la APT y los argumentos del responsable TIC centrados en mantener la funcionalidad de la red.

476. La colaboración con los cuerpos de seguridad del estado es necesario, en aquellos casos, que se considere que la acción de la APT puede ser, además, constitutiva de delito y se debe iniciar el proceso judicial pertinente.

477. El gran peligro de las APTs es que producen efectos silenciosos, que no llaman la atención y que no afectan a la operatividad y funcionalidad de los servicios y sistemas de la red, creando una falsa percepción de inocuidad en las autoridades no directamente implicadas en la ciberdefensa pero que a la postre son las que toman las decisiones sobre los recursos y las medidas necesarias para hacerles frente.

Caza de ciberamenazas

478. La *caza de ciberamenazas* (threat hunting) es el proceso dinámico y proactivo de ciberdefensa orientado a la detección y aislamiento de amenazas avanzadas que evaden las soluciones de seguridad tradicionales basadas en SIEM y dispositivos de ciberseguridad perimetral (cortafuegos, IDS, IPS, sandboxing[50], etc.).

479. La ciberdefensa tradicional se basa en la monitorización de la red propia, fundamentalmente en el perímetro, con la finalidad de detectar ciberataques mediante el reconocimiento de patrones, anomalías y amenazas previamente conocidas (firma).

480. La caza de ciberamenazas se basa en la monitorización de la red propia, en perímetro e internamente, con la finalidad de descubrir nuevos patrones de ciberataque mediante la identificación automática de comportamientos anómalos (comportamientos que no se ajustan a la actividad habitual de la red) de los usuarios, procesos y dispositivos de la red.

481. Un sistema de caza de amenazas eficaz es un proceso creativo (basado en hipótesis y suposiciones de incumplimientos) materializado a través de una metodología flexible que basa su éxito en el conocimiento, la experiencia y la destreza del personal que lo opera (cazadores o analistas) más que en las herramientas.

482. Una vez descubierto un nuevo patrón se debe generar una reacción (automática o humana) para repeler el ciberataque y a continuación se debe diseñar e implementar un nuevo plan, en colaboración con la seguridad tradicional, para reducir la superficie de ataque. Por último, la unidad de investigación forense puede iniciar sus investigaciones para descubrir las causas y el origen.

483. En cualquier caso, una sólida ciberdefensa necesita los dos tipos de herramientas y enfoques de ciberdefensa puesto que unas complementas a las otras.

484. La referencia mundial actual para el desarrollo de modelos y metodologías de ciberamenazas es la base de datos de libre acceso MITRE ATT&CK®[51] que proporciona información de las TTPs (tácticas, técnicas y procedimientos) basadas en observaciones reales.

485. La referencia MITRE ATT&CK proporciona un marco técnico y operativo común de ciberseguridad de uso habitual tanto en el sector público como en el privado facilitando el entendimiento y la cooperación público-privada.

PRINCIPIOS DOCTRINALES

486. La ciberdefensa es una capacidad de combate especializada en el ámbito de operaciones ciberespacial y no una función de los ámbitos convencionales. Es una opción más en manos del comandante de una misión para generar los efectos deseados en el campo de batalla o área de operaciones o para apoyar a otras fuerzas convencionales a generar sus efectos.

487. Para facilitar la organización y el uso de la ciberdefensa como una capacidad militar y para garantizar su integración fluida en la acción conjunta con las capacidades terrestres, marítimas y aéreas, es necesario que la ciberdefensa se rija por los mismos principios doctrinales (principios de la guerra) y adaptarlos a las peculiaridades del ciberespacio.

488. Las operaciones militares se basan en medios, recursos y tácticas diferentes por cada espacio, pero deben ser regidas por los mismos principios que garanticen el acuerdo intelectual y la acción conjunta.

489. Los principios doctrinales que guían la actuación de las fuerzas militares en las operaciones son los principios fundamentales del arte militar (*voluntad de vencer, libertad de acción y capacidad de ejecución*) y los principios operativos que se derivan de los fundamentales (*objetividad, aprovechamiento del éxito, concentración de esfuerzos, flexibilidad, economía de medios, unidad de mando, seguridad, sorpresa, sencillez, restricción y perseverancia*).

490. La *voluntad de vencer* es el firme propósito del mando y de las tropas de imponerse al adversario y cumplir la misión en cualquier situación por desfavorable que sea. En el ciberespacio la voluntad de vencer adquiere una especial relevancia debido a las numerosas ocasiones en las que un defensor se encontrará en una situación desfavorable debido a la asimetría en el enfrentamiento o en las que un atacante se encontrará con defensas aparentemente inexpugnables.

491. La *libertad de acción* es la posibilidad de decidir, preparar y ejecutar los planes a pesar de la voluntad del adversario. Requiere disponer de un conocimiento sólido de la capacidad de ciberdefensa del adversario y de sus redes y de la capacidad de ciberdefensa propia. Se adquiere cuando se alcanza y mantiene la situación de cibersupremacía o ciberperioridad.

492. La *capacidad de ejecución* es la aptitud de determinar, adaptar y usar, de manera eficaz y eficiente, los medios de ciberdefensa conforme a la misión, estableciendo los planes necesarios para el desarrollo de las ciberoperaciones, ejecutándolos de acuerdo a lo planeado y modificándolos según la situación aconseje.

493. Dada la naturaleza dinámica del ciberespacio la modificación de los planes de ciberoperaciones será algo habitual y no ocasional, necesitándose unos mecanismos que faciliten una reforma ágil para adaptarse a la nueva situación de acuerdo con la información obtenida de una sólida conciencia de la situación ciberespacial y unos indicadores previamente definidos.

494. La *objetividad* preconiza que las ciberoperaciones militares deben estar dirigidas a alcanzar un objetivo militar fijado que ha de ser claramente definido, decisivo y alcanzable.

495. Cada elemento participante en la ciberoperación debe conocer, de una manera clara y sin ambigüedad, cuál es su objetivo (sistema, red, servicio, usuario, información, etc.), cual es el efecto requerido (exfiltración, interrupción, degradación, destrucción, etc.) y las condiciones particulares de tiempo y seguridad (anonimato, efectos colaterales, etc.).

496. Los objetivos deben ser rentables. La rentabilidad se debe valorar de acuerdo a la comparación entre los recursos empleados y el beneficio para la misión y no en base a valoraciones exclusivamente dentro del ámbito de la fuerza ciberespacial.

497. El *aprovechamiento del éxito* consiste en aprovechar, retener y explotar la iniciativa y beneficiarse de la disminución, ya lograda, de la capacidad de ciberdefensa del adversario, anulando o desequilibrando sus posibilidades de acción o reacción.

498. El aprovechamiento del éxito se logra a través de alcanzar una situación de cibersupremacía o cibersuperioridad conocida o desconocida por el adversario.

499. La situación de cibersupremacía/superioridad conocida se alcanza cuando el adversario conoce nuestros movimientos en sus redes y a pesar de ello no tiene capacidad para evitar nuestra libertad de acción.

500. La situación de cibersupremacía/superioridad desconocida se alcanza cuando el adversario desconoce nuestros movimientos en sus redes y por ello no realiza acciones de respuesta para evitar nuestra libertad de acción.

501. Las ciberoperaciones ofensivas tienen la finalidad de mermar la capacidad operativa del enemigo en el ciberespacio y esto puede ser aprovechado por la propia fuerza ciberespacial o por las fuerzas de otros ámbitos. Un caso real de aprovechamiento conjunto de las ciberoperaciones se dio en el conflicto entre Rusia y Georgia en Osetia del Sur en el año 2008, en el que las operaciones militares armadas fueron planeadas y conducidas conjuntamente con las ciberoperaciones.

502. La *concentración de esfuerzos* es la concentración de los efectos producidos por la capacidad de ciberdefensa en el lugar y momento más ventajoso para generar resultados decisivos para la misión.

503. Un ejemplo de concentración de esfuerzos son los ataques de denegación de servicio distribuidos (DDoS) que buscan la saturación de un servicio mediante la inundación a través de masivas peticiones legitimas de acceso. El ataque DDoS procede desde muchos puntos simultáneamente sobre un objetivo único haciendo uso de la capacidad de redes secuestradas (Botnets[52]).

504. La *flexibilidad* es la facultad de los mandos para modificar las disposiciones adoptadas y adaptarse a las variaciones de la misión y la situación. Es fundamental en la ciberdefensa, debido a la necesidad de adaptar las medidas defensivas y de respuesta al cambio continuo en las TTPs de los ciberataques y a la necesidad de modificar las TTPs de las acciones ofensivas para llegar a ser efectivos en defensas robustas.

505. La *economía de medios* es el uso eficiente de los medios de ciberdefensa disponibles que lleva a dedicar a cada misión los indispensables para su cumplimiento. Este principio adquiere gran relevancia, en un entorno asimétrico en donde los recursos necesarios para defenderse de un ciberataque suelen ser mucho más costosos que los necesarios para realizar el ciberataque.

506. En entornos de carestía de recursos de ciberdefensa, las capacidades de ciberdefensa podrían centralizarse en el ámbito conjunto para conseguir un uso más eficiente.

507. La *unidad de mando* es la disposición de un único líder o autoridad por cada misión, operación u objetivo en todos los niveles del cibercombate.

508. La unidad de mando es de especial relevancia en aquellas ciberoperaciones que implican a otros actores aparte de la fuerza ciberespacial, en el entendimiento de que toda ciberoperación en el marco de la ciberdefensa nacional debe ser liderada por el comandante de la fuerza ciberespacial.

509. La *seguridad* es la capacidad de precaverse contra los ciberataques de un adversario mediante la debida prevención y reacción.

510. La prevención se basa en la implementación de medidas de seguridad que rechacen ciberataques conocidos y desconocidos o que los hagan improductivos y en la capacidad de explotación que proporcione información precisa y oportuna de las TTPs de potenciales adversarios con la finalidad de anticiparse.

511. La reacción se basa en la capacidad de resiliencia para seguir operando, en modo total o degradado, pese a estar sometidos a un ciberataque, en la capacidad de restauración de las funciones esenciales después de sufrir los efectos de un ciberataque (a través del establecimiento de un plan de continuidad de las operaciones) y en las capacidades ofensivas que puedan destruir o mermar las capacidades de ciberdefensa del adversario.

512. La *sorpresa* consiste en la realización de acciones de ciberdefensa en el lugar, momento y forma (TTPs) desconocidos por el adversario o para los que no está preparado.

513. La sorpresa es una característica inherente a las ciberamenazas, de tal manera que no sólo el lugar y el momento elegidos por los ciberatacantes son, en muchos casos, desconocidos por el defensor, sino que la propia naturaleza del ataque, su tipo, forma y táctica empleada cambian con gran celeridad.

514. Las emboscadas (señuelos, redes trampa, plataformas de ciberdecepción o señuelos armados) y los ciberataques de día cero son ejemplos de cibertácticas defensivas y ofensivas que se basan en el factor sorpresa.

515. La *sencillez* consiste en la preparación de planes claros y sin complicaciones y la emisión de órdenes precisas y concisas para evitar malos entendidos y confusión y facilitar su comprensión y cumplimiento.

516. Tener presente siempre el principio de sencillez es de vital importancia en la ciberdefensa debido a la complejidad del planeamiento y la conducción de ciberoperaciones y a la velocidad y dinamismo de su ejecución que obliga a continuas modificaciones y cambios de rumbo.

517. La *restricción* se refiere a la limitación de daños colaterales y la evitación del uso innecesario de la fuerza.

518. Este principio adquiere una especial relevancia en el ciberespacio por la dificultad de controlar el alcance de los efectos de un ciberataque y por la dificultad de la atribución y la posible utilización de ciberataques de falsa bandera que pudiera hacer que una reacción no se realice sobre el verdadero artífice del ciberataque sino sobre una tercera parte secuestrada o inculpada alevosamente por el atacante.

519. La *perseverancia* se refiere a la aptitud de garantizar el compromiso necesario para alcanzar la situación final estratégica.

520. La persistencia en ciberdefensa no significa mantener la actividad de manera continua y permanente, sino mantener las condiciones que garanticen el éxito, lo que, en ocasiones, podría conllevar conciliar periodos de actividad con periodos de inactividad. Las APT son un ejemplo de uso de la perseverancia.

521. La perseverancia implica unidad de mando que garantice el compromiso de todos los implicados con los objetivos estratégicos.

522. En el entorno de la ciberdefensa, donde se sabe de antemano que la protección total no es posible de alcanzar, la persistencia ante defensas robustas es un factor determinante para identificar vulnerabilidades que tarde o temprano saldrán a la luz.

523. Todos los principios doctrinales son una guía para todos los ámbitos de operaciones, pero obtienen especial relevancia en el ámbito conjunto (tierra, mar, aire y ciberespacio).

ECOSISTEMA CIBERESPACIAL

524. El *ecosistema ciberespacial* es el sistema compuesto por todos los elementos que se relacionan entre sí a través del ciberespacio, junto con el propio ciberespacio. Como tal ecosistema, el ecosistema ciberespacial genera sus propias normas y comportamientos específicos que permiten el desarrollo y evolución (individual y colectivamente) de sus habitantes.

525. Tres son las partes fundamentales del ecosistema ciberespacial: los *elementos* (habitantes) que interactúan entre sí (la infraestructura TIC, el software o las aplicaciones, la información, los protocolos de transporte, la energía eléctrica y las personas), el propio *ciberespacio* (hábitat) y las *relaciones* y actividades que se realizan en o a través de él.

526. La característica fundamental del ecosistema ciberespacial es la interacción que se produce entre personas, de forma individual o a través de colectivos organizados (empresas, administración pública, universidad, organizaciones internacionales, etc.) generándose actividades de toda índole, económicas, sociales, artísticas, divulgativas, formativas, colaborativas y también de defensa en toda su extensión.

527. La *ciberdefensa* no es sólo una actividad más de las que se desarrollan en el ecosistema ciberespacial sino es la actividad que permite, en el ámbito de sus competencias, el libre y legítimo ejercicio de todas las actividades.

528. En este sentido se entiende la *ciberdefensa militar* como la capacidad dirigida a la defensa del libre y legítimo ejercicio de todas las actividades del ministerio de defensa en el ciberespacio y, además, es la capacidad principal de la ciberdefensa nacional y uno de los pilares de la ciberseguridad nacional.

529. Aspectos relevantes del ecosistema ciberespacial relacionados con la ciberdefensa son la *ciberseguridad nacional, la ciberseguridad internacional, la cooperación público privada, los riesgos de terceros, los ciberriesgos asociados a los estados de pandemia y la información.*

Ciberseguridad nacional

530. La *ciberseguridad nacional* es la parte de la seguridad nacional enfocada a la protección de los intereses nacionales en el ciberespacio. Está fundamentada en tres pilares: *la Ciberresiliencia Nacional, la Ciberprotección Nacional y la Ciberdefensa Nacional.*

531. La *ciberresiliencia nacional* es el conjunto de capacidades nacionales de ciberseguridad enfocadas a la prevención y protección de las redes y sistemas TIC de la nación frente a potenciales ciberataques, al mantenimiento de la operatividad durante su transcurso y a la restauración de las funciones esenciales después de sufrir sus efectos.

532. La ciberresiliencia nacional se gestiona a través de los diversos CERTs nacionales establecidos; principalmente los CERTs de ámbito gubernamental, militar, infraestructuras críticas, universidades y sector privado.

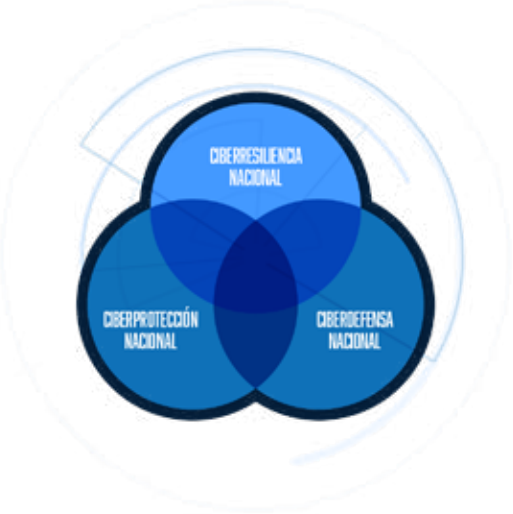


ILUSTRACIÓN 31. CIBERSEGURIDAD NACIONAL

533. La *ciberprotección nacional* es el conjunto de capacidades nacionales de ciberseguridad enfocadas a la protección frente al ciberdelito y ciberterrorismo. Es llevada a cabo por unidades especializadas de las fuerzas y cuerpos de seguridad del estado.

534. La *ciberdefensa nacional* es el conjunto de capacidades nacionales de ciberdefensa (defensiva, explotación y ofensiva) enfocadas a la defensa de los intereses nacionales frente a ciberamenazas procedentes de otros estados u otras ciberamenazas de gran magnitud que pudieran afectar a la defensa nacional. Principalmente, es llevada a cabo por las unidades de ciberdefensa de las fuerzas armadas, normalmente organizadas bajo una fuerza ciberespacial constituyendo la ciberdefensa militar, pudiendo ser apoyadas por otros poderes estatales en caso necesario (político, económico, diplomático, etc.).

535. La ciberdefensa nacional es parte fundamental de la defensa nacional apoyándola en el cumplimiento de la misión, contribuyendo al nivel de disuasión creíble, facilitando la cooperación con organismos internacionales, permitiendo un uso eficiente de los recursos, minimizando los riesgos a población civil y a fuerzas propias, fomentando la conciencia de defensa nacional (campañas de concienciación de ciberdefensa, ciberreserva) y cooperando con el sector privado y sector académico.

536. Para alcanzar una ciberseguridad nacional robusta es necesario fortalecer sus tres pilares (ciberresiliencia, ciberprotección y ciberdefensa), así como mantener una estrecha colaboración y cooperación entre ellos y con sus homólogos internacionales.

537. Una ciberseguridad nacional sólida necesita una *estrategia nacional de ciberseguridad* clara (expresada en un lenguaje entendible en todos los niveles de implicación), precisa (que establezca unas directrices y medidas eficaces adaptadas a la situación nacional), realista (que establezca objetivos concretos alcanzables) y práctica (que prevea los recursos necesarios para su implementación).

538. Una estrategia nacional de ciberseguridad debe identificar el estado final de ciberseguridad nacional deseado, definir un modelo de gobernanza específico que incluya a todos los actores nacionales principales, valorar los principales ciberriesgos a la seguridad nacional, establecer unas medidas concretas para mitigar los ciberriesgos previstos, facilitar la aplicación de las medidas a través de la provisión de los recursos necesarios y vigilar el cumplimiento y la eficacia de las medidas a través del establecimiento de un sistema de indicadores.

539. Existen algunas referencias generales para la elaboración de una estrategia de ciberseguridad nacional, como la "Guide to developing a National Cybersecurity Strategy"[53] de la ITU y otros organismos o la "National Cyber Security Strategy Guidelines"[54] del Centro de Excelencia de Ciberdefensa de la OTAN (NATO CCDCOE).

540. Existen numerosas referencias nacionales (España, Brasil, Reino Unido, Israel, China, Estados Unidos, France, Estonia, etc.), con diferentes aproximaciones, que pueden servir de ejemplo. En la biblioteca de la web del Centro de Excelencia de Ciberdefensa de la OTAN (NATO CCDCOE) se pueden encontrar estudios sobre la organización de la ciberseguridad en estos países.[55]

541. El desarrollo e implementación de una estrategia de ciberseguridad nacional es un proceso cíclico compuesto por cinco fases: *dirección, análisis, estrategia, plan de acción y evaluación.*

542. En la *fase inicial,* se establece un equipo de *dirección* para el desarrollo y seguimiento de la implementación de la estrategia, compuesto por una autoridad o responsable máximo, un grupo de expertos nacionales y todos aquellos actores nacionales, del sector

público y privado, que su participación y colaboración puntual, sea necesaria en alguna fase del ciclo.

ILUSTRACIÓN 32. CICLO ESTRATEGIA CIBERSEGURIDAD

543. En la *fase de análisis*, se analiza la situación actual, se determina el estado final deseado, se realiza un análisis de riesgos para valorar el ciberriesgo para alcanzar el estado final deseado, se analizan y valoran distintas estrategias nacionales con diferente aproximación y experiencia para contrastar ideas y se analizan y valoran las potenciales medidas a implementar.

544. En la *fase de estrategia*, se procede a la elaboración del borrador de estrategia conforme a los resultados de la fase de análisis y se pasa a todos los actores implicados, públicos y privados, para intentar llegar a un consenso nacional lo más extenso posible. Una vez alcanzado un consenso aceptable, se consolida el borrador y se pasa como documento final para su aprobación y publicación.

545. En la *fase de implementación,* se materializa la estrategia de acuerdo a un plan de acción que establece las líneas de acción, objetivos concretos a implementar, los responsables de su ejecución, el calendario y los mecanismos que facilitan los recursos humanos y económicos necesarios.

546. Finalmente, en la *fase de evaluación*, el equipo de dirección vigila el cumplimiento de las medidas establecidas en la estrategia y valora la eficacia de las medidas implementadas (a través de auditorías periódicas), identificando el nivel de madurez alcanzado y las lecciones aprendidas que ayuden a una mejora dinámica del proceso.

547. Uno de los aspectos más importantes en la ciberseguridad nacional es la protección de las *infraestructuras criticas nacionales* frente a ciberamenazas.

548. La protección de las infraestructuras críticas nacionales es responsabilidad de los operadores críticos (sector privado en su gran mayoría) que proporcionan la ciberseguridad que ellos consideran apropiada para prestar, sin interrupciones, el suministro habitual en periodos de paz o estabilidad.

549. La ciberseguridad preestablecida por los operadores críticos no suele ser suficiente para protegerse frente a ciberataques sofisticados que afecten a la seguridad nacional por lo que se tienen que prever procedimientos, en el marco de la ciberseguridad nacional, para generar medidas de ciberseguridad adicionales que compensen las carencias en los casos de extrema gravedad. Estos mecanismos de compensación pueden ser en forma de previsión y reserva de recursos económicos o humanos adicionales.

550. La fuerza ciberespacial debe estar preparada, en caso de necesidad nacional, para prestar apoyos puntuales a los operadores críticos que se determinen, mediante el empleo de sus capacidades operativas y técnicas; en especial, su capacidad de gestión de eventos de seguridad, auditorías, investigación forense digital y ciberdefensa desplegable.

Ciberseguridad internacional

551. Muchos de los ciberdelitos y ciberataques que afectan a ciudadanos, entidades o intereses de una nación proceden de territorios o medios pertenecientes a otras naciones. Además, la atribución técnica y legal del origen de los ciberataques es difícil de alcanzar sin la colaboración de los países implicados en la ruta de los ciberataques. Por todo ello, ningún país del mundo es autosuficiente para prevenir y perseguir la totalidad de los ciberdelitos y ciberataques que le afectan; consecuentemente, la *cooperación internacional* en materia de ciberseguridad es vital no solo para disponer de una ciberseguridad internacional sólida sino también, para la ciberseguridad de cada nación.

552. La ciberseguridad internacional se basa fundamentalmente en la cooperación entre los organismos responsables de cada uno de los pilares de la ciberseguridad nacional (ciberresiliencia, ciberprotección y ciberdefensa) y sus homólogos de otros países y de organizaciones internacionales.

553. Es necesario establecer acuerdos políticos y diplomáticos entre países y organizaciones internacionales para la persecución de ciberataques y ciberdelitos; y alcanzar un consenso lo más extenso posible en la aplicación del derecho internacional en el ciberespacio.

554. En el plano de la *ciberresiliencia* es importante que todos los CERTs nacionales, públicos o privados, sean oficialmente reconocidos y participen activamente en los foros y organizaciones internacionales dedicadas a la coordinación de los CERTs de todo el mundo o de una zona geoestratégica específica con la finalidad de compartir información sobre cibervulnerabilidades, ciberataques y ciberriesgo y las correspondientes medidas de mitigación.

555. A nivel mundial, el FIRST[56] (Fórum of Incident Response and Security Teams) destaca como la iniciativa predominante en la coordinación de CERTs.

556. A nivel europeo, destaca la agencia europea de ciberseguridad (ENISA) cuya finalidad es contribuir activamente a la política europea de ciberseguridad, apoyando a los Estados miembros y a las partes interesadas de la Unión Europea en la respuesta a ciberincidentes de gran escala que tienen lugar a través de las fronteras en los casos en que dos o más Estados miembros de la UE se han visto afectados. Además, ENISA contribuye al buen funcionamiento del mercado único digital.

557. ENISA trabaja en estrecha colaboración con los Estados miembros y el sector privado para ofrecer asesoramiento y soluciones, así como para mejorar sus capacidades, incluyendo, ejercicios paneuropeos de ciberseguridad, desarrollo y evaluación de estrategias nacionales de ciberseguridad, cooperación y desarrollo de capacidades de CERTs, estudios sobre internet de las cosas e infraestructuras inteligentes y análisis de ciberamenazas.

558. Los organismos principales de coordinación de CERTs europeos son la Asociación Transeuropea de Investigación y Educación de Redes (Trusted Introducer de TERENA)[57] y el EGC Group[58] (European Government CERTs).

559. A nivel interamericano, destaca el registro de direcciones de Internet de América Latina y Caribe (LACNIC[59]) cuya finalidad es contribuir al desarrollo de Internet en la región, mediante una política activa de cooperación, la promoción y defensa de los intereses de la comunidad regional y la colaboración; con la finalidad de generar las condiciones para que Internet sea un instrumento efectivo de inclusión social y desarrollo económico de América Latina y el Caribe. Son de destacar las reuniones anuales de CSIRTs (LAC-CSIRTs[60]) y el proyecto amparo[61]

560. En el plano de la *ciberprotección*, es importante que las unidades nacionales de protección frente al ciberdelito y ciberterrorismo cooperen con sus homólogos de otros países y de organizaciones internacionales.

561. A nivel europeo, es fundamental la relación, coordinación y cooperación de las unidades de ciberdelincuencia nacionales con el centro europeo contra el ciberdelito (*EC3*[62], European Cybercrime Center) de la EUROPOL, cuya finalidad es fortalecer la respuesta ante la ciberdelincuencia en la UE y ayudar a proteger a los ciudadanos, las empresas y los gobiernos europeos de ella.

562. También es importante la relación, coordinación y cooperación con la agencia europea para la cooperación judicial penal (*EUROJUST*[63]) cuya finalidad es ayudar a las autoridades europeas a cooperar en la lucha contra el terrorismo y las formas graves de delincuencia organizada que afectan a más de un país de la UE.

563. A nivel interamericano, es fundamental la relación, coordinación y cooperación de las unidades de ciberdelincuencia nacionales con los organismos responsables de la lucha frente al ciberdelito de la comunidad de policías de América (*AMERIPOL*), cuya finalidad es fomentar, potenciar y sistematizar la cooperación policial, el intercambio de información y la asistencia judicial entre los estados miembros.

564. En el plano de la *ciberdefensa* es importante que la fuerza ciberespacial nacional coopere con otras fuerzas ciberespaciales de su entorno geopolítico y con las organizaciones internacionales de defensa colectiva a las que pertenece (*OTAN*, Agencia Europea de Defensa, *Junta Interamericana de Defensa*, etc.).

565. También, es necesario la participación activa en los foros internacionales de ciberdefensa como el Foro de Cibercomandantes (*Cyber Commander´s Forum*), inicialmente fundado por países pertenecientes al Centro de Excelencia de Ciberdefensa de la OTAN (NATO CCDCOE) y actualmente abierto a otros Mandos de Ciberdefensa del mundo, cuya finalidad es fomentar la cooperación internacional en materia de ciberdefensa; o el *Foro Iberoamericano de Ciberdefensa* fundado en 2016 y que actualmente forman Argentina, Brasil, Chile, Colombia, España, México, Perú y Portugal, con la finalidad de mantener una cooperación fluida en materia de ciberdefensa, especialmente en las áreas de formación, ejercicios, intercambio de información e investigación y desarrollo.

566. La cooperación internacional en ciberdefensa suele alcanzarse de manera más sencilla en aquellos aspectos relativos a actividades defensivas que en aquellos relacionados con la ciberinteligencia y las actividades ofensivas. En estos últimos casos, es necesario sentar las bases de la cooperación, de manera gradual, mediante acuerdos bilaterales con socios con los que previamente se ha llegado a un estado de confianza mutua.

Cooperación público-privada

567. En tiempos pasados la industria militar era el motor y el referente de una industria civil que aprovechaba los avances de la investigación y desarrollo militar de doble uso en su beneficio. Actualmente la tendencia es la contraria, las grandes corporaciones multinacionales junto con las universidades realizan las grandes aportaciones tecnológicas de las cuales se nutre el estamento militar. Muchas de las tecnologías desarrolladas en el sector de las tecnologías de la información, de la ciberseguridad, de los videojuegos, de las redes sociales, etc., son de gran utilidad en el campo de la ciberdefensa militar.

568. El establecimiento de una *industria nacional de ciberdefensa* es esencial para evitar la dependencia de otros países en el desarrollo y empleo de capacidades de ciberdefensa críticas.

569. Para el desarrollo de la industria nacional de ciberdefensa, es necesario que desde el ministerio de defensa se fomente y establezcan *programas de desarrollo y obtención de capacidades de ciberdefensa* incluyendo sistemas de armas ciberespaciales (de la misma manera que se hace con los programas de desarrollo y obtención de armamento y material terrestre, naval, o aéreo) a través de acuerdos y consorcios con las principales empresas y corporaciones nacionales.

570. Los programas de desarrollo y obtención de capacidades de ciberdefensa tienen que definirse con especial cautela para favorecer el *equilibrio de intereses* de las dos partes; de tal manera que, se garantice el uso, evolución y personalización de los productos desarrollados por parte de las unidades de ciberdefensa de las fuerzas armadas en las condiciones que el ministerio requiera y se limite su venta a otros países sin la autorización del ministerio y, a la vez, se facilite el necesario beneficio económico de las empresas implicadas permitiendo la comercialización de los productos desarrollados de acuerdo a unas condiciones prefijadas.

571. En la mayoría de los casos será necesario que la *propiedad intelectual* de los productos desarrollados a través de programas de ciberdefensa financiados por el ministerio de defensa quede en el seno del propio ministerio.

572. La cooperación público-privada debe evitar convertirse en un juego de suma cero[64] y trabajar para llegar a modelos que garanticen situaciones de *beneficio mutuo* frente a ciberamenazas comunes; a través del establecimiento de una inteligencia superior con los datos aportados por el sector privado (datos optimizados de ciberamenazas, cibervulnerabilidades y ciberriesgos procedentes de sus extensas redes globales) y las capacidades de inteligencia y análisis de alto nivel político y estratégico del sector público.

573. Para un intercambio de información eficaz entre el sector privado y el público, es necesario crear un *estado de confianza* y un mecanismo eficaz que verifique que la aportación de ambas partes es equilibrada, que la información no se filtra a terceras partes sin autorización y que se hace un uso adecuado de la información por ambas partes.

574. La cooperación público-privada es esencial para garantizar la ciberseguridad y la ciberresiliencia de los sistemas de información y de control de las infraestructuras críticas nacionales estableciendo mecanismos conjuntos que permitan prevenir y responder a ciberamenazas avanzadas con capacidad para evadir los sistemas de ciberseguridad tradicionales implementados por los operadores críticos.

575. La cooperación público-privada en materia de ciberdefensa es necesaria por las siguientes *razones*:

- Alcanzar un estado de ciberseguridad nacional más eficaz y eficiente, creando situaciones de beneficio común y evitando situaciones de competición y duplicidad de esfuerzos.
- Minimizar la superficie de ciberriesgo de los dos sectores al gozar de una estructura de ciberseguridad común más robusta.
- Garantizar el alcance y la aplicación de las medidas derivadas de la estrategia de ciberseguridad nacional que en muchos casos deben ser implementadas por actores del sector privado.
- Poder responder de manera conjunta y ágil a una cibercrisis o ciberataque que afecte a la seguridad nacional.

- Concienciar al sector privado de su papel fundamental en la seguridad nacional más allá de su compromiso con sus clientes y socios.
- Garantizar el cumplimiento de la normativa en materia de ciberseguridad nacional.
- Ahorrar costes mediante la compartición eficiente de recursos.
- Acceso a una base de datos de información y conocimientos más completa.

576. La cooperación público-privada en materia de ciberdefensa requiere la *participación activa* de, al menos, la fuerza ciberespacial nacional; los servicios o agencias nacionales de inteligencia; CERTs nacionales; operadores críticos; organismos públicos de contratación; organismos de gestión de crisis; organismos reguladores; servicios jurídicos; observatorios tecnológicos, think-tanks, fundaciones y centros públicos y privados de investigación y desarrollo relacionadas con la ciberdefensa; y universidades y empresas de sectores aplicables a la ciberdefensa.

577. De acuerdo con un estudio realizado por ENISA, los *servicios más demandados* en la cooperación pública-privada en materia de ciberdefensa son el intercambio de información (83%), el análisis e investigación (62%), la concienciación (62%) y las alertas tempranas (59%). Otros servicios habituales son la gestión de crisis, estándares y guías de buenas prácticas, planes de contingencia y continuidad, auditorías de seguridad, ciberejercicios, estudios de mercado, estadísticas, planificación de estrategias y análisis de riesgos.

578. Hay cuatro áreas generales de cooperación público-privada en materia de ciberdefensa: la cooperación de base, la cooperación preventiva, la cooperación reactiva y la cooperación integral.

579. La *cooperación de base* se enfoca a la investigación y desarrollo de sistemas, productos, *herramientas* y TTPs de ciberdefensa en base a una estrategia y agenda conjunta o consensuada.

580. La *cooperación preventiva* se enfoca al establecimiento de un sistema de ciberdefensa para anticipar, prevenir, detectar, protegerse y alertar de ciberataques procedentes de amenazas comunes

581. La *cooperación reactiva* se enfoca al establecimiento de un sistema de ciberdefensa para reaccionar ante ciberataques procedentes de amenazas comunes y recuperar la operatividad.

582. La *cooperación integral* se enfoca a la implementación de un entorno completo de ciberdefensa que implemente, de manera coordinada, las tres áreas (básica, preventiva, reactiva) y establezca mecanismos de realimentación entre ellas.

Riesgo de terceros

583. La mayoría de los sistemas y capacidades de ciberdefensa utilizan componentes (hardware, software, firmware) que *dependen de terceros* (proveedores, cadena de suministro, soporte, consultores) para su fabricación, suministro, distribución, puesta en marcha, operación y mantenimiento.

584. La *lista de terceros* que puede afectar a los ciberriesgos de una organización incluye a los propios fabricantes de cada componente hardware; a los creadores de los códigos de cada pieza de software y firmware; a los integradores, transportistas, subcontratistas y proveedores finales; a los soportes técnicos para la instalación, puesta en marcha y mantenimiento; y a los consultores y servicios profesionales para operación, personalización o actualización.

585. La *gestión de riesgos de terceros* es de tal complejidad, detalle y extensión que debe ser planificada cuidadosamente de una manera realista evitando objetivos inalcanzables o poco rentables para el nivel de la organización. No obstante, el riesgo de terceros, y en particular en la cadena de suministro, es reconocido como una de las grandes amenazas actuales que toda organización debe hacer frente y gestionar adecuadamente.

586. Las grandes organizaciones y corporaciones nacionales tienen una capacidad de control de terceros no accesible para organizaciones medianas o pequeñas; como disponer de un cierto control en la propia cadena de fabricación, tener acceso a los códigos fuente de software o requerir a todos los terceros implicados unas medidas de seguridad específicas. Por ello, es importante que la gestión de terceros se centralice en el órgano de mayor competencia, y consecuentemente, de mayor peso para imponer medidas a terceros.

587. La gestión de riesgos de terceros tiene la finalidad de garantizar, en la medida de lo posible, que los productos, sistemas y servicios adquiridos hacen exactamente lo que se espera de ellos (conforme a los requisitos técnicos y operativos requeridos) y no hacen nada más de lo esperado, ni lo habilitan para hacerlo en un futuro (libres de puertas traseras, malware preinstalado, etc.).

588. A algunos productos, sistemas o procesos se les puede exigir una *certificación* reconocida, nacional o internacionalmente, de calidad o seguridad; pero en muchos casos esto no es viable o rentable, por lo que se debe proceder a realizar una gestión realista de riesgo de terceros.

589. En algunos casos relacionados con elementos o sistemas críticos de ciberseguridad (algoritmos criptográficos, SIEM, sistemas de caza de amenazas, honey nets avanzados, etc.), se puede exigir que la propiedad intelectual, diseño, fabricación, soporte y mantenimiento resida en una empresa o corporación nacional o en una nación aliada. No obstante, en el mercado actual, caracterizado por la globalización y el dinamismo, donde las empresas cambian de propiedad con facilidad, entre países con posiciones geopolíticas muy diferentes; esta medida no suele ser eficaz a medio y largo plazo.

590. La gestión de riesgos de terceros previene frente a la adquisición de productos, sistemas o servicios con defectos, vicios ocultos o con mecanismos malintencionados preinstalados. Una vez adquiridos e instalados los productos o prestados los servicios hay dos maneras habituales de comprobar que operan apropiadamente, mediante análisis de caja blanca o de caja negra.

591. En el *análisis de caja blanca* se estudia el detalle interno del producto (su esquema, diseño, código fuente, etc.) y con la información obtenida se diseñan unas pruebas para comprobar su funcionamiento y comportamiento. Este análisis solo es posible si el fabricante proporciona la información, lo cual en muchos casos no es posible por miedo al riesgo de filtración de información a potenciales competidores. Solo grandes clientes u organizaciones que puedan garantizar la confidencialidad y que puedan proporcionar al fabricante unos beneficios superiores al riesgo de filtración, estarían en disposición de obtener la información blanca necesaria.

592. En el *análisis de caja negra* se obvia el detalle interno del producto y se estudia su funcionamiento y comportamiento mediante un protocolo de pruebas basado en unas entradas especialmente diseñadas que requieren una salida determinada.

593. Todo *proceso de gestión de terceros* requiere seis fases: *definición y establecimiento del equipo de gestión, elaboración e implementación del plan de concienciación, inventario propio, inventario de terceros, plan de acción y evaluación.*

594. El *equipo de gestión de riesgos* debe dirigir todo el ciclo de gestión, desde la concienciación hasta la evaluación. Debe estar compuesto por expertos en ciberseguridad de los sistemas, productos y servicios de la organización, en control de la calidad, en los procesos de contratación y en los asuntos legales y jurídicos.

595. En la mayoría de los casos, será necesario elaborar y ejecutar un plan de *concienciación* sobre el riesgo de terceros orientado a perfiles directivos, debido a que, a pesar de que el riesgo de terceros puede acarrear consecuencias graves para la organización, no suele presentarse o percibirse de manera ostensible o evidente.

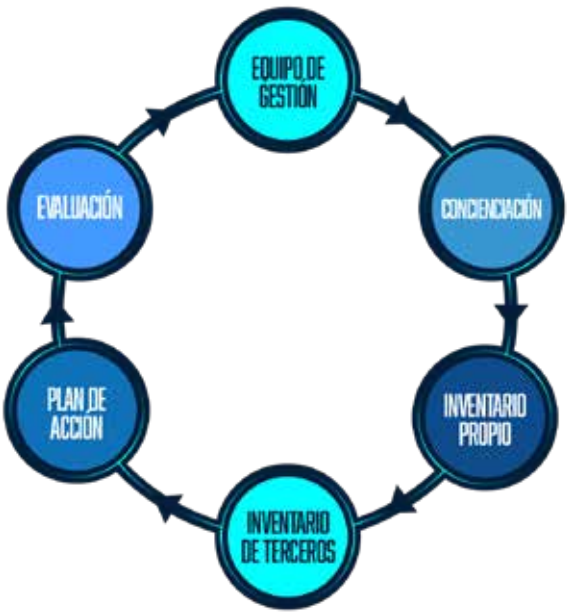


ILUSTRACIÓN 33. GESTIÓN DE RIESGOS DE TERCEROS

596. El *inventario propio* nos proporciona la información base para la identificación de terceros actuales en labores de soporte y mantenimiento y de potenciales futuros terceros (fabricantes, proveedores y distribuidores).

597. El *inventario de terceros* identifica aquellos fabricantes, proveedores, distribuidores, órganos de soporte y mantenimiento de productos, sistemas y servicios críticos para la organización y posibles brechas de seguridad durante todo el proceso, desde la fabricación, transporte, distribución, provisión e instalación hasta la operación, actualización, evolución, personalización y mantenimiento.

598. En el *plan de acción* se detallan las medidas concretas a implementar basadas en una estrategia realista y rentable. Algunos aspectos a considerar son los acuerdos de confidencialidad (NDA), los acuerdos de comunicación de vulnerabilidades por parte de los terceros, los controles de antecedentes de empleados, la acreditación o certificación de los terceros o sus productos como requisito en los procesos contractuales, los requisitos de ciberseguridad en todo el ciclo de los contratos desde el diseño hasta la puesta en marcha, las revisiones del cumplimiento de las medidas de ciberseguridad por terceros, el asesoramiento por parte de los terceros en el aseguramiento de los sistemas provistos, la posibilidad de soporte remoto, el requerimiento de pruebas periódicas, las auditorías de seguridad, los acuerdos de nivel de servicio (SLA) y las guías de buenas prácticas.

599. Existen numerosas medidas posibles orientadas a la gestión de terceros, fundamentalmente, medidas contractuales y medidas técnicas. La ISO 28000 es una buena referencia para identificar las medidas idóneas para la organización.

600. Durante la fase de *evaluación* se debe valorar el cumplimiento y la eficacia de las medidas y realimentar todo el ciclo con la finalidad de ir mejorando, de manera gradual, el plan de acción y alinearlo con los objetivos estratégicos de la organización.

Ciberriesgos asociados a estados de pandemia

601. La declaración de estado de pandemia por la Organización Mundial de la Salud por COVID19 ha derivado en unas medidas tomadas por los gobiernos de las naciones afectadas que conllevan unos riesgos de ciberseguridad adicionales.

602. Las personas que residen en territorios afectados por la pandemia focalizan toda su atención en la seguridad sanitaria y *relajan las medidas de ciberseguridad individual* dando por bueno cualquier comunicación, mensaje, email, link que reciben en relación con la pandemia sin realizar ningún tipo de comprobación. Esta relajación individual es percibida por los ciberdelincuentes y consecuentemente, incrementan su actividad.

603. Durante el estado de pandemia se produce una *sobresaturación de información* que dificulta su asimilación y filtrado por los usuarios y que puede generar colapso en las redes.

604. El estado de pandemia puede requerir medidas de confinamiento de la población y como consecuencia se produce una *hiperactividad en redes sociales* que junto con el relajamiento en la aplicación de las medidas de ciberseguridad individual generan un efecto llamada a la ciberdelincuencia a través de las redes sociales.

605. Uno de los grandes problemas de las sociedades modernas es la *desinformación* (bulos, fake news, operaciones de influencia). En los estados de pandemia, donde predomina la sobresaturación de información, se tiende a dar por bueno toda información que parezca que viene de una fuente oficial y prospera la hiperactividad en redes sociales, se dan las condiciones idóneas para que los bulos se extiendan con gran rapidez.

606. En muchos países en estado de pandemia se toman medidas dirigidas a la contención de la expansión del virus que requieren la paralización de actividades consideradas no esenciales y el confinamiento de los trabajadores no esenciales en sus domicilios. Esto lleva a muchas empresas y organizaciones a fomentar el *teletrabajo* y crear, a tal fin, accesos remotos a sus sistemas de información y control sin la debida planificación ni preparación, sin reparar en los riesgos de ciberseguridad que esto supone.

607. El teletrabajo conlleva un riesgo de ciberseguridad que hay que estudiar cuidadosamente y conciliarlo con los beneficios en operatividad. El riesgo es tanto para pequeñas empresas, normalmente no preparadas para establecer accesos remotos seguros, como para grandes organizaciones o corporaciones con sistemas de ciberseguridad muy robustos que están siendo permanentemente monitorizadas por sus competidores o adversarios en busca de alguna vulnerabilidad que les permita el acceso. Los accesos remotos son, con toda seguridad, una de las principales vías de penetración que serán analizadas.

608. Un ejemplo de un ciberataque a través de acceso remoto a los sistemas de una gran corporación fue el ciberataque realizado a la corporación de la industria de defensa Lockheed Martin de 2011 donde los ciberatacantes explotaron el sistema de acceso VPN[65] de Lockheed Martin, que permitía a los empleados iniciar sesión de forma remota utilizando mecanismos seguros de acceso (tokens de hardware RSA SecurID).

609. En estas situaciones de confinamiento, en la mayoría de los casos, los administradores de seguridad de las redes y sistemas de información serán considerados como no esenciales y se verán obligados a no desempeñar sus cometidos in situ y realizar su trabajo desde su domicilio, a través de accesos remotos, debilitándose así la ciberseguridad a todos los niveles.

610. Una de las medidas que algunos países implementan para contener la expansión del virus es el uso (normalmente con carácter voluntario) de *aplicaciones móviles* con la finalidad de identificar, aislar, probar y tratar cada caso de infección; conocer la trazabilidad de la enfermedad; crear mapas de intensidad epidemiológica y controlar la movilidad. Estas aplicaciones se basan en medidas que puede sen consideradas invasivas al requerir datos de especial protección como datos sanitarios, datos personales y datos de geolocalización. En esto casos la ciberseguridad nacional debe garantizar el uso legítimo de los datos exclusivamente para fines de contención epidemiológica y protegerlos frente a accesos no autorizados.

Información

611. La información es uno de los elementos principales del ecosistema ciberespacial, debido a que el ciberespacio es un medio idóneo para su elaboración, presentación, almacenamiento, procesamiento, transporte y destrucción.

612. En el ámbito de la ciberdefensa, hay cuatro aspectos relevantes a considerar en relación con la información: la gestión de la información y el conocimiento propio y las acciones contra la gestión de la información y el conocimiento del adversario; la protección de la confidencialidad, integridad y disponibilidad de la información propia y las acciones contra la protección de la confidencialidad, integridad y disponibilidad de la información del adversario; la protección frente a intentos de exfiltración no autorizada de información propia y las ciberoperaciones de exfiltración de información de adversarios de interés para la misión; y las ciberoperaciones de influencia y contrainfluencia.

613. La *gestión de la información y el conocimiento propio* es una capacidad de mando esencial para de la fuerza ciberespacial que debe fomentar y proteger.

614. Las *acciones contra la gestión de la información y el conocimiento del adversario* generan efectos de valor estratégico. Por ejemplo, acciones que afecten a la veracidad de la conciencia de la situación ciberespacial o acciones que afecten a la integridad de planes operativos pueden generar desconfianza en el sistema de mando y control y consecuentemente afectar de manera transcendente al proceso de la toma de decisiones. Es una capacidad más propia de las unidades de operaciones de información, aunque la fuerza ciberespacial puede prestar un apoyo especial por su conocimiento del medio.

615. La *protección de la confidencialidad, integridad y disponibilidad de la información* es un servicio de la fuerza ciberespacial y una capacidad propia de los organismos responsables de la seguridad de la información.

616. Las *acciones contra la protección de la confidencialidad y la integridad* de la información del adversario son más propias de los servicios de criptografía mediante sus técnicas de criptoanálisis, pudiendo apoyar a la fuerza ciberespacial en caso necesario. *Las acciones contra la disponibilidad* son propias de la fuerza ciberespacial a través de acciones ofensivas como los ciberataques DDoS.

617. La *protección frente a intentos de exfiltración* no autorizada de información es una responsabilidad de la fuerza ciberespacial a través, fundamentalmente, de su capacidad de caza de amenazas persistentes avanzadas.

618. Las *ciberoperaciones de exfiltración de información de adversarios* de interés para la misión es una responsabilidad de la fuerza ciberespacial que se debe realizar con extremo cuidado y que requerirá el concurso de sus capacidades de ciberinteligencia y ofensivas.

619. Las *operaciones de influencia* tienen la finalidad de elaborar, gestionar, modificar, denegar, presentar, destruir o usar la información pública o del adversario, para promover percepciones, actitudes y comportamiento en determinadas audiencias, favorables a las operaciones propias y así influir en la toma de decisiones, tanto humanas como automatizadas. Es una responsabilidad más propia de las unidades de operaciones de información (INFOP) y de las unidades de operaciones psicológicas (PSYOP).

620. Debido a que el ciberespacio es, actualmente, el principal medio de gestión de la información, la fuerza ciberespacial por su conocimiento del medio y sus capacidades para operar en él, puede servir de gran apoyo a las unidades INFOP y PSYOP en las operaciones de influencia.

621. Las *operaciones de contrainfluencia de la información propia* requiere un grado de control del ciberespacio propio (cibersupremacía o cibersuperioridad), un nivel de protección robusto de la confidencialidad, integridad y disponibilidad de la información y una concienciación a nivel individual de los riesgos y vulnerabilidades asociados.

622. Las *operaciones de contrainfluencia de la información pública* es un problema de gran complejidad que requiere el concurso de organismos privados y, sobre todo, de una concienciación robusta y continua, a nivel individual, de los riesgos y vulnerabilidades asociados.

623. En la mayoría de los casos, en los asuntos de operaciones de información e influencia se requerirá la acción conjunta de las unidades INFOP, las unidades PSYOP y la fuerza ciberespacial.

624. En el ámbito de la ciberseguridad nacional, son muy habituales las *acciones de desinformación* con la finalidad de cambiar la opinión de un público objetivo sobre un asunto concreto, reemplazándola por otra visión alternativa; y son consideradas por los poderes políticos como uno de los grandes problemas a resolver.

625. La resolución de este problema va más allá de la implementación de medidas puramente técnicas y necesita conciliar aspectos legales y de libertad de expresión, que se escapan del ámbito de responsabilidad de la ciberdefensa militar. No obstante, la fuerza ciberespacial puede servir de apoyo en la aplicación de medidas técnicas.

ASPECTOS LEGALES

626. La aplicación del derecho internacional al ciberespacio y a las ciberoperaciones ha sido materia de debate en la última década y continúa siéndolo en la actualidad. Durante este debate han surgido dos posiciones principales, la posición occidental y la posición oriental.

627. La *posición occidental*, respaldada por los países del entorno de la Unión Europea y la OTAN, sostiene que el derecho internacional actual es aplicable en los casos de ciberataques y ciberdelitos, con la correspondiente interpretación; y consecuentemente, no es necesario la elaboración de un derecho internacional específico para asuntos del ciberespacio.

628. La *posición oriental*, respaldada principalmente por Rusia y China, sostiene que es necesario el desarrollo de un derecho específico para asuntos del ciberespacio y que los estados deben tener un control soberano sobre su ciberespacio.

629. Debido a la naturaleza transfronteriza de los ciberataques y del ciberdelito, la capacidad de persecución de los infractores o ciberatacantes a través del ordenamiento jurídico nacional es muy limitada y por ello adquiere una gran relevancia llegar a un consenso internacional.

630. Actualmente, existe un apoyo mayoritario a la postura occidental, refrendado por la ONU, la OTAN, la Unión Europea y los países participantes en el Manual de Tallín y se considera que el derecho internacional sí es aplicable a las acciones delictivas y maliciosas en el ciberespacio, trasladándose el debate a cómo el derecho internacional se aplica en el ciberespacio.

631. En la actualidad el debate se centra en la aplicación de cada uno de los aspectos más relevantes, utilizando como base los temas y las reglas considerados en el *Manual de Tallín 2.0*: derecho internacional general y ciberespacio (soberanía, diligencia debida, jurisdicción, ley de responsabilidad internacional, ciberoperaciones no reguladas per se por el derecho internacional), regímenes especializados del derecho internacional y ciberespacio (derechos humanos, derecho diplomático y consular, derecho marítimo, derecho aeronáutico, derecho espacial, derecho internacional de las telecomunicaciones), seguridad y paz internacional y actividades en el ciberespacio (operaciones de mantenimiento de paz, prohibición de intervención, uso de la fuerza, seguridad colectiva) y la ley de los ciberconflictos armados (ley de conflictos armados, conducción de hostilidades, ciertas personas, objetos y actividades, ocupación, neutralidad).

632. En algunos aspectos, el consenso es generalizado, como en la prohibición de la intervención o el derecho a la defensa propia; en cambio en otros, sigue habiendo disparidad de criterio como en los aspectos de soberanía y diligencia debida.

633. Sigue habiendo división entre los países del entorno OTAN/Unión Europea y los países del SCO (The Shanghai Cooperation Organisation: China, Rusia, Kazajistán, Kirguistán, Tayikistán, Uzbekistán, India y Pakistán) acerca de si los tratados y el derecho consuetudinario existentes son adecuados o no. Mientras que los primeros consideran que la regulación existente es adecuada, los países de la SCO propugnan lo contrario.

634. A medida que los ciberataques procedentes de APTs asociadas a estados se hacen más frecuentes, las naciones sienten la necesidad de hacerles frente mediante medidas de respuesta o coercitivas apropiadas, en cualquier ámbito, técnico, militar, político, diplomático, económico o a través de cualquier otro poder del estado. Para ello es necesario una *atribución* (clara e indiscutida) a un Estado.

635. Muchos Estados reconocen que la proliferación de este tipo de ciberataques, en buena parte, se debe a la dificultad de alcanzar la atribución según los estándares probatorios judiciales tradicionales y cada vez más naciones consideran la atribución en el ciberespacio como una decisión política basada en el análisis técnico y de inteligencia de numerosos hechos que corroboran una autoría específica.

636. Este nuevo estándar legal para la atribución en el ciberespacio habilitaría a los estados a defenderse de ciberagresiones de otros estados y disminuiría la posición de desventaja en las que se encuentran las naciones víctima de ciberataques debido a un artificio legal.

637. Otro de los problemas con los que se encuentran los estados para responder a ciberagresiones de otros estados es que los estados agresores desencadenan *ciberataques de baja intensidad* y larga duración, de tal manera que, a largo plazo consiguen efectos graves, pero puntualmente nunca superan el umbral necesario para ser reconocidos internacionalmente como ataques armados, evitando así la respuesta a través de medidas legítimas de represalia. En este caso el debate se centra en la búsqueda de acciones legales que deriven en sanciones para el estado agresor.

638. La *respuesta colectiva* ante la agresión recibida por un estado miembro de la alianza es un asunto legalmente controvertido; a pesar de ello, organizaciones de defensa colectiva como la OTAN consideran esa posibilidad. La aplicación del artículo 5 de la OTAN en caso de ciberataque se analizaría caso por caso.

639. Es aceptado, por una amplia mayoría de países, que una ciberoperación que cause graves daños a los intereses nacionales puede ser considerada un *ataque armado*, aún en ausencia de bajas humanas, y consecuentemente puede aplicarse el derecho a la legítima defensa y desencadenar una represalia militar legítima y proporcionada de cualquier ámbito, convencional o ciberespacial.

640. Actualmente, se están dando pasos para promover normas internacionales, no vinculantes, de *comportamiento responsable* en el ciberespacio; aunque, de momento con poco éxito, ya que existen numerosas visiones sobre lo que debe ser un modelo de comportamiento responsable.

641. A pesar de la dificultad del reto, se están promoviendo iniciativas como el "llamamiento de París para la confianza y la seguridad en el ciberespacio de 2018"[66] en el que se propone una visión para la regulación en el ciberespacio y los principales principios asociados: la aplicabilidad del derecho internacional, el comportamiento responsable de los Estados, el monopolio estatal del uso legítimo de la violencia y el reconocimiento de las responsabilidades específicas del sector privado.

642. En materia del empleo de *ciberoperaciones de carácter ofensivo* o intrusivo por parte de las fuerzas armadas en conflictos armados o en operaciones de mantenimiento de la paz, se mantiene el debate legal en asuntos como los límites de la soberanía del Estado, el umbral del ataque armado que desencadena el derecho de legítima defensa, la aplicación de las normas del derecho internacional humanitario, la definición de los mandatos legales para las fuerzas ciberespaciales o de las reglas de enfrentamiento.

643. Las ciberoperaciones ofensivas siguen siendo en muchos países un asunto controvertido, a pesar de que es globalmente reconocido de que están sujetas a las mismas normas y principios del derecho internacional que las operaciones militares convencionales.

644. Las ciberoperaciones ofensivas son consideradas por la OTAN a través del mecanismo denominado SCEPVA[67] por medio del cual los comandantes de las operaciones de la OTAN podrán disponer de los ciberefectos proporcionados voluntariamente por las naciones.

645. Reconocidos expertos en derecho internacional, advierten que la ley ampara al comandante de una operación que elige usar ciberoperaciones ofensivas en vez de operaciones convencionales en aquellos casos en los que se considere que el uso de las ciberoperaciones causa los mismos efectos militares que las convencionales, pero con un menor riesgo de

daños colaterales (especialmente a civiles) y a fuerzas propias. En cambio, se encontraría en una situación difícil de justificar legalmente, el comandante que elija las operaciones convencionales a pesar de que conlleven más riesgo de daños colaterales y a fuerzas propias.

646. La aplicabilidad del *derecho internacional humanitario* en la ciberoperaciones es respaldada por la mayoría de los países; sin embargo, existen un pequeño grupo de países que lo cuestionan ya que consideren que esto podría implicar una militarización del ciberespacio.

647. El Manual de Tallín 2.0 es, actualmente, la referencia mundial en la aplicación del derecho internacional a las ciberoperaciones; no obstante, se recuerda que no es un documento vinculante.

ESTÁNDARES

648. La ciberdefensa militar se desarrolla a través de un cuerpo doctrinal que establece normas, criterios, principios, procedimientos, orientaciones, recomendaciones y buenas prácticas sobre el diseño, ejecución y planeamiento de las operaciones militares en el ciberespacio.

649. Las referencias internacionales en materia de doctrina de ciberdefensa son escasas. La OTAN, habitual referente doctrinal para las naciones aliadas, ha aprobado, recientemente, el estándar OTAN AJP-3.20 "Allied Joint Doctrine for Cyberspace Operations", el cual describe los conceptos básicos de la ciberdefensa.

650. Las naciones son reacias a compartir sus doctrinas de ciberdefensa, sobre todo en lo referente a las actividades de inteligencia y ofensivas; lo que obliga a las naciones a implicarse en el desarrollo de su propio cuerpo doctrinal de ciberdefensa militar.

651. En la práctica, asociaciones como ISO o NIST desarrollan estándares de referencia global circunscritos a la ciberseguridad o a la seguridad de sistemas de información y telecomunicaciones, lo cual cubriría una parte muy pequeña del entorno de la ciberdefensa.

652. La *Organización Internacional de Normalización (ISO)* dispone de una serie de normas o estándares dedicados a los sistemas de gestión de la seguridad de la información (familia ISO/IEC 27000[68]) en el que destaca la norma sobre requisitos de sistemas de gestión de la seguridad de la información (ISO/IEC 27001)

653. Las normas ISO tienen la desventaja de que no son de libre acceso (son de pago) y esto dificulta la libertad de circulación, compartición, consulta y distribución que se requiere para su estudio, implementación y monitorización; en contradicción con el espíritu de la estandarización que es llegar a todos los interesados de una manera ágil y efectiva.

654. El *Instituto Nacional de Estándares y Tecnologías de los Estados Unidos (NIST)* dispone de una serie de estándares dedicados, específicamente, a la ciberseguridad[69] destacando el estándar dedicado al "Marco de Ciberseguridad"[70].

655. Otro referente del NIST en materia de ciberdefensa es el NICE[71] (National Initiative for Cybersecurity Education), una iniciativa conjunta entre el gobierno de los Estados Unidos, el sector académico y el sector privado cuya finalidad es dinamizar y promover un ecosistema de educación, formación y adiestramiento en ciberseguridad.

656. Las normas NIST, aunque son normas federales de los Estados Unidos, son, de facto, también unas normas internacionalmente aceptadas y de gran reputación y tienen la ventaja de que su acceso es libre lo que facilita la labor de estandarización. En concreto sus normas de ciberseguridad destacan por su claridad, orden organizativo y por la inclusión de formación online.

657. El *Centro Criptológico Nacional* de España (*CCN-CERT*) dispone de un conjunto completo de normas de seguridad de las tecnologías de la información y las telecomunicaciones (normas STIC), en lengua española, y muchas de ellas de acceso público. Además, disponen de un conjunto propio de herramientas[72] y formación[73] STIC bastante completo. Es de destacar las herramientas EAR/PILAR[74] para el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT[75], de uso oficial en España y en la OTAN.

658. Otros estándares de seguridad de la información con bastante reputación y recorrido son los desarrollados por la Oficina Federal de Seguridad de la Información de la República Federal de Alemania que pueden dar otra visión de mucha utilidad.[76]

ACRÓNIMOS

AMERIPOL	Comunidad de Policías de América
APT	Advanced Persistent Threat
BSI	Federal Office for Information Security of Germany
ByOD	Bring your Own Device
CCN	Centro Criptológico Nacional de España
CCO	Centro de Ciberoperaciones
CERT	Computer Emergency Response Team
CNO	Computer Network Operations
COR	Centro de Operaciones de Red
COS	Centro de Operaciones de Seguridad
CRAMM	CCTA Risk Analysis and Management Method
CSA	Cyber Situational Awareness
CSIRT	Computer Security Incidents Response Team
CTC	Ciber Terreno Clave
CyOC	Cyberspace Operations Centre
DNS	Domain Name System
EAR	Entorno de Análisis de Riesgos
EC3	European Cybercrime Center
ENISA	European Union Agency for Cybersecurity
EUROJUST	European Union Agency for Criminal Justice Cooperation
EUROPOL	European Union Law Enforcement Agency
FIRST	Forum of Incident Response and Security Teams
FOC	Full Operational Capability
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IXP	Internet Exchange Point
LACNIC	Registro de Direcciones de Internet de América Latina y Caribe
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MISP	Malware Information Sharing Platform
NATO CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
NDA	Non-Disclosure Agreement
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology of US Department of Commerce
NOC	Network Operations Centre
OCTAVE	Operationally Critical Threat Asset and Vulnerability Evaluation
OSINT	Open Source Intelligence
PILAR	Herramienta de Análisis de Impacto y Continuidad de Operaciones
RAE	Real Academia Española
RAT	Remote Administration Tool
RFI	Request for Information
RPAS	Remotely Piloted Aircraft System
SCEPVA	Sovereign Cyber Effects Provided Voluntarily by Allies
SCO	The Shanghai Cooperation Organisation
SHODAN	Motor de búsqueda de dispositivos conectados a Internet
SIEM	Security Information and Event Management
SLA	Service-Level Agreement
SOC	Security Operations Centre
TCP	Transmission Control Protocol
TIC	Tecnologías de la Información y las Comunicaciones
TOR	The Onion Router
TTP	Tácticas, Técnicas y Procedimientos
UAV	Unmanned Aerial Vehicle

REFERENCIAS

- **ACT Report on NATO Cyber Defence Taxonomy and Definitions** [Informe]. - 2014.
- **AJP.3 Allied Joint Doctrine for the Conduct of Operations** [Libro] / aut. NATO Standardization Office (NSO). - 2019.
- **CCN-STIC-480F Seguridad en el controls de procesos y SCADA** [Libro] / aut. CCN-CERT. - 2009.
- **Ciberamenazas y tendencias** [Informe] / aut. CCN-CERT. - 2019.
- **Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio** [Libro] / aut. autores varios. - [s.l.] : Instituto Español de Estudios Estratégicos, 2010.
- **Cooperative Models for Effective Public Private Partnerships** [Informe] / aut. ENISA. - 2011.
- **Cyber Attack Trends** [Informe] / aut. Check Point. - 2019.
- **Cyber Commanders Handbook v1.0 (DRAFT)** [Libro] / aut. NATO CCDCOE. - 2019.
- **El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra** [Publicación periódica] / aut. Galizia Roberto Claudio.
- **Framework for Improving Critical Infrastructure Cybersecurity** [Libro] / aut. NIST. - 2018.
- **Guide to Developing a National Cybersecurity Strategy** [Libro] / aut. Co-publication of 12 partner organisations facilitated by ITU. - [s.l.] : NATO CCDCOE, 2018.
- **International Cyber Norms: Legal, Policy & Industry Perspectives** [Libro] / aut. Anna-Maria Osula Henry Rõigas (Eds.). - [s.l.] : NATO CCDCOE, 2016.
- **Internet Attacks: A Policy Framework for Rules of Engagement** [Publicación periódica] / aut. William Yurcik David Doss // Illinois State University.
- **ISO/IEC 27000 Information security management systems — Overview and vocabulary** [Libro]. - 2018.
- **ISO/IEC 27001Information Security Mangement** [Libro]. - 2018.
- **IT Security Predictions** [Informe] / aut. Splunk. - 2020.
- **Joint Doctrine for Military Cyberspace Operations** [Libro] / aut. Royal Danish Defence College. - 2019.
- **JP 5-0 Joint Planning** / aut. USA Defence Staff. - 2017.
- **Key Terrain in Cyberspace** [Publicación periódica] / aut. David Raimond Gregory Conti, Tom Cross, Michael Nowatkowski. - 2014.
- **La Ciberdefensa: un nuevo frente una nueva necesidad** [Publicación periódica] / aut. Javier López de Turiso Néstor Ganuza. Roberto Gil, Félix Estrada, Joaquín Corominas // Revista Aeronáutica num 817. - 2012.
- **M-Trends** [Informe] / aut. FireEye. - 2019.
- **National Cyber Security Organisation in Israel** [Libro] / aut. Housen-Couriel Deborah. - [s.l.] : NATO CCDCOE, 2017.
- **National Cyber Security Organisation in United States** [Libro] / aut. Piret Pernik Jesse Wojtkowiak, Alexander Verschoor-Kirss. - [s.l.] : NATO CCDCOE, 2016.
- **National Cyber Security Organisation Spain** [Libro] / aut. Cendoya Alexander. - [s.l.] : NATO CCDCOE, 2016.
- **National Cyber Security Organisation: Estonia** [Libro] / aut. Osula Anna-Maria. - [s.l.] : NATO CCDCOE, 2015.
- **National Cyber Security Organisation: France** [Libro] / aut. Brangetto Pascal. - [s.l.] : NATO CCCOE, 2015.
- **National Cyber Security Organisation: United Kingdom** [Libro] / aut. Osula Anna-Maria. - [s.l.] : NATO CCDCOE, 2015.
- **National Cyber Security Organization: Czechia** [Libro] / aut. Tomáš Minárik Taťána Jančárkov. - [s.l.] : NATO CCDCOE, 2019.
- **NATO ACO Cyber Defence Functional Planning Guide** [Informe].
- **NATO AJP 3-20 Allied Joint Doctrine for Cyberspace Operations** [Libro].
- **NIPP National Infrastructure Protection Plan** [Libro] / aut. CISA/US Department of Homeland Security . - 2013.
- **OM 10/2013 Creación del Mando Conjunto de Ciberdefens**a / aut. Ministerio de Defensa de España. - 2017.
- **On Cyber Defence** [Publicación periódica] / aut. Ali Col Rizwan.

- **Overview of the UN OEWG developments: continuation of discussions on how international law applies in cyberspace** [Libro] / aut. Tolppa Maria. - [s.l.] : NATO CCDCOE, 2020.
- **PDC-01(A) Doctrina para el Empleo de las FAS** / aut. Ministerio de Defensa de España. - 2018.
- **Public Private Partnership in a NATO Context** [Informe] / aut. NATO STO. - 2019.
- **Strategic importance of, and dependence on, undersea cables** [Libro] / aut. Henrik Beckvard (Ed.) Keiko Kono. - [s.l.] : NATO CCDCOE, 2019.
- **Tallinn Manual 2.0** [Libro]. - 2017.
- **The NATO Policy on Cyber Defence: The Road so Far** [Publicación periódica] / aut. Gergely Szentgáll. - 2013.
- **The next phase of russian information warfare** / aut. Giles Keir.
- **The Tallinn Manual 2.0 Highligths and Insights** [Publicación periódica] / aut. Jensen Eric Talbot.
- **Threat Landscape** [Informe] / aut. ENISA. - 2018.
- **Trends in International Law for Cyberspace** [Libro] / aut. Kaska Kadri. - [s.l.] : NATO CCDCOE, 2019.
- **UNE-ISO 28000: especificación para sistemas de gestión de seguridad de la cadena de suministros** [Informe]. - 2008.

NOTAS

[1] https://www.rae.es/consultas/normas-de-escritura-de-los-prefijos-exmarido-ex-primer-ministro
[2] NATO Bi-SC Initial Assessment of Recognising Cyberspace as a Domain
[3] MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España.
[4] PILAR, herramienta de análisis de riesgo del CCN-CERT que facilita la aplicación de la metodología MAGERIT.
[5] CRAMM, metodología de análisis de riesgo desarrollada por la British CCTA (Central Communication and Telecomunicación Agency).
[6] OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation), metodología de análisis de riesgos desarrollada por el CERT en Carnegie Mellon University.
[7] CIBERATAQUE de DÍA CERO es un tipo de ciberataque que se produce por aprovechamiento de una vulnerabilidad desconocida o para lo cual todavía no hay parche.
[8] EXPLOIT, es un código software, una porción de datos o una secuencia de comandos que aprovecha una cibervulnerabilidad para causar un impacto.
[9] PHISHING es un tipo de ciberataque dirigida a engañar a una víctima (a través de simular fuentes confiables para la víctima, normalmente por email) para que proporcione información confidencial o privada (usuario, contraseñas, detalles bancarios, de tarjetas de crédito, etc.).
[10] SPEAR PHISHING es un tipo de ciberataque dirigida a engañar a un grupo de personas específicamente seleccionadas (aparentando ser una entidad confiable para la víctima) con la finalidad de obtener información confidencial (nombres de usuario, contraseñas, detalles bancarios, de tarjetas de crédito, etc.) útil para el desarrollo de una ciberoperación.
[11] SPOOFING es un tipo de ciberataque mediante la suplantación de identidad de un dispositivo o usuario en una red.
[12] PHARMING es un tipo de ciberataque en el que se redirige el tráfico web a un sitio falso, explotando vulnerabilidades de software en los sistemas de nombre de dominio (DNS) o en los equipos de los propios usuarios.
[13] SNIFFING es un tipo de ataque dirigido a la captura de tráfico mientras se está transmitiendo por la red, mediante una herramienta específica (sniffer), con la finalidad de analizar la red, obtener información o leer las comunicaciones.
[14] WATERING HOLE es un tipo de ciberataque dirigida a engañar a un grupo de personas específicamente seleccionadas (mediante la infección de los sitios web que habitualmente usan) con la finalidad de obtener información confidencial útil para el desarrollo de una ciberoperación.
[15] ATAQUE de DENEGACIÓN de SERVICIO (ataque DoS) es un tipo de ciberataque que busca que una máquina, servicio o recurso de red no esté disponible para sus usuarios legítimos, mediante la generación masiva de solicitudes superfluas en un espacio corto de tiempo buscando la sobrecarga del sistema.
[16] ATAQUE de DENEGACIÓN de SERVICIO DISTRIBUIDO (ataque DDoS) es un ataque DoS usando múltiples fuentes diferentes (normalmente haciendo uso de botnets)
[17] ATAQUE MitM (Man in the Middle) es un tipo de ciberataque en el que se intercepta una comunicación, se suplanta un interlocutor y se hace creer a la otra parte que está comunicando con el auténtico interlocutor.
[18] INYECCIÓN SQL es un tipo de ciberataque en el que se insertan sentencias SQL (lenguaje de consulta de bases de datos) maliciosas en un campo de entrada de un sitio web basado en base de datos para su ejecución.
[19] FLAME, es un malware sofisticado modular (descubierto en 2012) con capacidad para propagarse a otros sistemas a través de la red, grabar audio, capturar pantallas, actividad del teclado y tráfico de red, explotar dispositivos conectados por bluetooth y realizar una conexión externa.
[20] STUXNET, Stuxnet es una ciberarma (descubierto en 2010) diseñada para atacar a los sistemas de control de supervisión y adquisición de datos (SCADA). Es considerado como el responsable del ciberataque a la plataforma nuclear de Irán.
[21] DUQU, es una ciberarma relacionada con STUXNET que incluye capacidades de robo de información y en segundo plano, controladores de kernel y herramientas de inyección.
[22] BLACK ENERGY, es una ciberarma (descubierta en 2007) como un kit de herramientas diseñada para generar ataques distribuidos de denegación de servicio (DDoS).

[23] CADENA DE CIBEREXTERMINIO (Cyber Kill Chain) es un modelo diseñado por la empresa Lockheed Martin.
[24] OSINT, Inteligencia de Fuentes Abiertas
[25] SHODAN, es un motor de búsqueda en internet que permite encontrar tipos específicos de dispositivos (cámaras web, enrutadores, servidores, etc.) conectados a Internet.
[26] SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es una herramienta software que facilita la gestión y correlación de eventos con la finalidad de proporcionar las organizaciones información útil sobre potenciales.
[27] CNO, Computer Network Operations
[28] CERT: Computer Emergency Response Team
[29] CSIRT: Computer Security Incident Response Team
[30] https://www.first.org/
[31] https://www.trusted-introducer.org/index.html
[32] http://www.egc-group.org/
[33] OFUSCACIÓN de código es la modificación deliberada del código fuente o código máquina de un programa informático para dificultar su comprensión y manteniendo el funcionamiento original.
[34] INGENIERÍA INVERSA DE SOFTWARE es un proceso de deconstrucción de un código software para revelar su diseño, arquitectura, funciones o extraer conocimiento.
[35] MACHINE LEARNING, es una rama de la Inteligencia Artificial que se encarga del estudio de algoritmos informáticos que mejoran automáticamente a través de la experiencia.
[36] BLOCKCHAIN o cadena de bloques es una lista creciente de registros, llamados bloques, que están vinculados mediante criptografía. Cada bloque contiene un hash criptográfico del bloque anterior, un sello de tiempo y datos de transacciones.
[37] BIG DATA, es una tecnología enfocada al tratamiento de conjuntos de datos demasiado grandes o complejos para ser tratados por software tradicional de procesamiento de datos.
[38] 5G es el estándar tecnológico de quinta generación para redes celulares que proporciona un mayor ancho de banda y velocidades de descarga más rápidas que la tecnología predecesora (4G).
[39] RANSOMWARE, es un tipo de ciberataque que amenaza con publicar datos de la víctima o bloquear permanentemente el acceso a ellos (normalmente a través del cifrado de los ficheros de la víctima) si no se aviene a pagar un rescate.
[40] WEBSITE DEFACEMENT, es un ciberataque diseñado para cambias la apariencia visual de un sitio web.
[41] ByOD, es la autorización a usar el propio dispositivo personal (smartphone, Tablet, portátil) para asuntos profesionales.
[42] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4041-ccn-cert-ia-13-19-threats-and-trends-report-executive-summary/file.html.
[43] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
[44] https://www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma
[45] https://www.checkpoint.com/downloads/resources/cyber-attack-trends-mid-year-report-2019.pdf
[46] https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
[47] https://www.kaspersky.com/blog/secure-futures-magazine/2020-cybersecurity-predictions/32068/
[48] CRIPTOMINADO, ciberataque diseñado para para secuestrar el procesamiento inactivo del dispositivo de una víctima y usarlo para extraer criptomonedas sin su consentimiento.
[49] ATAQUE DNS, es un dirigido a la disponibilidad o estabilidad del servicio DNS de una red.
[50] SANDBOXING es una tecnología diseñada para ejecutar programas o códigos no probados o no confiables de manera aislada para proteger los servicios o sistemas operativos.
[51] https://attack.mitre.org/
[52] BOTNET: Red formada por ordenadores virtualmente secuestrados o infectados (robots informáticos o bots) que ejecutan tareas de manera autónoma y automática sin el conocimiento ni consentimiento de sus legítimos propietarios o usuarios.
[53] https://ccdcoe.org/library/publications/guide-to-developing-a-national-cybersecurity-strategy/
[54] https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines/
[55] https://ccdcoe.org/library/publications/?focus_area=strategy
[56] https://www.first.org/

[57] https://www.trusted-introducer.org/index.html
[58] http://www.egc-group.org/
[59] https://www.lacnic.net/
[60] https://www.lacnic.net/lacnic33
[61] https://warp.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf
[62] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[63] https://europa.eu/european-union/about-eu/agencies/eurojust_es
[64] JUEGO DE SUMA CERO, situación en la que la ganancia o pérdida de un participante se equilibra con exactitud con las pérdidas o ganancias de los otros participantes
[65] VPN (Virtual Private Network) es una tecnología que permite una extensión segura de una red privada a través de Internet mediante el establecimiento de una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.
[66] Paris Call for Trust and Security in Cyberspace
[67] Sovereign Cyber Effects Provided Voluntarily by Allies
[68] https://www.iso.org/standard/73906.html
[69] https://www.nist.gov/topics/cybersecurity
[70] https://www.nist.gov/cyberframework
[71] https://www.nist.gov/itl/applied-cybersecurity/nice/about
[72] https://www.ccn.cni.es/index.php/es/ccn-cert-menu-es/soluciones-ccn-cert
[73] https://www.ccn.cni.es/index.php/es/menu-formacion-es
[74] https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html
[75] https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar/metodologia.html
[76] https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

GUÍA DE
CIBERDEFENSA

ORIENTACIONES PARA EL DISEÑO, PLANEAMIENTO, IMPLANTACIÓN Y DESARROLLO DE UNA CIBERDEFENSA MILITAR