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

**BOLETÍN INFORMATIVO Y DE ANÁLISIS N° 17-2016 Santiago, 5 de mayo del 2016**

# *"USO DE LA CIBERGUERRA EN CONTRA DEL ESTADO ISLÁMICO"*

**Estados Unidos divulga uso de la Ciberguerra en la lucha contra el Estado islámico.**

El Presidente Obama está comenzando a utilizar varias armas cibernéticas secretas que fueron anteriormente empleadas contra Irán. El Comando de Ciberguerra de los Estados Unidos ***(U.S. Cyber Command)***, ha sido instruido para comenzar una ofensiva compuesta por ataques a redes computacionales del Estado Islámico (EI), lo que constituye una novedad en el empleo y también en cuanto a la divulgación de su uso.

*Figura 1: Logo del U.S. Cyber Command. Fuente: www.defense.gov*

Aunque la Agencia Nacional de Seguridad (NSA) de ese país ha estado interceptando las comunicaciones del Estado Islámico a través de las redes, hasta la fecha esta información sólo formaba parte de los briefings de inteligencia pero no se había reportado acciones ofensivas. El Comando de Ciberguerra (que es la contraparte militar a la NSA), se había concentrado en Rusia, China, Irán y Corea del Norte (países de donde se originan la mayoría de los ataques a los Estados Unidos).

**Objetivos.**

La finalidad principal de esta nueva campaña, es la supresión de la capacidad del EI para difundir sus mensajes, atraer nuevos militantes, diseminar órdenes e incluso afectar acciones cotidianas como, por ejemplo, el pago de remuneraciones. Un efecto adicional que se busca, consiste en provocar "ruido" en las mentes de los comandantes, demostrándoles que por medio de técnicas sofisticadas se les está manipulando la información. Las acciones de reclutamiento se ven afectadas también por la conciencia de los eventuales reclutas de que sus comunicaciones no son seguras, lo que puede ser un importante disuasivo para quienes planean incorporarse al EI.

**Métodos.**

De acuerdo a entrevistas efectuadas a directivos técnicos y funcionarios de niveles medios, las acciones se iniciaron por medio de "implantes" en las redes informáticas de los militantes del EI seleccionados, de manera de conocer los hábitos informáticos de los comandantes[1] . La acción que sigue, consiste en alterar sus mensajes o imitarlos, instruyendo a los militantes del EI para concurrir a áreas en donde puedan ser atacados por medio de Drones o Fuerzas Especiales.

Otro método en uso, consiste en interceptar e interrumpir las transacciones electrónicas y redirigir las remesas de dinero, con lo que las adquisiciones y el pago de sueldos y de servicios son directamente afectados, induciendo a una "*ralentización"* de las actividades.


*Foto 1: Centro de Control de Ciberguerra. Fuente: Latimes.com*

**Lo comunicacional.**

Una importante novedad en lo que respecta al manejo de estas actividades desde el más alto nivel, se observa en el tratamiento de la información hacia los medios de prensa. De hecho, el que las autoridades se refieran públicamente a esta faceta de la guerra, representa un cambio radical, ya que hasta hace unos pocos años nadie mencionaba el uso de estas "armas". Ello se fundamentaba en los efectos que tiene la eventual violación de soberanía de otros Estados, al ejecutar acciones de ciberguerra. Como se sabe, la información fluye a través de amplias redes y múltiples servidores que están localizados en todas partes del mundo y ello es mirado con recelo, incluso por parte de los aliados tradicionales. Como muestra de esta nueva política comunicacional, el Presidente Obama declaró en marzo a la salida de una reunión en los cuarteles de la CIA en Virginia: "Nuestras Ciberoperaciones están interrumpiendo su sistema de mando y control y sus comunicaciones".


*Foto 2: El Secretario de Defensa Ashton B. Carter junto al Jefe del Estado Mayor Conjunto, Gen Joseph F. Dunford Jr., en una reciente conferencia de prensa relativa al tema de ciberguerra en contra de EI. Fuente: Newsweek*

El Jefe del Estado Mayor Conjunto, General Joseph F. Dunford Jr., aseguró en una rueda de prensa que estaban tratando de "aislar a ISIL tanto física como virtualmente, limitar su capacidad de

comunicarse y limitar su capacidad de conducir operaciones". A continuación, advirtió que estos comentarios serían todo lo que podrían informar al respecto, para sorprender al adversario. En la entrevista, cada vez que el Secretario de Defensa aludía a las "Ciberbombas", los asesores legales expresaron su incomodidad, ya que consideran que el uso de la ciberguerra debiera estar limitada a operaciones específicas en que se limite el daño colateral.

**Visiones Contrapuestas.**
En la disyuntiva sobre cómo y con qué intensidad emplear métodos y acciones de ciberguerra, conviven dos visiones contrapuestas:
El propio Presidente Obama ha apuntado cuestionando el hecho de que un arsenal de ciberarmas, desarrollado a un costo de cientos o eventualmente miles de millones, no estaba siendo usado en forma intensiva contra las organizaciones terroristas.
Algunos integrantes de la organización, han revelado que el Secretario de Defensa Carter ha protestado por el hecho que el Cyber Command está demasiado enfocado en los adversarios tradicionales, estableciendo a partir de ahora lineamientos para un paquete de planes de ciberguerra apuntados contra el Estado Islámico. Estos planes, ya fueron entregados por el Comandante del Cyber Command y por el director de la NSA.

*Frontis de la sede de la NSA y del Cyber Command, Fort Meade. Fuente: latimes.com*

Por otra parte, en la sede de la NSA y del Cyber Command, en Fort Meade, Maryland, los requerimientos de la Casa Blanca han generado resistencia. El argumento de los expertos de la NSA, es que ellos han gastado años penetrando redes en China, las comunicaciones de los submarinos de Rusia y otros objetivos, implantando comandos de espía en sus redes para mantenerlas en escucha, y no desean que se revele detalle alguno de su accionar.
Esta actitud de seguimiento furtivo y sin delatarse, a su vez, difiere de la intención del Cyber Command, que desea romper las redes como contraataque a las acciones de los adversarios. Los civiles de la NSA argumentan que si se utiliza estos implantes para atacar una red, el EI dejará de utilizarla y la reemplazará por otra, más difícil de detectar y penetrar, obligando a comenzar todo el trabajo "desde cero".

Este debate no es exclusivo de los Estados Unidos. En el Reino Unido, el Cuartel General de las Comunicaciones Gubernamentales ha sostenido una controversia parecida, lo que no es nuevo. Se dice que esta polémica proviene de los tiempos en que Winston Churchill, en plena Segunda Guerra Mundial, se debatía entre evitar o no el inminente bombardeo alemán sobre la ciudad inglesa de Coventry, revelando con ello que había utilizado la máquina *Enigma* para quebrar los códigos de encriptación enemigos, situación que nunca ha sido confirmada ni desmentida.

Otra arista que se discute respecto del empleo de la ciberguerra, se refiere a la contradicción entre el necesario secreto y la transparencia que se le exige a los actos estatales. Seguramente, este aspecto será un punto a considerar para todos los Estados que comiencen a incursionar en hacer frente al problema de ciberseguridad a nivel de las instituciones del Estado y en particular, a las del área de Defensa.

**Las Redes Sociales.**
Un aspecto nuevo, que no corresponde con exactitud al concepto de ciberguerra pero está íntimamente relacionado con ésta, es el concerniente al uso de las redes sociales. Éstas pueden ser utilizadas para reclutar militantes, coordinar acciones y difundir información, lo que obliga a adoptar acciones en un ambiente que tiene regulaciones legales definidas y que por consiguiente, no pueden ser violadas en forma indiscriminada.
En Estados Unidos, *Lisa O. Monaco*, Asesora directa del Presidente Obama para "Contraterrorismo", ha liderado los esfuerzos para interrumpir el uso de los medios de comunicación sociales para el reclutamiento de terroristas. Para ello, ha sostenido múltiples reuniones con ejecutivos de Silicon Valley, Austin y Boston, para introducir una contraofensiva comunicacional en las redes sociales, que contrarreste la propaganda del EI.
Aunque los efectos de la decisión de no informar en detalle sobre estas operaciones, algunos efectos parecen ser evidentes. Comentarios de funcionarios técnicos, señalaron que el tráfico de órdenes del EI a través de la web aparentemente ha disminuido, aunque declinaron responder si ello puede significar un cambio en los medios de transmisión, como se temía. En todo caso, se ha interceptado importantes sumas de dinero e impedido sean remitidas a sus destinos en los momentos en que se intentó transferir a cuentas en paraísos fiscales donde serían más difíciles de aislar.

**Reflexiones locales.**
Nuestro país no está ajeno a la amenaza cibernética. Ya en el pasado se ha tenido evidencias de ataques informáticos, a sitios web y correos de diversas organizaciones del Estado.
Si bien los sistemas de seguridad informática institucionales, detectan y detienen miles de intentos de incursionar en nuestras redes, lo que no sabemos a ciencia cierta, es cuantas intromisiones no han sido detectadas. Ante ello surge la necesidad de implementar políticas y técnicas adecuadas para enfrentar esta amenaza, ya que se trata de un problema que involucra a todas las instituciones del Estado y eventualmente, a organizaciones civiles a cargo de la administración de gran parte de infraestructura crítica del país, tales como la banca, red eléctrica, de abastecimiento de combustible y otros servicios básicos.
Ello ya ha atraído la atención del sector Defensa, por lo que en el año 2014 la ANEPE y la Subsecretaría de Defensa llevaron a cabo un seminario sobre *Ciberseguridad y Ciberguerra*, tratando una serie de materias técnicas y conceptuales. En agosto del año 2014, por Decreto Supremo, se creó un Comité Interministerial sobre Ciberseguridad.
A partir del año 2014, el problema de la Ciberseguridad comenzó a aparecer en la Cuenta Presidencial del 21 de mayo, incluyendo el anuncio, el 21 de mayo de 2015, de la formulación de una "Política de Ciberseguridad" para el Ministerio de Defensa Nacional, la cual se concretó en el mes de octubre a través de una Orden Ministerial, que dispone la inclusión de una Política en materia de Ciberespacio para ser considerada en el próximo Libro de la Defensa.
Lo que es seguro, es que el proceso decisional respecto de la actitud del Estado ante este tema, resulta ineludible. La ciberguerra es una realidad, que ha llegado para quedarse.

*Adaptado del artículo "US Cyberattacks target ISIS in a new line of combat", de David E. Sanger, The New York Times; más notas del autor. MLL.*