Una visión estratégica militar del ciberespacio

Capitán de navío Enrique Arnáez Braschi
Graduado de la Escuela Naval como alférez de fragata el 17 de diciembre de 1990. Calificado en Guerra de Superficie, Armas de Superficie y Misiles. Es graduado del Curso Básico de Estado Mayor, del Curso de Comando y Estado Mayor, del Curso de Alto Mando Naval en la Escuela Superior de Guerra Naval, de los Cursos de Preposicionamiento de Fuerzas Marítimas, Liderazgo y Proceso de Planeamiento Rápido en el Centro de Entrenamiento de las Fuerzas Expedicionarias del Atlántico de la Marina de Estados Unidos, y del Curso de Planeamiento para la Defensa en el Centro de Estudios Estratégicos Hemisféricos de Defensa Centro Perry de la Universidad de Defensa de Estados Unidos. Magíster en Ingeniería de Control y Automatización de la Pontificia Universidad Católica del Perú y en Política Marítima de la Escuela Superior de Guerra Naval. Fue dotación del BAP *Villavicencio* y el BAP *Almirante Grau*, en las áreas de Armamento, Misiles, Control de Tiro, Artillería, Guerra Electrónica y Radares. Asimismo, fue segundo comandante del BAP *Santillana*, y comandante del BAP *Larrea* y del BAP *Quiñones*. Fue dotación del Batallón Ligero de Infantería de Marina N.º 7 en el frente Ucayali. Ha prestado servicios en la Escuela Naval del Perú, en la Dirección General del Personal de la Marina, en la Comandancia General de Operaciones del Pacífico, en el Estado Mayor General de la Marina y en la Secretaría de la Comandancia General de la Marina como subsecretario del comandante general. Del mismo modo, ha prestado servicios como oficial enlace ante la Comandancia de las Fuerzas de las Flotas de la Marina de Estados Unidos, y como asesor del presidente del Consejo de Delegados de la Junta Interamericana de Defensa en Washington D.C. El 2 de agosto de 2018 asumió el cargo de comandante de Ciberdefensa de la Marina.



RESUMEN
En este artículo se describen conceptos relacionados al dominio del ciberespacio tales como Ciberseguridad y Ciberdefensa, y se muestran las amenazas y los tipos de operaciones que se realizan en él.

PALABRAS CLAVE
Ciberespacio, Ciberseguridad, Ciberdefensa, *hacker*.

ABSTRACT
This article depicts concepts related to Cyber Space Domain, like Cyber Security and Cyber Defense, likewise threats and kinds of operations that are carried out are shown.

KEYWORDS
Cyber Space, Cyber Security, Cyber Defense, hacker.

Para entrar en el tema, debemos reconocer que a los dominios tradicionales, tierra, mar, aire y espacio, está incorporándose, según varios autores, un quinto dominio: el ciberespacio. Este tema es el que abordaremos en el presente artículo, con la finalidad de llegar a aclarar si la definición se halla orientada correctamente.

Situación actual y algunos antecedentes

Cuando hablamos del ciberespacio, popularmente nos referimos a lo que ocurre dentro de las computadoras o al Internet y su conectividad. Sin embargo, estos son solo algunos de sus elementos que han facilitado muchos aspectos de nuestra vida, a través del comercio electrónico, la banca electrónica, las comunicaciones como las videoconferencias y la cantidad inmesurable que

• Artículo recibido el 12 de octubre de 2018, aprobado para su publicación el 18 de octubre de 2018

tenemos de información al alcance de nuestras manos. Pese a ello, creo que lo más perceptible son las redes sociales.

Habitualmente evitamos creer que existen riesgos y amenazas en el ciberespacio. Creemos que con un antivirus y un *firewall* ya estamos protegidos, pero estamos muy equivocados.

Para evidenciar el peligro que corremos, como la información inexacta, manipuladora y hasta mal intencionada colocada en Internet al alcance de todos, mencionaremos algunos ejemplos concretos de los últimos meses en Latinoamérica:

- Ataque a la red de bancos en agosto de 2018 en el Perú, mediante métodos de denegación de servicios. Ello implicó miles de solicitudes a todos los servicios de la web del banco y desbordó su capacidad. Los clientes no pudieron usarla. Se usó el *ransomware*, un tipo de *malware* que encripta la información para luego cobrar rescate. En el futuro sabremos las dimensiones de sus consecuencias.
- En mayo de ese año, fue hackeado el Banco de México. El robo alcanzó un monto mayor a los 400 millones de pesos mexicanos.



- En junio, hackearon el Banco de Chile. El robo llegó a los US$ 10 millones.
- En julio, hackearon el Banco de Chile y robaron los datos de todas las tarjetas de crédito.

Ahora veremos otros sucesos de impacto mucho mayor, por su forma o vector de ataque o por sus consecuencias:

- El 27 de abril del 2007, se produjo el ciberataque más grande en la historia. El Congreso, bancos, ministerios, la prensa y los ciudadanos de Estonia fueron el blanco de un ataque de denegación de servicios. En otras palabras, no podían emplear ninguna de sus páginas web y sus aplicativos *on-line* fueron saturados y desbordados por solicitudes orquestadas. Se acusa a Rusia del ataque, pero no existen evidencias.
- En 2012, se comprobó el hackeo en una planta nuclear de Irán, que buscaba la pérdida de control de las centrífugas, lo que implicaría dañar el proceso de enriquecimiento del uranio. Los rumores incluían la posibilidad de una castástrofe de grandes dimensiones, pero solamente bucaban sacar de servicio a las centrífugas por daños permanentes.
- En 2017, un *hacker* robó 10 GB de información confidencial de un casino en Estados Unidos, al que ingresaron por un sensor (IoT, Internet de las cosas) de una pecera conectada a la red interna.
- Ese mismo año, se produjo un ataque de escala global del *ransomware* WannaCry, que encriptó la información de los computadoras infectadas y solicitó un pago a modo de rescate para liberar la información. Fueron afectados cerca de un cuarto de millón de computadoras de más de 150 países. Las consecuencias fueron pérdidas millonarias por la paralización de las operaciones de las empresas atacadas.
- Otra modalidad evidenciada sucede hace varios años con el grupo armado Estado Islámico o ISIS, que recluta personas mediante el análisis del comportamiento y seducción a través de juegos *on-line*. Del mismo modo, gestiona o consigue su financiamiento mediante el Internet, y sus dimensiones ocultas denominadas Dark Net y Deep Web.

Explicada la situación y denunciadas las amenazas, deseo plantear ciertas interrogantes que orientarán esta exposición de ideas.

¿Qué es la Ciberseguridad?

La ciberseguridad tiene dos tipos de interpretaciones. La primera, de característica escolástica, se refiere a la percepción de sentirse libre de riesgo o peligros en el ciberespacio, y está vinculada a la seguridad en términos de bienestar de las personas. Sin embargo, la interpretación más común de la ciberseguridad se refiere a la protección de las redes, los activos informáticos propios o de la empresa a la que se pertenece, es decir, la protección de redes.

Los dos casos pueden ser empleados según el escenario en el cual nos desenvolvemos. A nivel político o estratégico, con los términos de la percepción de libertad de peligros. Y en un ambiente local o táctico, desde el punto de vista de protección de la información y de los activos informáticos.

¿Qué es la ciberdefensa?

La ciberdefensa se deriva de la ciberseguridad, referida a su vez a la percepción. La ciberdefensa es el conjunto de capacidades necesarias para asegurar la continuidad en el empleo del ciberespacio, inclusive a pesar de estar siendo atacado.

En este campo, podemos clasificar tres tipos de operaciones.
La primera, de carácter permanente, se denomina *operaciones de defensa* y se encarga de proteger la integridad y fidelidad de la información digital contenida en nuestros activos informáticos, así como el correcto empleo de sus herramientas



y aplicativos. En este tipo de operaciones se encuentra la concientización del personal en emplear el ciberespacio, ya que es el blanco más fácil a través de quienes se busca vulnerar y penetrar una red. También consideran las pruebas de vulnerabilidad que se aplican a todos los activos informáticos, incluso los que se encuentran en las unidades de combate, como aviones, buques, vehículos y todos los equipos que emplean, hasta en forma aislada, al ciberespacio.

La segunda se denomina *operaciones de explotación* y comprende el empleo de las capacidades de buscar, investigar y recolectar información útil en el ciberespacio respecto a datos de interés sobre vulnerabilidades propias, amenazas, potenciales adversarios como criminales y hasta extremos como el terrorismo y el narcotráfico. Las áreas de explotación comprenden el Internet, las redes sociales, la media y las redes ocultas como las mencionadas Deep y Dark Web.

Por último, el tercer tipo de operación corresponde a las *operaciones de respuesta*. En ellas se procura penetrar redes o sistemas informáticos de las amenazas de manera deliberada, siempre con las autorizaciones de las respectivas autoridades, con la finalidad de controlar sus activos, degradarlos o, en todo caso, neutralizarlos.

Estas operaciones, que son realizadas en tiempo real y conducidas bajo los esquemas de operaciones militares, son acompañadas por gestiones de investigación y desarrollo tanto de nuevas técnicas como del *malware* que emplea la amenaza, con la finalidad de comprender y aprender su comportamiento, y, si es necesario, convertirlo en un arma propia mejorada. Esto se consigue con métodos de análisis forense e ingeniería reversa.

¿Qué es y cómo está conformado el Ciberespacio?

El ciberespacio es real y va más allá de la conectividad y del Internet. Debemos ser conscientes de que un *smartphone* con sus aplicativos y su inmersión en Internet es parte componente de él y nosotros, las personas, somos los interactuantes.

Hay varios conceptos técnicos que definen una serie de capas del ciberespacio. Sin embargo, podemos emplear tres elementos para una clasificación más sencilla: la información, las redes informáticas (*hardware y software*) y las personas o usuarios.



El ciberespacio es el ambiente dentro de las redes, donde existe información que es empleada por personas y por otras máquinas, como computadoras, terminales o sensores conocidos como parte del IoT y su evolución a IoE (Internet of Everything) para sus propios intereses.

¿Resulta necesario conducir operaciones militares en el Ciberespacio?

Dado que el ciberespacio es un ambiente independiente por su característica digital, y que a la vez está vinculado con la realidad a través de sensores y actuadores, es factible realizar operaciones que tengan un resultado dentro del mismo ciberespacio y hasta fuera de él, tal como lo vimos en los ataques con consecuencias físicas citados al inicio de este artículo.

Podemos razonar lógicamente de la siguiente manera: si es factible realizar operaciones, entonces algunas de ellas pueden tener características militares.

¿Es necesario realizar operaciones militares? Sí, siempre y cuando esté comprometida la seguridad digital que comprometa a la seguridad nacional.

Uno de los mandatos principales de las Fuerzas Armadas a nivel mundial es defender la soberanía de su país. Si sabemos que la soberanía se refiere a la

capacidad de un Estado de ejercer el control con responsabilidad y autoridad sobre su territorio y nación, la pérdida de la soberanía se traduciría en el descontrol de su territorio o nación, es decir, la pérdida de su propiedad.

A modo de comparación, digamos que, si nosotros, como personas, somos dueños y propietarios de nuestra información digital y de nuestros activos informáticos, debemos estar en condiciones de controlarlos y protegerlos, porque a nadie le gusta el robo de información o el empleo de sus propias cosas sin su respectiva autorización (*webcams*, impresoras, televisores y otros artefactos). De lo contrario, no son nuestros de manera soberana y es necesario defenderlos. A escala del Estado sucede lo mismo. Por lo tanto, se tienen que realizar operaciones militares para defender nuestros intereses soberanos, incluso en el ciberespacio.

¿Es realmente un Quinto Dominio?

Para esta definición debemos tener en cuenta que los dominios actuales (tierra, mar, aire y espacio) son ámbitos que responden a las aplicaciones del arte operacional de la guerra y sus respectivos factores de tiempo, espacio y fuerza, así como a las funciones, que son comando y control, inteligencia, información, fuego, movimiento y maniobra, protección y sostenimiento.

Las velocidades actuales del empleo del ciberespacio vinculan a los factores tiempo y espacio en un solo factor tiempo-espacio fusionado, porque es posible atacar al otro lado del mundo con la velocidad de un clic.

En el futuro se podrá dividir nuevamente a estos dos factores, debido a la relatividad del espacio-tiempo definida por el doctor Albert Einstein en su teoría de la relatividad. Fuera de esta aclaración, todos los factores y funciones de la guerra se cumplen en el ciberespacio.

Este tema, durante el IV Simposio Internacional de Defensa y Seguridad, organizado por la Marina de Guerra del Perú en agosto de 2018, me llevó a una discusión extremadamente agradable con colegas en temas estratégicos de guerra y ciberespacio, como el doctor Geoffrey Till, el doctor Milan Vego, el capitán USN (r) Alfred Turner y el coronel USAF David Schilling, a quienes agradezco su predisposición. Sus puntos de vista ampliaban estas aproximaciones sobre la correcta definición del nuevo dominio asignado al ciberespacio, donde



existe la necesidad, como mencionó el doctor Till, del "comando y control del ciberespacio para el uso seguro y libre por todos".

La excepción fue el doctor Vego, quien fundamentó que el ciberespacio es un tema de exclusiva tecnología e información, y que no responde específicamente a aspectos de doctrina. Su trato como dominio recomendó que sea reflexionado de manera más profunda o menos ligera.

En mi opinión, vistas las descripciones fundamentadas en los párrafos precedentes, al poder emplearse para realizar operaciones militares y ataques con posibles consecuencias físicas, el ciberespacio debe ser tratado en el planeamiento militar como el quinto dominio que permite proteger nuestras redes de manera complementaria al resto de dominios, pero que es exclusivo para la ejecución de ataques en la defensa de los intereses y de la soberanía de los Estados.

Para finalizar, es conveniente resaltar que la velocidad de los ataques, los enormes daños que producen y la rápida evolución de estas amenazas son un desafío que se agrava por la ilegalidad de los atacantes y la falta de fronteras, como consecuencia de la carencia de legislación para ellos. La única forma de hacer frente a las amenazas transnacionales en el ciberespacio se puede conseguir con éxito mediante claros criterios de cooperación y colaboración internacional, intersectorial e interagencial, lo que compromete tanto a actores públicos como a privados.

Por lo tanto, mientras estamos en un periodo donde las normas aún no están claras y sabiendo que es necesario contar con el empleo seguro y libre del ciberespacio, es conveniente tratarlo como un quinto dominio. Debemos asignarle el comando y control correspondiente para tal fin, con el objetivo de realizar operaciones militares que defiendan los intereses y la soberanía del Estado en el ciberespacio, optimizando las operaciones con alianzas y coaliciones entre todos los actores involucrados, y enarbolando los principios de colaboración y cooperación.



