



LA CIBERDEFENSA Y SU APOORTE A LA SEGURIDAD DEL ESTADO

Mayo. de I.M Adrián Landázuri
Mayo. de E Byron Vega Moreno

RESUMEN

El ciberespacio constituye una nueva dimensión creada por el hombre que demanda una especial preocupación para los sistemas de seguridad y defensa de los Estados, puesto constituye un riesgo latente que no solo está en capacidad de vulnerar la seguridad de la información o infraestructura crítica de un país, sino incluso afectar cualquier actividad dependiente de una base digital.

En este contexto, se torna obligatorio para las Fuerzas Armadas, concebir al ciberespacio como una nueva dimensión de la guerra, que no tiene límites ni fronteras, donde existe una amenaza difusa, compleja e intangible, que permite la interrelación de un amplio espectro de actores y formas de actuación, que deben ser abordados integralmente desde una perspectiva tecnológica.

Hoy en día, la ciberdefensa, se presenta como una respuesta a una necesidad vital de los estados, que sin duda requiere de la generación de capacidades estratégicas que permitan la capacitación integral del personal, la adquisición, generación e implementación de sistemas de seguridad informática, pero sobre todo, la concientización sobre el alcance y efecto de las amenazas cibernéticas como un mecanismo de prevención y protección de una sociedad que depende de la tecnología y la información.

Palabras clave: Ciberespacio, ciberguerra, ciberdefensa, amenaza, Seguridad Nacional.

ABSTRACT

Cyberspace is the new dimension created by the human kind which demands a special concern for the security and defense systems of every State, because it became a latent risk not only capable of threaten security of the information and critical infrastructure of a country, this threat can also affect any activity related to a digital base.



In this context, it is mandatory for the Armed Forces to consider cyber space as a new dimension for the warfare, this new dimension has no limits or boundaries, where the threat is diffuse, complex and intangible. The cyber space allows a full spectrum of actors and different kinds of performances, this issue must be face in an integral way from a technological perspective.

Nowadays, cyber defense is shown like the answer to a vital necessity of the States. This answer demands the generation of strategical capabilities which allow the integral capacitation of personnel, the acquisition, generation and implementation of computing security systems, but much more important is the awareness about the scope and different effects caused by cybernetic threats as a mechanism of prevention and protection of a society that depends on technology and information.

Keywords: Cyberspace, cyberwar, cyber defense, threat, National Security.

1. Introducción

La modernidad introdujo un nuevo espacio y forma de conflicto que siempre está activo y nadie puede escapar de él. El ciberespacio constituye una nueva dimensión creada por el hombre en la que es difícil atribuir una agresión y que genera una nueva preocupación para los Estados.

Se trata de un ámbito común y global, donde existe una seria dificultad para definir fronteras, soberanía, lo que impacta en la seguridad del Estado. La ciberguerra no solo se trata de una guerra sin ruido ni armas, sino también de un delito rentable y, por ello, la ciberdefensa constituye un reto que impone equilibrar libertad y cooperación con seguridad y privacidad.

El presente ensayo pretende analizar el panorama actual del ciberespacio, a través de un estudio descriptivo de la evolución, tendencias, amenazas y oportunidades de la ciberdefensa en el contexto internacional, con el fin de comprender su alcance y uso en el ámbito de la seguridad nacional.

2. Análisis

Evolución y tendencias de la Ciberdefensa

Evolución de la Ciberdefensa

Para algunos autores, el ciberespacio se ha considerado como una nueva dimensión de la guerra, en el cual los Estados enfrentan ataques a las redes informáticas y de comunicación poniendo en riesgo su infraestructura crítica y su funcionamiento. En tal virtud los Gobiernos se ven en la necesidad de replantear los modelos de seguridad y defensa en base a la inclusión de nuevos conceptos como ciberespacio, ciberataques, ciberseguridad, ciberdefensa¹ entre otros.

Esta nueva realidad, responde a una evolución que comenzó en la segunda guerra mundial, mediante la convergencia de la empresa bélica con el desarrollo de computadores y red de comunicaciones e internet. Fue durante el período comprendido entre 1939-1989 en el que se consolidaron estos dos pilares tecnológicos. Durante la segunda guerra mundial, las tecnologías informáticas tuvieron su origen, mediante la invención y utilización por parte de los nazis de la máquina de encriptación de mensajes ENIGMA, la cual fue contrarrestada por el primer computador descifrador creado por los ingleses, denominado COLOSSUS. (GAITÁN, 2012)

En la década de los 60, en plena guerra fría, los Estados Unidos creó la red de uso militar llamada ARPANET (Advanced Resecar Projects) considerada como el primer modelo de internet. A inicios de los 80 se dio la transición de ARPANET a World Wide Web (www), y con ella, la expansión de las redes informáticas al campo académico y de investigación, permitiendo un rápido y masivo crecimiento del internet a nivel mundial y, a su vez la oportunidad de vulnerar la privacidad de información de las personas y de los Estados, a través de códigos dañinos² insertados en ordenadores, sistemas y redes informáticas. (IEEE, 2010).

A partir de ese momento, se concibe una nueva forma hacer la guerra, que consiste en atacar al enemigo mediante el uso de información a través de computadores y la comunicación en red, con el fin de lograr el desequilibrio psicológico de la población, la desarticulación de los sistemas logísticos; así como también el uso de las tecnologías de información para la organización estratégica, operacional y logística de los componentes y recursos de las fuerzas militares. (GAITÁN, 2012).

1 Kevil Coleman, <<The weaponry and strategies of digital conflict>>. Security and Intelligence Center at the Tecnolytics Institute, USA, 2010.

2 Término utilizado para definir software que tiene como objetivo infiltrarse en o dañar un ordenador sin el consentimiento de su propietario.



Control del ciberespacio a través de equipos del Comando de Ciberdefensa CC.FF.AA.
Fuente: Archivo fotográfico OPSIC - Ejército Ecuatoriano.

En este contexto, las temerarias prácticas para la obtención de información desde el ciberespacio, que han sido denunciadas por diferentes actores y aceptadas por líderes mundiales, promueve la necesidad de los Estados, de implementar un sistema de ciberdefensa que les permita protegerse de las amenazas, peligros o riesgos de naturaleza cibernética y a su vez hacer uso del ciberespacio con seguridad.

Tendencias de la Ciberdefensa

Las actuales tendencias de la sociedad digital, son la respuesta a la constante evolución de un mundo globalizado e interconectado, en el cual las TICs, (Tecnologías de la Información y Comunicaciones) son causa y efecto de este proceso. Entre los principales desafíos de los Estados, sociedades, Gobiernos, organizaciones internacionales y demás actores comprometidos con la gobernanza³ y paz global están en identificar y visualizar las tendencias emergentes y relevantes concernientes a las TICs, cuya exponencial evolución incrementa la incertidumbre y limita la capacidad de los Estados para garantizar su seguridad y defensa.

Las tendencias en Ciberdefensa de los Estados apuntan al desarrollo tecnológico de nuevas armas

informáticas, la conformación de ciberunidades, el entrenamiento de cibersoldados, el apareamiento de la disuasión informática por sobre la nuclear, mediante el desarrollo de una serie de capacidades informáticas para enfrentar o ejecutar ciberataques. Al mismo tiempo los políticos tomarán conciencia de la importancia de estos temas para los Estados, a través de iniciativas legales y económicas tendientes a mejorar las capacidades de Ciberdefensa de las naciones (CANO, 2015)

En resumen, el ciberespacio se ha convertido en una dimensión adicional de la guerra, donde la incidencia de las TICs, se traduce en una demanda obligatoria presente y futura para los Estados y sus FF.AA (Fuerzas Armadas); a fin de desarrollar capacidades de Ciberataque y Ciberdefensa, como prioridad para la seguridad nacional.

Amenazas y oportunidades de la Ciberdefensa

Amenazas

La creciente dependencia de países y personas en un mundo interconectado se traduce en riesgo para cualquier actividad que emprenda la sociedad digital, en consecuencia, mientras mayor sea la dependencia, mayor será la capacidad de las nuevas tecnologías para afectar la vida de las personas y el funcionamiento

3 MARÍA V. WITTINGHAM. Es la realización de las relaciones políticas entre diversos actores involucrados en el proceso de decidir, ejecutar y evaluar decisiones sobre asuntos de interés público, proceso que puede ser caracterizado como un juego de poder, en el cual la competencia y cooperación coexisten como reglas posibles; y que incluye instituciones formales como informales.

de los Estados, convirtiendo al ciberespacio en un escenario complejo y difuso (GAITÁN, 2014).

En la seguridad del ciberespacio se han identificado amenazas con características heterogéneas y de alta innovación, cuya evaluación será importante al momento de implementar políticas de seguridad. A continuación, mencionaremos aquellas que por sus repercusiones e impacto se han hecho populares en los últimos tiempos.

Los ataques distribuidos de denegación de servicio (DDOS), que básicamente es una forma de bloqueo on-line, en la actualidad se han convertido en una herramienta de guerra de información.

El código dañino “Stuxnet” que aparece en junio de 2010, estaba dirigido contra el programa nuclear iraní. Stuxnet mostró el riesgo potencial de malware que afecta a sistemas informáticos críticos que gestionan suministros de energía. (BEJARANO, 2013)

Los botnets (robots de la red) son redes de ordenadores zombis. Se emplean para realizar ataques, envíos masivos de correo basura y espionaje. El virus puede enviarse por correo electrónico, aunque lo habitual es ponerlo en una página web.

Zeus es un virus de botnet que se propaga por los navegadores, tanto Explorer como Firefox. El malware permite recopilar información del usuario, así como también contraseñas de internet y redes sociales, utilizándolas para suplantar la identidad y realizar robo de datos bancarios o enviar spam.

De acuerdo a un informe reciente de Cisco⁴, el futuro de las amenazas cibernéticas se centra en dos grandes áreas: ingeniería social (manipulación de formularios, llamadas no solicitadas, mensajes) y ataques multisectoriales donde se combinan diferentes tipos de soporte (correo electrónico, mensajes en blogs, redes sociales, wikis, voz, video, audio, entre otros), convirtiendo a la dimensión cibernética en el lugar propicio para ataques graves con consecuencias irreparables en el mundo real. Siendo importante mencionar que de acuerdo a la evaluación de los expertos, los actores más peligrosos del ciber-dominio⁵ siguen siendo los Estados. (IEEE, 2010)

Oportunidades

En el futuro cercano los Estados serán los encargados

de decidir en el ámbito de la ciberdefensa, llegando a definir si un ataque virtual a un individuo u organización pública o privada puede comprometer el desarrollo y la supervivencia del Estado. Por ello, se considera que la ciberseguridad y la ciberdefensa han evolucionado de ser temas netamente técnicos, para convertirse en una capacidad estratégica clave en la conducción de un Estado dentro de los diversos niveles de decisión o niveles internacionales cuando se habla de proyectos de seguridad. (SAMPER, 2015)

Para garantizar que los sistemas de información y comunicaciones utilizados por un país, posean el adecuado nivel de seguridad se debe potenciar las capacidades de identificación, detección, prevención, contención, recuperación, cooperación y mejora continua frente a las amenazas cibernéticas, lo que sin duda implica la asignación de recursos, la promulgación de un marco legal y la oportunidad de ampliar el entorno académico y de investigación.

Aporte de la Ciberdefensa a la seguridad del Estado

Con el desarrollo de la tecnología y la globalización como ente multiplicador de este desarrollo, se ha incrementado la dependencia de las sociedades modernas y de los países desarrollados de los sistemas de información. El desarrollo de la sociedad de la información en los países avanzados es a su vez su gran fortaleza y su gran debilidad. (IEEE, 2010)

Las potencias mundiales tomaron conciencia de esta amenaza luego de los ataques contra Estonia, que tuvieron gran trascendencia mundial en la primavera de 2007, estos ataques fueron considerados como el primer caso de operaciones cibernéticas que afectaron de manera clara, drástica y global a la seguridad de un Estado⁶.

En este contexto, para mayo de 2010, el Presidente Barak Obama aprueba la Estrategia Nacional de Seguridad de Estados Unidos, en la cual ya se considera el ciberespacio (secure cyberspace) en el que se afirma:

Las amenazas a la ciberseguridad representan uno de los retos más graves relacionados con la seguridad nacional, la seguridad pública y la economía a los que se enfrenta la nación [...] Nuestra vida diaria depende de la energía y de las redes eléctricas, pero adversarios potenciales podrían usar nuestras ciber-vulnerabilidades para interrumpir el suministro a

4 Empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

5 HOSTING, lo define como una forma de identificación que está asociada a un grupo de computadoras conectadas a internet. El propósito de los ciber – dominio es traducir una dirección IP (Es una etiqueta numérica que identifica, de manera lógica y jerárquica a un interfaz).

6 El 27 de abril del año 2007, las páginas de los bancos no funcionaban, no era posible sacar dinero de los ATM, las transacciones virtuales eran denegadas, los servidores de las páginas web del gobierno estaban colapsadas. Se había lanzado un ataque cibernético a Estonia. Fuente: <https://www.bocataidigital.es/ataque-informatico-estonia/>



Manejo de información a través de sistemas satelitales.
Fuente: Archivo fotográfico OPSIC - Ejército Ecuatoriano.

escala masiva. [...] Las amenazas a las que nos enfrentamos van desde hackers individuales a grupos de delincuencia organizada, desde redes terroristas a avanzados estados-nación» [...] La infraestructura digital es un recurso nacional estratégico y su protección una prioridad de la seguridad nacional. [...] Disuadiremos, prevendremos, detectaremos, nos defenderemos contra y nos recobramos rápidamente de las ciberintrusiones y ataques: Invirtiendo tanto en personal (campaña nacional de concienciación sobre ciberseguridad) como en tecnología para mejorar la protección y aumentar la “resiliencia” de los sistemas y redes gubernamentales y empresariales.

El principal aporte de la ciberdefensa a la seguridad de los Estados, ha sido la implementación de estrategias de seguridad y protección de infraestructura crítica, que entre otros aspectos consideran:

- La formación de personal especialista que realice los análisis de riesgos pertinentes, supervisar la implantación de las medidas mediante auditorias, adquirir tecnología o contratar servicios especializados.
- Para garantizar el nivel de seguridad adecuado en los sistemas de las instituciones públicas es necesario actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.
- El personal de las instituciones públicas recibirá la

formación necesaria para garantizar el conocimiento de las medidas de seguridad a implementar.

- Las Fuerzas Armadas de un Estado tienen una importancia significativa en la implementación de la ciberdefensa.

Considerando las Fuerzas Armadas y su importancia en la ciberdefensa de un Estado, recordamos a dos grandes pensadores militares, Sun Tzu (600 años a.C.) decía en su obra *El arte de la guerra*: “Cien victorias en cien batallas no es lo ideal. Lo ideal es someter al enemigo sin luchar”, por otra parte, Clausewitz pensaba que “La Guerra es un acto de fuerza para doblegar la voluntad del enemigo”. Podría deducirse que la ciberguerra aún a los dos pensamientos de estos grandes estrategas, ya que, produciendo una parálisis estratégica, se puede doblegar la voluntad del enemigo sin aplicación de la fuerza física⁷.

El ciberespacio es una nueva dimensión en la que se pueden materializar conflictos y guerras, que no tiene límites ni fronteras y que, sorpresivamente, parece no tener restricciones ni leyes, al menos efectivas. Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar y aire, a través del ciberespacio. (IEEE, 2010)

⁷ «Cyber Wars: A Paradigm Shift from Means to Ends». Autor: Amit Sharma, del Institute for System Studies and Analysis» del Ministerio de Defensa de la India.



Transmisión de información en tiempo real.
Fuente: Archivo fotográfico OPSIC - Ejército Ecuatoriano.

Las TICs se encuentran presentes en todas las actividades que realizan las Fuerzas Armadas, apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real, entre muchas otras. Esto hace que las Fuerzas Armadas pueden ser parte de un ataque cibernético que las volvería vulnerables a Fuerzas Armadas de otros Estados.

La ciberdefensa permitirá a las Fuerzas Armadas mantener seguros sus sistemas de mando y control, sistemas de información y telecomunicaciones mediante la implementación de estrategias que les permitan planear, dirigir y coordinar las actividades en materia de seguridad de la información.

3. Conclusiones

Si bien la responsabilidad de la seguridad nacional, ahora en el contexto del ciber espacio, es una realidad clave para mantener la gobernabilidad de una nación, también lo es la exigencia del desarrollo de una nueva competencia genérica en los individuos que permita comprender los riesgos y amenazas propias del nuevo ecosistema donde viven, y motivar actitudes positivas

frente al tratamiento de la información, no por castigo o recompensas sino por convicción, sabiendo que sus acciones efectivas en el aseguramiento de la información, serán trascendentes en otros. (CANO, 2015).

El ciberespacio es el nuevo campo de batalla donde se planifican, dirigen y ejecutan operaciones militares, (tierra, mar, aire, espacio y ciberespacio) en las cuales las acciones ofensivas son eficaces, eficientes y de bajo riesgo para el atacante por lo que las Fuerzas Armadas y el Estado deben disponer de las capacidades necesarias para proteger los intereses propios y responder de manera oportuna y legítima ante un ciberataque⁸.

La vertiginosa evolución de las tecnologías informáticas y de comunicación (TICs) y su impacto en la guerra requieren de una atención adecuada por parte del Estado a través de sus gobiernos, políticos, FF.AA, técnicos, empresarios y la universidad en general. En el mundo globalizado e interconectado de hoy, estudiosos militares consideran al ciberespacio como una nueva dimensión de la guerra, donde la información es usada como arma y objetivo a la vez, en contra de

⁸ Presentación: Ciberseguridad en España: Perspectiva del Mando Conjunto de Ciberdefensa, GD. Carlos Gómez López de Medina, 2015.

la infraestructura crítica o el robo de información clasificada que vulnera los sistemas de seguridad y defensa de los Estados, siendo necesario desarrollar capacidades de Ciberdefensa para contrarrestar este tipo de amenazas.

La amenaza cibernética no sólo puede afectar al normal desenvolvimiento de la vida de los ciudadanos de un país, sino que puede afectar a la infraestructura

crítica nacional conllevando riesgos de daños físicos para la población.

Todo Estado tiene el derecho y la obligación de establecer estrategias de defensa nacional y a disponer de ciber armamento⁹, para poder hacer frente, con los mismos medios, a aquellos que quieren perjudicar sus legítimos intereses. (IEEE, 2010)

9 Ciber arma es cualquier software diseñado para atacar. Instrumento, medio o dispositivo útil para operar en el ciberespacio, destinado a atacar o defenderse en el mismo. Fuente: <https://prezi.com/cghzod-r-w01/ciber-armas/>

REFERENCIAS

- [1] BEJARANO, M. J. (2013). La nueva dimensión de la amenaza global: la amenaza cibernética. Instituto Español de Estudios Estratégicos, 2-4.
- [2] CANO, J. (2015). Seguridad y control en el 2020. Reflexiones sobre el futuro. Asociación Colombiana de Ingenieros de Sistemas.
- [3] GAITÁN, A. (2012). El Ciberespacio: UN NUEVO TEATRO DE BATALLA PARA LOS CONFLICTOS ARMADOS DEL SIGLO XXI. Fuerzas Militares, Colombia.
- [4] IEEE. (2010). Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia, 73-74.
- [5] MINISTERIO COORDINADOR DE SEGURIDAD. (2014). PLAN NACIONAL DE SEGURIDAD INTEGRAL . QUITO: EL TELÉGRAFO.
- [6] SAMPER, E. (2015). Ciberdefensa en Colombia. Revista de Defensa de Colombia.
- [7] VELÁSQUEZ, A. S. (2007). LA SEGURIDAD INTERNACIONAL: VINO VIEJO EN BOTELLAS NUEVAS. REVISTA DE CIENCIA POLÍTICA, 82-83-84.