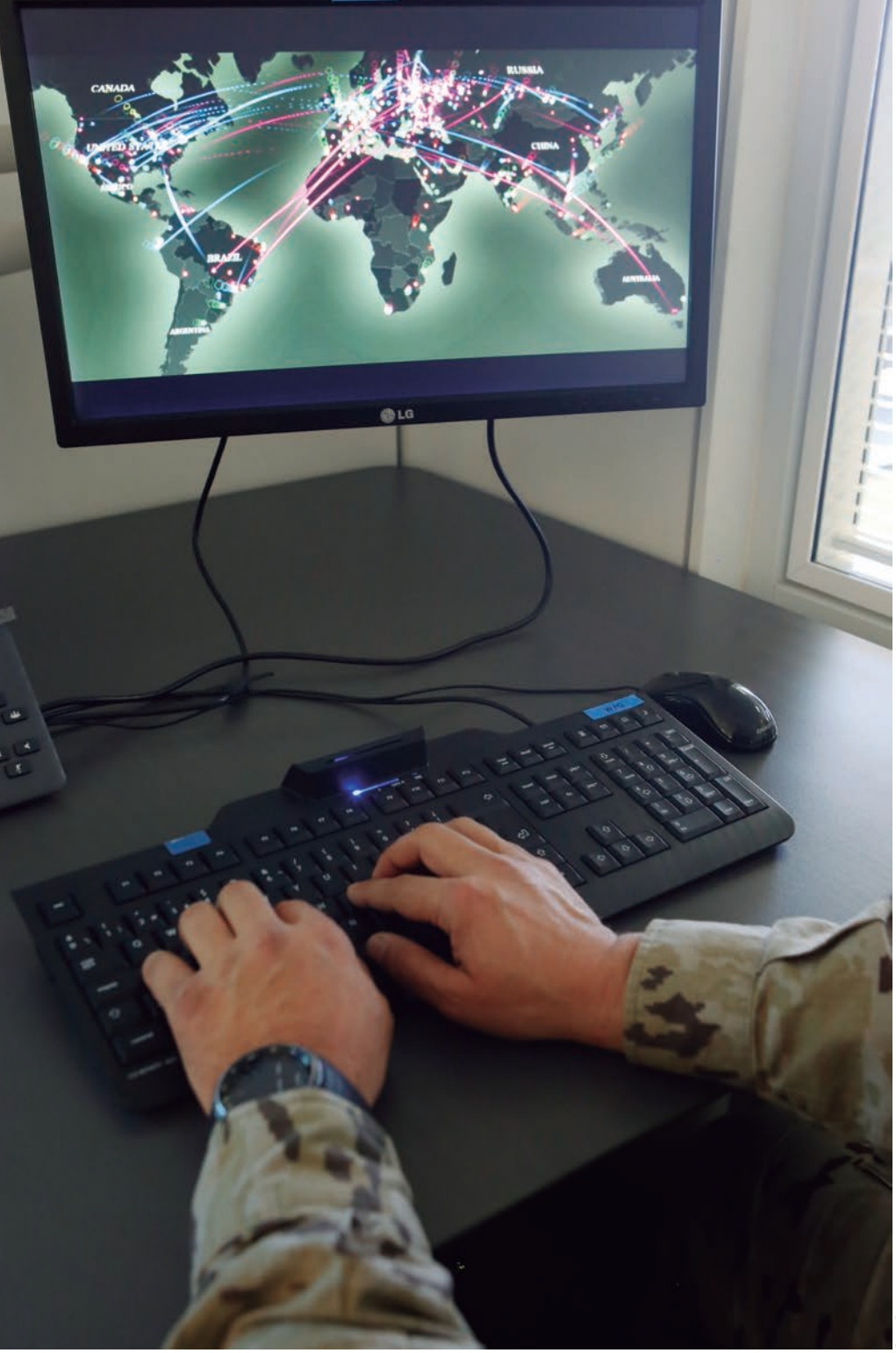


Pepe Díaz

Preparados ante la AMENAZA FANTASMA

La ciberdefensa es ya uno de los pilares de las capacidades de la OTAN, y la UE acaba de aprobar la creación de una Agencia Europea contra los ataques informáticos

«MANTENER la paz con la tecnología» es como define el secretario general de la OTAN, Jens Stoltenberg, la ciberdefensa. Algo que a primera vista parece sencillo, pero que es tremendamente complicado, quizás, como el propio Stoltenberg reconoce, «el más complejo de los retos a los que hemos tenido que hacer frente para garantizar la seguridad de un Estado y de sus ciudadanos». Porque si algo ha quedado claro en el nuevo *arte de la guerra* es que las amenazas son ahora híbridas, mutantes, imprevisibles, sofisticadas y prácticamente imposibles de acotar.

Si queremos estar a salvo, nuestras capacidades de respuesta deben serlo también. Lo que hace apenas unos años sonaba a ciencia ficción es ya una realidad: hace una década, Estonia sufrió el primer ciberataque contra un Estado; hoy, los virus informáticos invaden sin fronteras y los *hackers*, contratados por actores estatales y privados, tienen una capacidad más que constatada no sólo para destruir o dañar infraestructuras básicas, desviar la trayectoria de un misil o determinar el éxito o el fracaso de una operación militar, sino también para desinformar e interferir en las campañas electorales o mermar la credibilidad de cualquier gobierno. Además, es más que evidente el protagonismo de las nuevas tecnologías

en la operativa del yihadismo para captar, entrenar e, incluso, como constataron los servicios de inteligencia británicos tras los atentados de Londres de junio de 2017, coordinar las acciones terroristas. «Hay que trabajar mucho y rápido, pero la cualidad que ha permitido a la Alianza seguir siendo la principal organización defensiva del planeta es su capacidad de respuesta, su constante transformación. Y ahora, conseguir una ciberdefensa fuerte con capacidad de prevención, resiliencia y disuasión es nuestro gran campo de acción», detalla el informe anual de la Alianza Atlántica presentado por Stoltenberg el pasado 15 de marzo.

Porque todo apunta a que la ciberguerra no ha hecho más que empezar. Según un reciente análisis de la Comisión Europea, los ataques cibernéticos se han cuadruplicado desde 2015 y en algunos países miembros el 80 por 100 de los delitos que se cometen actualmente son de este tipo; se calcula que los ataques informáticos cuestan a la economía de la Unión unos 400.000 millones de euros al año. Los últimos informes aportados por la OTAN arrojan cifras escalofriantes: la Alianza sufre más de 500 ataques informáticos al mes y el crecimiento respecto al año anterior es de casi el 70 por 100 (algo superior a lo que ocurrió en 2016 respecto a 2015, que fue del 60 por 100).

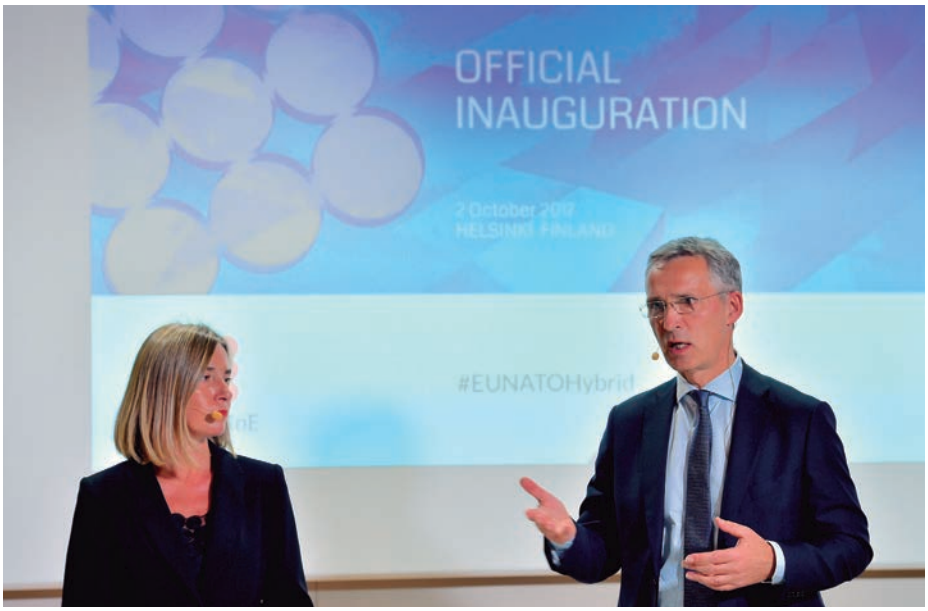
Por su parte, Naciones Unidas en su análisis sobre la situación en el mundo en 2017, habla de una «verdadera guerra entre países y grupos de influencia por lograr información, desestabilizar o conseguir una mayor parcela de poder cibernético que crece de manera exponencial», pero como no son agresiones tangibles, físicas, «son casi imposibles de imputar a un estado u organización criminal».

Una realidad ante la que la ONU, reconoce, ve limitada su capacidad de sancionar y su labor se ve acotada a la elaboración de un código ético y unas normas de actuación. Por ello, el último informe de 2017 del secretario general, Antonio Guterres, urge a los Estados a desarrollar capacidades defensivas en este ámbito «que garanticen la paz y el abastecimiento de necesidades de sus ciudadanos».

SOLUCIONES CONJUNTAS

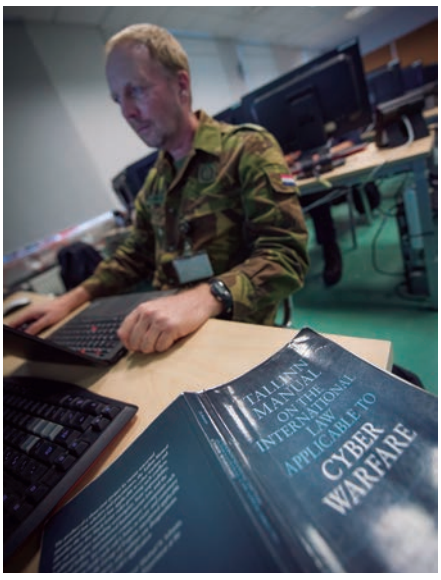
Plenamente conscientes de ello, las dos principales organizaciones defensivas occidentales saben que no hay tiempo que perder y, en los últimos meses, han emprendido una carrera contra el tiempo y el espacio para ofrecer a sus ciudadanos un sólido paraguas defensivo y, al mismo tiempo, aprovechar las ventajas que para el bienestar puede aportar la nueva era digital. Y, además, lo están haciendo implementado de una forma especialmente activa las medidas de colaboración, intercambio y complementariedad OTAN-UE. El pasado mes de noviembre, los titulares de Defensa de la Alianza Atlántica —que desde 2014 ya incluye la ciberdefensa como parte de la defensa colectiva contemplada en el artículo 5, de manera que si algún aliado recibe un ataque informático lo recibimos todos— dieron un paso sustancial al encuadrar en la nueva estructura de mandos el espacio cibernético. Los ministros dieron luz verde definitiva a la creación del Centro de Operaciones Cibernéticas (*Cyber Operations Centre*). Esta unidad, que estará ubicada físicamente como parte del Cuartel General Aliado en Europa (SHAPE), en Mons (Bélgica), ayudará a integrar la ciberdefensa en todos los niveles de la planificación y las operaciones. Es el paso definitivo que reconoce el cibernético como un dominio más, al mismo nivel que el aire, la tierra el mar y el espacio.

Por su parte, los jefes de Estado y Gobierno de la Unión Europea organizaron en octubre una Cumbre extraordinaria para analizar desde todas las perspectivas posibles esta nueva amenaza y adoptar un planteamiento común a la hora de enfrentarse a los *hackers*. El aviso a navegantes fue contundente: si cualquier socio sufre un incidente grave en el ciberespacio, el resto está obligado a prestarle asistencia militar. Poco des-



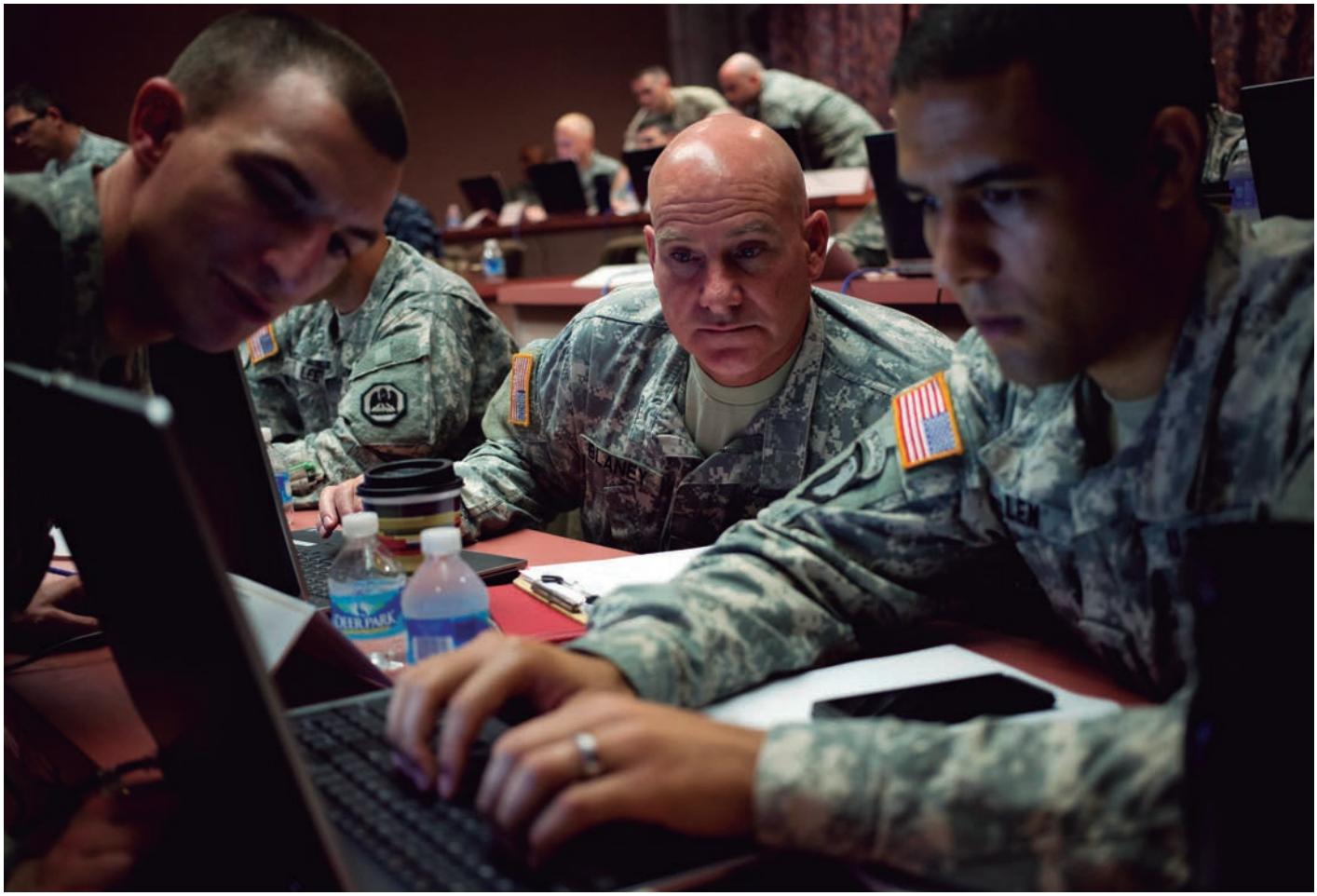
Consejo Europeo

Federica Mogherini y Jens Stoltenberg en la inauguración del centro de Excelencia contra las Amenazas Híbridas, el pasado 2 de octubre en Helsiniki.



OTAN

Un analista de la Alianza en el Centro de Excelencia de Ciberdefensa en Estonia.

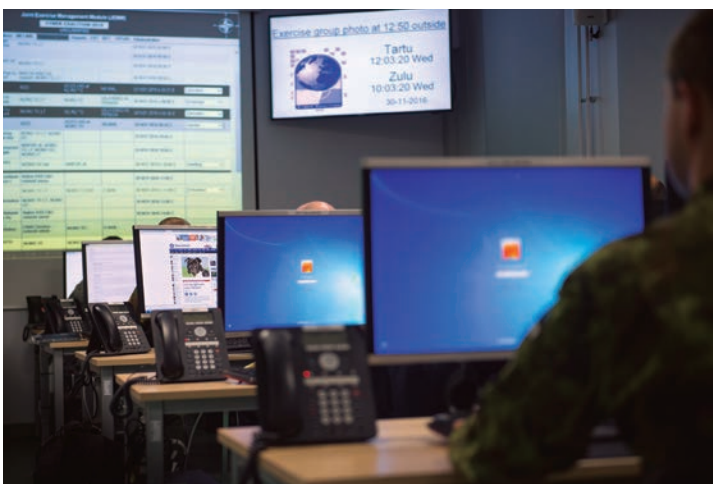


Secretaría de Defensa norteamericana

Militares norteamericanos durante el ejercicio *Cyber Coalition 2017*, que contó con la participación de la Unión Europea.

pués, el Consejo Europeo de diciembre dio luz verde a una nueva Agencia Europea de ciberseguridad y formalizó la creación de un Equipo de Respuestas Informáticas (CERT-UE). Los jefes de Estado también afianzaron la célula del Servicio Europeo de Acción Exterior destinada al intercambio de inteligencia cibernértica y crearon sendos grupos de trabajo para contrarrestar las campañas de desinformación y las de difusión sistemática de noticias falsas.

Y, además, respaldaron sin fisuras, con contundencia y convicción, la imprescindible colaboración con la Alianza Atlántica en esta área: «Las reglas del juego han cambiado en la seguridad —afirmó Jean Claude Juncker, presidente de la Comisión Europea— ya no existen fronteras, ni ficticias ni reales. Ahora, más que nunca, es necesario que trabajemos juntos». El día 2 de octubre, el secretario general de la Alianza y la Alta Representante de la Unión para Asuntos Exteriores y Seguridad, Federica Mogherini, habían inaugurado en Helsinki un Centro de Excelencia Contra las Amenazas Híbridas (*Hybrid CoE*) desde el que canalizar todas las acciones nacionales y conjuntas para enfrentarse a este tipo de ataques. Hasta el momento y además del anfitrión, Finlandia, ya se han sumado al memorando de adhesión al Centro una docena de países, entre ellos Estados Unidos, España, Francia, Reino Unido, Polonia, Letonia, Lituania, y Suecia.



OTAN

El nuevo Centro de Operaciones Cibernéticas, en SHAPE, coordinará todas las acciones de prevención y defensa aliadas.

Poco después, el 14 de noviembre, los ministros de Exteriores de la UE mantuvieron una reunión extraordinaria con sus homólogos de la OTAN con la ciberdefensa como protagonista indiscutible: aprobaron un paquete de 34 medidas conjuntas entre las que se incluyen fórmulas para mejorar la inteligencia común en la lucha contra el terrorismo, afinar los esfuerzos contra las noticias falsas y buscar sinergias a la hora de hacer frente a los ataques cibernéticos, en particular respecto a la activación de los equipos de respuesta rápida que hasta ahora tenían por separado las dos organi-

zaciones y la realización de maniobras conjuntas de forma regular (la UE ya fue invitada este año al mayor ejercicio en este campo que realiza la Alianza, el *Cyber Coalition*).

«La OTAN y la UE pueden ahora intercambiar alertas sobre ciberataques y virus en tiempo real», explicaron en rueda de prensa conjunta Stoltenberg y Mogherini. En este último aspecto, destacaron la importancia de ampliar la financiación y el alcance del Centro de Excelencia de Comunicaciones Estratégicas de la OTAN, una institución aliada pero abierta a que la utilicen sus socios europeos, cuya función es informar y capacitar a funcionarios y especialistas tanto en ciberdefensa como en maquinarias estatales de propaganda informática.

La Alianza ya reconoce el ciberespacio como un dominio militar

Los últimos informes presentados por este Centro habían aportado datos, cuando menos preocupantes: entre marzo y agosto del pasado año hubo 32.000 mensajes de 11.600 usuarios con menciones negativas a la Alianza Atlántica, alguna de sus misiones y, sobre todo, a algunas de las repúblicas bálticas o Polonia. También se constató que un 84 por 100 de los mensajes procedían de territorio ruso y que un 70 por 100 de ellos lo hacía desde cuentas falsas o activadas de forma remota, lo que convencionalmente se conoce como *bots*.

LA RESPUETA ALIADA

La batalla de la OTAN contra la amenaza informática no es nueva. Las alarmas saltaron en 1999 con un ataque sufrido durante la guerra de los Balcanes y, tres años más tarde, el comunicado de la Cumbre de Praga de 2002 ya incidió sobre la necesidad de incluir la ciberdefensa entre los objetivos aliados. En Riga, en 2006, los jefes de Estado y Gobierno refrendaron que las capacidades de la

España, en primera línea

LA ciberdefensa es un asunto destacado en las agendas tanto de la OTAN como de la UE, así como en todos los Estados miembros de estas organizaciones. España participa en ejercicios de ciberdefensa en los marcos de ambas organizaciones, multinacionales y nacionales, cubriendo todo el espectro desde la gestión de crisis a nivel estratégico, hasta el nivel táctico. Entre estos ejercicios cabe destacar *Cyber Coalition* (OTAN) y *Cyber Europe* (UE); el primero de ellos de carácter anual y el segundo bianual.

En el plano internacional, el Mando Conjunto de Ciberdefensa (MCCD) participa en múltiples iniciativas multinacionales relacionadas con el desarrollo de las capacidades militares de ciberdefensa. España es miembro, desde su fundación en 2008, del Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN (NATO CCD CoE) junto con Bélgica, la República Checa, Estados Unidos, Estonia, Francia, Alemania, Grecia, Hungría, Italia, Letonia, Lituania, Holanda, Polonia, Eslovaquia, Turquía, Reino Unido, Austria, Finlandia, Suecia y, próximamente, Portugal.

Pepe Díaz

España contribuye desde entonces con dos representantes, siendo un oficial de las Fuerzas Armadas españolas el jefe de su departamento de Operaciones y, además, se participa regularmente en sus ejercicios anuales *Locked Shields* y *Crossed Swords*. España también contribuye con personal a la estructura de ciberdefensa de la Alianza Atlántica.

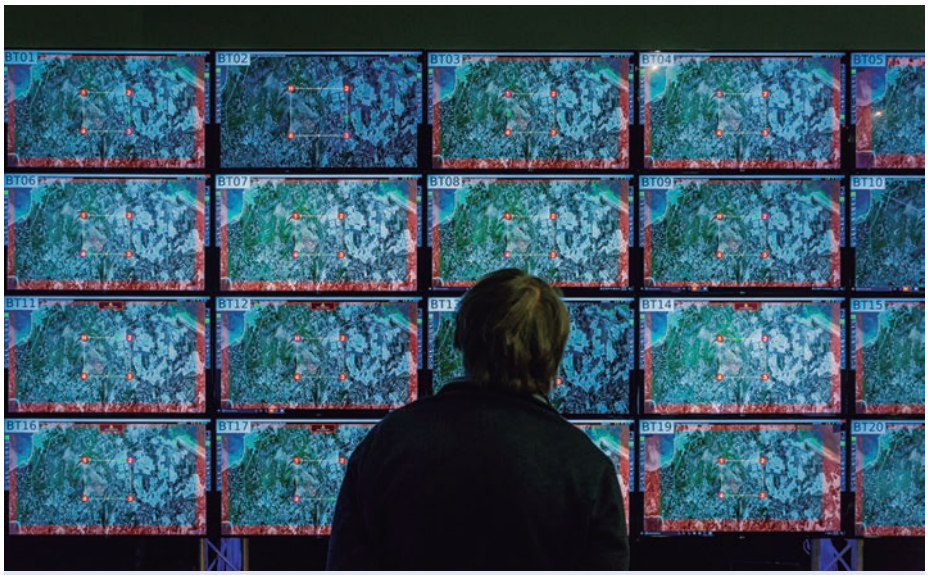
Dentro del campo de la formación, España también participa en el proyecto *Multi-National Cyber Defense Education & Training*. El Mando Conjunto de Ciberdefensa ha sido designado por el Ministerio de Defensa para participar en este proyecto, que, liderado por Portugal y bajo auspicios de la OTAN, constituye una iniciativa multinacional sobre formación y adiestramiento en ciberdefensa.

La finalidad principal del grupo de trabajo es desarrollar iniciativas que solucionen las posibles carencias que puedan tener las naciones en esta área e intentar el desarrollo de una plataforma de cursos y oportunidades formativas.

También relacionado, puesto que la Alianza Atlántica es uno de los impulsores, España participa en el proyecto denominado ICOPC (*International Cyberspace Operations Planning Curricula Project*), dentro de la iniciativa *Multinational Capability Development Campaing* (MCDC) para el desarrollo de un programas de estudios multinacionales destinados al planeamiento de operaciones relacionado con el ciberespacio.

En relación a aspectos doctrinales, el MCCD forma parte del Grupo de Trabajo, liderado por el NATO CCD COE, sobre la doctrina de operaciones conjuntas en el ciberespacio. Este trabajo va a suponer un referente doctrinal para OTAN y las naciones de la Alianza e incluso en el ámbito de la UE, ya que muchos países pertenecen a ambas organizaciones multilaterales.

CF Francisco de Asis Aznar Fernandez-Montesinos
Mando Conjunto de Ciberdefensa



OTAN

Nuevo campo de batalla

SIN duda, el ataque de virus *Wanna Cry* en mayo del 2016 fue el más mediático y el que hizo saltar algo más que las alarmas de empresas y particulares (en poco más de dos horas, este *ransomware* secuestró ordenadores de más de 100.000 compañías y organismos de 150 países, entre ellos varios hospitales británicos, solicitando un rescate en *bitcoins*), pero no fue ni el primero ni, nadie lo duda, será el último. Los ataques informáticos son, como la propia tecnología, múltiples, imprevisibles y en constante evolución. Además del cibersespionaje civil y militar o los robos de información en la red (en abril 2014 más de 500 millones de cuentas de *Yahoo* fueron pirateadas y, pocos meses más tarde, fue difundida toda la información de la compañía Sony como represalia por una película satírica sobre el presidente de Corea del Norte), en los últimos años se han producido importantes daños a infraestructuras básicas de diferentes países: en 2010, casi 1.000 de las 6.000 centrifugadoras iraníes dejaron de funcionar o sufrieron serios parones por la intromisión del virus *Stuxnet*; en noviembre de 2014 unos *hackers* accedieron al sistema de control industrial de unos altos hornos en la región alemana de Ruhr y los paralizaron; y el del 23 de diciembre de 2015 en Ucrania unos cibercriminales pudieron acceder a la central eléctrica de Prykarpattyaoblenergo y dejar a casi medio millón de personas sin calefacción y sumidos en la oscuridad. Y esto no ha hecho nada más que empezar: una reciente investigación del diario *The New York Times* indica que el gobierno de Corea del Norte tiene a más de 6.000 *hackers* engrosando las filas de su Ejército.

TAMBIÉN EN LA GUERRA CONVENCIONAL

La guerra de los Balcanes del 99 fue el primer ejemplo de que lo virtual era, además, un instrumento para la guerra convencional: durante los bombardeos de Kosovo, los *hackers* serbios dejaron varias horas sin servicio la web de la Alianza y algunas de sus comunicaciones mediante ataques de negación de servicio (DoS). Desde entonces, no hay conflicto, planeamiento o comunicación que no tema ser objeto de algo incontrolable. Durante la guerra de Ucrania de 2014, las hasta entonces hipotéticas opciones de atacar con la informática se demostraron pausibles: en su lucha contra los separatistas rusos, el ejército ucraniano había perdido el 20 por 100 de sus cañones de largo alcance *D-30* a causa de bombardeos rusos o prorrusos. Nadie se explicaba cómo eran localizados hasta que técnicos ucranianos descubrieron que habían introducido un *malware* bautizado como *Agente X* en una aplicación desarrollada por un oficial ucraniano para manejar el *D-30*. Gracias al *Agente X*, los piratas informáticos localizaban los cañones en cuanto alguien activaba la aplicación.

OTAN debían garantizar la seguridad y la resiliencia de todos sus sistemas de Tecnología de Información y Comunicaciones (TIC). Pero el punto de inflexión se produjo durante abril y mayo de 2007 cuando Estonia sufrió un ataque múltiple —mediante peticiones de respuesta a un servidor o usando *bots* con denegación de servicio— que colapsó buena parte de las infraestructuras del país.

La respuesta no se hizo esperar: en junio de ese mismo año, los ministros de defensa aliados solicitaron del Comité Militar que desarrollara medidas concretas dentro de la planificación aliada para la defensa cibernética. Apenas un año más tarde, el comunicado de la Cumbre de Bucarest de abril de 2008 señalaba expresamente «la necesidad de estructuras que permitan defender los sistemas de información clave» y, en este sentido, los aliados vieron con muy buenos ojos el sistema diseñado por Estonia que combina la defensa a la red con la propia doctrina militar. Por ello, llegaron a un acuerdo con el gobierno de Tallín para desarrollar un centro conjunto que coordinase la defensa cibernética y actuara como núcleo para el análisis, el intercambio de conocimientos y la formación Fue el embrión que culminó apenas un año después, con la creación en mayo de ese mismo año del Centro de Excelencia de Cooperación en Ciberdefensa (CCD CoE).

Ese mismo verano, el de 2008, la guerra entre Rusia y Georgia constató que los ciberataques se habían integrado en la guerra convencional interfiriendo en las comunicaciones o modificando trayectorias u órdenes de vuelo. El nuevo siglo exigía un nuevo modelo de Alianza y la ciberdefensa, también para las operaciones, tenía que ser ya parte incuestionable de ella. El concepto estratégico aprobado en la Cumbre de Lisboa de 2010 indica que los ciberataques son una de las principales amenazas de nuestro tiempo (al mismo nivel que el terrorismo o las armas de destrucción masiva); al año siguiente, los ministros de defensa aliados aprobaron la denominada Política de Ciberdefensa de la OTAN y, en julio de 2012, la Cumbre de Chicago integró la ciberdefensa en la iniciativa Defensa Inteligente (*Smart Defence*) para proceder al desarrollo conjunto de capacidades más baratos y eficaces.

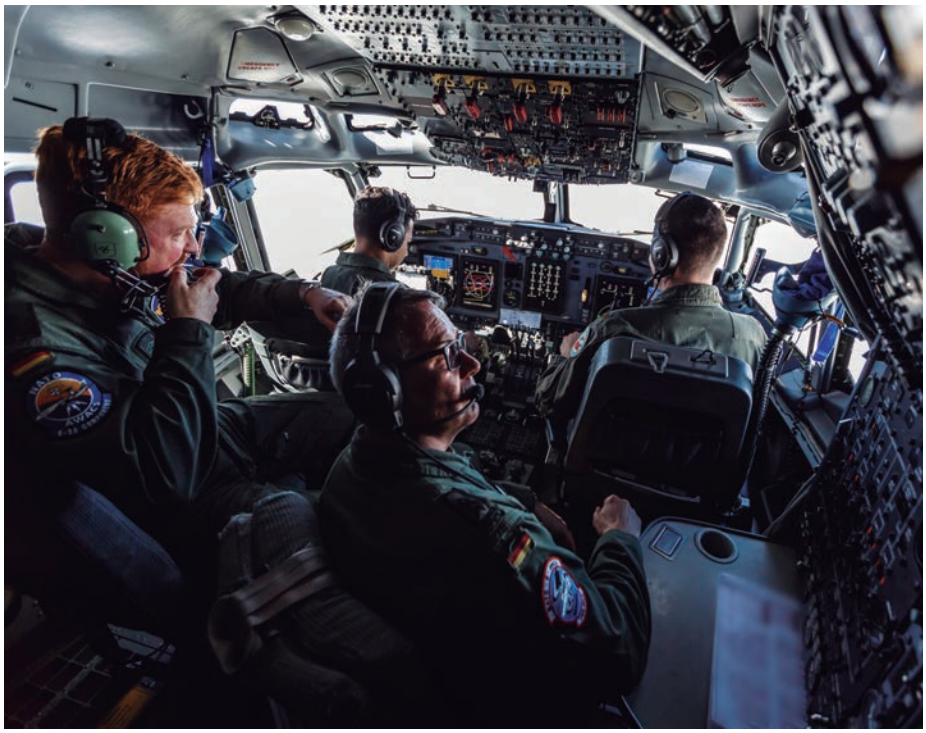
Apenas un año después, en octubre de 2013, los ministros de defensa dieron otro

La Unión Europea y la Alianza Atlántica han abierto en Helsinki un centro conjunto contra las amenazas híbridas

paso más al instar a las naciones a desarrollar sus propias capacidades defensivas en este campo y coordinarlas con las de la Alianza.

En la Cumbre de Gales de septiembre de 2014, los ciberataques se incluyeron en los supuestos del artículo 5 y de la defensa mutua. En Varsovia, en julio de 2016, se dio un nuevo paso al reconocer el ciberespacio como un dominio más de las operaciones de la OTAN —al mismo nivel que tierra, mar, aire y espacio—, y se aprobó el Plan de Acción de Ciberdefensa que define la política en esta área como prioritaria y aglutina todas las acciones aliadas en este dominio: formación, maniobras, intercambio de conocimiento, buena gobernanza, resiliencia, prevención y acciones defensivas. También los contactos para desarrollos conjuntos con la industria civil del sector a través de un organismo, para lo que se ha creado el *Nato Industry Cyber Partnership*.

Desde el punto de vista operativo, la Alianza dispone del *Nato Computer Incident Reponse Capability* (NCIRC), en Mons, con equipos y personal para la protección de los sistemas informáticos aliados y de sus estados miembros. La Agencia de Comunicación e Información, con sedes en Bruselas, Mons y La Haya, da soporte y cobertura a las operaciones y las redes de la Alianza.



OTAN

Militares de la OTAN a bordo de un avión de vigilancia AWACS desde donde se recibe y reenvía información sobre las misiones a la Agencia de Comunicaciones aliada.

OTAN

El Centro de Excelencia de Tallín acoge tanto a civiles como militares para la formación.

El *NATO Cyber Range* (Tartu, Estonia) coordina todos los ejercicios de ciberdefensa aliados (hay dos anuales y varios específicos o bilaterales). Para la formación y el análisis, además del Centro de Excelencia de Tallín, los 29 acaban de crear la Academia de Comunicación e Información de la OTAN, que con sede en Oeiras (Portugal) y operativa en el 2019, formará a cientos de civiles y militares de todos los países aliados en el campo de la ciberdefensa. También en el Colegio de Defensa, en Roma, y en la Escuela de la OTAN, en Obermmergau (Alemania), ya se ha incluido la ciberdefensa como una asignatura específica para todos los oficiales aliados.

Rosa Ruiz