ISSN: 2525-457X
Análise Estratégica
v. 38, n.3, jun./ago. 2025

ASPECTOS A TENER EN CUENTA PARA LA COOPERACIÓN DE UN SISTEMA CIBERNÉTICO RESILIENTE EN AMÉRICA LATINA DE ACUERDO A LAS NUEVAS AMENAZAS MUNDIALES

ASPECTS TO BE TAKEN INTO ACCOUNT FOR THE CO-OPERATION OF A RESILIENT CYBER SYSTEM IN LATIN AMERICA ACCORDING TO THE NEW GLOBAL THREATS

CRISTIAN IVÁN CABRERA

RESUMEN

La complejidad de los conflictos modernos, donde son imprescindibles los tiempos de respuesta para restablecer un sistema luego de un ciberataque que afecte a los habitantes de América Latina, hacen de la cooperación regional un factor determinante. Por tal razón, la integración de capacidades regionales de un sistema ciber-resiliente adquiere un rol importante para afrontar las amenazas mundiales en el espacio cibernético.

Las ciberoperaciones deberían ser consideradas un arma que afecta todos los dominios por los efectos que producen en el combate moderno. Por tal razón, es imprescindible planificarlas en todos los niveles de conducción, siendo fundamental hacerlo en el "Nivel Estratégico Militar". De esta manera, lograr la articulación de fines, modos y medios, los cuales coordinados regionalmente permitan conformar un sistema de ciberdefensa eficiente.

Palabras-clave: Regional; Ciberoperaciones; Ciberdefensa; Ciberataque; Ciber-resiliente

ABSTRACT

The complexity of modern conflicts, where response times are essential to restore a system after a cyber attack that affects the inhabitants of Latin America, make regional integration a determining factor. For this reason, the integration of regional capabilities of a cyber-resilient system plays an important role in confronting global threats in cyberspace.

Cyber operations must be considered a weapon that affects all domains due to the effects they produce in modern combat. Therefore, it is essential to plan them at all levels of management, and it is essential to do so at the "Military Strategic Level". In this way, the articulation of ends, ways and means is achieved that, coordinated regionally, allow the creation of an efficient cyber defense system.

Keywords: Regional; Cyber operations; Cyber defense; Cyber attack; Cyber resilience.

O AUTOR

Tenente-Coronel de Comunicações do Exército Argentino (CMN/2000), Oficial de Estado Maior e Oficial de Estado Maior Conjunto. Licenciado em Administração, Especialista em Condução Superior de Organizações Militares Terrestres, Especialista em Estratégia Operacional e Planeja-mento Militar Conjunto, Mestre em Estudos Estratégicos, Professor Universitário. Atualmente o Ten Cel CABRERA é Oficial de Ligação na 7ª Subchefia do EME. e Pós Doutora em Ciência Política

1 INTRODUCCIÓN

La continua evolución de esta nueva dimensión de la guerra pone de manifiesto la necesidad de la formación de equipos altamente especializados, lo que no sólo ha incidido gravemente en el mando y control de las diferentes plataformas de sistemas de armas, sino que lo ha concretado en acciones enfocadas especialmente a la conquista de las mentes y su voluntad de lucha, objetivo último del conflicto.

Es especialmente importante que nuestras Fuerzas Armadas Regionales se centren en desarrollar y comprender esta nueva dimensión, ya que su entorno de trabajo permanente es el ciberespacio, donde se llevan a cabo las operaciones cibernéticas. Las tecnologías informáticas han transformado la forma de pensar y actuar en el desarrollo de las operaciones, introduciendo importantes cambios estructurales al permitir modelar objetos de todo tipo en forma de información, posibilitando así su manipulación por medios electrónicos.

Es necesario, por tanto, establecer unas bases doctrinales que permitan concientizar, disponer de un lenguaje común y establecer las medidas a adoptar ante posibles transgresiones. Este sería el primer paso para mejorar las medidas de ciberseguridad, proteger nuestras redes y aplicar medidas preventivas que faciliten una actuación resiliente ante posibles ciberataques en Latinoamérica.

Este sistema debe operar bajo la premisa de que ningún medio o red informática es invulnerable. Por lo tanto, el objetivo general de este trabajo es proponer las características organizativas que deben tener las Fuerzas Armadas Regionales para que su sistema cibernético sea considerado resiliente. Para ello se tomarán como base los conflictos de Estonia en 2007, Ucrania en 2014 y Ucrania en 2022, donde se puso de manifiesto la importancia de las ciberoperaciones en el desarrollo de cualquier operación militar.

A la luz de los conflictos mencionados, es razonable considerar que cualquier ciberataque puede comenzar en el ámbito de la ciberseguridad (ciberdelincuencia) y terminar en el ámbito de la ciberdefensa.

Los actores implicados intentarán producir el caos en el adversario no sólo atacando los sistemas en cuestión, sino también en sus mentes y en su voluntad de luchar, con el fin de equilibrar el poder de combate. Por consiguiente, tratarán de lograr la victoria antes de desplegar su poder militar, lo que les implicará en otros conflictos. Por ello, la organización del sistema de ciberdefensa es un aspecto que no debe pasarse por alto.

2 EL CIBERESPACIO Y SUS DIMENSIONES

El ciberespacio está compuesto de tres dimensiones. La intangible o lógica, representada por los protocolos y, la interconexión de distintos componentes físicos que responden al diseño de algoritmos utilizados y el software que realiza el procesamiento de los datos. La física o material, integrada por los diferentes hosts, infraestructuras y la geografía. Por último, la social abstracta y real a la vez. En está interactúa el humano, cuya definición correcta es virtual, ya que en la misma las personas le dan vida al ciberespacio, utilizando parte de su tiempo y atención. Esta virtualidad conforma un ámbito propicio del proceso cognitivo del ser humano. (Moresi, Motta, Trama, Walker, & Amaya, 2023)

La integración de estas dimensiones en el ciberespacio que facilita humanos, infraestructuras, software, transporte, información y energía eléctrica interactúen. En este ámbito se desarrolla la guerra cibernética, la cual, para su desenvolvimiento requiere ciertas capacidades. La capacidad de entender el funcionamiento de las redes de comunicación e información, así como la integración de estas en sus niveles global, metropolitano y local. Además de esto, identificar sus vulnerabilidades para desarrollar herramientas que permitan reducir, anular, mitigar, neutralizar o al menos advertir la posibilidad que sean explotadas por alguna persona. Esto se materializa con la ciberseguridad. (De Vergara y Trama, 2017)

Por otro lado, desarrollar y operar sistemas que permitan el control y la vigilancia[1] de sistemas compuestos por tecnologías de la operación (TO/OT) y tecnologías de la información (TI/IT)[2]. Las TO/OT en su perspectiva estratégica se encuentran relacionadas con las infraestructuras críticas. Estas permiten la ejecución de operaciones defensivas en sus dos variantes (activas y pasivas), de explotación (activa contra el oponente y pasiva en el ámbito propio) y Ofensivas. Estas en occidente se las considera dentro de un conflicto declarado. Sin embargo, las TI/IT facilitan las tareas y acciones para generar o evitar la comunicación estratégica del enemigo. (Moresi, Motta, Trama, Walker, & Amaya, 2023)

El ultimo requerimiento es el ambiente operacional, para esto la Junta Interamericana de Defensa lo define como el entorno de interés donde se llevan a cabo actividades, funciones y operaciones para dar cumplimiento a la misión y ejercer el control del oponente con la finalidad de lograr los efectos deseados. Este entorno debe reunir seis criterios para ser considerado un ámbito de operaciones:

- Primero, va a requerir capacidades únicas para operar en ese ámbito.
- Segundo, no estar totalmente abarcado por ningún otro ámbito (tierra, mar, aire, espacio).
- Tercero, está caracterizado por una presencia compartida de capacidades aliadas y adversarias.
- Cuarto, ser capaz de ejercer control sobre un oponente a través de la influencia y el dominio.
- Quinto, debe brindar oportunidades de sinergia con otros ámbitos.
- Sexto, proporcionar oportunidades asimétricas entre todos los ámbitos.(Ganuza, 2020)

El nivel estratégico militar se ve influenciado permanentemente por las TI/IT en todo lo relacionado con operaciones del ámbito cognitivo o información. Sin embargo, el ambiente operacional desarrolla dependencia de las TO/OT, puntualmente en lo que respecta a logística, inteligencia, reconocimiento vigilancia, comando y control y operaciones de conectividad en los distintos sistemas de armas. Esto conlleva que la ciberdefensa intente asegurar las TI/IT para alistar sus sistemas con un alto nivel de seguridad.

1 El control es la capacidad del sistema para normalizar la situación detectada. Se puede lograr a partir de una situación de supremacía, superioridad, paridad, por degradación y/o incapacitación. La capacidad de Vigilancia y Control en los sistemas cibernéticos es función de la resiliencia de los mismos a las agresiones a los que son sometidos.

2 La Tecnología de la Información se caracteriza por la aplicación de equipos de telecomunicación como ordenadores para tratar datos. IT Suele utilizarse en el ámbito de los negocios y las empresas. En cambio, la Tecnología de las Operaciones está dedicada a detectar o cambiar los procesos físicos a través de la monitorización y el control de dispositivos también físicos, como tuberías o válvulas.

3 LAS OPERACIONES EN EL CIBERESPACIO Y SUS EFECTOS

Se define a las ciberoperaciones como operaciones ejecutadas en el ciberespacio para obtener información, negar, degradar o destruir la información existente en diferentes dispositivos que operan dentro de una red de computadoras o redes informáticas. (Smart, 2021)

Las ciberoperaciones ofensivas y defensivas operan dentro del ciberespacio, espacio operacional creado tecnológicamente por el hombre donde las organizaciones y personas utilizan las tecnologías de la información y la comunicación (TIC) necesarias para interactuar (Llongueras Vicente, 2013).

Las ciberoperaciones pueden ser activas o pasivas generalmente. En la parte activa están aquellas que ejecutan algún tipo de modificación, borrado o agregado de información. Los programas maliciosos se usan para ejecutar un ataque con un objetivo específico. Estos son programas informáticos diseñados generalmente para afectar infraestructuras, redes informáticas, una computadora en particular (personal o industrial) o alterar una base de datos. Estos tipos de programas maliciosos son los virus, gusanos, troyanos, rootkits, ransomware, adware, spyware y otros tipos de malware.(Maurer, 2018)

Por otro lado, las ciberoperaciones pasivas procuran la recopilación de información y la vigilancia sin alterar o interferir directamente con los sistemas. Estas operaciones suelen ser discretas y buscan evitar la detección, centrándose en observar, analizar y recopilar datos para obtener inteligencia. Los ejemplos incluyen la monitorización del tráfico de red, la interceptación de comunicaciones y el análisis de patrones de comportamiento en sistemas informáticos. (Maurer, 2018)

4 EFECTOS DE LAS CIBEROPERACIONES OFENSIVAS

La superpotencia cibernética de los Estados Unidos, a las misiones militares en el ciberespacio la describen por intenciones. Estas ciberoperaciones se ejecutan desarrollando capacidades que permitan generar los efectos en el ciberespacio. (De Vergara y Trama, 2017)

Por esto, un ciberataque está compuesto por las diferentes acciones que crean efectos directos de negación en el ciberespacio, tales como, degradación, interrupción o destrucción y la manipulación que conduce a la negación que se manifiesta en los espacios físicos. Las diferentes acciones desarrollan los siguientes efectos (America, 2018):

- El efecto de negar se traduce en degradar, interrumpir o destruir el acceso a, operación de, o disponibilidad de un objetivo por un nivel especifico durante un tiempo específico. La negación le impide al adversario el uso de recursos. La descripción de estos efectos es la siguiente: (De Vergara y Trama, 2017)

- De acuerdo al párrafo precedente, el primer efecto para negar es degradar, este se utiliza para negar el acceso a una operación de un objetivo en un nivel representado como un porcentaje de capacidad. El nivel de degradación debe ser especificado. Si se requiere un tiempo específico debe ser manifestado oportunamente.

- El segundo efecto de negar es interrumpir, este significa negar completamente durante un tiempo el acceso o la operación de un objetivo durante un período de tiempo. Normalmente, debe especificarse el tiempo de inicio y de finalización. La interrupción puede ser considerada un caso especial de degradación donde el nivel de degradación seleccionado es ciento por ciento.

- El tercer efecto de negar es destruir, el cual sirve para negar de forma permanente, completa e irreparable. En este efecto las funciones de tiempo y cantidad son maximizadas en el acceso a, o la operación de un objetivo. El efecto de manipular se utiliza para controlar o cambiar la información del adversario, sistemas de información y/o redes, de tal manera que respalden los objetivos del Comandante.

La degradación o destrucción de la capacidad de las redes y los sistemas informáticos enemigos puede realizarse por un tiempo limitado. La publicación JP 3-12121 Cyberspace Operations establece que "La ejecución exitosa de operaciones cibernéticas requiere el empleo integrado y sincronizado de las operaciones ofensivas, defensivas y DODIN" (operaciones de información en las redes) (America, 2018) (De Vergara y Trama, 2017)

5 OBJETIVOS DE LOS CIBERATAQUES (ESTONIA-UCRANIA)

Las ciberoperaciones tienen varios objetivos, entre ellos, políticos, económicos, ideológicos y bélicos. Con respecto a los políticos podemos destacar caso de Cambridge Analytics en 2016. Este hecho confirma el uso de cibercapacidades para influir en el resultado de una elección presidencial. A comienzo de ese año, la candidata a presidente Hillary Clinton sufrió una intromisión en su cuenta de correo personal en la cual disponía información confidencial.

Una ciberoperación con fines bélicos es aquella que se involucra al ámbito militar. Este tipo de ciberoperaciones pueden ejecutarse por el cibercomando de un Estado o estar tercerizadas a un actor no gubernamental, como puede ser una empresa de ciberseguridad o distintos actores.

Un ejemplo claro de esta ciberoperación es el caso Stuxnet 2010, gusano informático malicioso desarrollado por Israel y Estados Unidos aparentemente. El objetivo de este gusano fue atacar sistemas de control y adquisición de datos (SCADA) y de esta manera neutralizar el programa nuclear de Irán. Este tipo de ciberoperaciones son las que representan algunas acciones de guerra en la actualidad y van a configurar el campo de combate futuro. (Smart, 2021).

Por otro lado, una ciberoperación con objetivos económicos generalmente tiene otros objetivos implícitos, como puede ser una motivación política. En el caso de que un estado intente causar un caos económico otro actor, o generar una distracción para realizar un ataque mayor, utilizaran probablemente ciberoperaciones con motivaciones mixtas. (Smart, 2021)

En las ciberoperaciones mixtas, los ciberatacantes o hackers en todo momento intentan tomar el control de los dispositivos IoT estos son objetivos preciados ya que conforman lo que se llama botnets. Los botnets[3] son grupos de dispositivos controlados por atacantes que se utilizan en ataques de tipo distribuido de denegación de servicio (DDOS). Un ataque DDOS es aquel en el que se satura un servidor con un incremento masivo de peticiones. De esta forma, un servidor que no puede responder al exceso de peticiones que se le ejecutan, deja de responder a todas las peticiones y es así como se denegar el servicio del mismo. (Smart, 2021)

3 Según Sebastián Smart los bootnets son dispositivos, con acceso a internet que suelen tener plataformas online en las que se puede administrar el dispositivo. Los dispositivos IoT incluyen cámaras de seguridad, heladeras inteligentes, lavarropas inteligentes, sensores y todo tipo de dispositivo de uso cotidiano que tenga acceso a internet. Estas plataformas requieren un usuario y contraseña para poder acceder a ellas. Los usuarios ordinarios no suelen modificar las credenciales que vienen de fábrica, lo que facilita a los atacantes a poder acceder a ellos utilizando estas credenciales.

En 2007, un ciberataque de similares características se realizó contra sitios web de organizaciones estonias. Entre ellas, periódicos, emisoras, el sistema bancario y el parlamento por un supuesto desacuerdo con Rusia de la ubicación de la estatua de bronce de TALLIN, como las tumbas de guerra en este lugar de la era soviética. Los ciberataques duraron varias semanas en abril de 2007 provocando un caos en sus infraestructuras críticas. Sin embargo, el sistema de defensa cibernético de Estonia repelió el ataque. (McGuinness, 2017)

En 2020, al comienzo de las hostilidades entre Rusia y Ucrania, este último fue víctima de varios ciberataques de origen ruso. Durante el mes de febrero, Rusia lanzo una serie de ciberataques contra bancos e instituciones gubernamentales que llevaron al colapso a estos sistemas. Estos fueron advertidos como ataques DDoS, que por medio de bootnets, saturaron sus operaciones lo hasta bloquear el acceso a los usuarios legítimos. Este ciberataque, es una estrategia muy utilizada por el Kremlin, por medio de contrataciones a grupos de ciberdelicuentes como Killenet[4]. (Ganuza, 2020)

Tabla 1: Medidas de protección para contrarrestar las fases de un ciberataque

FASE	PROTECCIÓN	OBSERVACIONES
Reconocimiento	Ingeniería social.	El atacante busca vulnerabilidades en redes y en IICC.
Desarrollo del armamento	Parches de seguridad.	El atacante busca explotar las vulnerabilidades encontradas.
Entrega del malware en el sistema	Sandbox Ingeniería social. Separar placas de red de internet e intranet, Anular USB. Evitar drives MP3; MP4.	El atacante busca alojar el malware en los sistemas.
Explotación del malware insertado	Sandbox - Limitar uso de Plugs – in. (Java o Flash)	Obtener información. Afectar los sistemas.
Instalación	Inspecciones SSL. Filtros URL.	El atacante tomar el control de los datos.
Mando y control	Monitorear capa 3 y 4 del modelo OSI	Reconocer el sistema atacado.
Efectos deseados creados	Servidores con información sensible desconectados de internet.	El atacante busca permanecer lo más posible sin ser detectado.

Fuente: elaboración propia

4 Según Reliaquest Threat Research Team **Killnet** es un grupo de hackers pro-rusos conocido por sus ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS) hacia instituciones gubernamentales y empresas privadas en varios países durante la invasión rusa de Ucrania en 2022. El grupo se cree que fue formado alrededor de marzo de 2022. Killnet ha sido responsable de ataques en Rumania, Moldavia, República Checa, Italia, Lituania, Noruega, Letonia y Estados Unidos.

Tabla 2: Relaciones entre las ciberoperaciones y el ciberespacio

CIBEROPERACIONES	EFECTOS	CIBERESPACIO
Ofensivas	Negar, degradar, interrumpir, destruir, manipular.	
Defensivas (Activas/Pasivas)	Proteger, detectar, caracterizar, contrarrestar y mitigar.	
Exploración	Detectar y neutralizar.	
Información	Manipular, neutralizar, desgastar.	

Fuente: elaboración propia

Los efectos en estas ciberoperaciones incluyen proteger, detectar, caracterizar, contrarrestar y mitigar. Tales acciones defensivas son creadas generalmente por el Comandante Conjunto o por la Fuerza Armada específica que posee u opera la red. (America, 2018) (De Vergara y Trama, 2017).

6 CIBEROPERACIONES DE EXPLORACIÓN Y SUS EFECTOS

Son aquellas actividades que se ejecutan en las redes para obtener datos, siendo el fin último de estas detectar vulnerabilidades, debilidades y amenazas (America, 2018)

De esta forma, las ciberoperaciones de exploración, son aquellas que permiten partir de Posiciones Relativas Favorables (PRF), iniciar desde una ventaja frente al adversario que no realiza ninguna acción por sí misma. Las vulnerabilidades en las redes son creadas intencionalmente o por errores de programación, estas generan “Puertas Traseras”, ellas le van a permitir a un atacante acceder al sistema sin autorización. (Smart, 2021)

Las potencias desarrolladas en el ciberespacio, como Estados Unidos y Rusia dividen la exploración, en dos fases. En la primera se concentran en la recopilación de información, que atacan principalmente el software, hardware, el personal que opera las diferentes redes o sistemas y las políticas de seguridad informática operacional, como la conformación de sus redes desde el punto de vista de ciberseguridad. La segunda fase o ciberoperación se encarga de generar las condiciones para vulnerar un sistema más sofisticado, del cual, ya se posee la información básica, pero se precisa de datos específicos, avanzados y actualizados para sostener un efecto por un tiempo determinado (De Vergara y Trama, 2017), (America, 2018).

En el nivel estratégico, lo más correcto en las ciberoperaciones de exploración es hablar de acciones dirigidas contra los sistemas de tecnologías que protegen las infraestructuras críticas o el centro de gravedad del oponente. Estas ciberoperaciones serán ejecutadas para obtener información relevante que permitan producir un nuevo conocimiento de la situación y de esta manera detectar las vulnerabilidades en el oponente. Además, dirigir sobre estas vulnerabilidades ciberataques que permitan, interrumpir, negar, degradar, corromper o destruir, la información almacenada en redes de computadoras, dispositivos o comunicaciones del oponente (De Vergara y Trama, 2017).

A pesar de esto, esta información también sirve para proteger nuestro centro de gravedad cibernético contra cualquier ciberataque y permitir organizar un dispositivo, que sea lo suficientemente resiliente para poder contrarrestar estos ciberataques en contra de los dispositivos de origen. Este último permite aumentar la eficiencia de las redes, los diferentes dispositivos que interactúan en ellas y sistemas de armas mejorando de manera proactiva su ciberseguridad ante una posible situación de conflicto (Corletti Estrada, 2017), (De Vergara y Trama, 2017)

Otra herramienta que garantiza el correcto desempeño de una red dentro del hacking ético[5] es un penetration test, la cual ataca software, sistemas de computadoras y puertos para ejecutar un informe por períodos cortos. (Cabrera, 2019) En períodos largos se utilizan los Red Teams en ciberoperaciones ofensivas, Blue Teams en ciberoperaciones defensivas o, Purple Teams en metodología integradora del equipo Rojo y Azul. Este último sería al más apropiado para chequear los efectos y detectar vulnerabilidades en el nivel operacional (Miessler, 2019)

Finalmente, teniendo en cuenta lo que el nivel estratégico nacional desarrolla sus normas con respecto a la vigilancia y control del ciberespacio. El Nivel Estratégico debe poseer las capacidades necesarias que le permita en las ciberoperaciones en desarrollo o ante la conformación de un conflicto neutralizar cualquier tipo de amenaza. (Nacional, 2018)

Para lograr lo anterior, debe conducir las capacidades de vigilancia y control del ciberespacio a fin de anticipar y prevenir ciberataques y ciberexplotación en las redes informáticas que afecten cualquier Sistema de Defensa dentro del TO (Nacional, 2018).

También el Nivel Estratégico Nacional y Militar conducen ciberoperaciones para proteger la infraestructura crítica del país o la información que posibilite el acceso a ellas. Esta misión la desarrollara bajo la supervisión y el control de un Comandante Conjunto de Ciberdefensa, o equivalente y las diferentes agencias del estado. Los efectos que excedan al Comandante del Teatro de Operaciones se requerirán a la estrategia nacional (Nacional, 2018).

7 CIBEROPERACIONES DE INFORMACIÓN Y EFECTOS

Las ciberoperaciones de información buscan alterar el proceso de toma de decisiones en el oponente utilizando el ciberespacio. Un error frecuente es tratar de diferenciar aquellas ciberoperaciones que se desarrollan en el ciberespacio, tipificándolas como operaciones de información (De Vergara y Trama, 2017).

A pesar de que el control del ciberespacio otorga poder, también genera vulnerabilidades como puede ser la transmisión en tiempo real de imágenes o hechos por parte de los habitantes que

5 Hacking ético. Según el manual de Ethical Hacking en su glosario dice que, es el acto de una persona al usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, con el objeto de reportarlas y que se tomen medidas sin producir daño.

condicionan el proceso de toma de decisiones de las Fuerzas Armadas. Esto facilita la divulgación de información secreta otorgándole ventajas al oponente. La saturación de mensajes a través de las redes sociales dificulta el control y hace más compleja la información y desinformación (De Vergara y Trama, 2017) (Cabrera, 2019).

Por esto, las ciberoperaciones de información persiguen efectos que solo ellas pueden ejecutar y, en todo momento buscaran otorgar libertad de acción para la ejecución de la maniobra. Por tal razón, es pertinente vincularlas con las ciberoperaciones ofensivas y defensivas que busquen proteger el proceso de toma de decisiones propio e intenten alterar el del adversario (De Vergara y Trama, 2017).

El desarrollo de estas capacidades logrará introducir al oponente en el ciclo OODA (observación, orientación, decisión y acción) propio, lo cual contribuirá a la desarticulación del adversario (Rio, 2013).

La ejecuión de estas ciberoperaciones cobra gran importancia a lo largo de todo el conflicto. Sin embargo, el momento más sensible para desarrollarlas es durante la fase preparación donde se buscará inducir al enemigo erróneamente, buscando alterar su percepción sobre el conflicto y los actores participantes. El principal efecto a perseguir en esta etapa, será manipular la racionalidad interdependiente de quien debe tomar la decisión final para evitar el conflicto convencional y, como decía Sun Tzu, vencer al oponente sin entrar en combate abierto. (Cal, Di Tella, Ganeau, Grunschlager y Leal, 2016)

Por lo descripto anteriormente, las ciberoperaciones de información buscan explotar el uso de las capacidades del ciberespacio. Por esto, las ciberoperaciones ejecutadas en las redes informáticas tienen por finalidad modificar los datos o algoritmos de una red o sistema para que se produzcan resultados contrarios a los que se esperaban, estas conforman parte de las ciberoperaciones a ejecutar para generar las condiciones dentro del TO (De Vergara y Trama, 2017).

Sin embargo, el elemento determinante en este sistema hombre máquina, sigue siendo el factor humano, el cual se reconoce en ciberdefensa como ingeniería social.

8 ASPECTOS A TENER EN CUENTA PARA EL DESARROLLO DE CAPACIDADES CIBERNÉTICAS

Los medios de comunicación social y las diferentes redes informativas discuten y hablan a diario temas como ciberespionaje, ciberterrorismo, cibercrimen, hacktivismo o ciberguerra. Además de esto, la importancia de los ataques producidos, la incertidumbre que genera las consecuencias que pueden generar, el anonimato de sus autores y la falta de definiciones legales claras, han puesto a los diferentes gobiernos y a la comunidad internacional a trabajar tanto en sus jurisdicciones como en el ámbito regional y global. (Cornaglia, 2017)

La ciberdefensa no es algo simple, ya que su característica principal es el cambio constante. Este es el principal desafío que enfrentan todas las naciones del planeta, debido a que aún no existen tratados internacionales que establezcan normas claras en este dominio. También, en el ciberespacio las tecnologías digitales y las regulaciones son construidas con el paso del tiempo y es factible ver el diseño de tecnologías que produzcan los efectos de las regulaciones. (De Vergara y Trama, 2017).

9 CAPACIDADES TÉCNICAS Y OTROS ASPECTOS ESTRATÉGICOS A CONSIDERAR

9.1 ORGANIZACIÓN DE UN SISTEMA RESILIENTE EN LAS FUERZAS ARMADAS

Las fuerzas militares están dotadas de organizaciones de ciberdefensa para resguardar sus sistemas, redes y operaciones de las crecientes amenazas en el ciberespacio. Las principales causas de esto son:

- Las respuestas a ataques cibernéticos: esta organización debe estar preparada para responder rápidamente a posibles ciberataques que puedan deshabilitar sistemas críticos o impactar la seguridad nacional.
- La protección de infraestructura crítica: las fuerzas armadas poseen sistemas tecnológicos avanzados para comunicaciones, logística, inteligencia y operaciones. La protección de estas infraestructuras es vital para garantizar la continuidad de sus misiones.
- El resguardo de información sensible: los datos militares son un objetivo constante para actores maliciosos como hackers, terroristas o estados enemigos. La ciberdefensa ayuda a evitar fugas de información y espionaje.
- La ejecución de ciberoperaciones: además de la defensa, algunas organizaciones militares tienen capacidades ofensivas para neutralizar amenazas o atacar infraestructuras enemigas en casos específicos.
- La ejecución de operaciones multidominio: en el contexto actual, el ciberespacio es considerado un dominio clave, al igual que el aire, mar y tierra. Tener capacidades de ciberdefensa refuerza la preparación para conflictos modernos.
- El fortalecimiento de la soberanía nacional: una postura sólida en ciberdefensa demuestra la capacidad de un país para protegerse y disuadir posibles agresores.

Además, una organización de ciberdefensa resiliente es esencial para las organizaciones militares porque garantiza la continuidad operativa. En caso de un ciberataque, una ciberdefensa resiliente asegurará que los sistemas críticos puedan recuperarse rápidamente y continuar funcionando sin interrupciones graves. También, se adapta a amenazas avanzadas, las amenazas cibernéticas evolucionan constantemente. Una organización resiliente puede identificar, mitigar y adaptarse a ataques nuevos y sofisticados. De esta manera este elemento contribuye a la mitigación de daños a la seguridad nacional. Un ataque cibernético podría comprometer no solo a los sistemas militares, sino también infraestructuras nacionales determinantes. La resiliencia asegura una defensa proactiva y reactiva buscando su evolución en todo momento. Finalmente, la protección de los datos y comunicaciones estratégicos en contextos militares contienen información altamente confidencial. Una ciberdefensa resiliente minimiza riesgos de robo, manipulación o destrucción de esta información.

9.2 LA REDUNDANCIA DE ENLACE

La disponibilidad y estabilidad son dos aspectos importantes para el funcionamiento de los sistemas de tecnologías de la información (IT). Esta es una configuración de red, que busca establecer múltiples enlaces físicos o rutas para lograr la estabilidad y disponibilidad de la conexión en caso de que la ruta principal falle. Este aspecto es fundamental para que el tráfico datos no se interrumpa,

aunque alguna de las rutas o alternativas presente problemas. En la práctica sería, si una conexión falla cambia de manera automática a otra alternativa, acortando el tiempo de inactividad, lo cual favorece la confiabilidad de la red. (Cad&Lan, 2023)

Este tipo de configuración es imprescindible en entornos donde la interrupción del servicio es crítica como en los centros de datos donde se contiene información de gran valor, en este se busca la protección contra cortes de energía, fallas en el hardware o problemas de conectividad de red. También, en el ámbito empresarial, donde se busca conexiones redundantes para favorecer la continuidad de las operaciones. Además de estos, los proveedores de internet la utilizan para proveer un flujo continuo a los clientes de esta redes empresariales o centros de datos entre otras. (Cad&Lan, 2023)

La importancia de la redundancia en los sistemas IT, radica en la mejora de la seguridad, la continuidad del servicio, resiliencia ante fallos, la reducción de tiempos de inactividad y el rendimiento.

9.3 EL RESTABLECIMIENTO DE LOS SERVICIOS

Este aspecto se refiere a la capacidad de una organización de solucionar problemas y reanudar los servicios después de una interrupción. Esto puede incluir telecomunicaciones, servicios públicos y otros servicios esenciales. Este aspecto no se puede soslayar en un elemento que se relacione con la ciberdefensa, donde debe establecer planes de contingencia y garantizar la continuidad de los sistemas ante situaciones críticas.

9.4 LOS PUNTOS DE RESTABLECIMIENTO

Los puntos de restablecimiento en el ciberespacio, se refieren a las medidas y estrategias para recuperar y restaurar sistemas y datos después de una interrupción de servicio o incidente de seguridad. La implementación de estas medidas puede facilitar que la organización se recupere y enfrente cualquier interrupción. (Dacmos Team , 2024) Algunos aspectos claves son:

- Planes de recuperación ante contingencias: estos planes se utilizan para la restauración y operaciones luego de un incidente de magnitud y detallan los pasos a tener en cuenta.
- Copias de seguridad regulares: el mantenimiento de copias de seguridad de los datos críticos es importante para restaurar la información perdida o negligencia.
- Actualizaciones y parches de seguridad: el mantenimiento de los sistemas y software al día con sus parches de seguridad limita las vulnerabilidades y ataques.
- Sistemas de respuesta a incidentes: el establecimiento de protocolos claros contribuye a la recuperación y minimizar el impacto.

9.5 LA RESINCRONIZACIÓN EN EL CIBERESPACIO

Esta se refiere a la capacidad de restaurar y alinear sistemas y datos después de desincronizaciones. Este aspecto es fundamental para mantener la disponibilidad e integridad de la información. En lo que se refiere a ciberseguridad, la resincronización puede implicar la restauración de servicios en la nube, la recuperación de datos luego de un ataque cibernético o la restauración de los datos para confirmar su coherencia.

9.6 LAS POLÍTICAS DE BACK UP (RESPALDO)

Las políticas de back up son necesarias para la protección de los datos de la organización y su recuperación en caso de pérdida. Entre los puntos a incluir en estas políticas se encuentran, la frecuencia de backups, en esta se determina la frecuencia para realizar las copias de seguridad según el volumen y la importancia de los datos. Los métodos de backups, que permiten la implementación de distintos métodos para hacer copias diferenciales, completas e incrementadas con el objeto de optimizar tiempo y espacio.

También, se debe definir los datos a respaldar, donde se determinan los datos críticos a respaldar, otro aspecto a tener en cuenta es establecer un plan de recuperación de desastres, asegurando que los datos puedas ser restaurados en forma rápida. Por último, realizar las pruebas periódicas que permitan controlar la ejecución de los backups y la recuperación de los datos entre otras. Todas estas políticas contribuyen a favorecer la disponibilidad, integridad y confiabilidad de los datos respaldados. (Grupo ATICO 34, 2024)

9.7 CAPACIDADES TÉCNICAS DE RESILIENCIA

En el ámbito del ciberespacio un elemento es Ciber-resiliente (CR) cuando este desarrolló la capacidad de anticiparse, soportar y recuperarse, parcial o totalmente ante un ciberataque, a fin de proveer continuamente bienes y servicios hasta alcanzar un nuevo equilibrio, bajo condiciones diferentes al estado inicial. Esto es una definición que se asemeja a la realidad ya que en términos de la CR se seguirán suministrando bienes y servicios, pero bajo un nuevo escenario (o equilibrio). De esta forma, la definición también hace énfasis en su carácter "evolutivo y adaptativo" y no solamente preventivo, como en oportunidades lo manifiestan algunas organizaciones, sobre todo compañías comerciales que desean transmitir el mensaje de "resistir un ciberataque". Si bien la resiliencia pudiera tener una connotación preventiva, esta no es su naturaleza. (Garcia Hernández, 2022)

En concreto los tipos de ciberresiliencia buscan mitigar el impacto de un incidente, conforme a la naturaleza del propio concepto, solamente se logra una aplicación efectiva e integral en la adaptación. Esta persigue las continuas mejoras en estrategias y tecnologías basadas en lecciones aprendidas. Algunas organizaciones solo se focalizan en estándares preventivos o reactivos, sin alcanzar un nivel adaptativo ante cualquier circunstancia adversa. (Garcia Hernández, 2022)

En lo que respecta a la prevención se basa en la implementación de medidas para mitigar incidentes. La detención se refiere a la utilización de herramientas y técnicas para encontrar vulnerabilidades o amenazas. La respuesta se enfoca en poseer planes y procedimientos para responder a incidentes y amenazas. La etapa de recuperación busca restaurar sistemas y datos afectados para minimizar el impacto. Finalmente, estas etapas son importantes pero la más trascendente es la adaptación en este dominio, que busca la mejora continua. (Garcia Hernández, 2022)

9.8 LA INTEGRACIÓN DE LA INTELIGENCIA ARTIFICIAL AL CIBERESPACIO

Un aspecto que no se puede soslayar en el ciberespacio y en la actualidad es, que la IA está transformando este dominio como el resto del contexto actual. La Inteligencia Artificial (IA) es una ciencia dentro de la rama de la computación que actualmente se la considera como uno de los avances tecnológicos más disruptivos en la actualidad. Se la estima como la nueva revolución industrial del siglo XXI.

En el ámbito militar, la IA juega un papel crucial al proporcionar capacidades avanzadas de análisis de datos, toma de decisiones automatizada y sistemas autónomos, entre otros, permitiendo una mayor eficiencia en las operaciones y una respuesta más rápida y precisa en situaciones críticas. Sin embargo, su implementación también plantea desafíos éticos y legales que requieren una cuidadosa consideración.

En lo que respecta a ciberseguridad y ciberdelicuencia podemos ver que la misma mejora la detención y respuesta a amenazas, la IA permite detectar amenazas cibernéticas en forma rápida y precisa, estableciendo una respuesta eficiente ante un incidente. Esta utiliza algoritmos de avanzada y aprendizaje automático para analizar, grandes volúmenes de datos en tiempo real comportamientos inusuales que pueden indicar un posible cibertataque, esto permite adoptar medidas ante potenciales riesgos. (a3Sec, 2023)

Otro aspecto es el aumento de la eficiencia en los ciberataques, en la actualidad los ciberdelicuentes utilizan IA con el objeto de que los ataques sean más eficientes y difíciles de detectar. La integración del aprendizaje automático y la IA aumentaron la complejidad y eficacia de los ataques, los ciberdelicuentes utilizan herramientas basadas en IA para ejecutar sus actos criminales, entre ellos se destacan el pishing selectivo, el robo de identidad y la creación de Deepfakes, haciendo pistas de audio o clips de video falsos convincentes con muy pocos datos . (Ferré, 2023). También la ingeniería social o los ataques de denegación de servicio (DDoS) utilizan IA. Otro aspecto importante es la privacidad, en la actualidad cada vez más usuarios comparten información sensible con la IA.

La aplicación de la IA plantea debates normativos y técnicos, en cuanto a contramedidas y amenazas basadas en la IA. Estos controles se basan en la limitación del uso de la misma en el ámbito de ciberseguridad.

Estas contramedidas y controles orientados a limitar el uso malicioso de la IA en el ámbito de la ciberseguridad son parte del debate general sobre el cómo y cuándo abordar la regulación sobre el uso de la IA que asegure principios éticos y jurídicos a ciudadanos, empresas y estados.

9.9 VISIÓN ESTRATÉGICA DEL CONFLICTO DONDE ACTÚA EL ELEMENTO DE CIBERDEFENSA

La naturaleza objetiva de la guerra no ha cambiado, desde el pasado a la actualidad, podemos ya sea citar a Alejandro Magno, Julio Cesar, Clausewitz, Liddell Hart, Mao, Ho Chi Min, Eikmeier, no importa a quién, siempre el problema es dominar la voluntad del oponente economizando recursos. El ambiente ciberespacial provee notables ventajas y un cambio de paradigma de cómo hacer la guerra. (Moresi, 2023)

Por un lado, el campo de batalla se ha movido del mundo real a través del ámbito virtual a la mente de las personas, no importa cuál es la realidad, sino lo que la gente cree que la realidad es, más allá de los hechos que se muestren. Por esto la única realidad que importa es lo que la sociedad cree que es, desde ahí parte la decisión política acertada más allá de la realidad fáctica. El tiempo de permanencia en el ciberespacio por parte de la población se incrementa vertiginosamente, por esto el ciberespacio permite accionar a velocidades superlativas. (Moresi, Motta , Trama, Walker, & Amaya, 2023)

El campo de batalla en el siglo XXI es la mente de la sociedad, el rol de la infantería conquistando el objetivo será ocupado por una nueva clase de guerreros: los guerreros del ciberespacio, que serán los reyes de las mentes. Estos son equipos multidisciplinarios rodeados de especialistas,

como sociólogos, psiquiatras, neurocientíficos, ingenieros y psicólogos entre otras disciplinas. Este es el problema de la estrategia militar actual, en este ambiente operacional (ciberespacio). Por consecuente, la esencia de la guerra no mutó, sus modos han permanecido a lo largo del tiempo (guerra de información, velo y engaño, etc). Las nuevas tecnologías de la información y comunicación han llevado al conflicto a un nivel difícil de ponderar. (Moresi, 2023)

9.10 COMUNICACIÓN ESTRATÉGICA EN LA ERA DE LA INFORMACIÓN

Un aspecto que no se puede soslayar es la comunicación ya que esta organización se va a desplegar en la red de redes, la internet o la nube. En esta, la era de la información conserva los ambientes de la revolución industrial (máquinas y humano). Sin embargo, despliega entre ellos otro donde los individuos ahora perciben, interactúan y controlan su mundo físico a través del ambiente de la información. En ella, planifican y manipulan el uso masivo de las redes sociales, digitales y otros medios de comunicación, lo cual hizo posible llegar a audiencias más longevas con un contenido personalizado y dirigido a una velocidad inigualable. (Moresi, Motta , Trama, Walker, & Amaya, 2023)

Ilustración 6: Ambiente de la Información

Fuente: Elaboración del Almirante TRAMA (Trama, 2023).

En esta era las comunicaciones se apoyan en gran medida en internet, redes satelitales y terrestres o sistemas que ocupan gran parte del espectro electromagnético favoreciendo el flujo de información de la sociedad, los estados nación, las relaciones internacionales. (Trama, 2023)

Por otro lado, también se denomina la era de la post verdad, donde el planeta es una construcción humana concebida para explicar una verdad. Esta, elaborada por una narrativa, tiende a volverse subjetiva e imponerse temporalmente sobre otras verdades también subjetivas. Por esto la manipulación informativa crea una subjetividad la cual entiende la realidad acorde al discurso que prevalece. (Trama, 2023)

La opinión pública es moldeada por las redes sociales. Su explotación se realiza por cuentas y mensajes atribuidos a identidades falsas, la tecnología permite construir información muy difícil de corroborar su veracidad. (Moresi, 2023)

Las fuerzas armadas han abordado esta temática con una estrategia aceptable. Sin embargo, el uso que sus integrantes hacen de las mismas puede derivar en una amenaza a la seguridad nacional

o poner en peligro el cumplimento de la misión de un objetivo militar. Por tal razón debe, generarse una conciencia de este peligro mediante la capacitación. (Trama, 2023)

Por otro lado, el equipo responsable de la comunicación estratégica de esta organización cibernética debe conocer de este tema, actualizarse para minimizar los riesgos, detectar vulnerabilidades propias y en el oponente, y aprender a explotar las fortalezas. (Moresi, Motta , Trama, Walker, & Amaya, 2023)

La comunicación estratégica en la era de la información se conforma por el empleo planificado y coordinado de las capacidades y medios de comunicación que el Nivel Estratégico Militar dispone con el objeto de generar percepciones favorables, en los ámbitos de interés conducentes al logro de los objetivos y desafíos estratégicos de la Defensa Nacional. Por tal razón, se deben desarrollar acciones que faciliten la resolución y prevención de conflictos en todos los niveles de la conducción, en esto cumple un rol fundamental la preparación de nuestros cibersoldados y el accionar del elemento de ciberoperaciones. (Trama, 2023)

9.11 MARCO NIST (INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA)

Este fue concebido en 2013, por el aumento de incidentes en ciberseguridad en Estados Unidos, con el objeto de identificar las normas y directrices de seguridad aplicables a todos los sectores de infraestructuras críticas, marcando un enfoque repetible y flexible, que prioriza actividades y apunta a obtener un buen rendimiento de las infraestructuras, manteniéndose rentable para el negocio. Esta herramienta de gestión de riesgos en ciberseguridad hoy se conoce como *Cybersecurity Framework* (CSF). En esta, Estados Unidos identifica dieciséis infraestructuras críticas. (NIST Cibersecurity Framework, 2019)

La principal innovación del CSF está dada por abandonar estándares rígidos, que hasta aquel entonces era la norma. La principal mejora respecto de sus antecesores es su flexibilidad y simplicidad. La primera se caracteriza por su capacidad de adecuarse a cualquier organización y la segunda es por transmitir una estrategia técnica que el negocio comprenda. En este camino la OTAN, ya había avanzado en la creación de manuales para la protección de sus infraestructuras críticas. (NIST Cibersecurity Framework, 2019)

Estas cinco funciones del CSF en su *framework core* fueron seleccionadas porque representan los cinco pilares principales para un programa de ciberseguridad exitoso y holístico, el cual puede y debe ser analizado a la hora de conformar una organización responsable de la ciberdefensa a nivel estratégico. (NIST Cibersecurity Framework, 2019)

Identificar: esta contribuye a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los activos, los datos, las capacidades, las personas.

Proteger: menciona las medidas de seguridad para garantizar la entrega de servicios de las infraestructuras críticas. Explica la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.

Detectar: describe las actividades para identificar la ocurrencia de un evento en ciberseguridad, permitiendo su descubrimiento oportuno.

Responder: involucra actividades para tomar medidas ante incidentes en ciberseguridad que se detecten, para desarrollar la capacidad de contener a un incidente.

Recuperar: permite identificar las actividades a ejecutar para mantener los planes de resiliencia y restaurar cualquier servicio o capacidad que haya sufrido consecuencias luego de un incidente de ciberseguridad. La recuperación oportuna de las operaciones normales y esta función son compatibles, ya que favorecen la reducción del impacto en un incidente de ciberseguridad.

10 PRINCIPALES CARACTERÍSTICAS DE UN SISTEMA CIBERNÉTICO EN EL REGIONAL

Esto es algo difícil de predecir dado que el conflicto hoy abarca un amplio espectro. Sin embargo, ciertas características no deben faltar en función del análisis bibliográfico y la opinión de los diferentes especialistas y personal que conduce la ciberdefensa en la actualidad.

La segmentación sería una variable, si la agresión es sobre lo físico de las redes tanto OT como IT, interpreto que la solución más probable pasaría por la segmentación del sistema, vale decir tener una estructura orgánica, flexible y descentralizada, que permita la innovación, la creatividad y la autonomía de los actores involucrados. Si la agresión se materializa en lo cognitivo, solo cabe el accionar mediante equipos multidisciplinarios especializados. (Bustamante, 2023)

La flexibilidad sería fundamental, con la capacidad de adaptarse rápidamente a las condiciones cambiantes del entorno y de los adversarios. Este sistema debería contar con una inteligencia artificial avanzada que le permita analizar las amenazas, identificar las vulnerabilidades, diseñar las estrategias más adecuadas y ejecutar las acciones más eficaces para neutralizar o minimizar los daños. (Guerra, 2023)

La interoperabilidad es un acto disruptivo favorable, ya que esto permite concebir el ciberespacio en capas, por lo cual se plantea la visión de tres capas, la física, la lógica y la social de las cuales destaca cinco componentes. En la social a las personas se las denomina como componente ciberpersonas, la lógica compuesta por el componente redes lógicas y en la física los componentes geográficos y las redes físicas. Esto favorece los estudios que aplique la estrategia militar para determinar aspectos éticos, estándares, gobernanza, políticas, procedimientos y comportamiento humano en cada capa y la interoperabilidad entre ellas. (Moresi, 2023)

Para pensar la guerra en el ciberespacio requiere desde la perspectiva ciberespacial asegurar la información, la calidad de los datos, la conciencia situacional y el conocimiento que permita la mejor toma de decisiones. Por esto, la estratégia debe realizar una adecuada evaluación de las fortalezas y debilidades propias y del oponente para neutralizar los riesgos y amenazas a tiempo. (Moresi, Motta , Trama, Walker, & Amaya, 2023)

El mando es centralizado en el nivel estratégico, con una ejecución extremadamente descentralizada. Es por ello que, constituirá un factor de éxito la designación del / los responsables de concebir y llevar a la realidad un sistema cibernético en el nivel estratégico que se considere flexible, resiliente y eficiente. (Moyano, 2023)

La conducción se deberá ejecutar con el menor nivel de dependencia posible, dicho de otra manera, quien conduzca esta organización depende del ápice estratégico en forma directa, con una garantizada llegada inmediata al mismo. Vemos aquí la primera ruptura de paradigmas. Los soldados buscamos por formación, generar una división del trabajo que permita una extensa y formal supervisión de las tareas. (Guimpel, 2023)

Este camino será el primer obstáculo para lograr una respuesta acorde e inmediata a los problemas que enfrentará esta organización. Como ejemplo práctico, hablamos de un Comandante que dependa directamente del Jefe de Estado Mayor Conjunto, con acceso directo y simultáneo a las autoridades del Ministerio de Defensa competentes del área, que le permitan accionar o responder con eficiencia, en particular si se habla de operaciones ofensivas. (Moyano, 2023)

La integración en su organización como constelaciones de trabajo[6] : aquí se muestra uno de los grandes desafíos. Las características propias del ámbito del ciberespacio requerirán de estructuras flexibles, organizaciones integradas por profesionales civiles y militares, con mecanismos de coordinación que se adapten también a esta forma de trabajo, de variados orígenes, provenientes de distintas fuerzas u organizaciones estatales y privadas. Por esto, la norma es la organización y la gestión de conocimiento. (Moyano, 2023)

Otra característica que prevalece es la redundancia. Si bien, esto impone ingentes esfuerzos económicos y humanos, estos últimos en términos de captación y formación, el sistema debe poder soportar la amenaza permanente de ataques, debiendo estar en capacidad de sortearlos y eventualmente responderlos. El tipo de organización flexible ya detallada, cooperará con este concepto, sumado al de gestión del conocimiento. El punto es que, lo sencillo de su expresión, se opone a la realidad compleja que supera los aspectos tangibles. Los intangibles son los que complicarán la conformación de este sistema en estos niveles, ya que, las culturas organizacionales de quienes lo conforman colisionan en forma permanente, afectando la producción y outputs a la velocidad que requieren las amenazas. (Moyano, 2023)

11 EJERCICIOS DE COOPERACIÓN EN AMÉRICA LATINA

En el marco regional se realizan ejercicios de ciberdefensa para fortalecer e incrementar la resiliencia y la seguridad cibernética. En estos se destacan:

- Prácticas cibernéticas: estas actividades presentan los principios y reglas diseñados para planificar, construir y editar ejercicios de ciberseguridad. Se enfocan en mejorar la resiliencia cibernética de las organizaciones mediante programas anuales y plurianuales. El uso de la IA se está utilizando para identificar patrones de amenazas y prevenir ataques cibernéticos. Para mitigar las ciberamenazas del ramsomware, los ladrones de información en la nube, las brechas de seguridad en la nube, los puntos de acceso final las organizaciones cibernéticas se deben focalizar en las medidas de seguridad que enfaticen la prevención, incluyendo las de amenazas impulsada por IA. La inversión de amenazas en tiempo real, segmentación de redes y la capacitación de sus empleados sobre conciencia situacional reducirá los riesgos significativamente. (González, 2025)

- Foro Iberoamericano de Ciberdefensa: este foro reúne a países iberoamericanos para colaborar en formación, ejercicios, intercambio de información e investigación en ciberdefensa. Promueve la realización de ciberejercicios y fomenta el intercambio académico. Entre otros se destacan ejercicios combinados de esta temática ya realizados en España, Brasil y Colombia. La oferta de vacantes que mantiene Brasil para naciones amigas, plataformas para intercambiar información sobre ciberamenazas como la MISP "Mallware Information Sharing Platform" que afectan la ciberseguridad. El Ejercicio Guardián Cibernético 7.0 (EGC 7.0) para presentar cómo se planifica, coordina y ejecuta una ciberoperación. Este se trata de un ciberejercicio montado sobre las infraestructuras críticas de interés para la defensa nacional de Brasil con el propósito de incrementar la ciberprotección a través de la acción conjunta de las Fuerzas Armadas. (Costa, 2024)

6 Es una metodología que, desde una mirada amplia y sistémica, nos ayudan a comprender cuáles son los factores que están causando los problemas a los que nos enfrentamos en nuestra organización o empresa. Esto facilita observar dónde se halla el verdadero problema que está nutriendo el conflicto que estamos viviendo. Esta técnica se basa en la visión sistémica como nuevo paradigma para generar eficiencia en las organizaciones

- Ejercicios de Red Team: los ejercicios de Red Team son simulaciones de ciberataques diseñadas para evaluar la seguridad de una organización desde la perspectiva de un atacante real. En América Latina, estos ejercicios han cobrado relevancia debido al aumento de ciberataques sofisticados en la región. Por ejemplo, en 2024, empresas como Grupo Bimbo y Banco do Brasil enfrentaron incidentes graves de ransomware y filtración de datos. Estos ejercicios simulan ataques reales para evaluar la postura de seguridad de una organización desde la perspectiva de un atacante. Incluyen técnicas como ingeniería social, pruebas de penetración, escalamiento de privilegios y exfiltración de datos. Estos ejercicios son fundamentales para identificar vulnerabilidades, mejorar la respuesta a incidentes y fortalecer la cultura de seguridad en la región. (Figueroa, 2025)

12 CONCLUSIONES

Pensar un proceso de guerra cibernética desde la perspectiva ciberespacial requiere asegurar la calidad de los datos, la información, conciencia situacional y el conocimiento que permita la mejor toma de decisiones, alcanzando de esta manera una superioridad militar a partir de la superioridad de la información.

Se puede afirmar que, hace más de dos décadas, el ciberespacio se ha convertido en el centro de gravedad del poder nacional, financiero, diplomático y militar de cualquier estado nación que le importe el bienestar y la privacidad de sus ciudadanos.

El campo de batalla actual se está librando en la mente de las personas, teniendo en cuenta que las operaciones en el ciberespacio se basan en efectos y uno de ellos es manipular la realidad y, que esta realidad se maneja con información. Un sistema de cooperación en ciberdefensa dentro del marco regional de América Latina debes estar dotado de ciertas características para ser considerado resiliente, entre estas podemos mencionar:

1. En primer lugar, es que las fuerzas militares no se preparan de la noche a la mañana para su objetivo principal que es la guerra. Estas necesitan de un capital humano de excelencia, con pensamiento creativo y proactivo, acompañados de la última tecnología bélica. El pensamiento estratégico debe concretarse con planes cumplibles, acompañados por el máximo nivel de conducción para enfrentar las debilidades del sistema.

2. La inversión en el recurso humano de los países miembros, y como factor más importante es la selección del personal y su capacitación permanente. Esto se debe ejecutar teniendo en cuenta las competencias que requiere este dominio, de manera integral en su formación profesional militar y civil, involucrando varias ramas de conocimiento. Es por ello que constituirá un factor de éxito la designación del / los responsables de concebir y llevar a la realidad un sistema cibernético en el nivel estratégico que se considere flexible, resiliente y eficiente.

Los que conduzcan estas organizaciones deberán depender del ápice estratégico en forma directa o con una garantizada llegada INMEDIATA al mismo.

Las características propias del ámbito del ciberespacio requerirán de estructuras flexibles, organizaciones integradas por profesionales civiles y militares, con mecanismos de coordinación que se adapten también a esta forma de trabajo, de variados orígenes, provenientes de distintas Fuerzas u organizaciones estatales y privadas. La norma en este caso será la integración y la Gestión del Conocimiento, para lo cual la formación basada en Valores de quienes ocupen puestos sensibles, será primordial, sin descuidar los incentivos económicos para todos sus integrantes, aspecto que ocasiona siempre una traba para su reclutamiento para las FFAA, contra la oferta externa.

3. La adaptabilidad es otro factor importante. Como dijera el General de División Evergisto De Vergara "Todas las guerras son únicas e irrepetibles, y no hay ninguna guerra parecida a la anterior". Por lo tanto, la manera de organizase dependerá de las características, objetivos y contextos específicos, así como de los criterios que se utilicen para evaluar la optimización de los recursos. Algunos aspectos que podrían considerarse son: la flexibilidad y en especial el desarrollo del pensamiento innovación, que puede implicar diferentes formas de distribuir el poder, la autoridad, la comunicación, la coordinación y el control entre las partes del sistema. Por lo tanto, no hay una solución óptima universal, sino que se requiere un análisis situacional y una adaptación constante a las demandas del entorno que impliquen:

- distinguir los atributos y el alcance de la creatividad y la innovación;
- desarrollar un esquema mental que favorezca la adquisición de esas competencias;
- reconocer y emplear herramientas efectivas en esas áreas del conocimiento y la innovación;
- desarrollar una cultura innovadora.

En este punto se plantea la diatriba de lo seguro y lo práctico, esencia de la interoperabilidad cibernética debido a que lo muy seguro es poco práctico y lo muy práctico es poco seguro, ecuación que debe ser resuelta en el nivel técnico e implementada por la decisión estratégica en una adecuada evaluación de las fortalezas propias, las vulnerabilidades del adversario, las debilidades propias y las oportunidades que ellas dejan para la acción del oponente, determinando claramente los riesgos y amenazas que esa decisión involucra.

El desafío para las fuerzas armadas es utilizar las tecnologías de la información para construir una infraestructura de sistema altamente adaptable, de alto rendimiento e interoperable.

4. Otra característica vital para hacer frente a las múltiples amenazas es la Redundancia. Si bien, esto impondrá esfuerzos económicos y humanos, estos últimos en términos de formación y captación, el sistema debe poder soportar la amenaza permanente de ataques, debiendo estar en capacidad de sortearlos y eventualmente responderlos.

5. La Conducción centralizada y ejecución descentralizada es otra característica a tener en cuenta. Este concepto conocido por las organizaciones militares, pero no siempre dispuestas a ponerlo en práctica. Habrá que confiar en el "hombre en primera línea" a la hora de recibir la amenaza. Llevado también al ámbito de trabajo, el estratégico, obliga a delegar y asumir riesgos, escuchar no sólo en la etapa de asesoramiento, sino también, en la de asistencia. El ámbito de ejecución es fluido, cambiante, versátil, volátil y hasta difuso. Los conductores que se adapten a él podrán liderar organizaciones inteligentes y persistentes en el tiempo con éxito.

6. La integración con lo privado es esencial, las fuerzas armadas deberían conducir el ámbito cibernético. Así lo hacen con éxito países de la región. El mundo empresarial debe recurrir y someterse al control del estado mediante las herramientas y organizaciones ad hoc. Por allí vendrán las principales amenazas transnacionales. El enemigo en este ámbito evadirá las fortalezas y buscará las debilidades, intentando acceder a sistemas y objetivos fundamentales desde el interior de cada organización civil, ya sea estatal o privada. El ciberespacio transita por una nebulosa desde el punto de vista de la SOBERANIA que pocos entienden. Trataremos este punto más adelante.

7. Manejar los Enlaces regionales e internacionales, en este dominio no basta con lo interno. Los líderes del sistema cibernético deberán poseer características no solo técnico profesionales sino PERSONALES MUY PARTICULARES para poder tender puentes acordes con el exterior. Aquí juega también el concepto de SOBERANIA CIBERNETICA.

8. Replantear en el ámbito militar el concepto de SOBERANIA CIBERNETICA, este aspecto necesita ser tratado en profundidad. Amerita su estudio y dedicación, así como la necesidad de concientizar sobre ello a los líderes políticos y militares. Destacar que casi no hay jurisprudencia sobre esto. Se debe prevenir sobre el error de manejarse en el ámbito cibernético con conceptos de los otros dominios, afectando gravemente la Toma de Decisiones.

9. La Gestión del Conocimiento, los líderes del sistema cibernético que no gestionen el conocimiento a nivel nacional, estarán siempre un paso atrás, no importa el esfuerzo individual de cada uno de sus integrantes o células. Y aquí confluyen muchos de los condicionantes expresados en los primeros objetivos como, la necesidad de contar con el marco normativo adecuado a estos tiempos y no a ideologías puntuales que obstaculizan su trabajo; conocer y aplicar el concepto de SOBERANIA CIBERNETICA; estar integrado con los actores regionales y referentes internacionales; entre otros.

Para finalizar, se destaca que estas características deben ser analizadas a la hora de pensar una organización que va a interactuar en el ciberespacio a nivel regional, en todos los niveles, pero en particular en el nivel estratégico. La falta de atención sobre los intangibles, las relaciones interpersonales, las culturas organizacionales y la necesidad de ser redundantes, resilientes y formados, pueden provocar la creación de un elemento sin bases firmes y fácilmente permeable.

Como he desarrollado en este ensayo, con el aporte de la bibliografía utilizada, he podido corroborar que el centro de gravedad de las organizaciones que cooperan en el marco regional del ambiente cibernético. La característica principal de este sistema regional, a pesar del avance de la tecnología y el ritmo vertiginoso de la inteligencia artificial, es el componente humano.

Las operaciones cibernéticas han llegado para quedarse en nuestro ciberespacio; su uso eficiente favorecerá la convivencia normal de la sociedad. Esta convivencia debe ir acompañada de un cambio de paradigma para desarrollar capacidades cognitivas que nos permitan, como raza superior, imponernos a la IA.

Por lo dicho hasta ahora, el reto para afrontar el conflicto del presente y el futuro es conseguir nuevas capacidades cognitivas con la evolución de la inteligencia artificial, una tecnología que permita a los humanos seguir siendo la especie dominante. La oportunidad está a nuestro alcance y la neurociencia ha abierto la puerta a la comprensión de nuestro cerebro. El desafío consiste en crear una nueva cultura del aprendizaje, lo que requiere comprender y gestionar este nuevo escenario para evitar ser dominados por él. La confrontación actual no distingue entre seguridad interior y nacional, ni entre civiles, soldados o mercenarios; el conflicto tiene lugar dentro de cada uno de nosotros. El objetivo de esta era para la humanidad es desarrollar una cultura común y una forma de pensar propia que facilite la gestión de los conflictos y crisis actuales. Lo más importante, sin embargo, será el desarrollo de nuevos recursos que nos permitan utilizar la IA de forma eficiente.

FINALMENTE, para que este sistema sea considerado RESILIENTE en el marco regional el Centro de Gravedad debe estar concebido para proteger activos y sistemas de información críticos de las FFAA. Este debe incluir capacidades de ciberdefensa, medidas de seguridad, análisis de amenazas y respuestas a incidentes. También, tecnologías avanzadas de ciberdefensa y criptografía. La incorporación de sistemas de IA en el ciberespacio es algo que no se puede detener, sin embargo, debe estar perfectamente regulado y establecer los protocolos de seguridad para que esta tecnología no genere una debilidad. La IA debe ser tenida en cuenta para un trabajo en profundidad de otras investigaciones, principalmente su marco legal y ético, pese a que los conflictos a lo largo de la historia nos muestran que, en situaciones de guerra, el fin justifica la rudeza.

REFERENCIAS

A3SEC. **La importancia de la Inteligencia Artificial en la ciberseguridad.** Obtenido de https://a3sec.com/blog/ia-en-la-ciberseguridad, 2023

AMERICA, D. **Cyberspace Operations**. GL-4 (5-70). Washington DC, United States of America: Joint Publication, 2018

BUSTAMANTE, D. Anexo 3: **Organización de un sistema de ciberdefensa**. (I. Cabrera, Entrevistador), 2023

CABRERA. **Empleo de las redes informáticas en el marco de la Gran Unidad de Batalla**. CABA: UNDEF, 2019

CAD&LAN. **Conexión Redundante.** Obtenido de https://www.cadlan.com/noticias/que-es-conexion-redundante/, 2023

CAL, DI TELLA, GANEAU, GRUNSCHLAGER Y LEAL. **La Cuestión Estartégica**. Buenos Aires: Escuela de Guerra Naval, 2016

CORLETTI Estrada. **Ciberseguridad, Una Estrategia Informático/Militar**. Madrid, Madrid, España: Recuperado de http://www.darfe.es/joomla/, 2017

CORNAGLIA, S. La ciberdefensa y su regulación legal en Argentina (2006 - 2015). URVIO-**Revista Latinoamericana de estudios de seguridad**., https://revistas.flacsoandes.edu.ec/urvio/article/download/2601/2106, 2017

COSTA, A. D. **CIBERILATAM** "Los conflictos que ocurren a miles de kilómetros pueden afectar a la ciberseguridad de Latinoamérica". Obtenido de "Los conflictos que ocurren a miles de kilómetros pueden afectar a la ciberseguridad de Latinoamérica": https://www.segurilatam.com/ciberilatam/foro-iberoamericano-de-ciberdefensa-los-conflictos-que-ocurren-a-miles-de-kilometros-pueden-afectar-a-la-ciberseguridad-de-latinoamerica_20240404.html, 04 de Abril de 2024.

DACMOS TEAM. **Dacmos Team Group**. Obtenido de https://www.dacmosgroup.com/ciberespacio-riesgos-y-estrategias-de-proteccion, 25 de agosto de 2024.

DE VERGARA Y TRAMA. **Operaciones Militares Cibernéticas.** (E. S. Armadas, Ed.) Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina: Visión Conjunta, 2017.

FERRÉ, X. **Cómo la inteligencia artificial está cambiando la ciberdelincuencia**. Obtenido de https://www.ey.com/es_es/cybersecurity/como-la-inteligencia-artificial-esta-cambiando-la-ciberdelincuencia, 25 de mayo de 2023.

FIGUEROA, A. G. **Entelgy Security América**. Obtenido de Ejercicios de read team: clave para la ciberseguridad de América Latina.: AGUIAR, O. Comunicação Estratégica: a importância do Plano Estratégico de Comunicação Social na Marinha do Brasil. Trabalho de Conclusão de Curso apresentado ao Centro Universitário de Brasília (UniCEUB), Brasília, 2022.

GANUZA, N. e JID. **Guía Ciberdefensa**. Orientaciones para el diseño. Planeamiento, Implantación y Desarrollo de una ciberdefensa Militar. Ontario: Copyright © 2020 Junta Interamericana de Defensa. Canada: Junta Interamericana de Defensa. Obtenido de https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf, 2020.

GARCIA HERNÁNDEZ, A. La contribución de la ciberresilencia al poder nacional. **Revista Internacional sobre la Sociedad, la Política y la Cultura** SOCIOTAM . (Centro Multidisciplinario de Investigaciones Regionales (CeMIR)), 129-131. Obtenido de https://sociotam.uat.edu.mx/index.php/SOCIOTAM/article/view/173, 2022.

GONZÁLEZ, D. **Ciberseguridad en América Latina 2025:** El impacto de la IA y la inteligencia sobre amenazas. Obtenido de Ciberseguridad en América Latina 2025: El impacto de la IA y la inteligencia sobre amenazas: https://www.diariodelsur.com.co/ciberseguridad-en-america-latina-2025-el-impacto-de-la-ia-y-la-inteligencia-sobre-amenazas/, 25 de Febrero de 2025.

GRUPO ATICO 34. **Política de copias de seguridad para empresas**. Obtenido de https://protecciondatos-lopd.com/empresas/politica-copias-seguridad/, 30 de Sep de 2024.

GUERRA, C. . **Anexo4: Organización de un sistema de ciberdefensa**. (I. Cabrera, Entrevistador), 25 de octubre de 2023.

GUIMPEL, L**. Anexo 5: Organización de un sistema de ciberdefensa**. (C. I. Cabrera, Entrevistador), 6 de 11 de 2023.

LLONGUERAS Vicente. **La Guerra Inexistente, la Ciberguerra. Ciberdefensa.** Saarbruchen, Saarbruchen, Alemania: Académica Española, 2013.

MAURER, T. **Cyber Mercenaries (The state Hacker and Power).** Washington DC: Cambridge University Press, 2018.

MCGUINNESS. **BBC NEWS - Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país.** Obtenido de Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país: https://www.bbc.com/mundo/noticias-39800133, 6 de mayo de 2017.

MIESSLER, D. **The Difference Between Red, Blue, and Purple Teams.** Recuperado el 15 de octubre de 2019, de The Difference Between Red, Blue, and Purple Teams: https://danielmiessler.com/study/red-blue-purple-teams/, 2019.

MORESI. **La Guerra Cibernética.** En T. M. Motta, Operaciones en el ambiente de la información (págs. 78-88). Bs As: UNDEF, 2023.

MORESI, A., MOTTA , G., TRAMA, G., WALKER, M. S., & AMAYA, C. **Operaciones en el ambiente de la información.** CABA: Visión Conjunta, 2023.

MOYANO, R. **Anexo 1: Organización de un sistema de ciberdefensa.** (I. Cabrera, Entrevistador), 16 de septiembre de 2023.

NACIONAL, P. E. Directiva de Política y Defensa Nacional. República Argentina, Ministerio de Defensa, CABA, 2018.

NIST Cibersecurity Framework. Un abordaje integral a la Ciberseguridad. México: Obtenido de file:///C:/Users/Asus/Desktop/Estudio/TESIS/TESIS/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP%20(1).pdf, 2019.

RIO, A. G. **El Ciclo OODA y la toma de decisiones en el Planeamiento**. Trabajo Final Integrador (Planeamiento Operacional), 4-13. CABA, Buenos Aires, Argentina: CEFA digital, 2013.

SMART, S. **Aportes sobre el protagonismo de contratistas en ciberoperaciones entre estados**. CABA: Maestría en ciberdefensa y ciberseguridad, 2021.

TRAMA, G. **La comunicación estratégica y la estratégia de la comunicación**. En E. 2023, Operaciones en el ambiente de la información (págs. 117-162). BsAs, 2023.