Fuerza Aérea de Chile
Centro de Estudios Estratégicos y Aeroespaciales
Estrategia, Aeronáutica, Espacio, Tecnología & Innovación

BOLETÍN INFORMATIVO Y DE ANÁLISIS N° 38-2018 Santiago, 27 de Julio del 2018

"Ciberseguridad en Chile y en su Defensa"

Durante la ejecución de la Feria Internacional del Aire y del Espacio, el CEEA efectuó un seminario denominado "Cyberday", en el cual destacados expositores internacionales se refirieron a los desafíos que esta materia representa para el Estado y las formas en que la "inseguridad informática" está afectando hoy a las personas, las organizaciones y a la infraestructura crítica de los países. En ese contexto, el CEO del Centro Nacional de Ciberseguridad del Reino Unido, Ciaran Martin, Explicó cómo los modelos de ciberseguridad enfocados en proteger desde el Estado sólo los principales componentes de la seguridad de la infraestructura estatal, entregando a los privados la tarea de protegerse a sí mismos, no daba resultado y había obligado a una alianza público-privada en torno a la protección de todo aquello considerado infraestructura crítica del país, independiente de su condición privada o estatal. Para ello, explicó, fue necesario establecer una planificación estratégica que coordinara los esfuerzas multisectoriales para sumar esfuerzos, reducir interferencias y crear relaciones de desarrollo colectivo en un área que siempre se caracterizó por su hermeticidad.
Esta conceptualización del accionar en ciberdefensa también puede ser aplicado al sector Defensa, el cual, aunque tiene características particulares, también tiene relaciones de interdependencia con otros actores, tanto en cuanto al desarrollo de sistemas como en lo referido a políticas y técnicas.

Tal como está siendo incorporado en los conceptos doctrinarios de varias Fuerzas Aéreas del mundo y también en la Fuerza Aérea de Chile, a los 4 dominios actualmente asumidos (Terrestre, Marítimo, Aéreo y Espacial) se está agregando en la forma de quinto dominio el "ciberespacial", donde las Fuerzas Aéreas y toda la Defensa requieren actuar en la búsqueda del dominio de esta dimensión en beneficio de sus objetivos estratégicos. Allí, los conceptos tradicionales de "Situación Favorable", "Superioridad" y "Supremacía" y sus definiciones, que expresa la doctrina básica aeroespacial, tienen plena vigencia. Incluso la limitación referida a la temporalidad de los grados de control del aire, es aplicable a esta materia.

La disperso de la amenaza, que involucra desde actores estatales hasta ciberdelincuentes, representa una amenaza real para los sistemas militares, cuyos conductores deben enfrentar una suerte de carrera contra el tiempo para detectar en forma oportuna tales amenazas y establecer las medidas para neutralizarlas, así como –en el caso de tener una estrategia ofensiva- detectar las vulnerabilidades del adversario y explotarlas antes de que éste reaccione, en una versión "Cyber" del ya famoso OODA Loop del Coronel USAF John Boyd.

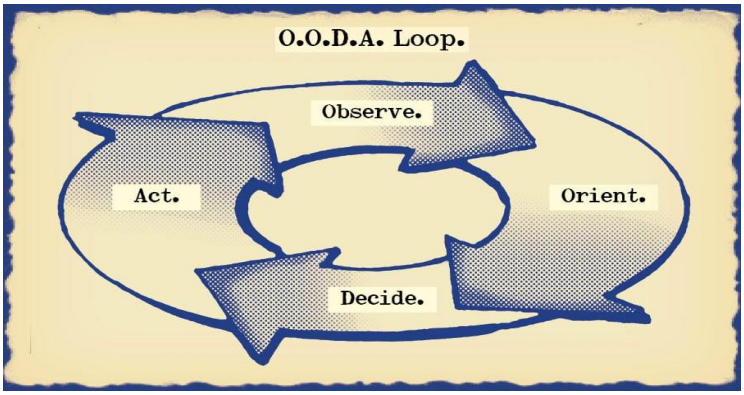

Figura 1: Concepto de OODA Loop

La alianza civil-militar es imprescindible, ya que los proveedores de sistemas y de servicios están directamente involucrados en el problema. Debido a ello y a la escala de sus investigaciones y programas de desarrollo, grandes proveedores representan una ventaja para desarrollar sistemas y medidas específicas para la Defensa. Los pequeños desarrolladores, normalmente son integradores de tecnologías que las grandes empresas han creado luego de millonarias inversiones, que deben beneficiar también a la Defensa, junto con representar una oportunidad de negocios para dichas empresas. En los Estados Unidos, empresas como IBM o Raytheon trabajan junto con las Instituciones de la Defensa en el manejo de riesgo cibernético, desde el diseño e implementación de sistemas hasta la supervisión de los administradores de esos sistemas. Esto representa un doble desafío: establecer las confianzas entre privados y los actores de la Defensa, como también –y esto puede resultar más complejo- establecer relaciones de confianza entre empresas que normalmente son competidoras.

Otro aspecto a considerar, radica en la importancia de no limitar el esfuerzo al mero desarrollo e implementación de sistemas, sino también al perfeccionamiento y capacitación continua de los operadores y a la investigación respecto de procesos. En la guerra en el dominio ciberespacial, la capacidad operativa del personal, sus procedimientos, doctrina y disciplina operacional resultan claves para obtener ventajas en las acciones preventivas, defensivas u ofensivas.

La resiliencia, como concepto, adquiere su mayor expresión como necesidad cuando se aplica a los sistemas de la Defensa Nacional y de sus componentes. Resulta ilusorio pensar que un sistema está libre de ser afectado, por lo que cobra una gran relevancia contar con diseños técnicos y procedimentales que permitan recuperar las capacidades afectadas, en el menor plazo posible. Ello obliga a diversificaciones en las redes y a contar con sistemas alternativos, en prácticamente todos los niveles de conducción y ejecución, desde los sistemas de Mando y Control hasta los dispositivos integrados a los sistemas de armas.

Figura 2: Concepto de Big Data. Fuente: ISDI education

Big Data, representa un inmenso desafío. La inmensidad de data que actualmente se genera, hace difícil sino imposible acceder y procesar toda esa data en forma oportuna. Por ello, resulta de gran ayuda y relevancia la introducción del concepto de Inteligencia Artificial (AI), que permite que se utilice sistemas para recolectar la data y tomar determinadas decisiones, en el marco de tiempo requerido para el éxito militar. El "Machine Learning", esto es, que los sistemas "aprendan" de la data recogida, puede ser el elemento que

proporcione la ventaja sobre el adversario. Sin embargo, cuando estamos hablando de estos conceptos, estamos refiriéndonos a aspectos controlados por software y, en consecuencia, vulnerables a ataques cibernéticos que pueden provocar un efecto desastroso en la data recogida y, en consecuencia, en las decisiones posteriores.

El campo de batalla actual, se caracteriza por la presencia de múltiples actores, la mayoría de ellos interconectados, que generan tanta información que se hace muy difícil para el personal mantener una vigilancia y seguimiento de todas las amenazas. Es por ello, que la IA ayuda a coordinar las operaciones proveyendo decisiones o sugerencias de decisión enriquecidas por la fusión de data y la aplicación de complejos softwares de inteligencia artificial que analizan la data previamente caracterizada como amenaza, como asimismo aquella que los sistemas clasifican como "sospechosa" de provenir de una nueva fuente o método de ataque.

Como informa la revista Jane´s de Junio de 2018, hay empresas como Lockheed Martin, que tiene empleados repartidos en más de 50 países y se ve obligada a establecer para ellos una red mayor a la de muchos países. Lo anterior los obliga a contar con un sistema de protección de sus redes, que detecta intrusiones en los distintos niveles y que por sus buenos resultados ahora pone a disposición de otras compañías y servicios como un servicio. Ello es una demostración de que la cooperación entre compañías es posible y exitosa, por lo que no podría concebirse que estos niveles de confianza no se obtengan entre los servicios del Estado, particularmente los del sector Defensa en este caso.

Figura 3: Centro Nacional de Ciberseguridad en el Reino Unido

La falta de especialistas con las competencias más actualizadas, es un problema que ya se aprecia en el sector Defensa. Las compañías, por su tamaño, están en condiciones de invertir permanentemente grandes sumas en la capacitación permanente de personal, que debe conocer las tendencias y los usos de los atacantes, tanto para concebir las defensas requeridas como para usar esas técnicas en forma ofensiva. Para ello, países como los Estados Unidos y el Reino Unido han recurrido al trabajo conjunto con Universidades y laboratorios tecnológicos para promover la creación de especialistas en ciberguerra.
Asimismo, la falta de especialistas ha forzado a aprovechar soluciones como la automatización, para que se ocupe de materias de más bajo nivel y permita la disponibilidad de los especialistas de punta para acometer las tareas más avanzadas.

Como aseguró Ciaran Martin en su exposición en FIDAE, la encriptación se ha convertido en un elemento vital para permitir la transferencia segura de data. Como informa Neil Timms de la empresa CGI en la revista Jane´s, empresas como Thales UK están incrementando el foco en el desarrollo de tecnologías de encriptación, que incluyen la protección ante el advenimiento de "la internet de las cosas", la creciente interconectividad y todos los desafíos que el futuro va a entregar. En ello es fundamental la colaboración entre compañías, para obtener la interoperabilidad necesaria entre sus desarrollos.

Figura 4: Cuartel General de Thales en el Reino Unido

Un ejemplo de lo mencionado radica en la empresa Thales, que abrió en el Reino Unido un cuartel general para las actividades en ese país, uniendo las necesidades militares y civiles, incluso internacionalmente en algunos casos. Esas instalaciones, que también fueron mencionadas por Ciaran Martin, se enfocan adicionalmente en otras áreas de interés: conectividad, Big Data e IA.
Todo ello demuestra que el centro de gravedad en estas materias se está desplazando desde una posición anterior, basada en la creación de infraestructura de comunicaciones e informática, hacia la protección de plataformas y sistemas. Esto, según los especialistas, se está convirtiendo en el gran punto pivote del gasto militar para los años venideros

Como se aprecia, la creciente interconectividad de los sistemas presentes en la Defensa y en las plataformas y sistemas que emplea, es lo que direcciona los requerimientos para mejorar la seguridad. La particularidad de las amenazas a la ciberseguridad, de alta variabilidad y evolución, está obligando a las compañías, los organismos de Defensa y los gobiernos a moverse con celeridad en un área en la que los esfuerzos individuales obtienen resultados limitados, agravado por la falta de especialistas del más alto nivel.
La capacidad de estos actores para visualizar esto a tiempo y actuar en consecuencia, resultará vital para obtener el desarrollo de infraestructuras críticas seguras, que conduzcan con éxito a la obtención de ventajas en esta área por sobre cualquier potencial amenaza, para defenderse de sus efectos, reaccionar ante los daños y para afectar aquellos sistemas que se defina como sistemas víctima.
La ciberseguridad, como parte de la conquista del "quinto dominio" como se concibe ahora el ciberespacio, llegó para quedarse.

Boletín elaborado en base a las conclusiones del Seminario efectuado en FIDAE 2018 e información de la Revista Jane´s . MLL.