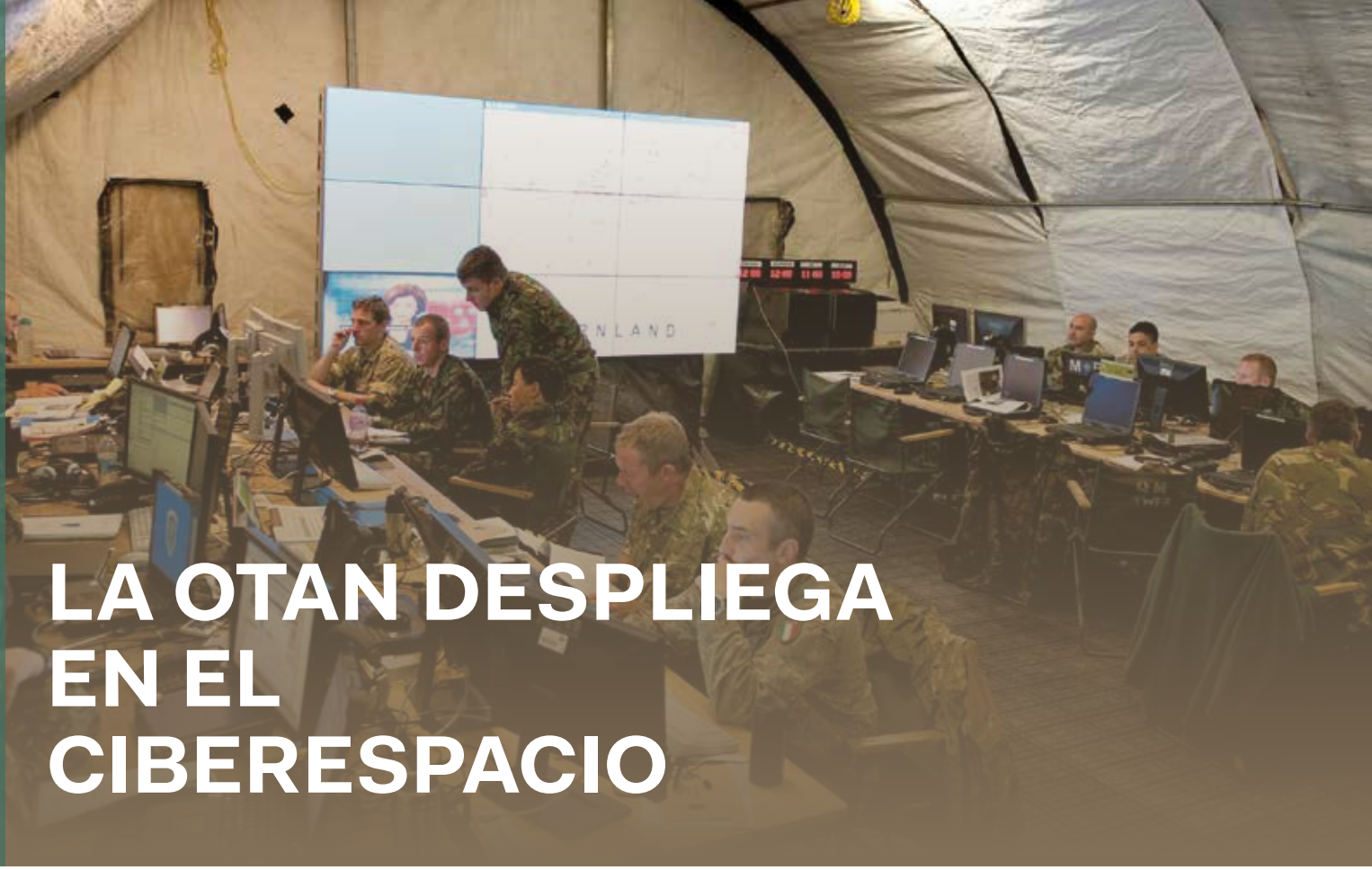


LA OTAN DESPLIEGA EN EL CIBERESPACIO

En la pasada Cumbre de Bruselas era necesario encontrar una aproximación a la disuasión más activa, creíble y modulada en un entorno cambiante de riesgos y amenazas procedentes del ciberespacio. En Bruselas se dieron los primeros pasos, al abrir la posibilidad de que los miembros proporcionen capacidades cuasi-ofensivas para disuadir y responder a una amplia gama de amenazas que se sitúan por debajo del umbral del conflicto armado

Guillem Colom Piella

Doctor en Seguridad Internacional

En julio de 2018 se celebró la última Cumbre de jefes de Estado o de Gobierno de la OTAN. Aunque las crónicas se centraron en las agrias críticas del presidente estadounidense Donald Trump a sus socios europeos, la agenda del encuentro cubrió varios aspectos de actualidad, la mayoría de los cuales estaban relacionados con la Federación Rusa (la asertividad en su área de influencia, el uso de estrategias híbridas o las operaciones de información sobre sociedades y procesos electorales extranjeros), los compromisos suscritos en la Cumbre de Gales de incrementar el gasto en defensa, la cooperación entre la OTAN y la Unión Europea o un posible cambio de rumbo en una ciberdefensa con signos de agotamiento.

Desde su arranque en la Cumbre de Praga (2002), el enfoque aliado a la ciberdefensa se había basado en la protección, la defensa y la resiliencia de sus redes y sistemas de información y comunicaciones, la posibilidad de que un ciberataque relevante pudiera activar la defensa colectiva y la integración del ciberespacio como dominio de las operaciones. Sin embargo, las limitaciones de esta aproximación basada en una concepción tecnocéntrica del ciberespacio fueron observándose a medida que la red también permitía realizar operaciones informativas contra el conjunto de la sociedad y las ciberactividades ilícitas se integraban en tácticas híbridas utilizadas por debajo del umbral del conflicto. Era necesario encontrar una aproximación a la disuasión más activa, creíble y modulada al cambiante entorno de ciberamenazas, y en Bruselas se dieron los primeros pasos.

Refrendando el valor del ciberespacio como dominio de las operaciones y asumiendo que la ciberdefensa es consustancial a la defensa colectiva, en la capital belga se tomaron importantes decisiones. La primera fue «cómo integrar los ciberefectos soberanos —facilitados por los aliados de manera voluntaria— en las operaciones y misiones de la Alianza, en el marco de una sólida supervisión política»[1]. Oficiosamente se entiende que esta decisión —ya adelantada por su secretario general a finales de 2017— es «plenamente coherente con el

mandato defensivo de la OTAN, al alinear la forma de defenderse en el ciberespacio con la manera en que lo hace en el resto de los dominios, con los aliados contribuyendo con tanques, aviones y buques a las operaciones y misiones de la OTAN»[2]. Sin embargo, quedan en el aire varios asuntos relevantes.

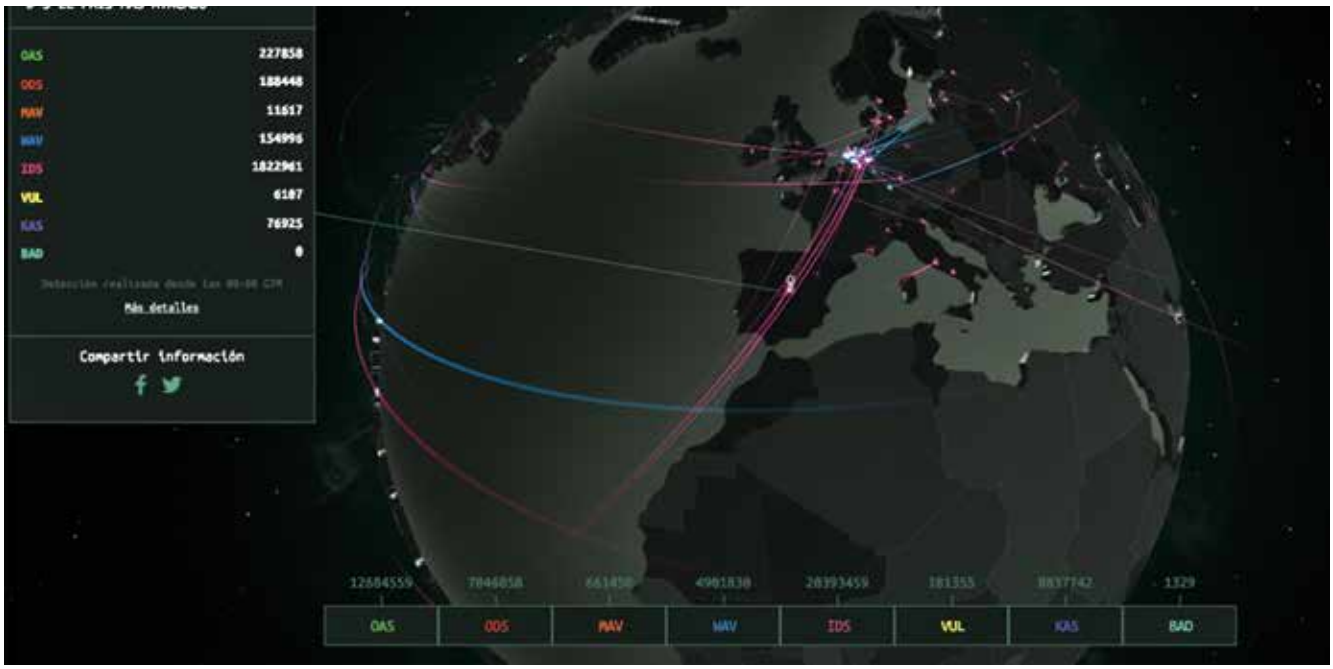
Primero, la declaración sugiere que cada país —Reino Unido, Países Bajos, Dinamarca, Estonia o Estados Unidos ya se han ofrecido a proporcionar cibercapacidades nacionales[3]— proporcionará al mando aliado los «ciberefectos» que, producidos por su propia ciberarma, servirán para la conducción de las operaciones aliadas. Haciendo una analogía, el socio no proveerá un grupo de artillería sino la destrucción del objetivo. Segundo, estos «ciberefectos» serán soberanos: aunque el efecto deseado será identificado y su consecución supervisada por la OTAN, no puede descartarse que tanto la inteligencia para identificar el objetivo como su selección y el mando y control de la ciberarma recaigan sobre cada país. Esta posibilidad parece corroborarse cuando un mando aliado argumenta que «solicitaremos un efecto utilizando ciberarmas durante una operación y uno de los aliados nos lo proporcionará sin más información»[4] o Washington sostiene que mantendrá el control sobre su personal y capacidades[5]. Tercero, si estos efectos son soberanos, ¿cómo se integrarán en el mando y control aliado de las operaciones?, ¿cuál será la responsabilidad de la Alianza en su consecución?, ¿y si estos producen «ciberefectos» no deseados o desproporcionados sobre las infraestructuras críticas del adversario debido a un fallo de inteligencia que motiva una escalada de tensiones?, ¿cómo se producirá la aprobación política de los ciberefectos?, ¿se fijarán medidas de confianza para que el resto de los aliados acepten los efectos sin conocer cómo se producen? Finalmente, aunque la inclusión del ciberespacio como dominio de las operaciones debería facilitar el planeamiento de la defensa —que traduce los objetivos políticos en necesidades militares y contribuciones nacionales en términos de fuerzas terrestres, navales y aéreas—, no parece que en un futuro cercano se integren las ciberarmas nacionales en este proceso cuatrienal. En cualquier caso, la decisión de proporcionar «ciberefectos soberanos [...] en el marco de una sólida supervisión política»[6] puede parecer controvertida, pero permite reforzar la capacidad disuasoria de la OTAN sin que los miembros que los suministren deban revelar unos ciberarsenales cuyo desarrollo habrá requerido enormes recursos humanos y materiales y que otros aliados podrían imitar. Aportando los «ciberefectos», estos ni deberán revelar la ciberarma ni tampoco las tácticas, técnicas y procedimientos que guiarán su empleo operativo, lo que reduce el riesgo de *free-riding* y obligan a que todos los aliados desarrollen cibercapacidades propias.

Cumbre de jefes de Estado o de Gobierno de la OTAN, 11-12 de julio de 2018, Bruselas

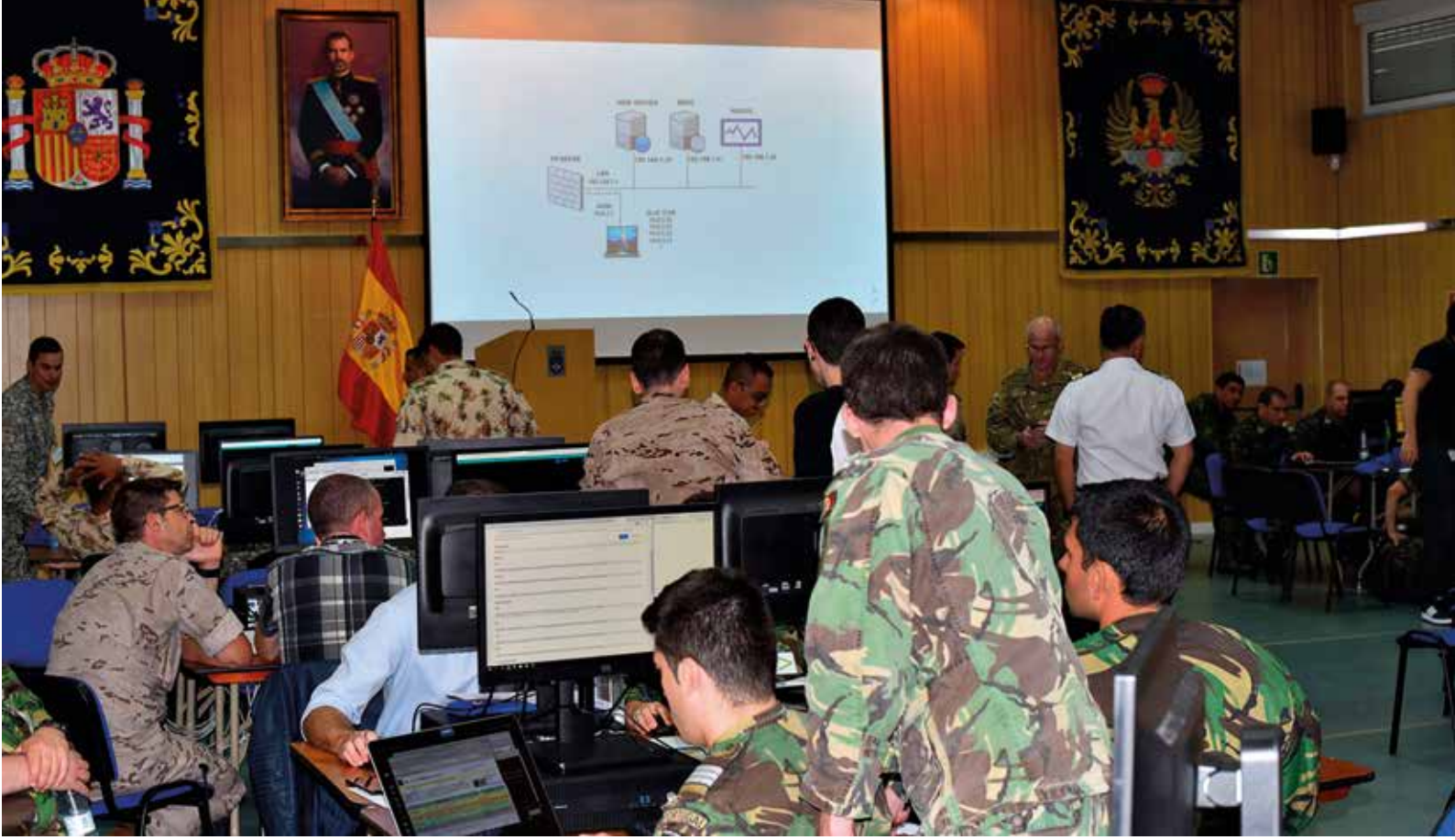
Cada país proporcionará al mando aliado los «ciberefectos» que, producidos por su propia ciberarma, servirán para la conducción de las operaciones aliadas

En segundo lugar, otra interesante novedad es que «los aliados pueden considerar apropiado realizar una atribución de una ciberactividad maliciosa y responder de forma coordinada, reconociendo que la atribución es una prerrogativa nacional soberana»[7]. Antes de que la OTAN avalara formalmente esta posibilidad, miembros como Dinamarca, Estonia, Lituania, Países Bajos, Reino Unido o Estados Unidos ya habían realizado atribuciones públicas de ciberactividades ilícitas —la mayoría vinculadas con amenazas persistentes avanzadas (APT) procedentes de Pekín, Moscú o Pyongyang[8]— contra su soberanía. Aunque continuará generando controversias debido a la misma naturaleza del ciberespacio, una atribución transparente, creíble y apoyada por un exhaustivo análisis forense no solo es esencial para establecer responsabilidades legales y posibles sanciones, sino también para desincentivar al adversario y lograr que este cumpla con la legalidad[9]. No obstante, cabe preguntarse qué efectos prácticos tendrá para la OTAN que sus miembros puedan atribuir responsabilidades de ciberincidentes —que los adversarios mantendrán bajo el umbral de la defensa colectiva— sin el apoyo manifiesto de Bruselas: ¿mejorará la disuasión?, ¿motivará una escalada de tensiones?, ¿generará controversias políticas en el seno de la Alianza?, ¿desincentivará a estos países que han hallado en el ciberespacio una forma barata y asimétrica para proyectar su poder?

En tercer lugar, «reafirmando el mandato defensivo de la OTAN, estamos decididos a usar toda la gama de capacidades, incluido el ciberespacio, para disuadir, defendernos y contrarrestar todo el espectro de ciberamenazas, incluyendo aquellas que se ejecutan como parte de una campaña híbrida»[10]. Las operaciones de información rusas en el exterior han puesto de manifiesto el potencial de las nuevas tecnologías para realizar actividades de subversión y desestabilización[11]. Aunque su concepción apenas ha variado desde la década de 1920, internet ha permitido aumentar el alcance y la efectividad de estas labores —difundiendo desinformación, realizando propaganda computacional, inteligencia invasiva, filtrando información o llevando a cabo ciberataques de bajo perfil[12]— que pueden formar parte de una campaña híbrida. Situados en la amplia zona gris que separa la paz de la guerra, estos actos aislados difícilmente podrían constituir un *casus belli* y motivar la activación del Artículo 5 del Tratado de Washington, pero su impacto agregado utilizando la «táctica del salami» sí podría



Ejemplo de mapa de ciberataques sobre España elaborado en tiempo real por la empresa de ciberseguridad Kaspersky

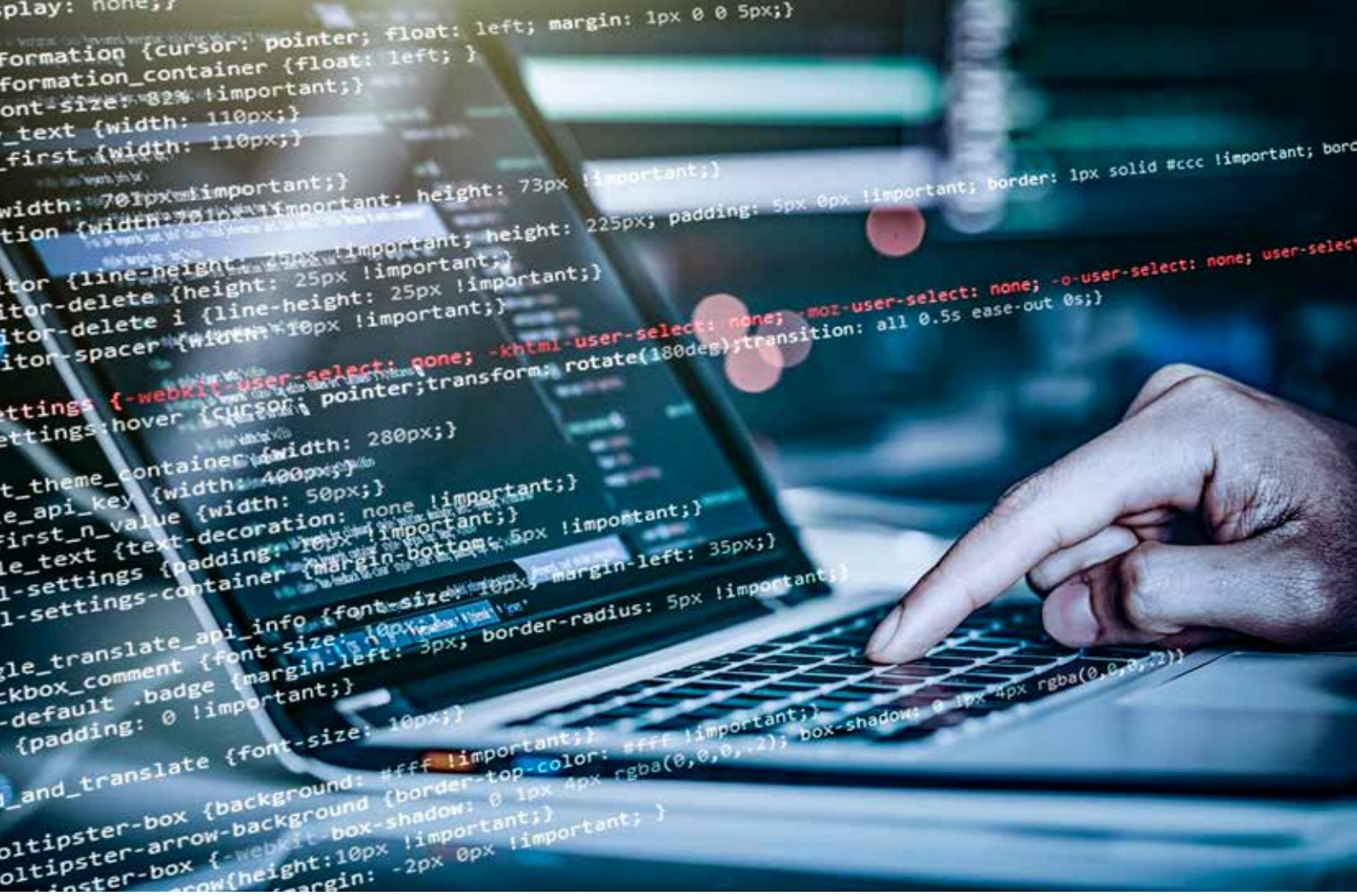


Las ciberoperaciones deberán estar coordinadas por todos los miembros de la OTAN

alterar la correlación de fuerzas[13]. En consecuencia, además de invalidar la disuasión por castigo, la propia naturaleza de estas actividades también convierte en irrelevante la ciberdisuasión por negación aliada, basada en la protección, defensa y resiliencia de sus redes, sistemas e infraestructuras pero no en los corazones y mentes de su población. En otras palabras, al impedir cualquier respuesta efectiva y proporcionada estas actividades comprometen la credibilidad de la disuasión aliada, tal y como sucedió durante la Guerra Fría con la inutilidad de la represalia masiva para responder a crisis limitadas en Europa.

La tradicional ciberdisuasión por negación se complementará por una disuasión por castigo

En consecuencia, si para enfrentarse a amenazas híbridas se ha resuelto «usar toda la gama de capacidades, incluido el ciberespacio, para disuadir, defendernos y contrarrestar todo el espectro de ciberamenazas»[14], y para todo el espectro de amenazas «implementar medidas que permitan imponer costes a quienes nos hacen daño»[15], se abre la puerta a que la Alianza Atlántica adopte una postura más activa en el ciberespacio. Su tradicional ciberdisuasión por negación (basada en el refuerzo de la seguridad, la defensa y la resiliencia de sus redes y sistemas) se complementará por una disuasión por castigo, que podrá contener respuestas convencionales, cibernéticas e incluso nucleares. Es probable que esta decisión vaya acompañada por el desarrollo de distintas opciones de respuesta que, proporcionadas a la agresión sufrida, permitan controlar la escalada bélica en el mundo físico y virtual. Además, es probable que Bruselas no solo responda a ciberataques enemigos mediante *hack back* utilizando los «ciberefectos» soberanos, sino que también realice actividades de «defensa avanzada» para prevenir ciberataques. Codificada en la ciberestrategia militar estadounidense de 2018, esta pretende «interrumpir o detener cualquier ciberactividad maliciosa en su origen, incluida la que se sitúa por debajo del umbral del conflicto armado»[16] mediante la identificación del potencial agresor o la degradación o destrucción de las redes y sistemas que usará para realizar las operaciones de inteligencia, informativas, de explotación o de ataque[17]. Realizadas en el marco de la provisión de cibercapacidades estadounidenses a la OTAN, estas actividades pueden mejorar la seguridad y reforzar la disuasión aliada frente a una amplia gama de amenazas procedentes del ciberespacio. Sin embargo, su ejecución también puede motivar grandes controversias políticas porque Washington difícilmente proporcionará la inteligencia de amenazas ni detallará las actividades realizadas para minimizar la amenaza, y sus acciones difuminarán la demarcación entre las operaciones aliadas y las estadounidenses. Además, sus efectos operativos, estratégicos y políticos pueden provocar tanto grietas en la unidad de acción de la OTAN como motivar respuestas contra los aliados con las ciberdefensas más débiles e incluso escaladas militares de consecuencias impredecibles.



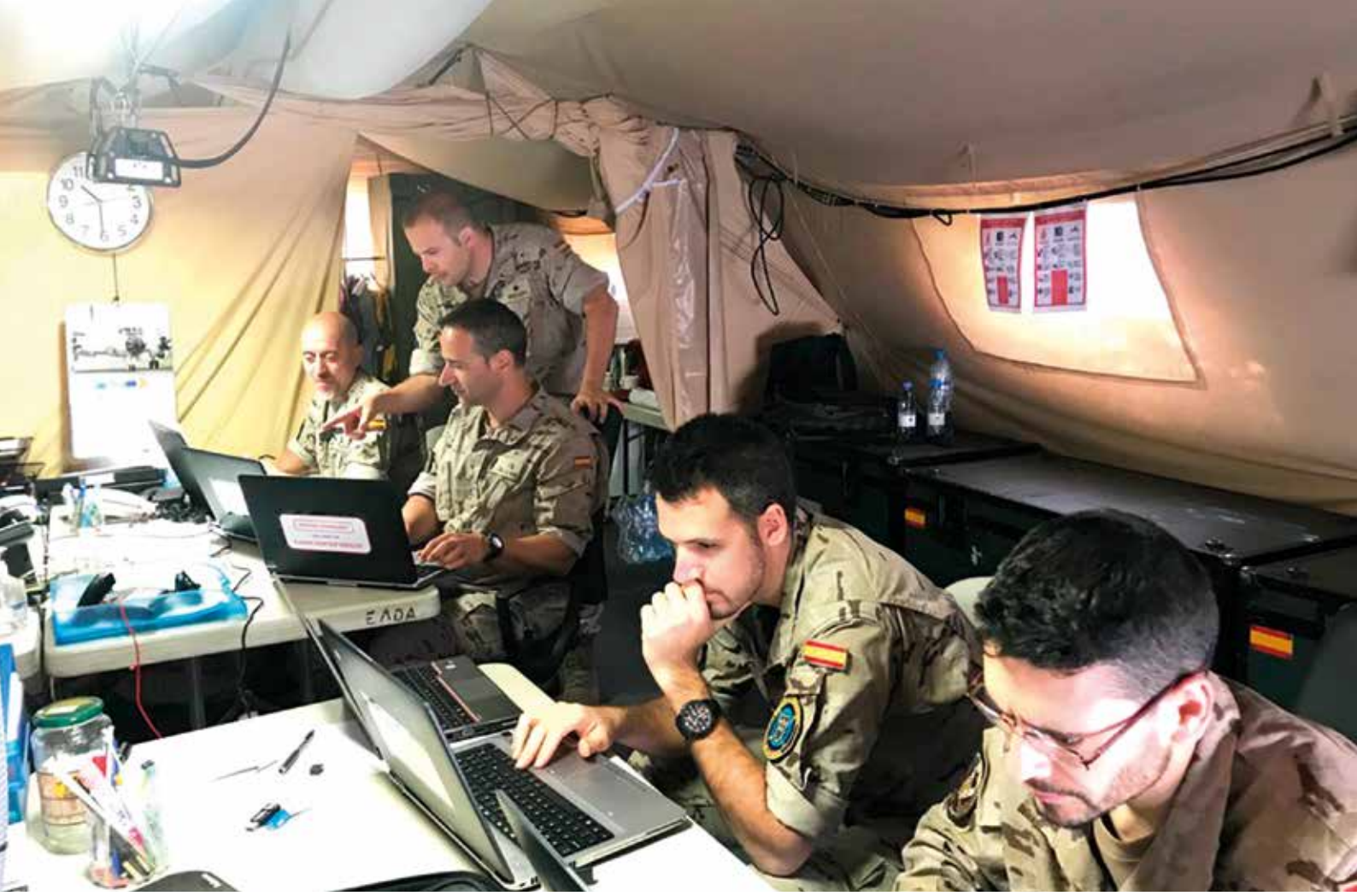
El vector informativo puede transformarse en una fantástica herramienta para realizar actividades en la zona gris del conflicto

Finalmente, los jefes de Estado o de Gobierno aliados también refrendaron la creación de un centro de ciberoperaciones para facilitar la coordinación de las actividades en este dominio. Pactado por los ministros de Defensa en febrero de 2018, este mando que deberá lograr la plena capacidad operativa en el año 2023 integrará el ciberdominio en el planeamiento y la conducción de las operaciones aliadas. Sin embargo, queda por ver si se compartirá la inteligencia sobre los ciberespacios adversarios, cómo se definirán e integrarán los «ciberefectos» nacionales y cómo se ostentará el mando y control de las ciberoperaciones.

Este conjunto de decisiones puede motivar un antes y un después en la ciberdefensa aliada. De implementarse, estos cambios transformarán la manera en que la OTAN concibe, opera, se relaciona y disuade en el ciberespacio.

En conclusión, desde los primeros ciberataques contra los sitios web de la OTAN hasta la promulgación de su primera doctrina de ciberoperaciones habrán pasado veinte años. Durante este tiempo, la Alianza Atlántica y sus miembros han tomado conciencia de la utilidad del ciberespacio para paralizar un país (Estonia, 2007), la integración de lo «ciber» en las operaciones militares (Georgia, 2008), la militarización de la información y las redes sociales (Crimea, 2013), la combinación del vector cibernético, informativo y electromagnético (Ucrania, 2014) o la posibilidad de emplear el ciberespacio para realizar actividades de desestabilización, subversión e influencia política (Estados Unidos, 2016). Sin embargo, quizás la lección que mejor han aprendido es que la limitada regulación, la anonimidad, la apertura, la libertad de acción o la asimetría que caracterizan este entorno permiten a muchos actores proyectar su poder enmascarando sus actividades, dificultando la atribución de sus acciones y burlando cualquier posible respuesta aliada. Ello consolidó el vector informativo como una fantástica herramienta para realizar actividades en la zona gris del conflicto y expuso las limitaciones del enfoque aliado a la ciberdefensa basado en la ciberdefensa y ciberresiliencia, y la necesidad

Los jefes de Estado o de Gobierno aliados refrendaron la creación de un centro de ciberoperaciones que deberá lograr la plena capacidad operativa en el año 2023



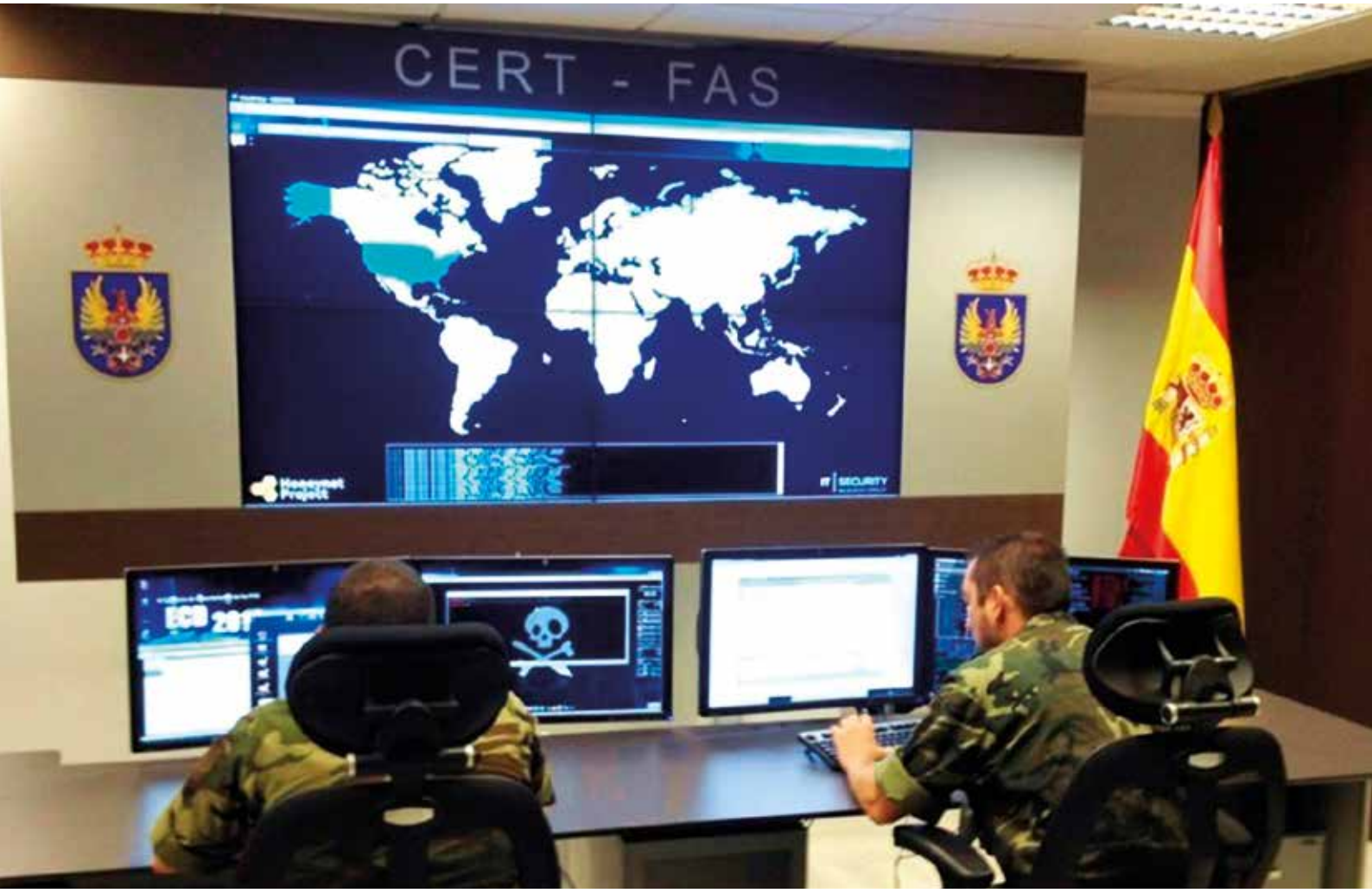
El Mando Conjunto de Ciberdefensa en el *Destacamento Marfil* en Dakar (Senegal)

de hallar una aproximación a la disuasión más activa, creíble y modulada al actual entorno de riesgos y amenazas procedentes del ciberespacio.

En el seno de la OTAN cada país es responsable de generar sus propias capacidades en ciberdefensa

En este sentido, aunque es probable que en la capital belga se haya dado un nuevo impulso —quizás el definitivo— en el desarrollo de la ciberdefensa aliada, quedan dos importantes asuntos pendientes que pueden comprometer su marcha. Por un lado, homogeneizar las cibercapacidades de los Estados miembros. Desde la firma del Compromiso de Ciberdefensa, los aliados han acelerado el desarrollo de sus propias cibercapacidades, mejorado la resiliencia de sus redes, establecido modelos de gobernanza de la ciberseguridad o reforzado la colaboración pública y privada en esta materia. Teniendo en cuenta que la ciberseguridad de cualquier organización se mide por el eslabón más débil de la cadena, estas acciones han redundado en la ciberdefensa aliada. Sin embargo, el grado de madurez tecnológica, doctrinal u organizativa de los Veintinueve en esta materia continúa siendo muy desigual. Esta misma heterogeneidad —que también se extiende a la metodología utilizada para cuantificar y caracterizar los ciberincidentes— ha motivado toques de atención por parte de la OTAN al recordar que sus capacidades de ciberdefensa cubren las necesidades operativas del cuartel general, la estructura de mandos y sus organismos asociados y que, en línea con el Artículo 3 del Tratado de Washington, cada país es responsable de generar sus propias capacidades. También ha provocado que varias potencias cibernéticas se muestren reticentes a intercambiar información de amenazas, cooperar en el desarrollo de capacidades, desvelar su arsenal cibernético o proporcionar «ciberefectos» soberanos si ello implica poner bajo mando aliado la ciberarma, el proceso de selección del objetivo, el personal implicado o el mando y control de la operación.

Será vital que los miembros tomen conciencia de que la defensa hace mucho que dejó de ser analógica



Equipo de Respuesta ante Emergencias Informáticas *(Computer Emergency Response Team)* de las Fuerzas Armadas

El otro asunto pendiente sería consolidar la integración del vector «ciber» en el planeamiento y la conducción de las operaciones aliadas. Aunque la consideración del ciberespacio como dominio operativo, la aprobación de la primera ciberdoctrina y la creación de un mando de ciberoperaciones son pasos positivos, continúan quedando varios asuntos pendientes que comprenden desde la armonización de la atribución de autorías, la provisión de «ciberefectos» nacionales en las misiones aliadas, la simplificación y racionalización de los procesos de toma de decisiones, su integración en todo el espectro operativo y su empleo en apoyo a las actividades cinéticas —incluyendo el eventual uso de ciberoperaciones ofensivas en el marco del mandato defensivo— hasta la clarificación de las provisiones de la defensa colectiva, la definición de umbrales más precisos sobre los ciberataques que podrían activarla y, sobre todo, fijar opciones de respuesta proporcionadas, efectivas y disuasorias para las actividades informativas en la zona gris.

La explotación del ciberespacio en las tácticas híbridas, las operaciones informativas en la zona gris o las actividades maliciosas realizadas por actores estatales en el ciberespacio bajo el umbral del conflicto están obligando a que la Alianza clarifique su estrategia y refuerce su disuasión y capacidad de operar en el ciberespacio tal y como lo hace en tierra, en el mar o en el aire. Y para ello será vital que los miembros tomen conciencia de que la defensa hace mucho que dejó de ser analógica.

NOTAS

1. Declaración final de la Cumbre de Bruselas (11 de julio de 2018), para. 20.
2. Brent, L.: «NATO's Role in Cyberspace». *NATO Review* (12 de febrero de 2019).
3. Arts, S.: *Offense as the New Defense: New Life for NATO's Cyber Policy*. The German Marshall Fund of the United States, Washington DC, p. 2; 2018.
4. Palabras del coronel Ali Rizwan, antiguo director de seguridad de la información de la Task Force Cyber de la Alianza Atlántica, en: Ricks, T. y Rizwan, A.: «NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons». Foreign Policy (7 de diciembre de 2017).
5. Ali, I.: «With an eye on Russia, U.S. pledges to use cyber capabilities on behalf of NATO». Reuters (3 de octubre de 2018).
6. Declaración final de la Cumbre de Bruselas (11 de julio de 2018), para. 20.
7. Ibídem.
8. *FireEye: Advanced Persistent Threat Groups. Who's who of cyber threat actors.* En línea: https://www.fireeye.com/current-threats/apt-groups.html

9. Davis, J. et al.: *Stateless Attribution: Toward International Accountability in Cyberspace*. RAND Corporation, Santa Mónica; 2017.
10. Declaración final de la Cumbre de Bruselas (11 de julio de 2018), para. 20.
11. Interpretando que Occidente utiliza el poder blando y el espacio informativo para atacar los valores y símbolos rusos, movilizar y desmovilizar a la sociedad, incitar revoluciones de colores, provocar cambios de régimen o justificar intervenciones externas, la comunidad estratégica rusa ha sido muy reacia a la entrada de internet en el país. Por ello, la Federación Rusa no solo ha blindado el ecosistema informativo nacional (de las licencias de radiotelevisión a los servicios de telefonía e internet) frente a cualquier injerencia externa, sino que también ha desarrollado capacidades para combatir en el espectro informativo. Precisamente, su jefe de Estado Mayor de la Defensa expresó algo que tanto sus antecesores como los teóricos militares del país planteaban desde la década de 1990: «el uso del internet global permite ejercer un impacto masivo y dedicado sobre la conciencia de los ciudadanos de los Estados objeto de la agresión. Los recursos informativos se han convertido en una de las armas más efectivas, cuyo empleo permite desestabilizar un país en cuestión de días» [Gerasimov, V.: «Po opytu Sirii. Gibridnaâ vojna trebuet vysokotehnologičnogo oružiâ i naučnogo obosnovaniâ». *Voenno-promyšlennyj kur´er*, 9(624), 2016].
12. Téngase en cuenta que la definición de *ciberataque* propuesta por el Manual de Tallin es: «una ciberoperación, ofensiva o defensiva, susceptible de causar lesión o muerte a las personas o daño o destrucción a los objetos» y no solo deja mucho lugar a la interpretación, sino que obvia numerosas actividades potencialmente más lesivas pero situadas bajo el umbral del conflicto. Schmitt, M. (ed.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Regla núm. 30, pp. 106-12. Cambridge University Press, Nueva York; 2017).
13. Esta idea también fue planteada por Estados Unidos al argumentar que «los adversarios operan continuamente bajo el umbral del conflicto armado para debilitar las instituciones y lograr ventajas estratégicas [...] extendiendo su influencia sin utilizar la agresión física [...] sin miedo a consecuencias legales o militares» (U.S. Cyber Command: *Achieve and Maintain Cyberspace Superiority*. p. 3. GPO, Washington DC; 2018).
14. Declaración final de la Cumbre de Varsovia (11 de julio de 2018), para. 20. Recopilado de https://www.nato.int/cps/en/natohq/official_texts_156624.htm
15. Ibídem.
16. Department of Defense: *DoD Cyber Strategy*. p. 1. GPO, Washington DC; 2018.
17. Chesney, R.: *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes.* Lawfare blog (25 de septiembre de 2018). En línea: https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes.■

Comando cibernético del ejército de EE. UU. Fort Belvoir, Fairfax (Virginia)