OPERACIONES CIBERNÉTICAS

Su naturaleza, propósito y conducción

PALABRAS CLAVE: **REVOLUCIÓN TECNOLÓGICA / GUERRA CIBERNÉTICA / DEFENSA CIBERNÉTICA / OPERACIONES DE INFORMACIÓN / OPERACIONES CIBERNÉTICAS**

Por **Gustavo Adolfo Trama**

La convergencia tecnológica de las redes de computadoras y de telecomunicaciones; los sorprendentes adelantos en tecnología óptica, alámbrica e inalámbrica; la proliferación a nivel mundial de nuevas tecnologías de las comunicaciones y de la información (TIC) y su consiguiente efecto en las redes sociales y en la sociedad han cambiado radicalmente el ambiente operacional.

La diversa y amplia cantidad de agentes que utilizan o explotan esta revolución tecnológica plantean una grave amenaza a la infraestructura crítica de los estados y las misiones operacionales pues los efectos de ataques cibernéticos sobre objetivos civiles podrían llegar a ser tan desastrosos que requerirían la ayuda de las tropas que, en caso de guerra, serán sustraídas del frente convencional.

Estos agentes abarcan desde los estados-nación tradicionales hasta los no combatientes, las empresas transnacionales, las organizaciones criminales, los terroristas, los hackers sindicalizados y los hackers independientes y los inconscientes que no tienen una intención maliciosa pero que pueden llegar a causar daños. Colectivamente se combinan para crear un estado de perpetua turbulencia sin estados finales tradicionales o resolución de los conflictos.

Esto, que hasta hace poco parecía ser un asunto de película de ficción, ya ha dejado de serlo. La guerra cibernética o guerra "por control remoto" no es novedosa, pero es una estrategia que ha irrumpido en los nuevos escenarios de conflicto, pues permite ser accionada a distancia. Incorpora nuevas tecnologías y las fuerzas que son necesarias desplegar dejan pocos rastros de su presencia. Ello habilita a quienes deben tomar decisiones de carácter estratégico a aprobar la ejecución de operaciones que difícilmente autorizarían si se emplearan en su lugar medios convencionales. Lanzar un ciberataque seguramente podría ser más barato y rentable que ejecutar un ataque físico.

Hasta no hace mucho tiempo atrás, y en algunos países aún lo siguen siendo, las operaciones cibernéticas y las operaciones con fuerzas especiales eran consideradas como complementarias a las tradicionales y, por lo tanto, tomadas en consideración después de que se formulan los planes esquemáticos. Sin embargo, en el caso de la guerra entre Rusia y Georgia en 2008 y entre Rusia y Ucrania en 2014, las fuerzas convencionales fueron dejadas como operación complementaria en un papel disuasorio y como parte de un plan de engaño, en tanto que las operaciones cibernéticas y las fuerzas especiales tuvieron la prioridad de las operaciones militares.

Esto pareciera indicar que el vocabulario actual, que incluye términos tales como operaciones en red de computadoras (CNO), guerra electrónica (EW), y operaciones de información (IO) de manera separada, estaría un tanto desactualizado.

La realidad indica que hay tres dimensiones interrelacionadas de operaciones en el espectro del conflicto de paz a guerra, cada una con su propio conjunto de lógica causal y que requiere un desarrollo de soluciones diferentes.

La primera dimensión es el enfrentamiento psicológico de voluntades enfrentadas. La segunda dimensión es el compromiso estratégico, que consiste en crear y mantener aliados y generar apoyo o empatía para la misión y la tercera dimensión es la competencia tecnológica cibernética que implica ganar, mantener y explotar una ventaja tecnológica.

La primera y segunda dimensión se centran en cómo los comandantes y el personal orquestan y aprovechan el poder de la información para lograr sus misiones. La tercera dimensión se centra en ganar y mantener una ventaja en los medios convergentes del ciberespacio y el espectro electromagnético (EMS). Se necesitan conceptos y capacidades diferentes para cada una de estas dimensiones.

Las operaciones de información abarcan estas tres dimensiones, pero es un término cada vez más sobrecargado que se refiere a cualquier uso de la información.

En un principio, existía la aviación en el Ejército y en la Armada, hasta que se conformó la Fuerza Aérea como ámbito independiente. No obstante, las fuerzas terrestres y navales continuaron manteniendo elementos aéreos necesarios en apoyo directo para cumplir las misiones de su ambiente específico. El poder aéreo no cambió la naturaleza de la guerra, ni su propósito, pero sí la forma en que fue conducida.

Actualmente no existen teóricos militares especializados en guerra cibernética, como en su momento fueron Alfred Thayer Mahan, Giulio Douhet y B.H. Liddell Hart que razonaron, respectivamente, sobre los dominios marítimo, aéreo y terrestre, generando marcos, modelos y principios para la guerra. En la actualidad, estas teorías ayudan a los estrategas y planificadores a pensar, planificar y generar las fuerzas de combate conjuntas, pero no existe ninguna teoría militar estándar para las operaciones en el espacio cibernético, aunque la teoría militar es un componente primario del arte operacional.

La doctrina militar actual analiza las experiencias y teorías de la guerra cinética entre los estados - nación en espacios de batalla que existen casi exclusivamente en una zona

La diversa y amplia cantidad de agentes que utilizan o explotan esta revolución tecnológica plantean una grave amenaza a la infraestructura crítica de los estados y las misiones operacionales.

físicamente reconocible y comprensible (aire, tierra, mar y espacio) pero, contrariamente a ello, la guerra cibernética ocurre en un ámbito ubicado simultáneamente en capas lógicas, físicas y de las personas que cruzan actividades en el espacio electromagnético, a través o en relación con él, el cual atraviesa ininterrumpidamente otros ámbitos al igual que fronteras geográficas y políticamente reconocidas.

A pesar de este panorama incierto, no solo se puede afirmar que la guerra cibernética es como dijeron los pensadores militares desde hace mucho tiempo: “no hay guerra parecida a la anterior”, sino que se pueden extraer algunas conclusiones.

La guerra cibernética difiere fundamentalmente del conflicto armado tradicional pues a diferencia de la conducción de la guerra en el pasado, los oponentes pueden librarla de manera rápida, económica, anónima y devastadora, desde lugares apartados del globo. Puede decirse entonces que las operaciones cibernéticas tienen una naturaleza diferente.

Con la conectividad global del espacio cibernético, no es necesario que un enemigo se encuentre próximo físicamente

para planear y ejecutar una amenaza. Si los hackers pueden acceder a un sistema y obtener el control de funciones del teclado, pueden ocultar los éxitos, eludir las defensas y dejar abiertas las puertas para volver a entrar en el futuro. Si pueden allanarse los caminos para decidir la oportunidad más conveniente, las operaciones cibernéticas pueden tener un propósito diferente.

"Hoy en día, los mapas no pueden describir un campo de batalla en el cual el enemigo puede subir un video para una audiencia de millones de personas desde cualquier casa en cualquier suburbio"[1].

En un mundo global y digitalizado, la revolución tecnológica ofrece grandes ventajas, pero también importantes riesgos que deben ser acometidos con eficacia para evitar daños económicos y problemas de seguridad y defensa. Permanentemente ocurren hechos nuevos como el ciberataque global de ransomware que afectó, el 12 de mayo de 2017, a empresas privadas y entes estatales de casi un centenar de países. Si se trató de operaciones en red, las operaciones cibernéticas requieren una forma diferente de ser conducidas.

Este caso no es el primero y seguramente no será el último de estas características. Dado el rango de posibles amenazas y el ritmo al que pueden aparecer, se hace imposible preservar todo, en todas partes, todo el tiempo, pero al menos debe ser posible asegurarse de que los recursos más valiosos estén debidamente protegidos.

De manera similar a lo que sucede en otros dominios, como el aire y el mar, en el espacio cibernético no es posible defender todo; se debe defender lo que es relevante. "El que pretenda defenderlo todo termina por no defender nada"[2].

No puede esperarse que las entidades comerciales y privadas se defiendan en el ciberespacio de los ataques de gobiernos extranjeros o grupos paraestatales pues no tienen la capacidad, la habilidad, ni la autoridad para responder de una manera que sea plenamente eficaz. Tampoco que lo puedan hacer las fuerzas armadas por un lado y las de seguridad y policiales por otro. Si bien el intercambio de información y la colaboración no son un fin, son un medio para alcanzar una mejor seguridad y defensa nacional cibernética.

La velocidad con que se suceden los hechos hace que los individuos y las organizaciones se vean forzados a tomar decisiones apresuradas y poco eficaces debido, generalmente, a una mayor dependencia en supuestos no probados. Por ello, es que resulta imperioso contar con mecanismos y herramientas que permitan identificar y afrontar correctamente estos supuestos para mejorar los procesos de toma de decisiones y poder, de forma exitosa, defender, atacar, y adaptarse en el campo de batalla cibernético.

Al estar involucrado no solo el estado, sino también toda la Nación, a nuestro entender, fundamentalmente se debería comenzar por analizar cómo el gobierno y el sector privado se relacionarán el uno con el otro para defenderse de agresiones, amenazas, riesgos y peligros en el ciberespacio y explicitar autoridades, reglas claramente definidas e incluir la identificación de las áreas donde habrá una superposición de responsabilidades y definiendo líneas de acción precisas y las tareas de cada uno de los involucrados, de manera de "poder brindar a las personas un nivel de seguridad que les permita el normal desarrollo de sus actividades personales, sociales y comunitarias en el ciberespacio, junto con el ejercicio de derechos fundamentales como la libertad de expresión, el acceso a la información, la protección de la vida privada y la propiedad"[3].

Todo ello tendría que concretarse en una política o estrategia nacional de seguridad y defensa cibernética.

En dicho documento debería quedar plasmada la manera de trabajar entre agencias estatales, no estatales, gubernamentales, no gubernamentales, en un ambiente de coo-

La guerra cibernética o guerra "por control remoto" no es novedosa, pero es una estrategia que ha irrumpido en los nuevos escenarios de conflicto.

1. McChrystal, Stanley, Gral. US. Army, (Ret.) Teams of Teams: New Rules of Engagement for a Complex World, Portfolio/Penguin, 2015; P. 25
2. Apotegma atribuido a Federico el Grande. Citado por Ferdinand Foch en su Libro "Los principios de la guerra".
3. Gobierno de Chile; Política Nacional de Ciberseguridad 2017 - 2022; Disponible en: www.ciberseguridad.gob.cl

Hay tres dimensiones interrelacionadas de operaciones en el espectro del conflicto de paz a guerra, cada una con su propio conjunto de lógica causal y que requiere un desarrollo de soluciones diferentes.

peración para enfrentar las amenazas a la nación en el espacio cibernético. Al igual que las fuerzas armadas argentinas luego del conflicto del Atlántico Sur han aprendido a entrenar, ejercitar, funcionar y operar en un entorno conjunto, también hoy en la República Argentina los sectores público y privado, las universidades, las fuerzas de seguridad y las fuerzas armadas, deberían entrenar, ejercitar y operar de manera cooperativa en el ciberespacio.

En el campo militar se requerirá desarrollar una comprensión común de la forma en que los avances tecnológicos transforman el entorno operacional, de la manera en que los líderes deben pensar en las operaciones en el ciberespacio y del modo en que se deben integrar con las operaciones tradicionales para, de esa manera, poder determinar cuáles son las capacidades cibernéticas necesarias.

El espacio cibernético permite llevar a cabo múltiples operaciones: buscar el engaño, la disuasión, la interferencia de sistemas de comando y control, el empleo de drones, confundir sistemas de información militar y/o civil, anular servidores para que no puedan emplearse determinadas computadoras y redes, causar eventos o fenómenos naturales que obliguen al oponente a distraer tropas, confundir sistemas logísticos gobernados por computadoras, descriptar códigos criptográficos, interferir el tráfico aéreo, los sistemas de distribución eléctrica o de salud, alterar sistemas bancarios, difundir propaganda o conducir operaciones de acción psicológica y generar percepciones erróneas en la mente del oponente. La lista es muy extensa y no finaliza aquí, pero principalmente se debe tener en cuenta que inadvertidamente puede causarse un efecto cascada no deseado y difícil de revertir que puede afectar a los sistemas propios. Es decir, causarse daños a uno mismo.

Frente a ello, surgen una serie de interrogantes tales como: ¿de qué manera las operaciones cibernéticas influyen en las operaciones militares?, ¿son de aplicación los principios de la guerra cinética a la guerra cibernética?, ¿cómo influyen en el nivel operacional y táctico las decisiones cibernéticas de los niveles superiores de dirección estratégica?, ¿cuáles deberían ser las coordinaciones con otros elementos del estado nacional involucrados en el uso de la informática y las telecomunicaciones, que pueden requerir posteriormente el empleo del componente armado del poder nacional?, ¿cómo pueden emplearse los medios cibernéticos en el nivel operacional tanto en lo que hace al planeamiento como a la ejecución de las operaciones?, ¿qué consideraciones debieran tenerse en cuenta para la ejecución de las operaciones cibernéticas ofensivas?, ¿qué debería contener el Anexo de Operaciones Cibernéticas del Plan de Campaña de un Teatro de Operaciones?, ¿cómo pueden las fuerzas conjuntas integrar las operaciones en el espacio cibernético para apoyar a las operaciones conjuntas?, ¿cuál debería ser el rol que debiera jugar el Comando Conjunto de Ciberdefensa?, ¿cuáles deberían ser los de cada uno de los Comandos de Componente en la guerra cibernética?, ¿cómo podrá un comandante de un Teatro de Operaciones incorporar las actividades cibernéticas al planeamiento de una campaña y conocer qué requerir de ellas en la ejecución de operaciones militares bajo su responsabilidad?

Finalmente, y no por ello menos importante: ¿qué conocimientos debería tener un oficial del cuerpo de comando no especializado en informática para comprender el ciberespacio e integrar las operaciones cibernéticas dentro del amplio espectro de las operaciones militares y participar en el desarrollo y evaluación de doctrinas, planes, programas y proyectos de ciberseguridad y ciberdefensa?

La guerra cibernética es relativamente nueva, por lo que muchos de sus parámetros e implicancias esperan ser aun descubiertos. Tan nueva es que la Armada de los Estados Unidos está investigando la posibilidad de un ciberataque en la colisión de dos de sus buques, el USS Fitzgerald, el 17 de junio y el USS John S McCain el 21 de agosto, ambos de 2017, donde murieron 7 y 10 tripulantes respectivamente.

Esto significa que sólo una larga discusión y el debate pueden iniciar el proceso de identificación de los principios, acciones y consecuencias más importantes de la guerra cibernética. Cuanto antes empiecen los expertos, mejor.

Gustavo Adolfo Trama
Contraalmirante en situación de retiro. Oficial del Estado Mayor de la Armada Argentina. Magíster en Relaciones Internacionales por la Universidad de Belgrano y Master in Arts (Management) por la Universidad Salve Regina, Newport, Rhode Island, Estados Unidos. Autor de diversas publicaciones, entre ellas, "Reglas de Empeñamiento", tomos 1, 2 y 3, editados por la Escuela Superior de Guerra Conjunta. Actualmente se desempeña como profesor asesor en el área de Ejercicios de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

〉 ARTÍCULO CON REFERATO