Hacia una ciberdefensa más proactiva de las redes OTAN

AUTOR: Félix Nieto Ortega
@FlixNieto3

Fuente. CyberDBNBC News

A finales de 2020, el U.S. Cyber Command llevó a cabo una operación sobre las redes informáticas de las Fuerzas de Defensa estonias junto a las Fuerzas Armadas de este país. El objetivo, según la nota de prensa del Departamento de Defensa estadounidense,[1] era contrarrestar actividad maliciosa en dichas redes.

Durante algo más de un mes, los equipos de "caza avanzada" (*hunt forward teams*) norteamericanos y unidades especializadas estonias buscaron e identificaron software malicioso, poniéndolo a continuación a disposición de los aliados y de la industria privada de ciberseguridad.[2]

La nota de prensa del New York Times[3] fue algo más explícita a la hora de identificar al actor responsable de introducir *malware* en los sistemas de información y comunicaciones estonios, apuntando directamente a Rusia y destacando el interés norteamericano por obtener información de valor para proteger las elecciones presidenciales de noviembre.

Esta colaboración entre los Estado Unidos y Estonia es un ejemplo tangible de la reorientación promovida por la *U.S. Cyber Command Vision* de 2018. El propósito de esta nueva aproximación es lograr la superioridad estadounidense en el ciberespacio manteniendo la iniciativa mediante la interacción continua con los adversarios, maniobrando

1 U.S. Department of Defence, "Estonia, U.S. Conduct Joint Defensive Cyber Operation", 03 de diciembre de 2020. https://www.defense.gov/Explore/News/Article/Article/2434474/estonia-us-conduct-joint-defensive-cyber-operation/ Última visita: 13 de enero de 2021.

2 Ibid.

3 BARNES, Julien, "U.S. Cyberforce Was Deployed to Estonia to Hunt for Russian Hackers", 03 de diciembre de 2020. https://www.nytimes.com/2020/12/03/us/politics/cyber-command-elections-estonia.html Última visita: 13 de enero de 2021

Fuente. NATO

entre la defensa y la ofensiva en ciberespacio y operando a nivel global, lo más cerca posible de los adversarios[4].

En esta visión juegan un papel destacado los socios y aliados, con quienes se busca promover las operaciones en coalición.[5] Así, la colaboración llevada a cabo por el US Cyber Command y las Fuerzas de Defensa estonias no consiste en una asistencia técnica o un intercambio de información sino de una operación militar. Más concretamente, una Operación Defensiva en el Ciberespacio.

Según la doctrina militar estadounidense[6], las Operaciones Defensivas en el Ciberespacio (Defensive Cyberspace Operations o DCO) son aquellas operaciones que se ejecutan para defender la porción del ciberespacio asignada de amenazas activas. Son misiones que tratan de preservar la capacidad de utilizar el ciberespacio propio y proteger datos, redes y aquellos medios que dependen del ciberespacio, de actividad maliciosa en el ciberespacio en curso o inminente.

A diferencia del enfoque más genérico y mecánico de la seguridad en los Sistemas de Información y Comunicaciones (Seguridad CIS), las DCO luchan contra amenazas específicas que han penetrado o amenazan con penetrar las medidas de seguridad propias. Las DCO son específicas para una amenaza en particular y su objetivo final es derrotar a la amenaza y devolver una red comprometida a un estado de funcionamiento seguro.

En definitiva, las DCO son ejecutadas con una mentalidad operativa frente a un perfil más administrativo de la Seguridad CIS, más propio de organizaciones civiles.

Una de las tareas fundamentales de la OTAN en el ciberespacio es la protección de sus propias redes, aquellas que permiten la comunicación y el intercambio de información entre los principales entes de la organización, esto es, el

4 U.S. Cyber Command, "U.S. Cyber Command, Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command", abril 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010. Última visita, 16 de enero de 2021

5 Ibid.

6 Joint Chiefs of Staff, "Joint Publication 3-12 Cyberspace Operations" 08 de junio de 2018.

"Una de las tareas fundamentales de la OTAN en el ciberespacio es la protección de sus propias redes, aquellas que permiten la comunicación y el intercambio de información entre los principales entes de la organización, esto es, el Cuartel General de la OTAN, la Estructura de Mandos y las Agencias, entre otros."

Cuartel General de la OTAN, la Estructura de Mandos y las Agencias, entre otros. Es lo que se conoce como la "*NATO Enterprise*".

Esta función protectora es llevada a cabo principalmente por el *NATO Cyber Security Centre (NCSC)*[7]. Esta entidad es parte de, la *NATO Communications and Information Agency,* organismo civil que cuenta con un buen número de especialistas en el ámbito de la ciberseguridad, actuando además como centro para el intercambio de información técnica sobre ciber amenazas entre la OTAN y los aliados.

Hasta hace poco, la aproximación de la OTAN a la defensa de sus redes ha sido eminentemente reactiva. Los esfuerzos de la institución se han centrado en instaurar medidas de seguridad que supuestamente debería elevar el coste de lograr una penetración en el sistema, evitando que sea rentable para el adversario. Es lo que se denomina disuasión por negación.

En los últimos años, la Alianza ha realizado importantes avances para mantener el ritmo de los acontecimientos en el ámbito del ciberespacio. Así, en la Cumbre de Varsovia de 2016, los aliados declararon el ciberespacio como dominio de operaciones a la vez que se acordaba el compromiso de ciberdefensa, mediante el que las naciones se obligaban a mejorar sus propias defensas para asegurarse que son capaces de defenderse en el ciberespacio como lo son en el aire, en tierra y en el mar.[8]

Posteriormente, en la cumbre de Bruselas de 2018, los aliados expresaron su determinación de emplear todas sus capacidades, incluidas las ciber, para disuadir, defenderse y contrarrestar el espectro completo de amenazas cibernéticas, incluida aquellas que forman parte de una campaña hibrida.

Estos importantes cambios se complementan con otros de carácter organizativo, como la creación del Centro de Operaciones en el Ciberespacio (CyOC) en Mons (Bélgica) que servirá para fortalecer la estructura de mandos de la OTAN y facilitará la integración del nuevo dominio cibernético en las actividades, operaciones y misiones aliadas.[9]

7 NCI Agency, "NATO's Cyber Security Centre". https://www.ncia.nato.int/what-we-do/cyber-security.html. Última visita, 16 de enero de 2021.

8 NATO, "NATO Cyber Defence Pledge," Press Release (2016) 08 de julio de 2016, https://www.nato.int/cps/su/natohq/official_texts_133177.htm. Última visita, 16 de enero de 2021

9 NATO, "Cyber Defense," https://www.nato.int/cps/en/natohq/topics_78170.htm. Última visita, 16 de enero de 2021

La mayor parte de estas medidas están dirigidas al ámbito de las operaciones. Sin embargo, conviene no perder de vista las redes permanentes, es decir, aquellas que permiten las consultas y el mando y control entre las entidades de carácter político-estratégico, y que no se encuentran incluidas en un área de operaciones.

> "La inminente instauración del Chief Information Officer (CIO) en la OTAN supone una novedad importante, dado que será la primera vez en la historia de la Alianza en la que una autoridad OTAN disponga de una esfera de responsabilidad que abarque el Cuartel General, los Mandos Estratégicos y otras 39 entidades que componen la NATO Enterprise"

En ese ámbito, destaca la inminente instauración del *Chief Information Officer* (CIO) en la OTAN, de quién se espera que pueda llevar a cabo importantes tareas en el ámbito de la ciberdefensa. La puesta en marcha de esta figura supone una novedad importante, dado que será la primera vez en la historia de la Alianza en la que una autoridad OTAN disponga de una esfera de responsabilidad que abarque el Cuartel General, los Mandos Estratégicos y otras 39 entidades que componen la *NATO Enterprise*[10].

No obstante, a pesar de lo significativo de este avance, la percepción general es que la OTAN debe hacer más para estar en condiciones de proteger sus propias redes con la agilidad necesaria para hacer frente a las amenazas actuales y futuras en el ciberespacio. Ello hace necesario introducir en el debate conceptos que van más allá de la defensa pasiva de las redes.

Uno de ellos son efectos cibernéticos proporcionados voluntariamente por los aliados (conocidos por su acrónimo en inglés SCEPVA – Sovereign Cyber Effects Provided Voluntarily by Allied), anunciados en la declaración de Bruselas[11] y que permite que aquellas naciones con capacidades ofensivas en el ciberespacio puedan ponerlas a disposición de la OTAN, integrándolas en las operaciones de la Alianza.

Pero aún son muchas las cuestiones que necesitan ser aclaradas antes de que este instrumento se convierta en

10 TARGETT, Ed, "NATO is hiring its first CIO: Why? TECHMONITOR, 09 octubre 2020. https://techmonitor.ai/boardroom/strategy/camille-grand-nato-cio-vacancy#:~:text=Why%20hire%20a%20CIO%3F,communication%20technology%20as%20an%20enterprise. Última visita, 16 de enero de 2021.

11 NATO "Brussels Summit Declaration," Press Release 11 de julio 2018 https://www.nato.int/cps/en/natohq/official_texts_156624.htm Última visita, 16 de enero de 2021

una herramienta verdaderamente operativa a disposición de la OTAN, tales como el control político, su integración en el planeamiento operativo y la voluntad de intercambiar inteligencia altamente sensible, tanto la referente a los objetivos como a la relacionada con las propias ciberarmas.

Por ello, quizás haya que poner el énfasis en un tipo de operaciones menos delicadas desde el punto de vista político y que podrían encontrar un mejor acomodo en una organización de carácter defensivo. Se abre pues una oportunidad para desarrollar Operaciones Defensivas en el Ciberespacio en las propias redes de la OTAN, a semejanza de la realizada recientemente por el U.S. Cybercom en las redes de las Fuerzas de Defensa de Estonia.

Sin embargo, no podemos olvidar que la OTAN carece de fuerzas propias de combate, salvo contadas excepciones. Por ello, quizás merezca la pena explorar la idea expuesta recientemente por el Capitán de Navío Enrique Cubeiro, antiguo Jefe del Estado Mayor de Mando Conjunto de Ciberdefensa[12], acerca de crear una Standing NATO Cyber Force siguiendo el exitoso modelo de las Standing Naval Forces en el ámbito marítimo.

De esta manera, la OTAN podría contar con una fuerza permanente, responsable de ejecutar Operaciones Defensivas en el Ciberespacio, constituida a partir de una un núcleo permanente, en tanto que el resto sería proporcionado por las naciones mediante rotaciones periódicas.

12 CUBEIRO, Enrique. "Una idea para potenciar la capacidad de disuasión de la OTAN en el ciberespacio". Cuadernos de Pensamiento Naval. Número 29. Diciembre 2020, https://publicaciones.defensa.gob.es/cuadernos-de-pensamiento-naval-29-revistas-pdf.html