Escenarios Actuales

Seminario
"Ciberespacio: desafíos a la seguridad y defensa de Chile en el siglo XXI"

Centro de Estudios e Investigaciones Militares
Ejército de Chile

Año 23, N° 4, diciembre, 2018
ISSN 0717-6805

El Centro de Estudios e Investigaciones Militares (CESIM) fue creado el 12 de diciembre de 1994, con el objeto de contribuir en materias relacionadas con las ciencias militares a diferentes organismos del Ejército. Asimismo, aportar al intercambio de ideas y desarrollar diversas actividades de investigación y extensión académica en las áreas de seguridad y defensa, manteniendo para ello una activa relación con la comunidad académica nacional e internacional.

The Military Studies and Research Center (CESIM) was created on December 12, 1994 in order to help different bodies of the Chilean Army in matters related to military science. It also contributes to exchange ideas and develop research and academic extension in the areas of security and defense. To fulfill its tasks the Center maintains an active relationship with the national and international academic community.

"Escenarios Actuales" es editada y difundida gratuitamente por el Centro de Estudios e Investigaciones Militares. Las ideas vertidas en los artículos son de exclusiva responsabilidad de los autores y no representan necesariamente el pensamiento, doctrina o posición oficial del CESIM o del Ejército de Chile.

"Escenarios Actuales" is a free publication of The Military Studies and Research Center (CESIM). The ideas expressed in the articles are those of the authors and do not necessarily represent the thought, doctrine or official position of CESIM or the Chilean Army.

La revista está indexada en las siguientes bases de datos:

Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal **(LATINDEX)**, http://www.latindex.org.
De Citas Latinoamericanas en Ciencias Sociales y Humanidades **(CLASE)**, de la Universidad Nacional Autónoma de México, http://clase.unam.mx.

The journal is indexed to the following data base:

*On-line Regional Information System for Scientific Journals of Latin America, the Caribbean, Spain and Portugal **(LATINDEX)**, http://www.latindex.org.*
*From Latin American Quotes in Social Sciences and Humanities **(CLASE)**, of the Universidad Nacional Autónoma de México, http://clase.unam.mx.*

Área de Estudios e Investigación: 2 2668 3835
Área de Extensión Académica : 2 2668 3832
Biblioteca: 2 2668 3839
CESIM
Bandera Nº 52, Santiago de Chile
email: extension.cesim@ejercito.cl
escenariosactuales.cesim@ejercito.cl
www.cesim.cl

Escenarios Actuales, año 23, diciembre, Nº 4, 2018
ISSN 0717-6805

Escenarios Actuales

Contenidos

Editorial

Escenarios Actuales, año 23, diciembre, Nº 4, 2018
ISSN 0717-6805

Editorial

La Declaración sobre seguridad de las Américas en 2003, de la Organización de Estados Americanos, constató la diversidad de amenazas que enfrentaba el Hemisferio. Si bien muchas de ellas no eran nuevas, su rápida evolución planteaba desafíos cada vez más importantes a los gobiernos, teniendo como principal ejemplo los atentados en Estados Unidos de 2001. Por lo tanto, y bajo una visión compartida, los Estados ahí representados consensuaron el alcance multidimensional que estas tenían, ampliando así el enfoque hacia un modelo que pusiera al ser humano en el centro.

En este contexto, los ataques a la seguridad cibernética se encontraban como parte de las nuevas amenazas. Desde aquel entonces, su proliferación a nivel mundial ha sido evidente, teniendo como casos ejemplificadores lo ocurrido en Estonia en 2007 y, recientemente en 2017, las repercusiones del ataque a nivel mundial del virus WannaCry que impactó a empresas transnacionales, dejando de manifiesto las vulnerabilidades que existían en cerca de 150 países.

Chile no ha estado ajeno a esta realidad, siendo afectado también por ataques cibernéticos, lo que ha constatado la necesidad de desarrollar instrumentos que permitan resguardar la infraestructura crítica del país. Prueba de ello es la promulgación de una Política de Ciberseguridad en 2017 y una Política de Ciberdefensa en 2018.

Esta edición especial de *Escenarios Actuales* tiene como principal propósito presentar las ponencias del seminario "Ciberespacio: desafíos a la seguridad y defensa de Chile en el siglo XXI", organizado por el Ejército de Chile el día 13 de septiembre de 2018 en Santiago.

Como ha sido tradicional, en el mes conmemorativo de las Glorias del Ejército, la institución organiza un encuentro que permita abordar una problemática de especial interés nacional, y por lo tanto también para las Fuerzas Armadas, generando un punto de encuentro entre las distintas comunidades del país para reflexionar sobre temas que impactan el desarrollo de Chile.

Es por ello que el seminario reunió a representantes de las Fuerzas Armadas, de los distintos ministerios y reparticiones gubernamentales vinculados a la temática, académicos, investigadores, especialistas y líderes de opinión, entre otros, contribuyendo así a enriquecer el debate e intercambio de ideas.

De esta forma, la presente edición contiene, en primer lugar, las palabras de apertura del seminario por parte del Comandante en Jefe del Ejército, GDE Ricardo Martínez Menanteau. A continuación, se presentan las exposiciones de los disertantes: General Robert H. Latiff, Pasi Eronen, General de División Carlos Gómez López de Medina y el Brigadier Mark Proctor (OBE).

Todos ellos, destacados profesionales con vasta trayectoria que entregaron sus experiencias y renovadas perspectivas, permitiendo contribuir a la generación de conocimiento especializado y de interés estratégico para la toma de decisiones.

Por consiguiente, esta edición complementa las líneas investigativas que busca difundir la revista, al constituir una materia propia del ámbito de la seguridad y defensa que requiere una permanente actualización, a fin de generar nuevas interrogantes que inspiren los estudios en esta área.

El CESIM aprovecha esta oportunidad para invitarlos a visitar nuestro sitio web, en el cual podrán conocer nuestras actividades académicas y descargar íntegramente las publicaciones (www.cesim.cl).

DIRECTOR CESIM

ISSN 0717-6805

Seminario

"Ciberespacio: desafíos a la seguridad y defensa de Chile en el siglo XXI"

Edificio Ejército Bicentenario
13 de septiembre de 2018

Santiago de Chile

Escenarios Actuales, año 23, diciembre, Nº 4, 2018
ISSN 0717-6805

Escenarios Actuales, año 23, diciembre, Nº 4 (2018), pp. 7-10.
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

Discurso de apertura del Seminario "Ciberespacio: desafíos para la seguridad y defensa de Chile en el siglo XXI"

GDE Ricardo Martínez Menanteau*

Resumen:

Como una forma de contribuir a la generación de conocimiento especializado, el Ejército de Chile organizó el 13 de septiembre de 2018 el seminario "Ciberespacio: desafíos a la seguridad y defensa de Chile en el siglo XXI", instancia académica que contó con la participación de destacados expositores nacionales y extranjeros, quienes con su vasta trayectoria entregaron enfoques actualizados sobre la materia. El presente artículo contiene las palabras de apertura del Comandante en Jefe del Ejército, General Ricardo Martínez Menanteau.

Summary:

As a contribution to specialized knowledge creation, on September 13, 2018, the Chilean Army hosted the seminar "Cyberspace: challenges to the XXIst Century Chilean security and defense". This academic activity had the participation of distinguished national and foreign speakers. The present article includes the inauguration speech by the Chilean Army Commander in Chief, General Ricardo Martínez Menanteau.

Sean mis primeras palabras para saludar y recibir, muy cordialmente, a las autoridades, académicos e invitados especiales que hoy participarán en esta nueva instancia de reflexión, enmarcada en un acontecimiento relevante para el país, como es el mes de la patria y de las Glorias del Ejército de Chile.

Palabras Clave
Ejército de Chile
Ciberdefensa
Ciberseguridad
Seguridad multidimensional
Defensa

Keywords
Chilean Army
Cyberdefense
Cybersecurity
Multidimensional Security
Defense

* Oficial de Estado Mayor, del Arma de Infantería. Licenciado en Ciencias Militares, Academia de Guerra del Ejército de Chile (ACAGUE). Magíster en Gestión y Planificación Estratégica, ACAGUE. Magíster en Administración de Empresas, Universidad Adolfo Ibáñez. Diplomado en Operaciones Conjuntas, Instituto de Cooperación y Seguridad Hemisférica, y Diplomado en Estudios de Seguridad y Defensa, Colegio Interamericano de Defensa, Estados Unidos. Entre los cargos que ha desempeñado en el Ejército, se encuentran el haber sido Comandante de la Compañía de Comandos N° 8 en Valdivia, Comandante del Regimiento Reforzado N° 10 "Pudeto" de Punta Arenas, Director de la Escuela de Suboficiales del Ejército, Director de la Dirección de Proyectos e Investigación, Subjefe del Estado Mayor Conjunto y Jefe del Estado Mayor del Ejército. El 9 de marzo de 2018 asumió como Comandante en Jefe del Ejército.

GDE Ricardo Martínez Menanteau

Saludo muy particularmente a los distinguidos expositores y les agradezco la oportunidad que nos brindarán de compartir sus conocimientos y experiencias, y poder así debatir respecto de uno de los mayores desafíos del siglo XXI.

El Ejército es una institución fundacional y fundamental de la República y, como tal, se siente en la obligación de ser un aporte permanente y efectivo a la paz, la seguridad y la defensa de Chile. Es por ello que anualmente, durante el mes de septiembre, hemos organizado sendos seminarios para abordar temáticas de primera importancia, como "El significado de la ocupación del territorio y la disuasión", "Los recursos naturales y la seguridad" y "La consolidación de la defensa nacional", entre otros.

Este año, queremos abordar un tema que preocupa y ocupa transversalmente a los Estados, a las instituciones, a las empresas y a la sociedad civil en general, como es la necesidad de asegurar la información contenida en los servidores conectados a las redes de comunicación, evitando que esta sea objeto de ataques por parte de individuos u organizaciones delictuales.

Nuestra propuesta, en consecuencia, es el ciberespacio y los desafíos que este representa para la seguridad y para la defensa de Chile en el siglo XXI.

Más allá de las múltiples definiciones e interpretaciones existentes, el ciberespacio es un ambiente de interacción social, cuyas capacidades se han multiplicado como consecuencia de la evolución de las tecnologías de la información y de los efectos de la globalización, posibilitando el almacenaje, procesamiento y circulación de una cantidad cada vez mayor de información, permitiendo así análisis y estudios complejos, en tiempos cada vez menores y con bajos requerimientos de recursos.

De su definición y características, se desprende que esta dimensión ofrece múltiples oportunidades, pero a la vez enormes incertidumbres, algunas de las cuales se expresan como amenazas y riesgos: las denominadas "ciber-amenazas", que obligan entonces a generar capacidades de ciberseguridad y de ciberdefensa que generen las condiciones necesarias para que todos podamos beneficiarnos del uso fiable del ciberespacio.

Entre las principales amenazas asociadas al ciberespacio, destacan las acciones ejecutadas por los propios Estados, los ataques patrocinados o ejecutados por privados, los ataques terroristas o ciberterrorismo de tipo económico, político o ideológico, el robo y la manipulación de información con diversos fines, el espionaje, los ataques a redes y sistemas y los ataques contra la infraestructura crítica.

En consecuencia, esta quinta dimensión, como se le ha denominado, es altamente vulnerable, principalmente porque es muy fácil acceder a ella y, por lo tanto, está expuesta a una multiplicación permanente de actores y de riesgos.

Este desafío está siendo abordado por el Estado de Chile a través del Comité Interministerial sobre Ciberseguridad, coordinado por el Ministerio de Defensa, teniendo entre sus principales objetivos, en el corto plazo, el diseño e implementación de una política de defensa, así como también una planificación de nivel primario y secundario.

Siendo la seguridad muldimensional una condición esencial para la institucionalidad y finalmente para la gobernabilidad de los Estados, estimo conveniente exponer algunas precisiones y compartir algunas reflexiones en torno a ciertos conceptos que constituyen el marco de los desafíos del ciberespacio.

Hasta la segunda mitad del siglo XX, seguridad y defensa eran conceptos considerados sinónimos. En ambos casos, el Estado constituía el sujeto referente, proporcionador de seguridad y objeto a la vez de las amenazas. En este modelo las fuerzas militares, policiales y los servicios de seguridad eran los actores predominantes sino únicos del sistema de seguridad.

Hoy, en un contexto multipolar y globalizado, la seguridad ha superado la tradicional noción de la defensa militar para abarcar y englobar otros aspectos como la economía, la salud, el medioambiente, la infraestructura crítica y, en fin, todo aquello que pueda ser calificado como bienes esenciales al servicio de la comunidad.

También se acostumbraba a hacer una diferencia entre la seguridad externa, esto es aquella que buscaba contribuir a la generación de un mundo estable y al resguardo de los espacios territoriales y, por otra parte, la seguridad interna, vinculada al normal funcionamiento de los países, de sus sistemas políticos y de la vida cotidiana de sus habitantes. Hoy, sin embargo, bien sabemos que las nuevas amenazas no aplican a aquel modelo de clasificación tradicional, imbricando aún más los conceptos de seguridad y defensa, y multiplicando y haciendo cada vez más inciertos y difusos los riesgos y las amenazas.

La soberanía, por su parte, también es un concepto en constante evolución. Si en una definición original se le consideraba como el poder de un Estado nación para decidir "soberanamente" al interior de su espacio territorial, hoy se le observa más bien como un deber del Estado, aquel de proteger y resguardar los estándares que permitan la vida y el desarrollo del país, de sus instituciones y por cierto de los ciudadanos.

La era de las comunicaciones y de la información está produciendo cambios profundos en la forma en la que los Estados deben enfrentar las amenazas. La mayor gravedad de ello es que frecuentemente los modos o las estrategias son más bien reactivas, pues los cambios se suceden a una velocidad mayor a la capacidad de adaptación o de anticipación.

En la dimensión del ciberespacio, aquella que paradojalmente no ocupa "espacio" y por tanto no puede ser dimensionada, ni medida ni percibida, la superioridad militar no proporciona necesariamente un efecto disuasivo ni menos asegura la victoria militar. Es por ello que las estrategias de ciberseguridad y de ciberdefensa buscan abordar el problema desde una perspectiva global, ya que una de las condiciones que genera el ciberespacio es la posibilidad real de que se incorporen múltiples y nuevos actores que antes no participaban en un conflicto o en una crisis de carácter convencional.

A partir de los criterios anteriores, los estudios especializados sostienen que, en las crisis y en los conflictos del futuro, el ciberespacio jugará un rol preponderante, por lo que serían completamente aplicables los conceptos de ciberguerra y de ciberarmas, siendo estas últimas los ataques informáticos dirigidos a las infraestructuras críticas del oponente.

Ciberseguridad y ciberdefensa son conceptos vinculados, complementarios e interdependientes. El primero de ellos, la ciberseguridad se define como un conjunto de herramientas multidisciplinarias destinadas a proteger los activos de una organización y a los usuarios del ciberentorno. De esta definición se desprende que la ciberseguridad requiere de esfuerzos colectivos, desde el nivel político hasta la cultura individual de los usuarios, existiendo consenso en que desde una perspectiva sistémica, existen cinco elementos que no deben estar ausentes: el desarrollo de un marco legal que sustente las acciones; el desarrollo y la aplicación de medidas técnicas y procedimientos; la definición de las estructuras o la arquitectura de seguridad; el desarrollo y la difusión de una cultura de ciberseguridad; y la cooperación internacional.

Tanto de la definición como de las condiciones esenciales expuestas, se deduce que la ciberseguridad es una responsabilidad primaria del Estado e indispensable para asegurar el desarrollo del país y de los individuos.

La ciberdefensa, por su parte, se define como la capacidad desarrollada, igualmente por el Estado, para prevenir y contrarrestar las amenazas que atenten contra los intereses soberanos del Estado-nación. Se trata de un concepto asociado directamente a la planificación político-estratégica, que vincula las amenazas y las vulnerabilidades de la infraestructura crítica de un país. Por ello, la ciberdefensa se relaciona con el desarrollo de capacidades tácticas y técnicas que aseguren los sistemas y la información que ellos contengan, así como también permitir la explotación y respuesta sobre los medios que garanticen el libre acceso al ciberespacio.

Sin pretender establecer una desagregación del concepto de ciberdefensa, separando el nivel político del militar, es necesario reconocer que este posee características que condicionan directamente el ámbito militar, entre las que destacaré las siguientes:

- En primer término, el ciberespacio es un quinto dominio de las operaciones militares, afectando en consecuencia el análisis de cada uno de los factores del campo de batalla.
- Por otra parte, la inexistencia de fronteras físicas genera cambios importantes en la percepción de los entornos operacionales y una relativización de las variables "distancia" y "tiempo".
- Como tercer aspecto, los actores se multiplican en el campo de batalla, con motivaciones, métodos y objetivos disímiles.
- En cuanto a los daños materiales de una ciberguerra, estos eventualmente podrían tener consecuencias personales y materiales menos graves que en un conflicto que privilegie las operaciones convencionales. Sin embargo, las consecuencias de un ataque informático exitoso contra la infraestructura crítica de un país puede tener enormes repercusiones en los servicios básicos, la industria, la banca, el transporte, entre otros.
- Por último, señalar que las características antes resaltadas, sumadas a tantas otras que son materia de estudio y preocupación, suponen cambios importantes en las doctrinas operacionales de las fuerzas militares y, por cierto, en la preparación intelectual y psicológica de sus integrantes.

Así, al analizar el conflicto en sus diferentes estadios: latencia, crisis y guerra, desde una perspectiva de la gestión y del control de la información, me asiste la convicción, hoy más que nunca, que la victoria militar se inclinará del lado de quien sea capaz de observar con mayor amplitud, pensar con mayor creatividad, decidir con mayor precisión y actuar con mayor rapidez, para lo cual el aseguramiento de la información y de las comunicaciones es y será un aspecto vital de las operaciones militares.

Finalmente, junto con reiterar el compromiso del Ejército para continuar siendo un actor relevante y referente en el ámbito de la investigación y el desarrollo, y en la promoción de instancias académicas, como la que hoy nos convoca, agradezco una vez más a las autoridades, expositores e invitados especiales, en su condición de audiencia especializada, el interés y el tiempo que se han dado para concurrir a este histórico Edificio Bicentenario y compartir esta iniciativa que, estamos seguros, será un gran aporte para los intereses del país.

Muchas gracias.

Escenarios Actuales, año 23, diciembre, Nº 4 (2018), pp. 11-18.
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

Un enfoque diferente del conflicto del siglo XXI: tecnologías avanzadas, guerra de la información y la apremiante necesidad nacional

General Robert H. Latiff*

Resumen:

La relevancia que han adquirido las tecnologías emergentes plantean diversos desafíos y, a su vez, potenciales inconvenientes. En este contexto, el autor advierte las consecuencias que podrían surgir, producto de su rápida evolución, en el ámbito moral y ético, particularmente, para Fuerzas Armadas. Lo anterior, considerando el campo de batalla futuro y la renovada importancia de la guerra electrónica.

Summary:

The relevance that emerging technologies have reached is the source for several challenges and potential inconveniences. In this context, the author warns of the consequences that could arise due to their rapid evolution in the moral and ethics dimension, particularly, for the Armed Forces. The aforementioned, taking into account the future battlefield and the renewed importance of electronic warfare.

Palabras Clave
Operaciones de información
Tecnología
Guerra futura
Inteligencia artificial
Guerra cibernética

Keywords
Information operations
Technology
Future warfare
Artificial intelligence
Cyberwar

Permítanme comenzar mi intervención agradeciendo al ministro de Defensa, señor Alberto Espina, al comandante en jefe del Ejército

* Oficial en retiro de la Fuerza Aérea de Estados Unidos. Su última destinación la realizó en la Oficina Nacional de Reconocimiento, donde sirvió como Director de Sistemas Avanzados y Tecnología, y como Director subrogante de Ingeniería de Sistemas. Además, sirvió en el Ejército en la rama de Infantería, donde se desempeñó como Comandante de una unidad de armas nucleares tácticas. Doctor en Ciencia de Materiales de la Universidad de Notre Dame, Estados Unidos, y graduado del Programa de Becarios de Seguridad Nacional en la Escuela JFK de Gobierno de la Universidad de Harvard. Actualmente, se desempeña como asesor privado para clientes corporativos, gubernamentales y universidades. Es miembro adjunto de la facultad con el Centro Reilly para ciencias, tecnología y valores en la Universidad de Notre Dame y profesor de investigación en la Universidad George Mason. Recibió la medalla de distinción de servicio en inteligencia nacional y la medalla de distinción de servicio de la Fuerza Aérea. Autor del libro *Future War: Preparing for the New Global Battlefield.*

general Ricardo Martínez, al Estado Mayor General del Ejército y en especial al general John Griffiths, quien fue el responsable de invitarme. Es un gran honor el que me hayan invitado a su hermoso país y a su Cuartel General para participar en este importante seminario de alto nivel. El tema de este encuentro, Ciberespacio: desafíos para la seguridad y defensa de Chile en el siglo XXI, es ciertamente oportuno y crucial para el Ejército y en general.

Como científico y oficial militar de carrera, he pensado profundamente en la tecnología y en los impactos de esta en la guerra. Como profesional militar y excomandante, a menudo he pensado en las formas en que usamos y cuidamos a nuestros soldados, marinos, aviadores e infantes de marina. En cada caso, como científicos y líderes militares, tenemos la obligación de enseñarles a nuestros soldados las herramientas que van a usar, cómo las van a utilizar y también cómo apegarse a los estándares estrictos de la conducta profesional. Estas preocupaciones son igual de importantes en la guerra de alta tecnología (incluida la cibernética) y en el combate cercano.

En términos generales, seguiré la línea de la tecnología, la ética y el uso del ejército, para finalizar con un debate sobre los desafíos del conflicto cibernético y las operaciones de información.

El año pasado tuve el agrado de publicar mi libro *Future War: Preparing for the New Global Battlefield,* cuyo mensaje principal es que en general las tecnologías de guerra emergentes van muy de prisa y estamos tan acelerados por incorporarlas rápidamente que no nos planteamos de manera suficiente los potenciales inconvenientes y consecuencias no deseadas que pudiesen ocurrir; además de la posible repercusión moral y ética que pudieran provocar. En el mundo se han cometido graves equivocaciones morales con armas nucleares, biológicas y químicas, es por ello que debemos asegurarnos de que no vuelvan a suceder.

En *Future War* existen varios temas que procuro destacar: primero, que la tecnología y la guerra siempre han estado entrelazadas. Segundo, que nos vemos seducidos por, y a menudo adictos, a la tecnología. Tercero, que las nuevas tecnologías cambiarán dramáticamente el concepto que conocemos de conflicto. Cuarto, que las nuevas tecnologías desafiarán a los soldados y a los líderes en lo ético. Finalmente, que nuestros líderes políticos y públicos deben prestar más atención a los problemas en materia de tecnología, asuntos internacionales y conflicto, lo que tendrá un impacto directo, cada vez mayor, en los ciudadanos.

El rápido crecimiento de la tecnología en sí supone un desafío ético. En el año 2000, Stewart Brand escribió en la revista *Time*: *"El cambio que sucede muy rápido puede resultar ser sumamente disgregador; si solo una élite le puede seguir el ritmo, el resto crecerá estupefacto de cómo funciona el mundo".* Tal como él indicó: *"Podemos entender la biología natural, por más sutil que sea, porque aún se mantiene. Pero, ¿cómo seremos capaces de comprender la informática cuántica o la nanotecnología si su sutileza sigue alejándose de nosotros?".* Cabe señalar que actualmente también se pueden sumar la biología sintética y la inteligencia artificial. ¿Y qué es lo que pasa? Las personas solo se rinden y rendirse es igual de malo tanto en el ámbito comercial como el civil.

De verdad deberíamos tener algún tipo de entendimiento respecto a las herramientas que utilizamos cada día, pero rendirse es una idea terrible cuando se habla de armas y guerra. Tendemos a vernos seducidos por la tecnología, todo desde la electricidad hasta los antibióticos, smartphones, aviones de combate y armas nucleares. Robert Oppenheimer, uno de los padres de la bomba atómica incluso dijo: *"Así mismo fue que sucedió con la bomba atómica. La tecnología era tan seductora que simplemente decidimos seguir adelante y preocuparnos después".* Los consumidores hacen filas para comprar teléfonos nuevos de USD 1.000 solo porque están disponibles. Las Fuerzas Aéreas necesitan aviones de combate de última generación, cuando la generación anterior aún no ha sido entregada. Y ahora Estados Unidos está planificando construir una nueva arma nuclear, aparentemente porque Rusia tiene una.

Escenarios Actuales, año 23, diciembre, Nº 4, 2018
ISSN 0717-6805

Existen algunas desventajas en la innovación de la tecnología, por lo que debemos ser prudentes y considerarlas detenidamente. Evidentemente, algunas de estas innovaciones son buenas y otras, claramente malas. Muchas son ambiguas, como los pesticidas que matan parásitos y al mismo tiempo contaminan el agua; o los antibióticos que son maravillosos y que, sin embargo, la resistencia por el abuso de estos mata a miles de personas cada año. Por otra parte, las nuevas tecnologías de vigilancia podrían aumentar la productividad en los trabajadores, pero dejan a las personas preocupadas por su derecho a la privacidad y a sus libertades civiles. Y, ¿quién sabe cuáles serán los efectos que tendrán a largo plazo nuestras nuevas formas de comunicación?

El Departamento de Defensa de Estados Unidos ha sido conocido desde hace mucho tiempo por apoyar la innovación tecnológica. Sus intereses de investigación básica incluyen la biología sintética, la ciencia de la información cuántica, la neurociencia cognitiva, el desarrollo del modelo del comportamiento humano y los materiales novedosos; por supuesto, también se ha añadido la inteligencia artificial. La Fuerza Aérea está en búsqueda de vehículos hipersónicos y armas láser, y todas las fuerzas armadas están interesadas en las armas autónomas. Al reconocerse la renovada importancia de la guerra electrónica, el Departamento de Defensa también se propone hacer una demostración de las nuevas tecnologías y técnicas en el espectro electromagnético.

Como consecuencia de las tecnologías emergentes, es probable que el campo de batalla del futuro esté poblado de una gran cantidad de humanos perfeccionados de alguna forma, con mejoras de rendimiento a través de implantes electrónicos u otros sistemas físico-cibernéticos.

La toma de decisiones será altamente automatizada y el modelado cognitivo del oponente, mediante el empleo de inteligencia artificial avanzada, se utilizará para anticipar las acciones del enemigo antes de que estos las decidan y ejecuten.

Los robots serán omnipresentes y operarán en equipo con los seres humanos o por sí solos, ya sea individualmente o en masa. Habrá un entorno denso de señales electromagnéticas, tanto para, como contra las comunicaciones y, probablemente, con fines antipersonal. La piratería dinámica y la suplantación de identidad serán incontrolables, con información sensible, operaciones psicológicas y el uso de la desinformación como arma.

De este modo, la guerra será cada vez más sobre la superioridad de la información, donde habrá adversarios que intentarán destruir la capacidad del otro para percibir, decidir y luego actuar. Las naciones pares se involucrarán en la guerra cibernética, la guerra electromagnética, la guerra de la información y en la guerra con drones o robots.

En todo este contexto, ¿dónde está el debate sobre la pertinencia de las nuevas armas tecnológicas y los factores éticos de su uso? En el reciente anuncio de la Casa Blanca sobre su Iniciativa en Inteligencia Artificial (IA), no se hizo mención alguna de los innumerables problemas (técnicos y éticos) asociados a ella.

El tema ético

Buscaba que mi libro se tratara tanto de la ética de la guerra y las armas como de las armas mismas. He conversado con muchos veteranos de guerra, de los cuales muchos han sido alumnos míos. Por ejemplo, Maj Bill Martin, un capellán del Ejército cuya unidad sufrió muchas bajas en Irak, quien me habló de los conceptos relativos a la Teoría de la Guerra Justa y el Derecho de los Conflictos Armados, así como de la importancia de asegurar su aprendizaje para el bienestar moral y espiritual de las tropas de su unidad. Los soldados deben entender que existe una base sólida para lo que se les pide que hagan.

Como en cualquier tipo de guerra o con cualquier tecnología de armamento, existen consideraciones éticas y morales a la hora de decidir desarrollar o desplegar armas cibernéticas, y algunas pueden tener consecuencias letales. Si bien las naciones soberanas deben hacer lo que sea necesario para protegerse a sí mismas y a sus ciudadanos, no debiéramos precipitarnos en incorporar la tecnología a las armas (incorporar armas cibernéticas), sin haber contemplado dichas consecuencias. Las operaciones cibernéticas son notoriamente difíciles de atribuir. A veces los ataques son demasiado sutiles y, por tanto, difíciles de detectar, ya que los atacantes mismos no quieren ser detectados. Existe gran incertidumbre en el conflicto cibernético, y ambos bandos deben ser cautelosos y asegurarse de que sus objetivos son los indicados y de que existe una necesidad militar real para ejecutar sus operaciones.

La Guerra Justa y el Derecho de los Conflictos Armados siguen siendo muy importantes. En una nueva era de guerra y armamento, es aún más importante analizar los efectos recíprocos entre los cambios y los antiguos conceptos de necesidad militar, identificación de combatientes, proporcionalidad y evasión de sufrimiento innecesario. En el libro dedico bastante tiempo a estos análisis. Por ejemplo, respecto al sufrimiento innecesario, las tropas con acceso a comunicación que tienen la capacidad suficiente para enterarse de la rendición del enemigo. Aún no está claro si los sistemas automáticos de IA tienen la capacidad de desistir de un ataque motivados por la empatía. Los soldados en combate demuestran gran lealtad a sus compañeros. ¿Tendrá un robot la voluntad de 'sacrificarse' por un ser humano? ¿Puede un robot o un sistema de IA comportarse de forma altruista? ¿Puede acaso pedírsele a un ser humano que proteja a un robot a costa de su propia vida?

Históricamente, Estados Unidos ha sido bastante local y agresivo en su promoción del apoyo a los derechos humanos. Un aspecto clave de cualquier ejército profesional debe ser la adherencia a las normas del Derecho de

Escenarios Actuales, año 23, diciembre, Nº 4, 2018
ISSN 0717-6805

Conflictos Armados y del Derecho Internacional Humanitario, como ejemplo La Haya o los Convenios de Ginebra, entre otros. Muchos de los altos mandos militares de Estados Unidos han declarado públicamente al menos la necesidad de continuar considerando dichas normas en esta nueva era de robots y humanos mejorados, guerra cibernética e inteligencia artificial, láseres y armas hipersónicas. Lamentablemente, a pesar de que varios autores y grupos independientes se esfuerzan por defender este Derecho, veo poca evidencia real de que, al nivel de los altos cargos gubernamentales, se estén abordando estas cuestiones.

Paul Scharre, autor de Army of None, ha dicho, refiriéndose a las armas autónomas (lo que abarca armas de IA como las cibernéticas) que *"existen (sólidas) razones (filosóficas) para que la responsabilidad humana de asesinar se mantenga humana: el situar la carga de la guerra sobre máquinas debilita nuestra propia moralidad".* Además, la dificultad moral de asesinar es la mejor restricción contra los mayores horrores de la guerra. El problema es que los sistemas autónomos cambian la relación que existe entre los seres humanos y la violencia y, por tanto, cómo se sienten respecto al acto de asesinar.

La percepción sobre nuestros soldados como profesionales, no solo como herramientas

Muchos altos cargos de poder ven al ejército como una simple herramienta para implementar sus políticas, por lo cual recurren cada vez más al uso de la fuerza y los despliegues militares. De acuerdo al Congressional Research Service, se ha acudido al ejército estadounidense más de 50 veces desde el término de la Guerra de Vietnam y del servicio militar obligatorio, hace más de cuatro décadas. Solo en 2017 las fuerzas especiales estadounidenses se desplegaron en 143 países alrededor del mundo. Los líderes políticos encuentran poca resistencia económica o política al desplegar al ejército.

La actual Estrategia de Defensa Nacional de Estados Unidos requiere de importantes alzas en la inversión destinada a las tecnologías ya mencionadas. Esta estrategia gruesamente basada en la tecnología no es ninguna sorpresa. Nos hemos acostumbrado a un flujo incesante de nuevos y mejores dispositivos. Nos enfrentamos, ahora más que nunca, debido a la velocidad del desarrollo tecnológico, al peligro de apresurarnos en implementar el uso de estas tecnologías. Muchos altos cargos en el Departamento de Defensa y el Congreso exigen la superioridad de Estados Unidos en inteligencia artificial y capacidades cibernéticas sin saber siquiera qué son o lo que pueden hacer. Están seguros de que las necesitamos y desestiman cualquier debate relativo a las repercusiones generales que su uso podría tener.

Reinhold Niebuhr, un teólogo del siglo XX, escribió en su libro *The Irony of American History,* que el poder militar estadounidense creaba la *"tentación de volverse impaciente y desafiante en cuanto a la lentitud y, a veces, contrariedad de los procesos de la historia".*

Hoy nos enfrentamos a tecnologías cuya velocidad de desarrollo es muy incongruente y contraria a aquellos procesos contradictorios y lentos a los que se refiere Niebuhr. Refiriéndose a las capacidades cibernéticas, el escritor Lucas Kello señala en su libro *The Virtual Weapon,* que en esta era de rápidos avances tecnológicos, las amenazas y oportunidades que surgen de esta nueva clase de armamento nos presionan para actuar antes de haber finalizado el arduo proceso de determinación de la estrategia.

Si pensamos que los últimos 50 años se caracterizaron por un rápido crecimiento y avance, los próximos 50 años verán un crecimiento mayor que nunca en la población, drásticos avances tecnológicos y una competencia por recursos e influencia que se tornará cada vez más violenta.

El director de Inteligencia Nacional de Estados Unidos, en uno de los últimos informes relativos a las tendencias mundiales, señala que el futuro será tanto más peligroso, como más rico que nunca en términos de oportunidades.

Veremos crecientes tensiones tanto dentro como entre los países, el crecimiento mundial se ralentizará a medida que se presenten desafíos mundiales cada vez más complejos, mientras que la cooperación internacional y la acción gubernamental serán mucho más difíciles.

Lamentablemente, no percibo intención alguna por parte de las naciones o de nuestro propio gobierno de apaciguar la sed de apresurarse a adoptar nuevas tecnologías de guerra, menos considerar la idea de limitar su proliferación. Competencia, no cooperación y un continuo afán de superioridad y dominio parecen ser las metas estándar.

Creo que somos mejores que eso, y podemos lograr cosas mejores. Podemos, aunque sea levemente, pisar el freno en el desarrollo tecnológico y plantear preguntas de sondeo a nuestros investigadores y desarrolladores de armamento. Además, podemos asumir un rol de liderazgo e involucrar a otras naciones, enemigos pares y naciones en desarrollo parecidas, en comprometerse a considerar los acuerdos internacionales que limitan y controlan la implementación de armas, lo que incluye particularmente a las cibernéticas.

El tema cibernético

Las revoluciones nucleares y cibernéticas tienen orígenes similares, ambas provienen de avances radicales en la tecnología. Hemos vivido durante 70 años con el azote de las armas nucleares y eso, lamentablemente, nunca cambiará. Sin embargo, como señala Kello, la fuerza impulsora de la revolución cibernética es tremendamente diferente, basada en el poder perjudicial de la información. A diferencia de la revolución nuclear en la que el impresionante poder destructivo cambió el orden político y social, en la revolución cibernética, las ideas subversivas son los medios a través de los cuales las personas y los grupos debilitarán las órdenes políticas y sociales.

Escenarios Actuales, año 23, diciembre, Nº 4, 2018
ISSN 0717-6805

Debemos dejar de pensar en la guerra cibernética solo como un conflicto centrado en los computadores. Si bien es todo lo anterior, lo cibernético es más que la tecnología de información, el Internet de las cosas y las redes informáticas, y *"nuestra asimilación de esta complejidad técnica de las armas virtuales en realidad sirve para ocultar los objetivos que impulsan su uso".*

Se debe considerar lo cibernético en el contexto amplio de la guerra de la información, que abarca la negación, el engaño, las operaciones psicológicas, la mensajería estratégica e influencia de las operaciones, piratería informática, parodias y muchas otras maneras de ocasionar problemas. El concepto de 'Operaciones de Información' reconoce que los temas de información impregnan la gran variedad de operaciones, desde la paz hasta la guerra global. Existe un impacto operativo de la información en cada uno de los escalones de mando.

Las entidades, desde hackers a organizaciones terroristas y Estados-nación, pueden influir en las redes e información hasta diversos grados y con mayor o menor grado de daño económico o militar. Creo que las mayores amenazas nacionales son las operaciones de información que nos causarán, ya sea en lo financiero, comercial, militar o público, perder la esperanza en nuestros datos e información y, básicamente, en nuestras instituciones.

Las operaciones cibernéticas pueden provocar y han provocado que los países y las instituciones cuestionen su información y pueden generar que los partidarios pierdan la confianza. Como prueba de esto analicemos las elecciones de 2016 en Estados Unidos. Es un asunto tanto socio-político como técnico. No hay soluciones a corto plazo. La tecnología es fundamental, pero la tecnología por sí sola no es suficiente, se requiere una solución de sistemas, no soluciones individuales.

Según el especialista en relaciones internacionales Erik Gartzke, *"la guerra cibernética es probable que no sirva como el árbitro final de una competencia en un mundo anárquico y, por lo tanto, no debe considerarse como algo aislado de las formas más tradicionales de violencia política o militar".* Una operación cibernética ofensiva no debería considerarse por sí misma, sino como una referencia de sus efectos tanto directos como indirectos en el conflicto. Lo cibernético es solo un elemento de una operación de armas combinadas.

Lo cibernético es mucho más que proteger las redes de la intromisión y ataque. Debe incluir una forma de pensar que considere la información como un recurso nacional valioso que se debe proteger. Tiene que incluir la educación de todos en la organización y también de los ciudadanos sobre el comportamiento seguro en Internet y en todas las formas de comunicaciones digitales, de hecho, en todas las formas de comunicación en general. La información, en todas sus formas, se debe proteger y resguardar, ya que es el motor del ejército, el gobierno y el comercio.

Casi del mismo modo en que los aviones, tanques y barcos no pueden funcionar sin combustible, repuestos y personal capacitado, esos elementos también están en peligro si están funcionando sin información o con información incompleta o corrompida. La educación y el entrenamiento en operaciones cibernéticas y de información deben ser afianzadas en la sociedad civil y el ejército.

El ejército por sí solo, o el sector comercial por sí solo, no puede defendernos satisfactoriamente y proteger nuestros sistemas e información críticos. Requerirá una alianza verdadera. El ejército, el gobierno y el sector privado están tan profundamente entrelazados e interdependientes que es realmente imposible separar los efectos de uno de los efectos del otro. En Estados Unidos, el ejército no podría existir sin su industria de defensa, y esa industria no podría existir sin el ejército. El sector privado debe compartir la información cibernética con el gobierno y viceversa. Los gobiernos deben encontrar vías legales para ayudar al sector privado a defenderse, y vías legales "no amenazantes" para que las industrias compartan información comercial sensible con el gobierno. Los gobiernos

deben comprometerse con el sector privado en formas realmente operativas para identificar a nuestros adversarios cibernéticos y aumentar considerablemente nuestras defensas.

Como señaló Tom Bossert, exasesor presidencial de Seguridad Nacional de Estados Unidos, el mercado libre tiene éxito por normas básicas respetadas entre las personas y normas diseñadas por los gobiernos. El sistema global funciona, en parte, porque aquellos que infringen las normas sufren las consecuencias y aquellos que actúan bien no. Entonces, si las personas o naciones eligen manipular el ciberespacio para obtener ventaja financiera o geopolítica, nosotros debemos actuar. Debemos buscar la cooperación internacional para imponer sanciones a aquellos que actúan contra este creciente consenso.

Estados Unidos tiene la oportunidad aquí y en otros foros internacionales de demostrar liderazgo. Debido a que es una zona de conflicto nueva y mal entendida, muy similar a los primeros días de la era nuclear, obviamente existe la necesidad de contar con acuerdos internacionales y normas de comportamiento en el ámbito cibernético.

La guerra cibernética es real, tratamos con ella todos los días. En algún momento en el futuro puede que sea parte de una guerra verdadera. George Lucas, profesor de la Escuela de Postgrado Naval de Estados Unidos, escribió que la posibilidad de una guerra cibernética ilimitada depende de la existencia de normas de conducta ética y legal sumamente discutidas, cuyas aplicaciones prácticas son muy difíciles. Los planificadores del gobierno y del Ejército deben seguir manteniendo esas normas éticas y legales como máxima prioridad.

Conclusión

Para concluir, un amigo y colega, quien es un experto en el tema cibernético muy respetado en la comunidad de inteligencia en Estados Unidos, resume la situación así:

El impacto del fracaso defensivo, por una parte –y la consecuencia para el atacante, por la otra– están fuera de equilibrio. Es dolorosamente obvio que los líderes políticos y los altos funcionarios no entienden esto. Parece que les falta bastante curiosidad y, por consiguiente, bastante comprensión de lo crítico y complejo que es este tema.

Un país debe tener a alguien a cargo, responsable de todo el espectro de las amenazas. De otra manera, los resultados podrían ser desastrosos.

Por esta razón, aplaudo al gobierno de Chile y al Ejército de Chile por asumir el liderazgo con esta importante reunión.

Escenarios Actuales, año 23, diciembre, Nº 4, 2018
ISSN 0717-6805

Escenarios Actuales, año 23, diciembre, Nº 4 (2018), pp. 19-26.
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

Las consecuencias de los avances técnicos en la preparación nacional y la ciberdefensa

Pasi Eronen*

Resumen:

En esta exposición se analiza el contexto de la revolución digital y cómo esta afecta a las personas, sociedad y los intereses de los Estados, en donde el dominio cibernético y la influencia que se ejerce de otros Estados, empresas, grupos o personas se transforman en amenazas y ataques permanentes, los que, en algunos casos, resultarán exitosos. Se plantea la necesidad de que en el nivel internacional se impulse la cooperación y reciprocidad entre las democracias liberales para favorecer el libre flujo de la información y el dominio digital. Asimismo, en el ámbito nacional, señala que cada país debe fomentar e impulsar el desarrollo de sus propias capacidades de seguridad y defensa cibernética para protegerse de las operaciones de influencia adversaria y de los ataques a la infraestructura crítica, por medio de establecer asociaciones entre el sector público y privado, civil y militar, y los ciudadanos.

Summary:

This presentation analyses the context of the digital revolution and how it affects people, society and the state´s interests. In it, the influence of states, companies, groups or individuals are transformed in permanent threats and attacks which, in some cases, will be successful. The speaker establishes the need for an international-level boost for cooperation and reciprocity amongst liberal democracies in order to benefit free information flow and digital

Palabras Clave
Revolución digital
Ciberdefensa
FAMGA
Dominio cibernético
Infraestructura crítica

Keywords
Digital revolution
Cyberdefense
FAMGA (Facebook-Apple-Microsoft-Google-Amazon)
Cyber domain
Critical infrastructure

* Pasi Eronen es analista, asesor y consejero en materia de seguridad internacional. Ha enfocado su trabajo de investigación y análisis en las tácticas de confrontación no convencionales, también conocida como guerra e influencia híbrida. Adicionalmente se desempeña en otros campos de especialización que incluyen la ciberseguridad, la guerra de la información y las operaciones de influencia. La labor política, ideas y observaciones de Pasi han sido destacadas por varios medios informativos tanto nacionales como internacionales. Dentro de estos se encuentran CNN, *The Wall Street Journal, The Washington Post* y Bloomberg. Posee vasta experiencia en oratoria tanto en eventos locales y regionales como en conferencias de gama internacional. Fuera del área de la investigación, en el desarrollo de su carrera profesional, Pasi ha trabajado en la consolidación de la defensa finlandesa y en organizaciones gubernamentales dedicadas a la seguridad integral y a contrarrestar las amenazas híbridas. También se ha desempeñado como asesor en un emprendimiento finlandés del área de la ciberseguridad y ha servido en misiones sobre el terreno en el área de gestión de crisis tanto para la UE como la OTAN. Posee un Magíster en Estudios de Seguridad de la Universidad de Georgetown, EE.UU., y un Magíster en Ciencias Informáticas de la Universidad de Joensuu, Finlandia.

domain. Likewise, in the national sphere, he argues that each country must foster and drive the development of their own cybersecurity and cyberdefense, to protect themselves against threat influence operations and attacks to critical infrastructure, by means of establishing associations between the public, private and military sectors and the citizens.

La aceleración de la revolución digital transforma todas las partes de nuestra sociedad y vida diaria

Si bien se han experimentado transformaciones en varias ocasiones de la historia humana del desarrollo tecnológico, hoy en día estamos viviendo en medio de una agitación tecnológica indudablemente importante o como muchos la llaman: la cuarta revolución industrial.

La revolución en curso tiene sus raíces en la cantidad de avances logrados durante las últimas dos décadas en la infraestructura de las comunicaciones a nivel global, y los servicios globales que se construyen sobre esta revolución; en las herramientas más poderosas de análisis y administración de datos, y en el rápido desarrollo de la inteligencia artificial junto con sus áreas de aplicación.

Además, la tecnología se ha vuelto más barata y, de esa manera, más asequible a un número mayor de personas y negocios. Se puede considerar como un gran nivelador, ya que ofrece puntos de partida similares a los usuarios de todo el mundo, ya sean civiles o militares.

Esta revolución radical penetra en todos los aspectos de nuestras vidas: transforma la manera en que vivimos, nos comunicamos y el modo en que opera nuestro entorno; y perturba los negocios, destruyendo algunos y dando lugar a otros completamente nuevos.

El aumento de la infraestructura y los servicios digitales globales también han empoderado a un número de empresas fundadas recientemente (provenientes de lugares como Silicon Valley y Hangzhou), permitiéndoles obtener mayor peso e importancia en la competencia global por el poder. Un conjunto de empresas como FAMGA[1] proveen los conductos digitales para el flujo de datos sin fronteras, las plataformas para realizar negocios digitales y los dispositivos finales para que las personas y negocios se puedan comunicar, provocando así que ambos, e incluso las sociedades, dependan de su existencia.

La revolución digital tiene serias implicancias en materia de seguridad

Los avances tecnológicos ofrecen, tanto a los individuos como a las sociedades, mayor eficiencia y nuevas maneras de hacer las cosas, obteniendo resultados que se habrían considerado inalcanzables unos cuantos años atrás.

No obstante, estos mismos avances –barreras de acceso reducidas, contracción de la geografía, el poder concentrado en la industria de la tecnología y la tecnología omnipresente que ofrece acceso a todas las partes de nuestra sociedad, incluidas nuestras facultades cognitivas– ofrecen una superficie de ataque en permanente expansión. Esta superficie de ataque comprende nuestra sociedad, sus procesos democráticos, las capacidades de la defensa nacional, la infraestructura crítica, las entidades comerciales, a los ciudadanos y nuestras mentes y corazones.

1 FAMGA: abreviación hecha a partir de las iniciales de cinco empresas exitosas de la era moderna (Facebook, Apple, Microsoft, Google y Amazon).

Escenarios Actuales, año 23, diciembre, Nº 4, 2018
ISSN 0717-6805

Las redes globales reducen la geografía y las fronteras nacionales, provocando, en particular, que los líderes autoritarios y sus regímenes teman perder su alcance sobre el poder y el dominio de la información. Mientras que la revolución de Gutenberg hizo que la información estuviera disponible para aquellos que podían leer, la revolución en curso hace que nuestra sociedad y mentes individuales tengan acceso a agentes externos de una manera sin precedentes.

La competencia geopolítica entre las potencias rivales, el bloque autoritario que desafía al *status quo* y a los defensores del actual orden mundial –específicamente las potencias occidentales–, parece empeorar cada día, impactando a su vez en el entorno de seguridad global. El aumento de la inestabilidad en nuestro entorno de seguridad hará que los riesgos sean mayores a medida que más agentes amenazantes posean, además de las capacidades, una gran cantidad de objetivos potenciales, donde su voluntad e intención será la de utilizar estas capacidades para alcanzar sus objetivos políticos.

La participación en el juego es obligatoria

En el mundo de los riesgos en aumento, no funcionará esconderse detrás de la fachada: "pero no somos interesantes como objetivos". Los atacantes encontrarán la forma y, en la mayoría de los casos, para efectos de planificación, es seguro asumir que ya han penetrado en muchos de los sistemas críticos, habiendo creado y mantenido un punto de apoyo allí.

Incluso las potencias más pequeñas tienen distintos tipos de activos estratégicos globalmente interesantes, tales como su posición geoestratégica; empresas que funcionan a escala mundial en sectores clave como telecomunicaciones y logística; ser proveedor clave de minerales estratégicos o líder en investigación e innovación en áreas de interés como la inteligencia artificial, lo que los hace convertirse en objetivos interesantes.

Para hacer las cosas un poco más desalentadoras, no funcionará construir muros de seguridad en el perímetro digital. Sugerir que cualquier país podría convertirse en una isla imaginaria completamente autosustentable no es cierto en el dominio cibernético y de la información. Además, el aislamiento del espacio común del patrimonio global digital tendría un enorme impacto en la eficiencia, ya que nos obligaría a duplicar gran parte del trabajo ya realizado por uno de esos gigantes comerciales mundiales que ofrecen precios más baratos, mayor calidad y, lo que es más importante, a menudo también mejor seguridad.

Actualmente, en muchos casos es simplemente imposible, o por lo menos no es rentable ni eficiente, que cualquier nación pueda replicar los avances técnicos clave en áreas como los chips informáticos y otro tipo de hardware informático y para redes; diseñar sistemas operativos específicos para cada país o desplegar adecuadamente los servicios disponibles, altamente escalables a nivel mundial, tales como la nube en todas sus variaciones.

Si bien es cierto que, a partir de ejemplos conocidos comúnmente, algunas potencias han encontrado cierto éxito limitado al declarar la soberanía digital, por ejemplo, al fomentar la balcanización del Internet global a través del aislamiento de sus ciudadanos de los flujos de información y servicios globales mediante la introducción de firewalls artificiales, y al forzar a las empresas extranjeras a compartir sus innovaciones a cambio de acceso al mercado, es todavía demasiado pronto para decir si dicha estrategia tendrá éxito a largo plazo.

El desarrollo de la resiliencia requiere un enfoque interconectado tanto a nivel nacional como internacional

Las capacidades nacionales de seguridad y defensa cibernéticas se deben desarrollar para que estén al nivel del entorno operativo más riesgoso, teniendo en cuenta la importancia y huella mundiales de la nación, para que sea considerada como parte del esfuerzo por compartir la carga mundial.

El desarrollo de la resiliencia tanto a nivel nacional como internacional juega un papel relevante en el funcionamiento dentro de este tipo de ambientes. Como ya se señaló, la planificación de las operaciones debería basarse especialmente en organizaciones dedicadas a la seguridad nacional, en el supuesto de que todo el entorno operativo digital es hostil.

A nivel nacional, una mayor resiliencia se presta para actividades que apuntan a mejorar la conciencia general sobre la interdependencia sistémica y la capacidad de cooperar estrechamente en todo tipo de brechas, silos y capas, como el sector público y privado, militar y civil, a nivel nacional, regional y local; y entre organizaciones de todo tipo y ciudadanos individuales.

A nivel internacional, dado que algunos países se están dirigiendo en contra del libre flujo de datos, información y servicios en el dominio digital, las naciones que piensan lo contrario deberían colaborar de manera aún más estrecha. Depende de las democracias liberales garantizar que tales prácticas no se acuerden ni consoliden en el derecho internacional y en las normas que rigen el Internet, sus usos aceptables y reglas de tránsito. Los países con ideas afines también deberían compartir la responsabilidad de defender el dominio cibernético e impulsar la capacidad de resiliencia del otro a través del aumento de la interconexión, interdependencia y confianza mutua.

Dicha cooperación y reciprocidad de gran alcance entre las partes, tanto a nivel nacional como internacional, no es una opción, sino más bien una necesidad para asegurar el dominio digital.

Se deben fomentar las asociaciones público-privadas

En la mayoría de los países las entidades del sector privado son las que empujan los límites de la tecnología, disponen de parte de la infraestructura crítica y se encargan de operar aquellos servicios de los que dependen las autoridades. Las funciones gubernamentales, incluidas las militares, descansan en el funcionamiento de dicha infraestructura tanto en tiempos de paz aparente como de crisis.

Por tanto, la ciberseguridad, capacidades y madurez de las entidades privadas críticas son cruciales dentro del panorama global amplio. Además, el sector privado produce gran parte de la capacidad que poseen y aplican los miembros del aparato de seguridad nacional en operaciones cibernéticas. De esta forma, se vuelve evidente que las asociaciones y la cooperación público-privada son elementos necesarios, no opcionales.

En términos prácticos, dicha cooperación puede manifestarse de diversas formas, lo cual incluye –pero no se limita– la cooperación comercial y la innovación compartida entre el sector privado y el sector público; el intercambio de información y la organización de ejercicios compartidos y eventos de entrenamiento que desarrollan no solo capacidades en común, sino que redes humanas y confianza entre los integrantes. Existen distintos tipos de plataformas y espacios que representan una gran oportunidad para intercambiar las experiencias y lecciones aprendidas de un sector al otro.

Producto de este desarrollo, se podría decir que los límites entre la infraestructura y los servicios civiles y los militares es a lo sumo, imaginaria. Esto por la interacción entre las partes y sus interdependencias complejas. Además, hacer una clara separación entre ambas se vuelve aún más esquivo debido a los efectos de segundo y tercer orden a los que un atacante podría estar apuntando al poner como blanco la infraestructura que parece ser civil.

Todo y todos constituyen un objetivo

Un astuto análisis de la situación actual sugiere que, a pesar de que existe una mejor postura de seguridad, una cooperación nacional e internacional y todos los esfuerzos dedicados a aumentar la resiliencia, algunos ataques serán exitosos. Cuando esto ocurra, vale la pena recordar que no se debe simplemente esperar que las cosas fallen de forma estrepitosa para recién considerar esto como una señal de que el adversario ha vencido.

Aparte de las operaciones de inteligencia y la sustracción de información almacenada en los sistemas objetivo, las operaciones cibernéticas pueden considerar la tecnología como una vía, además de un blanco en sí misma. Entre estos objetivos pueden figurar: la información y la integridad de la misma; los procesos, desde la toma humana de decisiones hasta la manufactura; las personas y su forma de entender el mundo y los acontecimientos que se desarrollan; y, en el sentido más amplio de la palabra, las fracturas de la sociedad mediante la intensificación de asuntos que generan división.

Un ejemplo concreto y más bien actual de lo anterior es el hecho de que la naturaleza universal de nuestro desarrollo tecnológico ha provocado que las operaciones de influencia antagonistas, que buscan llegar al público objetivo por la vía del dominio digital, se vuelvan más efectivas en comparación con las del pasado, que lo hacían por la vía de la prensa y los medios audiovisuales.

Existen operaciones pertenecientes al ámbito de la información basada en hechos y operaciones de configuración pertenecientes al ámbito digital que podrían considerarse similares a una práctica occidental conocida como comunicaciones estratégicas. No obstante, las operaciones de influencia adversarias suelen apoyar a los extremos políticos, sembrar confusión y división y explotar las vulnerabilidades ya presentes en la sociedad, es decir, los adversarios estarían tendiéndole una mano de ayuda a la sociedad que ha sido definida como blanco para que esta se destruya por sí misma.

La propaganda pagada, los canales gubernamentales de noticias, los trolls y bots virtuales, y diversas organizaciones de fachada son utilizados para difundir reportes sesgados, desinformación flagrante y filtración de información al público objetivo con el fin de influir en sus opiniones y acciones. El bombardeo continuo de desinformación ayuda a configurar el ámbito de la información a largo plazo y a formar público más receptivo a cualquier mensaje posterior. Los cambios en la narrativa, las verdades aceptadas y las preferencias de ideologías y temas ocurren de forma relativamente lenta, en pequeños incrementos, y no necesariamente de manera revolucionaria.

Dichas operaciones de influencia no se dan en el vacío, donde el adversario sería el único operador. Aprovechándose de las ambiciones políticas, las cuestiones políticas más sensibles, las quejas de las minorías y los movimientos populares virales que crecen a gran velocidad, las operaciones de influencia pueden ganar una ventaja y un empuje que sería difícil e incluso imposible de obtener de manera artificial. Parte del trabajo de las organizaciones de inteligencia, por tanto, lo ejecutarán gestores pagados, oportunistas e idealistas crédulos.

Para simplificar, en la práctica las operaciones de influencia han incluido, además de los esfuerzos por parte de los sistemas de análisis, recolección, infiltración y reconocimiento, una fase más activa, donde la información recabada se filtra al público mediante proxis autogenerados y agentes externos de pensamiento similar, y se intensifica mediante el uso activo de los recursos de las redes sociales y los medios tradicionales de comunicación social.

Hasta cierto grado, las poderosas y modernas empresas nativas digitales (por ejemplo, las plataformas de redes sociales, sus algoritmos de caja negra y sus modelos de monetización) también apoyan dicha labor, muy probablemente sin saberlo. Los datos que se pierden en las numerosas filtraciones proporcionan al adversario perfiles personales ricos en información, mucho más ricos que aquellos que posee cualquier actor comercial en el mercado. Estos perfiles tienen diversos usos, como el de apuntar a las personas y grupos correctos, identificación de usuarios de entre la masa e influencia hecha a medida.

La amplia variación en los posibles objetivos, vectores de entrega y mecanismos de impacto sugieren que para aplicar contramedidas efectivas, además del desarrollo de la resiliencia, es necesario tener un entendimiento actualizado de la estrategia y las metas del adversario, no solo de sus tácticas y tecnología.

Existen muchas formas de avanzar

En un plano general, dado que los desarrollos tecnológicos son ubicuos y globales, podemos suponer que dichos desarrollos se irán debilitando producto de los cambios culturales que los avances en inteligencia artificial, por ejemplo, aportarán a la vida laboral y a las exigencias a sus empleados.

Como es imposible controlar o contener las disrupciones, será esencial para los altos cargos políticos construir vías inclusivas para los ciudadanos hacia la próxima etapa de desarrollo, especialmente para aquellos que son

más vulnerables al cambio y a la irrupción de estas nuevas etapas. Los posibles impactos negativos en la sociedad deben ser internalizados por los agentes innovadores en tecnología, quienes son, en parte, responsables de la disrupción en marcha.

Pasando del nivel general al dominio cibernético, se evidencia en las operaciones de influencia ya documentadas y en los preparativos para operaciones futuras, que los países están desarrollando activamente sus capacidades cibernéticas y preparando asideros para desbaratar infraestructura crítica.

Muchas de las capacidades, entre ellas las dirigidas a la obtención de información, el ejercicio de la influencia, intimidación y el acoso, se han exhibido en conflictos en desarrollo y en contextos occidentales de elecciones y referéndums. Además de los impactos a nivel físico y social, algunas operaciones han logrado provocar disrupciones potencialmente mortales en la atención de salud y daños económicos severos en las compañías occidentales. Dichos acontecimientos subrayan la importancia de un rápido desarrollo de capacidades y de una cooperación extensa dirigida a mejorar la postura de seguridad y a crear resiliencia en la sociedad.

Desde una perspectiva más operacional, de acuerdo a la información disponible en fuentes abiertas, las operaciones cibernéticas exigen vasta preparación. Además de ejecutar misiones de reconocimiento para entender el objetivo, construir herramientas para infiltrarse y permanecer en el sistema y en la infraestructura de apoyo tecnológico (como lo son las conexiones protegidas y una red de servidores de mando y control); para que una operación funcione exitosamente parece ser necesario disponer de elementos no cibernéticos de apoyo, tales como identidades falsas en los países objetivo, la habilidad de generar, almacenar y transferir recursos financieros, y la capacidad que permita llevar las operaciones a la ubicación geográfica del objetivo

utilizando recursos humanos propios. Asimismo, particularmente en el caso de las operaciones de información, conocer al adversario y las vulnerabilidades de su sociedad es un factor clave para su eficiencia. Lo anterior es una buena noticia desde la perspectiva de los defensores, ya que sugiere que la ofensiva puede tener la ventaja en el combate por el dominio cibernético, pero que la defensa aún dispone de diversas vías cibernéticas y no cibernéticas para identificar y desmantelar las operaciones en curso y preparativos para ellas.

Finalmente, una gran cantidad de operaciones de alta visibilidad, cubiertas en detalle al público, indicarían, a primera vista, que las fuerzas cibernéticas que operan en el mundo están bastante provistas de recursos; sin embargo, de acuerdo al número de personas imputadas, incluyendo criminales cibernéticos buscados y atrapados, sugiere que el número de actores en el núcleo de las fuerzas cibernéticas no es tan grande ni tan talentoso. De hecho, los emprendedores más atrevidos pueden causar muchos problemas si las estructuras de soporte y de orientación política existen. Si bien hay muchos elementos que pueden contribuir a la cantidad relativamente baja de agentes operativos cibernéticos abiertamente identificados, tal como la falta de voluntad política para atribuir, imputar y procesar a dichos agentes, parece ser que la habilidad para obtener y mantener un talento de nivel mundial y para ejecutar operaciones de calidad es un pilar para tener éxito en el dominio cibernético también.

Escenarios Actuales, año 23, diciembre, Nº 4 (2018), pp. 27-34.
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

La ciberdefensa en España

General de División Carlos Gómez López de Medina*

Resumen:

Producto de la evolución que han experimentado las amenazas no tradicionales, en 2013 España creó el Mando Conjunto de Ciberdefensa (MCCD), el cual se estructura en el Sistema de Seguridad Nacional. A continuación, se explica cómo dicho país, a nivel Defensa, se ha organizado para enfrentar las ciberamenazas, abordando los organismos responsables, sus principales misiones y cómo estos interactúan con los otros organismos del Estado y Fuerzas Armadas. Asimismo, se profundiza en las lecciones aprendidas durante estos años de funcionamiento del MCCD tanto en el ámbito vinculado a la infraestructura, doctrina y recursos humanos, entre otros.

Summary:

As a result of the evolution experienced by non-traditional threats, in 2013, Spain created the Joint Cyberdefense Command (MCCD), which structure is based on the National Security System. Next, he explains how Spain, at the level of defense, has organized itself to face cyberthreats, mentioning the responsible organizations, their main tasks, and how they interact with the other governmental organizations and the Armed Forces. Additionally, the speaker delves into the lessons learned during the function period of the MCCD, in the field of infrastructure, doctrine, and human resources, amongst others.

Palabras Clave
España
Mando Conjunto de Ciberdefensa (MCCD)
Seguridad nacional
Ciberespacio
Ciberseguridad

Keywords
Spain
Joint Cyberdefense Command (MCCD)
National security
Cyberspace
Cybersecurity

Mi intención es tratar "La ciberdefensa en España", vista desde el punto de vista del Ministerio de Defensa. Les proporcionaré una información que considero necesaria para ponerles en contexto, haré una breve descripción de mi antigua unidad, el Mando Conjunto de Ciberdefensa

* Oficial del Ejército del Aire de España. Cuenta con una amplia trayectoria en la implementación de numerosos proyectos como el diseño e implantación del sistema de defensa aérea de Canarias, la realización de mejoras al sistema de defensa aérea de la península y baleares, así como en la redacción de la documentación española del "Air Command and Control System (ACCS) Master Plan". Entre sus diversos cargos, se ha desempeñado como experto en la NATO ACCS Management Agency, en Bruselas. En el Mando del Apoyo Logístico lideró el Programa de Mando y Control Aéreo en la Dirección de Sistemas de Armas. Además, fue Jefe del Grupo de Transmisiones del Ejército del Aire (GRUTRA), participando en la integración de la Red de Microondas del Ejército del Aire en el actual Sistema Conjunto de Telecomunicaciones Militares. Fue Jefe del Grupo Central de Mando y Control y posteriormente Subdirector de Gestión de Programas de la Dirección de Sistemas de Armas. Desde el año 2013 se desempeñó como Comandante Jefe del Mando Conjunto de Ciberdefensa; cargo que ha entregado recientemente.

(MCCD), y pasaré a continuación a la que estimo es la parte más significativa de la ponencia: ¿qué hemos aprendido desde la creación del MCCD en 2013? Finalizaré con unas conclusiones.

Para comenzar, los siguientes son los documentos relevantes para la Ciberseguridad Nacional en España:

- Ley 36/2015, de Seguridad Nacional:[1] tiene por objeto regular los principios básicos, órganos superiores, autoridades y los componentes fundamentales de la Seguridad Nacional; el Sistema de Seguridad Nacional, su dirección, organización y coordinación; la gestión de crisis y la contribución de recursos a la Seguridad Nacional.
- Real Decreto-Ley 12/2018, de Seguridad de las redes y sistemas de información:[2] este transpone al ordenamiento jurídico español la Directiva 2016/1148 de la Unión Europea, conocida como Directiva NIS, y tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, así como establecer un sistema de notificación de incidentes en nuestro país. Su contenido trasciende a la propia Directiva y aborda determinados aspectos que permitirán reforzar la ciberseguridad a nivel nacional, extendiendo su aplicación a ámbitos que se consideran fundamentales para ofrecer un enfoque global y cohesionado, adaptado a las particularidades de España.
- Estrategia de Seguridad Nacional 2017:[3] es el marco de referencia para la Política de Seguridad Nacional, una Política de Estado que concibe la seguridad de forma amplia al servicio del ciudadano y del Estado. La Estrategia actual (2017) profundiza en los conceptos y las líneas de acción definidas en 2013, y avanza en la adaptación de dicha política y de los instrumentos y recursos del Estado que la conforman ante un entorno de seguridad en cambio constante.
- Estrategia de Ciberseguridad Nacional 2013:[4] esta es el marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía. Para el logro de sus objetivos, la Estrategia crea una estructura orgánica que se integra en el marco del Sistema de Seguridad Nacional.

A continuación, cito los organismos que considero más importantes, a nivel nacional, con responsabilidades en la Ciberseguridad Nacional.

- Consejo de Seguridad Nacional:[5] en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional, así como ejercer las funciones que se le atribuyan en la Ley de Seguridad Nacional y se le asignen por su reglamento.
- Consejo Nacional de Ciberseguridad:[6] es un órgano colegiado de apoyo al Consejo de Seguridad Nacional. El Consejo Nacional de Ciberseguridad se crea por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013 y se reunió por primera vez el 25 de febrero de 2014. Su misión es reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas administraciones públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilitará la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional. Se significa que el cargo de vocal del Ministerio de Defensa en este Consejo es desempeñado por el Comandante del MCCD.

1 https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389
2 https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257
3 http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017
4 http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional
5 http://www.dsn.gob.es/es/sistema-seguridad-nacional/consejo-seguridad-nacional
6 http://www.dsn.gob.es/es/sistema-seguridad-nacional/comités-especializados/consejo-nacional-ciberseguridad#collapseTwo

- Departamento de Seguridad Nacional.[7]
- Ministerio de Defensa:
  - Centro Criptológico Nacional,[8] perteneciente al Centro Nacional de Inteligencia.
  - Mando Conjunto de Ciberdefensa, perteneciente al Estado Mayor de la Defensa.[9]
- Ministerio del Interior.[10]
- Secretaría de Estado para el Avance Digital:[11] perteneciente al Ministerio de Economía y Empresa.

El Mando Conjunto de Ciberdefensa

El MCCD fue creado el 19 de febrero de 2013 por el ministro de Defensa Excmo. Sr. D. Pedro Morenés y Eulate, siendo jefe de Estado Mayor de la Defensa (JEMAD) el almirante general Excmo. Sr. D. Fernando García Sánchez. El motivo para crear el MCCD fue hacer frente al creciente riesgo que suponían las ciberamenazas para la Defensa Nacional, en general, y para el Ministerio de Defensa, en particular.

Se decidió que fuese una unidad conjunta, integrada fundamentalmente por personal militar perteneciente a los Ejércitos y la Armada, con dependencia directa del JEMAD.

7 http://www.dsn.gob.es/es/sistema-seguridad-nacional/departamento-seguridad-nacional
8 https://www.ccn.cni.es/index.php/es/
9 http://www.emad.mde.es
10 http://www.interior.gob.es
11 http://www.mineco.gob.es/portal/site/mineco/avancedigital

La misión del MCCD, según el art.15 del Real Decreto 872/2014,[12] es el planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudiera tener encomendadas, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional.

Según el Concepto de Ciberdefensa Militar (2011) del JEMAD, el MCCD debía obtener tres capacidades para cumplir la misión asignada. Estas eran: la capacidad de defensa, que debía ser preventiva, proactiva y reactiva; capacidad de explotación para proporcionar alerta temprana, conocimiento de la situación e inteligencia táctica; y la capacidad de Respuesta o ataque, bajo los condicionantes de oportunidad, legitimidad y proporcionalidad.

Los cometidos del MCCD incluyen las operaciones militares defensivas y ofensivas en el ciberespacio y la concienciación, formación y adiestramiento en ciberdefensa.

Operaciones defensivas: el comandante del MCCD (CMCCD) es responsable de la defensa del ciberespacio, de responsabilidad del Ministerio de Defensa. Constituye la misión permanente (24/7) del MCCD, según el Plan de Operaciones Marco (OPLAN Marco) del comandante del Mando de Operaciones (CMOPS), que es el comandante de la Fuerza Conjunta a nivel operacional. Para un mayor conocimiento, se puede revisar el documento "Doctrina para el empleo de las Fuerzas Armadas" (PDC-01).[13]

El planeamiento, conducción y control de las operaciones se centraliza en el CERT[14] del Ministerio de Defensa (ESPDef-CERT), operado por el MCCD. La ejecución se descentraliza, delegándola a los Centros de Operaciones de Seguridad (COS) del propio MCCD, Ejércitos y Armada (OPLAN Derivado de Ciberdefensa, enero 2015).

Los COS de los Ejércitos y Armada realizan funciones de defensa de sus sistemas específicos y sistemas de armas. En tanto, el MCCD coopera con CERTs nacionales e internacionales, en representación del Ministerio de Defensa.

Operaciones ofensivas: el MCCD obtiene información del ciberespacio en beneficio del Centro de Inteligencia de las Fuerzas Armadas (CIFAS), del Mando de Operaciones (MOPS) y del propio MCCD.

Las operaciones de ataque se realizan según los distintos Planes de Operaciones del CMOPS, conforme a las RoEs[15] pertinentes y siguiendo los criterios mencionados anteriormente de oportunidad, legitimidad y proporcionalidad. En el caso de las operaciones ofensivas, tanto su planeamiento como su conducción y ejecución es realizada por el MCCD. No se asignan cometidos ni a los Ejércitos ni a la Armada.

Concienciación, formación y adiestramiento: el MCCD es responsable de su definición, dirección y coordinación para todo el Ministerio de Defensa (Orden DEF/166/2015).[16]

¿Qué hemos aprendido en cinco años?

Para revisar las enseñanzas obtenidas desde la creación del MCCD en 2013, utilizaré la metodología MIRADO, en la que se analizan las áreas de material, infraestructura, recursos humanos, adiestramiento, doctrina y organización.

12 https://www.boe.es/buscar/doc.php?id=BOE-A-2014-10520
13 http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/PDC-01_A_Doctrina_empleo_FAS_27feb2018.pdf
14 CERT: *Computer Emergency Response Team*
15 RoE: *Rules of Engagement*
16 https://www.boe.es/buscar/act.php?id=BOE-A-2015-1232

Material: se han utilizado fundamentalmente productos comerciales tanto en hardware como en software. Hemos evitado "reinventar la rueda" y sí hemos tratado de desarrollar nuevas ciberherramientas con criterios de eficacia y eficiencia. En este proceso, el MCCD participa en proyectos nacionales en asociación con la industria y/o la universidad, así como también en programas internacionales. Además, se han hecho desarrollos con recursos orgánicos del MCCD. La experiencia ha demostrado, hasta ahora, que los proyectos internacionales requieren de un excesivo tiempo y que el apoyo proporcionado por la universidad es muy eficiente. Disponer de capacidad de desarrollo con recursos propios del MCCD se ha mostrado vital en numerosas ocasiones.

En cuanto al sostenimiento de capacidades obtenidas, se ha llegado a la solución mixta de hacerlo con recursos orgánicos propios del MCCD y mediante el apoyo de la industria, obtenido por medio de contratos plurianuales.

Infraestructura (obra civil): en el momento de la creación del MCCD, España sufría una crisis económica muy significativa. Este hecho obligó a utilizar las infraestructuras disponibles y a hacer en ellas modificaciones y ampliaciones de coste reducido, teniendo que adaptar la operación a esas limitaciones. Posteriormente, aprovechando la mejoría de la situación económica, se han diseñado y construido nuevas infraestructuras, teniendo presente, por orden de importancia, la misión, cometidos, número de personas y la necesidad de cooperar con la industria y universidad.

Recursos humanos: el MCCD está integrado por personal de tres procedencias distintas. El personal militar es ampliamente el más numeroso, pertenece al Ejército de Tierra, la Armada y al Ejército del Aire, y están presentes todos los empleos en las categorías de oficiales, suboficiales y tropa/marinería, tanto de los Cuerpos Generales como de los Cuerpos de Ingenieros y Cuerpo Jurídico. Se cuenta también con personal civil funcionario de la administración que, además de aportar capacidad técnica, normalmente proporciona más continuidad en el puesto de trabajo que el personal militar. Finalmente, el MCCD dispone de personal civil procedente de contratos de asistencia técnica, que es una forma muy flexible de obtener capacidad, adecuando los recursos humanos a las necesidades operativas y a la disponibilidad económica. En todos los casos, el personal debe contar con una habilitación personal de seguridad, en el nivel que corresponda, según los criterios nacionales, de la Unión Europea y de la OTAN. La combinación de orígenes utilizada se ha mostrado muy eficaz y enriquecedora para todos.

La definición de puestos de trabajo y la certificación de niveles operativos, normalmente cuatro, para cada puesto ha sido muy útil para establecer los itinerarios formativos del personal del MCCD.

La operación permanente ha supuesto definir también una serie de puestos de trabajo 24/7, atendidos por varias personas en turnos.

Hay algunas iniciativas para crear una Ciber-Reserva estratégica, que permita hacer frente a situaciones excepcionales. Esta es una solución adoptada por algunas naciones occidentales que manifiestan estar satisfechas con los resultados obtenidos.

Adiestramiento: por su especial importancia, desglosaré este apartado en Concienciación, Formación y Adiestramiento. Como indicaba anteriormente, el MCCD es responsable de su definición, dirección y coordinación para todo el Ministerio de Defensa.

Concienciación

La comunidad objetivo para concienciar es la totalidad del personal del Ministerio de Defensa (140.000 personas), e incluso sus propias familias, que pueden constituir un "camino" para acceder a ellos. El Plan de Concienciación en Ciberdefensa (CONCIBE) está en vigor desde diciembre de 2015. El Plan CONCIBE se articula en campañas.

La primera de ellas ("Si estás conectado estás en riesgo"), ya finalizada, ha generado multitud de acciones de concienciación, incluyendo un curso on-line (realizado por miles de usuarios), conferencias a "grupos de riesgo" (contingentes de relevo en las operaciones, agregados militares, etc.) y boletines informativos quincenales, que se distribuyen masivamente por correo electrónico. La segunda campaña ("Delante del teclado todos somos combatientes") se inició hace unos meses. La experiencia ha demostrado que la inversión en concienciación es extraordinariamente eficiente, una pequeña inversión proporciona un aumento importante en la seguridad de los sistemas de información. No hay que olvidar que un usuario concienciado constituye la primera línea de defensa del sistema que utiliza. En cambio, un usuario que no está concienciado se convierte en el elemento más débil y de más riesgo para ese mismo sistema.

Formación

Desde el principio, fuimos conscientes de que era necesario y urgente capacitar técnicamente en ciberdefensa al personal que iba a trabajar en esta nueva capacidad operativa y que también había que proporcionarles titulaciones oficiales del Ministerio de Defensa. Pensamos en crear una escuela de ciberdefensa, pero llegamos a la conclusión de que era más eficaz y eficiente apoyarnos en las muy experimentadas escuelas CIS (Communication and Information Systems) de los Ejércitos y la Armada, añadiéndoles los recursos que fueran necesarios.

Para ello, se elaboró el Plan de Formación en Ciberdefensa (FORCIBE), en vigor desde marzo de 2015, que incluye los niveles de capacitación a alcanzar. El Plan FORCIBE recoge distintos cursos. Entre ellos destacan los denominados "Básico", liderado por la Armada, "Avanzado", liderado por el Ejército de Tierra, y los "Orientados al puesto de trabajo", liderados por el Ejército del Aire. El MCCD define el perfil de egreso, las condiciones de acceso y la distribución de plazas entre todo el Ministerio. Los Ejércitos y la Armada cuentan con el apoyo de la industria y la universidad para impartir los cursos. Los resultados están siendo muy satisfactorios desde que se iniciaron los cursos, en 2016.

Adiestramiento

También se ha elaborado un Plan de Adiestramiento en Ciberdefensa (ADCIBE) que tiene por objetivo mantener la capacidad operativa de las unidades de ciberdefensa (MCCD y Centros de Operaciones de Seguridad de los Ejércitos y Armada). El adiestramiento se basa fundamentalmente en la realización de ciberejercicios. Estos ciberejercicios, de muy variada complejidad y alcance, permiten certificar y practicar la doctrina, así como aprender de otras naciones y organizaciones. Además, son esenciales para facilitar la cooperación entre aliados. Desde el principio decidimos participar en todos los ciberejercicios que nos ofrecía la OTAN y obtener una capacidad nacional para diseñarlos y realizarlos. Por este motivo, desarrollamos un campo de maniobras virtual (cyberrange) propio, que nos permite realizar ejercicios y probar productos, técnicas y procedimientos. Para aumentar la eficiencia, estamos externalizando parte del adiestramiento a la industria.

Doctrina

Pronto aprendimos que no hay paz en el ciberespacio. Se reciben ataques permanentemente, aunque su importancia y agresividad es muy variable. Desde el inicio aplicamos el principio de que el ciberespacio es el 5º ámbito de las operaciones, principio que fue confirmado oficialmente por la OTAN en julio de 2016.

Inicialmente, éramos incapaces de generar doctrina y procedimientos operativos de ciberdefensa. Comenzamos trasladando nuestras experiencias previas, obtenidas de los ámbitos "tradicionales" (tierra, mar y aire). Personalmente, siempre he encontrado grandes similitudes entre la defensa del ciberespacio y la defensa del espacio aéreo; en ambas existen las fases de detección, identificación, calificación y neutralización, y en ambas es muy importante la

alerta previa y la coordinación con los aliados. Para poder generar doctrina y procedimientos, fue esencial participar en ciberejercicios y, sobre todo, obtener experiencia real propia. En este sentido, fue extremadamente importante ser capaces de obtener, explotar y diseminar inteligencia de ciberamenazas (Cyber Threat Intelligence), que constituye la inteligencia táctica en el ciberespacio.

Hemos comprendido que la integración de la ciberdefensa en "todas" las operaciones es una necesidad y que, por tanto, debe estar presente en todas las fases del planeamiento. En este sentido, consideramos crítico disponer de un concepto de operaciones que facilite la integración mencionada. Por otra parte, es importante que la doctrina nacional esté alineada con la de organizaciones internacionales, en nuestro caso con la OTAN y la Unión Europea, con las ventajas e inconvenientes derivados del hecho de que estas organizaciones internacionales también están actualmente dando sus primeros pasos en la elaboración de doctrina y las naciones miembros intervenimos en dicha elaboración.

Organización

En relación con la organización del MCCD, hay que destacar que se trata de una unidad conjunta, integrada por personal civil y militar. Que el personal militar constituye la gran mayoría, que procede de los Ejércitos y la Armada. El MCCD está integrado en la estructura de la Fuerza Conjunta, en concreto en el Núcleo de Fuerza 1, por tener asignada la misión permanente de defender las redes y sistemas de información que son responsabilidad del Ministerio de Defensa.

El Comandante del MCCD tiene una dependencia directa, tanto orgánica como operativa del JEMAD, y una dependencia directa operativa del CMOPS cuando el MCCD opera integrado en un Plan de Operaciones, que es lo habitual.

Hay que resaltar que, en la estructura de Fuerza Conjunta, el MCCD tiene el papel de Mando Componente del Ciberespacio, constituyendo el quinto Mando Componente en dicha Fuerza, añadiéndose a los Mandos Terrestre, Naval, Aéreo y Operaciones Especiales. En España, la ciberdefensa está orientada a las operaciones, destacando la enorme sinergia generada por la convivencia, en la misma unidad, de personal especializado en acciones defensivas con el que lo está en acciones ofensivas.

Conclusiones

Como conclusiones más relevantes de la ponencia, destacaría las siguientes:

a. Es esencial disponer de un organismo de coordinación a nivel nacional como el Consejo Nacional de Ciberseguridad que tenemos en España.

b. Es una decisión acertada que la responsabilidad de la ciberdefensa recaiga en una unidad conjunta con dependencia directa del JEMAD. Este es un modelo cada vez más frecuente en las naciones occidentales.

c. El modelo seguido por España es el de la ciberdefensa orientada a las operaciones, que es también el más frecuente en las naciones occidentales.

d. El mayor desafío en la creación de la unidad es obtener y retener al personal adecuado, en calidad y en cantidad.

e. Es una ventaja que el personal militar que integra la unidad tenga experiencia en otros ámbitos operativos (tierra, mar, aire).

f. Es muy importante invertir en concienciación. Es la acción más eficiente que podemos llevar a cabo para mejorar el nivel de ciberseguridad.

g. Hay que disponer de un Concepto de Operación en Ciberdefensa. Normalmente, es difícil de obtener debido a posiciones frecuentemente encontradas de ejércitos y órganos conjuntos, pero es absolutamente necesario.

h. Resaltar la sinergia generada por la coexistencia de personal defensivo y ofensivo en la misma unidad.

i. Hay que aumentar progresivamente el reclutamiento y la inversión económica. No es necesario que sean muy elevados al principio, pero sí han de tener un crecimiento constante en el tiempo y al ritmo adecuado.

j. Hemos aprendido que "lo mejor es enemigo de lo bueno". Hay que decidir, probar y corregir, manteniendo el riesgo controlado, pero no hay que temer al error, hay que temer a la pasividad.

k. Es esencial la cooperación entre aliados en el adiestramiento (ciberejercicios) y en la elaboración de doctrina. Es necesaria para conocerse y poder operar juntos.

Escenarios Actuales, año 23, diciembre, Nº 4 (2018), pp. 35-43.
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

La contribución de las ciberoperaciones en la defensa del Reino Unido

Brigadier Mark Proctor (OBE)*

Resumen:

El rol que han adquirido las ciberoperaciones es cada vez más relevante, considerando los crecientes desafíos que impone el ciberespacio. A continuación, se abordará la experiencia desarrollada por el Reino Unido, a través de las diversas políticas implementadas y el desarrollo de capacidades ofensivas y defensivas de las Fuerzas Armadas en contribución de la seguridad nacional. Cabe destacar, también, la relevancia que se le ha asignado a la capacitación y entrenamiento del personal a lo largo de las distintas etapas de la carrera, permitiendo de esta forma contar con personal especializado en los distintos estamentos de la toma de decisiones.

Summary:

The role that cyberoperations have acquired is each time more relevant, taking in account the expanding challenges presented by cyberspace. The speaker addresses the experience obtained by the United Kingdom through policies and the development of offensive and defensive capabilities for the Armed Forces, in contribution to the National Security. It should be noted, as well, that the relevance assigned to the training of personnel throughout their careers has allowed to have having specialists in the decision-making structure.

Palabras Clave
Reino Unido
Cibercapacidades
Ciberespacio
Reserva cibernética
Disuasión

Keywords
United Kingdom
Cyber capabilities
Cyberspace
Cyber reserve
Deterrence

General Martínez, damas y caballeros, muchas gracias. Agradezco la oportunidad que me han brindado para poder hablar hoy. Debo señalar, en relación a los expositores anteriores, que mucho de lo que les voy a decir, si bien es similar, personalmente creo que es pertinente, quizás lo podamos juzgar después.

---

* Ingresó al Ejército Británico en el año 1991. Después de tres años de servicios como soldado, en virtud de su buen desempeño, ingresó a la Real Academia Militar de Sandhurst en el año 1995 y, luego de su egreso como Oficial, se integró al Cuerpo de Inteligencia. Posee una vasta experiencia en el área de inteligencia y ha participado de múltiples despliegues en operaciones, tanto en Irlanda del Norte como en Bosnia, Irak y Afganistán. Ejerció el mando del 2º Batallón de Inteligencia Militar y también se desempeñó como Subjefe Estado Mayor en el Cuartel General Conjunto Permanente del Reino Unido. En abril del presente año asumió el mando del Grupo de Actividades Conjuntas de Ciber y Electromagnéticas, liderando diversas unidades, dentro de las que se destaca el Grupo de Fuerzas Conjuntas de Ciber.

Mark Proctor

Me gustaría compartir con ustedes el pensamiento del Reino Unido acerca del rol de las ciberoperaciones en la Política de Defensa británica y en una variedad de políticas nacionales que tiene el gobierno. A continuación, explicaré cómo algunas de nuestras capacidades contribuyen a la seguridad nacional del Reino Unido, y si bien me enfoco en el rol de las fuerzas armadas, también voy a explicar cómo funciona con otras partes del gobierno del Reino Unido y las diferentes responsabilidades que tiene nuestro sistema nacional.

He considerado, deliberadamente, presentar una interpretación amplia de la ciberdefensa. Lo central de mi posición es que la defensa del ciberespacio es superada en importancia por la defensa de lo cibernético.

Desde el término de la Guerra Fría, el Reino Unido ha invertido considerables esfuerzos para implementar y mejorar sus doctrinas de defensa. Durante este período se produjo una transición desde los conceptos tradicionales hacia la interrogante ¿cómo puede existir una mejor gestión?, que es más efectiva en contra de la habilidad de lucha de nuestro adversario. Esto también se aplica a las diferentes herramientas que tenemos para combatir los distintos ataques y lograr nuestros objetivos estratégicos.

Este cambio gradual en el énfasis nos permite, como fuerzas armadas, generar una revisión de la estrategia de defensa y seguridad de 2010, como también afrontar los conflictos internacionales. Esto ha significado un importante cambio en la dirección, que continúa afectando la modernización y el programa de defensa del Reino Unido.

Posteriormente, se generó un programa nacional de inversión en cibercapacidades a lo largo de todo el Reino Unido y sus instituciones gubernamentales, lo que incrementó nuestra convicción de que estas herramientas son esenciales para tener éxito en el campo de batalla virtual. En 2017, debido a la preocupación por los cambios

Escenarios Actuales, año 23, diciembre, Nº 4, 2018
ISSN 0717-6805

que existían, especialmente en el entorno estratégico, iniciamos una revisión de las capacidades de seguridad nacional, estudio que fue publicado en marzo de este año y que permitió articular las actualizaciones del pensamiento militar para la defensa. Este informe reconoce que muchísimos de los esfuerzos estaban bajo el umbral que generaría una respuesta del Estado y que, por lo tanto, existía un desafío para los tomadores de decisiones y generadores de políticas nacionales e internacionales.

También en marzo, durante el discurso de nuestro jefe de Inteligencia de la Defensa sobre la situación de seguridad global, observó que la guerra está siendo cada vez más estratégica e incluye características de competencias de un espectro más amplio, con nuevos dominios para la defensa, tales como el ciberespacio.

La seguridad del Estado también ha desarrollado un programa de modernización que nos dice que la defensa debe estar dispuesta y lista para analizar las operaciones de nuestros adversarios, y que para ello requiere de un rol fundamental dentro de un enfoque integral para la seguridad nacional, además del fortalecimiento de nuestra red global de alianzas y asociaciones. Nuestras fuerzas armadas, principalmente, deben estar listas para responder rápidamente a crisis futuras y en nuestros términos.

Acerca de los roles específicos de nuestras fuerzas en el ciberespacio, la Estrategia de Defensa y Seguridad de 2015 reconoce que el rol de las fuerzas armadas es contribuir a la estrategia de las siguientes formas:

- Primero, debe tener grandes defensas en el contexto del Reino Unido, en referencia a la habilidad que tienen nuestras fuerzas armadas para defenderse en el ciberespacio.
- En segundo lugar, tenemos que ser capaces de proyectar poder en el ciberespacio al igual que lo hacemos en otros ambientes operativos.
- En tercer lugar, estar listos para asistir al Reino Unido y su gobierno en un incidente cibernético importante, al igual como se haría con las diferentes fuerzas mencionadas anteriormente.
- Finalmente, ser capaces de responder a un ciberataque de la misma forma como se haría en otro tipo de ataque y con las capacidades que sean las más apropiadas, pero no necesariamente las cibernéticas.

El rol cibernético implica que las capacidades de defensa del Reino Unido deben incluir una combinación de capacidades de defensa y también de ofensiva, lo que es propio de las estrategias de alta defensa que tenemos. Un ejemplo sería la Doctrina Táctica de las fuerzas armadas actual, que tiene como fuerza central la ofensiva y también es consciente de la imposición de los costos. La combinación óptima de estas dos estrategias nos permite tener un mayor apoyo y evitar las desventajas. En este punto, nuestro conocimiento de ciberseguridad nos dice lo difícil que es asegurar los sistemas resilientes, no podemos confiar de manera absoluta en una postura pasiva en base a la ciberseguridad, porque sabemos que el atacante tendrá sus ventajas.

Sin embargo, debemos recordar que esta certeza de nuestros sistemas se entenderá como una amenaza para potenciales ataques y será la consecuencia de sus propios sistemas, esto puede amplificar las diferentes capacidades de defensa que tengamos.

En noviembre de 2015, se confirmó que el Reino Unido estaba desarrollando una capacidad dedicada a contrarrestar los ataques cibernéticos a un espectro completo y se anunció que la defensa está entregando esta capacidad en asociación con las oficinas de comunicación del gobierno y las autoridades de inteligencia a través del programa cibernético de Defensa.

Este programa está mejorando las habilidades y talentos que tiene el Ministerio de Defensa y las oficinas de comunicación del gobierno para establecer una capacidad ofensiva de clase mundial. Hemos confirmado

previamente que las fuerzas armadas tienen esta capacidad como parte de su campaña en contra de diferentes grupos, como DAESH (ISIS) en Medio Oriente.

Me gustaría destacar la importancia de otro compromiso de la Estrategia de 2015, un Centro Nacional de Ciberseguridad (NCSC) del Reino Unido, lo que refleja el rol primordial que tiene para el gobierno la ciberdefensa en la seguridad, más allá de los límites de sus propias redes y sistemas, como se mencionó anteriormente.

La NCSC comenzó su operación en octubre de 2016, para lo cual reunió a muchas organizaciones ya existentes que tenían un rol en ciberseguridad nacional, con el propósito de crear una única organización que, a su vez, es parte de nuestra oficina de bienestar. Por motivos de tiempo, no es posible discutir esto en términos extensos ni detallando todas las actividades nacionales, pero voy a centrarme en cuál es la relación específica con el Ministerio de Defensa.

Un elemento clave de la relación es compartir información del ciberespacio sobre amenazas, lo que ayuda al Ministerio de Defensa a proteger su sistema de información y a intercambiar evaluaciones. La NCSC además juega un rol fundamental, ya que proporciona consejos sobre ciberseguridad a nuestra industria de defensa, y esto no es una responsabilidad del Ministerio de Defensa. Sin embargo, el Ministerio es responsable de apoyar a la NCSC en caso de incidentes significativos como parte de su rol de apoyo al gobierno del Reino Unido. Es por ello que consideramos esta relación como una parte integral, que, además, permite compartir el personal. Por estos motivos estamos felices con los logros que se han obtenido hasta la fecha.

Las operaciones tienen algunas similitudes con las operaciones convencionales, pero las diferencias son los focos de interés. Las operaciones cibernéticas tienen un amplio rango, pueden ser anónimas, simétricas y pueden lograr diferentes objetivos al ser muy versátiles.

El alcance de lo cibernético y los efectos de la proximidad de los atacantes significan un gran potencial para influenciar a los tomadores de decisión. Con estos factores en mente, las operaciones cibernéticas también pueden ser dirigidas a las siguientes cosas:

- En primer lugar, pueden moldear y determinar el comportamiento de los adversarios.
- En segundo lugar, pueden constreñir y destruir los comportamientos militares para disminuir el daño.
- Finalmente, pueden apoyar el combate tradicional al negar las capacidades del adversario y combatir la infraestructura.

Como parte de esta evolución, es importante que las fuerzas armadas sean realistas acerca de lo que pueden lograr las innovaciones que tendrán a largo plazo. Como nación debemos ser rigurosos al considerar el amplio rango de la influencia y las herramientas económicas a nuestra disposición e imaginativos en cómo las vamos a utilizar en conjunto para lograr los objetivos de seguridad nacional.

Esta fusión nos ha permitido analizar y operar de manera más eficiente en un mundo tan volátil y que cambia constantemente. También debemos reconocer que muchas de las capacidades que entrega a los objetivos de defensa nacionales están fuera de los tradicionales departamentos gubernamentales.

También podría decir que la misma transición se requiere en el espacio de diferentes gobiernos, tantos nacionales como internacionales. Debemos desarrollar un plan de acercamiento y coordinación que nos permita lograr el mayor beneficio de esta fusión entre gobiernos. También se debería incluir la focalización en la toma de decisiones de los adversarios y la planificación militar para lograr los efectos deseados.

A pesar de las características únicas de las ciberoperaciones, las fuerzas armadas del Reino Unido han concluido que, generalmente, es un error pensar que las ciberoperaciones pueden ser tratadas de manera aislada como operativos especiales o algo puramente técnico, por ello debemos normalizar las operaciones cibernéticas.

De manera similar, existe otro aspecto de las capacidades militares tradicionales que puede ser un aporte a las ciberoperaciones o del cual las ciberoperaciones pueden obtener lecciones valiosas. En las operaciones modernas, las fuerzas militares tienen que trabajar con otras áreas del gobierno como Defensa nacional y organizaciones de seguridad, integran cada vez más su inteligencia estratégica en el Mando y Control, así como sus capacidades de planificación, todas apoyadas por el entrenamiento y ejercicios.

Para realizar estas operaciones cibernéticas lideradas por el Ejército, existe la necesidad de tener una mayor comprensión y profundidad de las fortalezas y debilidades de los posibles adversarios, lo cual debe realizarse en paralelo a entender nuestras propias fortalezas y debilidades.

A continuación, me voy a referir a la influencia y la disuasión. Como forma de influencia, la disuasión es un efecto cognitivo, por lo tanto, es difícil predecir su efectividad con un grado elevado de confianza. Siempre hay incertidumbre, con frecuencia significativa, a la hora de intentar influir en las decisiones de otros, particularmente en una época de alta tensión, por este motivo la comprensión tradicional de las órdenes de batalla, capacidades militares y geografía, entre otros, no es suficiente y tampoco pueden ser los únicos factores para tener un panorama completo.

Por otro lado, entender los elementos gubernamentales y sociales se está volviendo cada vez más importante. Las estructuras de Mando y Control tienen que estar establecidas no solo para dar coherencia a las campañas, sino también para apoyar el intercambio de información oportuno y preciso, así como para la colaboración y toma de decisiones.

Las autoridades y organizaciones también tienen que tener procesos ágiles para delegar autoridad en los niveles inferiores, que permitan una aplicación oportuna de los distintos mandatos. Las operaciones militares en cualquier dominio deben estar sincronizadas con actividades diplomáticas, económicas y de información, como parte de una estrategia nacional e internacional más amplia.

Esto nos deja con un poder estatal que puede tener efectos potentes al usarse en forma colectiva, lo que requiere de una integración exitosa, con amplia variedad de efectos complementarios, de tal forma que reduzca el potencial conflicto y la agresión.

Es necesario que la planificación en todos los departamentos del gobierno sea realizada en un nivel más amplio que solamente los temas militares, asegurándose, además, de que todas las partes tengan un estándar en común de competencias de planificación, tecnologías y doctrinas en común, así como las mismas capacidades para enfocarse a largo plazo.

Se necesita también de una interoperatividad más que de una simple interconectividad. Tanto a nivel gubernamental como militar se debe mejorar la comprensión de cómo lograr efectos disuasorios.

Actualmente, diría que se asume en gran medida que los planificadores van a saber cómo hacer esto. El desafío es asegurar que la planificación sea basada en efectos disuasorios, las operaciones militares convencionales se han centrado en gran medida en esto.

La doctrina y entrenamiento del Reino Unido probablemente están optimizando lo anterior, pues hemos experimentado operaciones de información y operaciones psicológicas, y el personal militar con las competencias correctas ha sido limitado. Este problema se complica con las medidas de seguridad que se usan para restringir el acceso al conocimiento detallado de nuestras capacidades ciberofensivas. Así la mayoría del personal militar va a tener poco entendimiento de las distintas capacidades que podrían implementarse y cómo estas funcionan, incluso en el nivel más básico.

El punto es que el entrenamiento y la educación son áreas cruciales. Es posible aprender de nuestro personal, así como de otros roles de seguridad nacional y sobre cómo realizan su trabajo.

No podemos asumir que todo el gobierno o que este enfoque de integración van a ser efectivos y rápidos sin la debida práctica. Es un requerimiento crucial un régimen de ejercicios que se adapte a nuestras ambiciones y que permita que los procesos se pongan a prueba y que se mejoren.

En cuanto a la disuasión, esta debe ser creíble, y un oponente debe percibir una combinación tanto de amenaza como de incentivo, para que efectivamente vean que existe una voluntad de llevarla a la práctica, lo que requiere mantener elementos de capacidades creíbles y críticas en el tiempo. La planificación disuasoria debería ser una actividad continua, realizada por analistas permanentemente asignados a esta tarea.

Reconocemos también que la seguridad se fortalece a través de la colaboración internacional, mientras que la seguridad nacional se integra y es dependiente de la seguridad de nuestros socios y vecinos. Esto funciona igualmente para la disuasión, donde las acciones colectivas amplifican los posibles impactos a una escala que una nación no podría lograr por sí sola. Un buen ejemplo de una acción colectiva es el uso de la atribución para determinar actividades cibernéticas maliciosas, este es un enfoque que el Reino Unido ha utilizado ampliamente. Para ilustrar este punto, en mayo de 2017 el Servicio de Salud del Reino Unido fue afectada por uno de estos ciberataques, a través del uso de capacidades forenses avanzadas se pudo identificar a WannaCry y a los actores norcoreanos detras de él en diciembre de 2017, en paralelo a los anuncios oficiales de Estados Unidos, Australia, Canadá, Nueva Zelandia, Dinamarca y Japón.

Ahora bien, respecto a los detalles del Ministerio de Defensa y sus aproximaciones a las cibercapacidades, nuestras actividades de desarrollo las maneja, principalmente, nuestro propio programa cibernético y gran parte de este financiamiento está dedicado a mejorar las cibercapacidades defensivas, lo que es resultado de las decisiones tomadas en el SCR 2015. Las escalas en los acuerdos defensivos son inmensas debido al tamaño de las redes, con alrededor de 300 mil usuarios que operan en distintos niveles de seguridad en todo el mundo.

Además, esos acuerdos defensivos tienen que mantenerse durante un tiempo importante en nuestras redes, las que a su vez han sido el proyecto más grande de su tipo en Europa.

A continuación vamos a abordar brevemente algunos elementos claves de nuestro trabajo defensivo cibernético: primero que todo, el Global Operations and Security Control Centre, GOSCC, es un centro de capacidades cibernéticas sofisticadas que existe para operar y defender nuestras redes, así como para proporcionar comunicaciones a nivel mundial en términos de defensa. El Ministerio de Defensa no se ha dejado estar en términos defensivos, y continúa revisando y modificando nuestras medidas de seguridad.

Actualmente, el foco está en un nuevo centro de operaciones de ciberseguridad, la inversión en este está teniendo lugar a medida que mejoramos la coordinación entre nuestras fuerzas existentes de ciberseguridad.

Desde que el secretario de Defensa anunció el centro, ha habido una tendencia a pasar de la palabra centro a capacidad, en un afán por reconocer que las distintas organizaciones que contribuyen a la ciberdefensa del Ministerio de Defensa no estarán ubicadas en un único lugar.

En 2016, nos comprometimos también, públicamente, a invertir 165 millones de libras cada 10 años en profundizar nuestro entendimiento sobre las cibervulnerabilidades de nuestras plataformas militares y de otros sistemas dependientes en el área cibernética. Hoy, esa inversión está destinada en parte a mi organización, la cual ayuda a dar prioridad en la planificación a los riesgos más significativos.

Por supuesto que los ataques siempre dependen de estas capacidades. Cabe destacar que la Asociación de Ciberdefensa y Protección fue una asociación del Ministerio de Defensa y la industria de defensa, y que el NCSC proporcionó un valioso apoyo a esta iniciativa, la que apunta a proteger nuestras capacidades militares al mejorar la defensa cibernética a través de la cadena de suministros, a la vez que se mantiene la inversión existente en las medidas de ciberseguridad.

Como parte de esta asociación, el Ministerio de Defensa ha especificado estándares de ciberseguridad que deben cumplirse para realizar un contrato, esto es parte de una serie más amplia de reformas para asegurarse de que se introduzcan nuevos equipos con distintos niveles de ciber-riesgos que sean apropiados para su rol.

En esta ponencia he hablado mucho sobre la contribución de las distintas cibercapacidades para la defensa del Reino Unido, ahora bien, todas estas capacidades dependen de las personas. Si bien estos operadores cibernéticos están altamente capacitados, debemos estar al tanto de la importancia del personal no especializado que compone la mayor parte de nuestras fuerzas.

Lo anterior es un punto crucial para la defensa de las ciberoperaciones, donde una única persona puede tomar una decisión incorrecta y hacer clic en un correo electrónico que abre la puerta a un ataque contra todos nuestros sistemas. Reducir este riesgo es complejo y que requiere de educación constante, donde el esfuerzo esté apoyado por una cultura cibernética. Es necesario tener claro estos procedimientos al usar los sistemas, así como diferentes aspectos de la vida militar.

En la guerra moderna, las consecuencias van a ser igual de importantes; afortunadamente existe una comprensión de esta amenaza. Sin embargo, hay un pequeño porcentaje de personas que dicen que es muy complicado mejorar esta cultura cibernética. El Ministerio de Defensa busca educar y entrenar al personal en ciberseguridad y operaciones cibernéticas en todas las etapas de su carrera en forma progresiva. Este proceso inicia en el reclutamiento, entrenamiento y sigue hasta los rangos de oficiales del alto mando, como un curso de toma de conciencia o clase magistral de ciberseguridad.

Esta Clase Magistral de Ciberseguridad es un curso ofrecido por nuestra, recientemente abierta, Escuela de Ciberdefensa, y es parte clave de nuestra academia defensiva, la que ha asumido la responsabilidad del ciberentrenamiento centralizado del personal de todos los servicios, de la industria de defensa y vigilancia, así como del personal de nuestros distintos socios en el gobierno. Esta capacitación va desde cursos técnicos hasta entrenamientos de alto nivel que educan a personas seleccionadas, y el nivel de maestría en ciberdefensa.

La inversión en la escuela de ciberdefensa refleja, desde el punto de vista del Reino Unido, que las personas capacitadas son fundamentales para la generación exitosa de capacidades ciberneticas en el Ejército. También hemos dado pasos para crear estas ciberoperaciones para nuestros reservistas militares, y hemos creado fuerzas de reserva conjunta cibernética en 2013, las cuales apoyan a las unidades regulares, así como a las distintas unidades cibernéticas.

La reserva cibernética es una unidad conjunta de personas cuidadosamente seleccionadas, que se les da la oportunidad de ser parte de la orgullosa historia e hitos de las reservas de la Armada, Ejército o la Real Fuerza Aérea. Hoy en día ha resultado ser bastante exitoso y este reclutamiento se mantiene extremadamente competitivo debido a la limitada cantidad de puestos disponibles y el alto calibre de los candidatos requeridos, lo que permite que nuestras fuerzas aprovechen un talento civil increíble, ya que estos reservistas también traen experiencia de nivel mundial de muchas partes de la industria de ciberseguridad, incluyendo la banca y finanzas. Por lo tanto, esta reserva cibernética conjunta sigue siendo un aporte significativo a nuestra seguridad nacional.

Finalmente, y para resumir, en este mundo cada vez más peligroso e impredecible, el rol de las fuerzas armadas se amplía en el ciberespacio para cumplir con los objetivos de políticas del Reino Unido, lo que incluye desarrollar una mayor huella operacional en base a nuestras cibercapacidades ofensivas y defensivas, para influir en el comportamiento de posibles adversarios.

Para lograr lo anterior, se requieren procesos correctos de Mando y Control que permitan tomar decisiones coherentes y efectivas en todo el gobierno. Es cada vez más importante determinar cómo aprovechar de mejor manera los planes militares, capacidades de inteligencia y operación, entre otras, para apoyar futuras acciones del gobierno.

Para la disuasión moderna es esencial desarrollar un entendimiento completo del riesgo de algunas acciones, pero también de la falta de acciones, de la explotación de vulnerabilidades, así como también de la protección de nuestra vulnerabilidad.

El éxito del Centro Nacional de Ciberseguridad es un referente para las actividades cibernéticas a nivel nacional dentro del Reino Unido, reflejando que el enfoque del Ministerio de Defensa es su propia red de extensión. Como ya se dijo, las dos organizaciones trabajan muy de cerca en una variedad de actividades.

La inversión militar en nuevas capacidades de defensa cibernéticas está aumentando como parte del programa cibernético del Ministerio de Defensa. Esta inversión incluye la Escuela de Defensa Cibernética, que otorga un mayor reconocimiento al personal capacitado, a los ciberespecialistas y al resto de las fuerzas armadas como elementos vitales para la defensa exitosa de las capacidades militares claves, así como del Reino Unido en general.

Habiendo dicho todo esto, nuestro viaje ciertamente no termina y probablemente nunca vaya a terminar. Sin embargo, así como estamos felices porque hemos aprendido, lo estamos al poder compartir nuestras experiencias, especialmente, con amigos como Chile.

Importante:

Los artículos presentados en esta edición especial de *Revista Escenarios Actuales*, corresponden a las ponencias presentadas durante el Seminario *Ciberespacio:* "desafíos a la seguridad y defensa de Chile en el siglo XXI", los que cuentan con la autorización de los autores para su difusión y publicación.

Asistentes al seminario

"Ciberespacio: desafíos a la seguridad y defensa de Chile en el siglo XXI"

Impreso en los Talleres del Instituto Geográfico Militar.
Avda. Santa Isabel 1651
Santiago, Chile

Centro de Estudios e
Investigaciones Militares

Bandera Nº 52, Santiago de Chile.
Teléfono: (56) 226683800
email: extension.cesim@ejercito.cl
escenariosactuales.cesim@ejercito.cl
www.cesim.cl

IGM TALLERES GRÁFICOS