Documento de trabajo 20/2018
13 de diciembre de 2018

Amenazas híbridas: nuevas herramientas para viejas aspiraciones

Carlos Galán

Amenazas híbridas: nuevas herramientas para viejas aspiraciones

Carlos Galán | Licenciado y doctor en Informática, abogado especialista en Derecho de las TIC, profesor de la Universidad Carlos III de Madrid, presidente de la Agencia de Tecnología Legal, asesor del Centro Criptológico Nacional (Centro Nacional de Inteligencia-Ministerio de Defensa) y miembro del Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano.

Índice

Resumen

Desde hace unos años, los términos *amenazas híbridas*, *guerra híbrida*, *fake news*, *posverdad*, *desinformación*, etc. se han venido incorporando al universo y al diálogo de la seguridad y, muy especialmente, de la ciberseguridad sin que, en ocasiones, se hayan usado adecuadamente, confundiendo unos con otros o simplemente otorgándoles un nombre y unas características muy alejadas de la realidad, como si su encuadramiento constituyera un ejercicio más de la posverdad que pretenden denotar. En cualquier caso, de lo que no cabe duda es de que, sea lo que fuere lo que representan, su materialización constituye una realidad incuestionable que está afectando seriamente el desenvolvimiento de los Estados, de las sociedades y de sus instituciones.

El presente Documento de Trabajo pretende examinar esta realidad y sus matices más significativos, distinguiendo lo que hay de nuevo en ella de lo que no es más que un *aggiornamento* de comportamiento clásicos; analizar su arquitectura para aislar sus elementos constituyentes y acotar sus límites —si ello es posible, como se verá—, y estudiar las respuestas que están ofreciendo las instituciones para terminar presentando unas conclusiones y proponiendo algunas acciones concretas, especialmente desde los puntos de vista jurídico e institucional.

Introducción

Aunque un poco más adelante definiremos con mayor formalidad cada uno de los elementos en estudio, conviene ahora realizar una primera inmersión en su conceptualización básica.

En primer lugar, podemos apuntar que las denominadas *amenazas híbridas* son acciones coordinadas y sincronizadas —con origen habitualmente, pero no solo, en los servicios de inteligencia de los agentes de las amenazas— que atacan deliberadamente vulnerabilidades sistémicas de los Estados y sus instituciones a través de una amplia gama de medios y en distintos sectores objetivo (políticos, económicos, militares, sociales, informativos, infraestructuras y legales) utilizando el ciberespacio como la herramienta más versátil y adecuada para sus propósitos.

Una característica definitoria de este tipo de amenazas es su capacidad para explotar los umbrales de detección y atribución de tales acciones —lo que en sí mismo puede considerarse una vulnerabilidad sistémica—, así como la frontera jurídica entre guerra y paz, y con ello, por ejemplo, impedir la activación del compromiso de "asistencia mutua" recogido en el art. 5 del Tratado de la OTAN. El objetivo de los denominados *ataques híbridos* es casi siempre el mismo: influir en los diferentes mecanismos de toma de decisiones de la víctima (Estado u organización), ya sean decisiones a nivel local, estatal o institucional, para favorecer o alcanzar los objetivos estratégicos del atacante al tiempo que socava la credibilidad, la estabilidad o la moral de la víctima.

Definiciones y conceptos concordantes: amenazas híbridas y guerra híbrida

Como señalábamos al principio, no es infrecuente encontrar en la literatura relacionada términos tales como *guerra híbrida*, *amenazas híbridas*, *ataques híbridos*, etc. utilizados como si se tratara de conceptos semánticos intercambiables. No es así. Abordar con rigor cualquier disciplina pasa, en primer lugar, por establecer un marco de conceptos definidos, como los siguientes:

Amenaza híbrida (*hybrid threat*)	Fenómeno resultante de la convergencia e interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional.[1]
Conflicto híbrido (*hybrid conflict*)	Situación en la cual las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y a la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas.
Guerra híbrida (*hybrid war*)	Situación en la que un país recurre al uso abierto de la fuerza (armada) contra otro país o contra un actor no estatal, además de usar otros medios (por ejemplo, económicos, políticos o diplomáticos).

Según el Consejo de Europa, cuando no existe confrontación armada (encubierta o no) y atendiendo a las medidas de protección de la seguridad nacional de los Estados y sus límites legales, parece más exacto y conveniente utilizar los términos *amenaza híbrida* o *conflicto híbrido* que *guerra híbrida*. Según el Servicio de Estudios del Parlamento Europeo, las amenazas híbridas pueden comprender varias situaciones, incluidos los actos terroristas (de Boko Haram, al-Qaeda o Daesh, por ejemplo), acciones contra la ciberseguridad de los Estados o sus organizaciones, acciones de grupos delictivos armados (como los de los cárteles de la droga mexicanos), disputas marítimas (como las que se ubican en el mar de la China Meridional), restricciones al uso del espacio, actos económicos hostiles (como el bloqueo de las exportaciones japonesas por parte de China en 2010) y operaciones militares encubiertas (como el caso de los *little green men* en Crimea).[2]

En todo caso, las amenazas híbridas pueden partir tanto de Estados como de agentes no estatales y abarcar formas de enfrentamiento tanto violentas como no violentas, aunque, como hemos señalado, desde el punto de vista jurídico es más preciso utilizar el término *guerra híbrida* solo cuando existe un conflicto armado declarado y no encubierto y, en consecuencia, se activa la aplicación del Derecho Internacional Humanitario (DIH).[3]

El concepto *guerra híbrida* combina capacidades cinéticas convencionales (acciones armadas no encubiertas) con tácticas irregulares tales como el terrorismo y crímenes transnacionales, especialmente cuando son cometidos por actores que, aparentemente patrocinados o dependientes de un Estado, dan la impresión de no encontrarse bajo su autoridad. Estas acciones también suelen recurrir al empleo de otros medios —ciberataques, desinformación y propaganda—, dirigidos a poblaciones enteras o incluso a minorías nacionales u otras minorías significativas, medios entre los que se incluyen

[1] "At a Glance: Understanding Hybrid Threats", Servicio de Estudios del Parlamento Europeo, junio 2015.

[2] "Legal challenges related to the hybrid war and human rights obligations", Doc. 14.523, 6 de abril de 2018, Consejo de Europa, Asamblea Parlamentaria, Comité de Asuntos Legales y Derechos Humanos.

[3] El DIH es una rama del Derecho Internacional Público que busca limitar los efectos de los conflictos armados protegiendo a las personas que no participan en las hostilidades y regulando los medios y métodos de guerra y conducta en los conflictos armados (*ius in bello*). Se compone de una serie de normas, en su mayoría reflejadas en los Convenios de Ginebra de 1949 y sus protocolos adicionales.

la corrupción de agentes esenciales mediante uso de dinero negro o la habilitación de presupuestos paralelos.

Numerosos especialistas conciben la *guerra híbrida* como un tipo de amenazas intrínsecamente nuevo. Su proliferación se ha visto alentada por la aparición de nuevos actores subestatales, nuevos tipos de armas y una nueva representación ideológica, mientras que el concepto de *amenazas híbridas* debe reservarse para situaciones en las que los Estados o actores no estatales emplean medios no violentos como instrumentos de guerra y los integran con el empleo de la fuerza armada o la amenaza de la fuerza. El sector académico no ha mostrado mucho interés en los aspectos legales de la guerra híbrida, ya que la mayoría de los problemas legales relacionados con este concepto, como la violación de la integridad territorial, el apoyo a los movimientos separatistas o el incumplimiento de los acuerdos internacionales, no son nuevos.

¿Qué persiguen y por qué existen las amenazas híbridas?

Los *little green men* en Ucrania, el ataque a los servidores de correo electrónico del Comité Nacional Demócrata de los Estados Unidos, las protestas y contraprotestas en relación con una mezquita en Houston…, acciones, en estos casos, presuntamente orquestadas por elementos rusos[4] constituyen solo unos pocos ejemplos de las amenazas híbridas del siglo XXI. Como hemos señalado, las amenazas híbridas persiguen alcanzar sus objetivos estratégicos influyendo en la toma de decisiones de sus víctimas y socavando sus valores, su estructura social y la confianza de la población.

En general, las amenazas híbridas han venido persiguiendo, entre otros objetivos[5]:

- Erosionar la confianza de los ciudadanos en sus instituciones.
- Generar desconfianza en el sistema democrático.
- Socavar la cohesión social o los modelos sociales de los Estados, de las comunidades políticas (como la UE) o de las organizaciones internacionales (la OTAN, por ejemplo).
- Fragilizar el sistema de gobierno de sus víctimas.
- Convencer de la decadencia de un sistema (tanto a la población de la víctima como a su propia población).

La razón primigenia más probable para la existencia de las amenazas híbridas hay que buscarla en la naturaleza cambiante del orden mundial, cuyos componentes sociales,

[4] El informe del German Marshal Fund "Policy Blueprint for Countering Authoritarian Interference in Democracies" señaló que el gobierno ruso había utilizado ciberataques, desinformación e influencia financiera para interferir en los asuntos internos de, al menos, 27 países europeos y norteamericanos desde 2004 (Alemania, España, Estados Unidos, Francia y Reino Unido, entre otros).

[5] Alejandro Alvargonzález, secretario general adjunto de la OTAN, ponencia en la Jornada sobre "Guerra híbrida: nuevas amenazas", Instituto de Seguridad y Cultura, mayo de 2018, Senado de España.

políticos y económicos no han dejado de alterarse desde el fin de la Guerra Fría. El denominado *poder relacional*, es decir, el poder de modificar las creencias, actitudes, preferencias, opiniones, expectativas, emociones o predisposiciones de los demás para actuar, es hoy, seguramente, más importante que el poder material, y el medio facilitador de esta realidad es, sin duda alguna, el ciberespacio. El ciberespacio ha venido a difuminar las dimensiones internas y externas de la seguridad de los Estados, lo que posibilita que actores estatales y no estatales menos favorecidos económicamente puedan amplificar fácilmente sus intentos de influencia.

En este estado de cosas, ¿hasta qué punto podemos seguir hablando del papel del Estado nación? ¿Hasta qué punto caben alianzas basadas en normas que limitan la respuesta a acciones antagónicas asimétricas? Si algo tenemos claro es que el rápido desarrollo tecnológico ha dado lugar a un nuevo dominio —el ciberespacio— donde las reglas de juego nacionales e internacionales aún están en su infancia. No podemos considerar el ciberespacio como una frontera, sino como un verdadero ámbito operativo —un dominio— que representa un desafío a la idea tradicional de seguridad.

Por otro lado, si el orden mundial es cambiante, no lo es menos el ecosistema de la información pública y el panorama de los medios de comunicación. La digitalización de la sociedad, la penetración y el uso masivo de las redes sociales y la aparición de nuevos creadores de opinión, la forma en la que se produce la información, su velocidad para expandirse planetariamente y la forma en la que las personas acceden a la misma traspasando fronteras nacionales han evidenciado la necesidad de tomar en consideración diferentes culturas, políticas y modos de entender la vida, porque la información producida en un país puede interpretarse de maneras muy diferentes en otros lugares. La información, por tanto, no es una excepción: Internet se ha convertido en un nuevo campo de batalla donde las reglas aún se están formulando. Las noticias falsas, la desinformación y los *hechos* basados en opiniones convulsionan el dominio público. Como resultado, se está erosionando la confianza, que es uno de los pilares fundamentales de las sociedades.

La naturaleza cambiante de conceptos tan tradicionales como los conflictos armados o la guerra también ha sido señalada como uno de los factores que han alentado la aparición de las amenazas híbridas, que, situándose por debajo del umbral de lo que podría considerarse un conflicto armado convencional o una guerra declarada, están en condiciones de alcanzar sus objetivos reduciendo significativamente las bajas militares y evitando en lo posible las bajas civiles. En un escenario “híbrido”, suele afirmarse, el enfrentamiento que se pretende es el de las sociedades involucradas, no el de los ejércitos.

Finalmente, se ha producido un cambio generacional. Se ha dejado atrás la Guerra Fría, cuyas pretensiones de orden mundial pasaban por las relaciones entre las superpotencias —y la lucha ideológica entre el comunismo y el capitalismo— y el temor a la guerra nuclear. Con posterioridad, la globalización puso el acento en los conceptos de integración e interdependencia y cambió la forma de entender el mundo y las relaciones entre sus habitantes, desarrolladas por las nuevas generaciones en la cultura digital y en el ciberespacio.

Casos para el análisis

Las amenazas híbridas contra el sector privado

El sector privado tiene un papel esencial en la protección de las infraestructuras críticas (energía, transporte, salud pública, etc.), en las que un ataque no convencional basado en acciones híbridas podría provocar una grave perturbación económica o social. Los Estados pueden regular las obligaciones de las entidades afectadas, ya sean del sector público o privado, con normas tales como la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, para la protección de infraestructuras críticas, pero el 80-90% de las denominadas "infraestructuras críticas" en los países democráticos son propiedad o están operadas por el sector privado, lo que significa que, en muchas ocasiones, la primera línea de defensa se sitúa directamente bajo la responsabilidad de la industria privada.[6]

Ataques contra las instituciones democráticas

En 2016, 126 millones de ciudadanos estadounidenses estuvieron expuestos a la desinformación rusa antes de las elecciones presidenciales. Según *The Washington Post*, esto ocurrió porque el gobierno no estaba preparado para enfrentar amenazas asimétricas de esta naturaleza: la infraestructura electoral estaba obsoleta, las ciberdefensas eran insuficientes, las empresas tecnológicas y de servicios no anticiparon cómo se podían manipular sus plataformas y la cooperación público-privada fue escasa. Además, la polarización de los ciudadanos, del sistema político y de los medios de comunicación amplificaron la desinformación.[7]

El Parlamento Europeo también se ha interesado en analizar la desinformación.[8] Entre sus conclusiones, destaca que, gracias a las tecnologías digitales, el acceso a las noticias se ha vuelto más fácil y barato y su consumo ha tenido un crecimiento sin precedentes. Lo anterior ha facilitado el incremento de los intermediarios *online* en un marco regulatorio que los hace no responsables del control editorial y de la mala conducta de sus usuarios, por lo que, frecuentemente, las noticias *online* se caracterizan por la falta de verificación de los hechos y su escasa originalidad. En el mismo sentido, producir y difundir desinformación es mucho más barato y fácil gracias a la disponibilidad de una infraestructura de plataformas digitales de extremo a extremo para el intercambio de información. En la era anterior a Internet, solo los medios de comunicación con recursos suficientes podían llegar a las grandes audiencias, pero hoy en día se ha roto la correlación entre la divulgación de noticias y los controles de calidad, con lo que cualquiera puede ser un editor con alcance global. Además, no hay motivos para esperar que las plataformas digitales renuncien a la desinformación mientras las noticias falsas generen tráfico y dinero (vía publicidad, por ejemplo) sin la contrapartida de la

[6] Jarno Limnell, "Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed", *Strategic Analysis*, Hybrid Center of Excellence, marzo de 2018.

[7] Craig Timberg, "Russia used mainstream media to manipulate American voters", The Washington Post, 15 de febrero de 2018.

[8] Parlamento Europeo-CEPS, "The legal framework to address "fake news": possible policy actions at the EU level", junio de 2018. El documento distingue cuatro formas de *fake news*: "content bubbles (echo chambers)", "unintentional fakes/opinions (misinformation)", "intentional fakes or amplifiers (disinformation)" y "disinformation (influence) operations".

responsabilidad; no hay una razón sólida para esperar que las plataformas digitales tengan un incentivo para tomar decisiones contundentes contra la desinformación. En consecuencia, la respuesta más efectiva a la desinformación en un mundo rico en información es la concienciación y la alfabetización (que podría ayudarse de la inteligencia artificial).

Lo nuevo y lo viejo

Aunque pueda parecer sorprendente: la mayoría de las acciones híbridas no son nuevas.[9] Como afirma el director del Centro Nacional de Inteligencia (CNI): "No está ocurriendo nada nuevo. Durante toda la historia, la guerra ha servido para que el genio militar ponga el progreso a trabajar en favor de sus intereses para ganarla".[10] La novedad, según el subdirector del Centro Criptológico Nacional (CCN-CERT), sería el uso del ciberespacio, que potencia las nuevas herramientas y reduce el coste de entrada para usarlas. Es decir, nos encontramos con "nuevas herramientas" (cibertecnología, esencialmente) dirigidas a satisfacer "intereses tradicionales"; en definitiva, "nuevas herramientas para viejas aspiraciones", como reza el título de este trabajo.

Dicho lo anterior, en la actualidad podemos mencionar dos elementos nuevos y diferenciadores: la "guerra de la información" (*information warfare*) y los ciberataques. El primero se refiere al "conflicto entre dos o más grupos en el ámbito de la información"[11] que pretende imponer un punto de vista específico a una determinada población.[12] Se trata de una combinación de guerra electrónica (*cyberwarfare*, incluidas las contramedidas electrónicas) y operaciones psicológicas cuyo objetivo es degradar la moral y el bienestar de los ciudadanos de una nación difundiendo, por lo común, información falsa a través de redes sociales y medios de comunicación. Son campañas de desinformación que parecen tener más éxito en regiones que ya son inestables, como las rusas en Crimea y la región del Donbas, que cayeron en terreno fértil donde una parte de la población ya estaba inclinada a aceptar la narrativa rusa de los acontecimientos.

En relación con la desinformación, han venido apareciendo los denominados *online trolls*, personas y actores no estatales que expresan opiniones afines a la agenda política de un Estado en particular y crean una *zona gris* en la que es muy difícil distinguir dónde situar la frontera entre la libertad de expresión de los activistas y la injerencia en el Estado víctima.[13] La dificultad de atribución de la autoría —lo que condice a la impunidad, en definitiva— dificulta que los Estados puedan determinar lo que cae dentro

[9] Algunos autores han apreciado ya "operaciones híbridas" en la guerra del Peloponeso. Véase A. Sari, "Hybrid Warfare, Law and the Fulda Gap", Universidad de Exeter, Facultad de Derecho, 2017, p. 9.

[10] Félix Sanz Roldán y Luis Jiménez Muñoz, respectivamente, ponencias en la Jornada sobre "Guerra híbrida: nuevas amenazas", Instituto Seguridad y Cultura, mayo de 2018, Senado de España.

[11] I. Porche III y otros, "Redefining Information Warfare Boundaries for an Army in a Wireless World", RAND Corporation, 2013, p. XV.

[12] Christian Bahnareanu, "The evolution of warfare from classic to hybrid actions", *Strategic Impact*, Issue 2/2015, pp. 61-62, y B. Renz y H. Smith, et al., "Russia and Hybrid Warfare, Going Beyond the Label", *Aleksanteri Papers 2016/1*, Kikimora Publications, Universidad de Helsinki, 2016, p. 11.

[13] Amnistía Internacional, "Dangerously Disproportionate, the Ever-Expanding National Security State in Europe", enero de 2017.

del ámbito de la libertad de expresión y lo que podría calificarse como interferencia extranjera.

Finalmente, la transmisión de programas audiovisuales a través de las fronteras de los Estados plantea cuestiones tales como el control y la jurisdicción sobre el contenido transmitido en aquellos casos en los que el medio de comunicación no está establecido en los Estados receptores de la comunicación, lo que, a juicio del Consejo de Europa, podría requerir una revisión de la Directiva del Servicio de Medios Audiovisuales de la UE de 2010 y del Convenio Europeo del Consejo de Europa sobre Televisión Transfronteriza de 1989.

Pasando a los ciberataques, como han venido señalando en los últimos años los Informes anuales de Amenazas y Tendencias del Centro Criptológico Nacional, varios países —como Alemania, Estados Unidos, Estonia, Finlandia, Georgia, Holanda, Lituania, Reino Unido o Ucrania— han denunciado haber sido víctimas de ciberataques rusos. Como respuesta, algunos países europeos han tomado medidas[14] o aprobado leyes antiterroristas que pueden utilizarse contra tales amenazas, aunque algunas de estas medidas podrían llegar a violar los derechos humanos[15] y suscitan dudas sobre su compatibilidad con la libertad de expresión. Sea como fuere, no debemos olvidar que el objetivo esencial de las amenazas híbridas es lograr resultados sin recurrir a la guerra real, enfrentando a las sociedades, no a los ejércitos, con lo que se desmorona casi por completo la distinción entre combatientes y ciudadanos, borrosa durante décadas.

Arquitectura de las amenazas híbridas

Todos los sectores presentan vulnerabilidades de las que se sirven los atacantes para perpetrar sus ataques. Entre otros, en el sector militar pueden aprovecharse del descontento del estamento militar o las deficiencias o limitaciones en los medios de defensa o en su despliegue. En el sector civil, actúan en situaciones de descontento de la población (o de un sector de ella), ausencia de cohesión social o división económica, religiosa o sectaria de la sociedad, especialmente en situaciones de crisis económica. También pueden explotar los momentos de debilidad de los sistemas políticos democráticos, las divergencias multilaterales, la falta de regulación o el escaso rigor de los medios de comunicación en la debida diligencia informativa (contraste informativo).

Por su origen, podemos realizar la siguiente clasificación:

- La localización de su autoría puede ser en el interior o en el exterior.

[14] Entre otros, el presidente de Ucrania, Petro Poroshenko, firmó en mayo de 2017 un decreto que bloqueó el acceso a numerosos sitios web rusos (incluidas redes sociales); en junio de 2017, el Bundestag alemán aprobó la Network Enforcement Act, que posibilita sanciones de hasta 50 millones de euros a las compañías de medios sociales que no eliminen en 24 horas el discurso de odio, las incitaciones a la violencia y la difamación, y en enero de 2018 el presidente francés, Emmanuel Macron, anunció que estaba analizando la posibilidad de una ley especial para combatir las “noticias falsas”.

[15] “Addressing Hybrid Threats”, Hybrid Center of Excellence for Countering Hybrid Threats, 2018.

- La localización de su destino puede ser el Estado propio, terceros (aliados, no alineados o potencialmente enemigos) o el atacante.

- Los agentes que están detrás pueden ser Estados, empresas, corporaciones, delincuencia organizada, hacktivistas y grupos de presión.

Por las herramientas empleadas por los agentes según los sectores:

- Militar: guerra no declarada, tropas no uniformadas, acciones encubiertas, utilización de organizaciones como la Contra centroamericana, los muyahidines en Afganistán o los *little green men* en Ucrania, los Lobos de la Noche en Crimea o la movilización de civiles.

- Civil/Social: Movimientos de protesta organizados por *intereses* extranjeros (Estados, corporaciones, troles…) y de contraprotesta; creación de organizaciones locales de carácter económico (empresas), cultural o de opinión afines a los atacantes o patrocinadas por ellos; aprovechamiento de la influencia religiosa, lingüística o cultural para favorecer el "nihilismo social" o el "relativismo posmoderno", que alimentan campañas de desinformación.[16]

- Infraestructuras críticas: denegación de servicio y pérdida de integridad o confidencialidad de la información tratada.

- Medios de comunicación: propaganda (fácil y barata) mediante el uso de redes sociales originada en el exterior o incluso localmente; noticias falsas (*fake news*) con mensajes de texto, audio o vídeo que provocan desinformación; operaciones psicológicas; uso de medios de comunicación afines o patrocinados (por ejemplo, RT y Sputnik en el caso de los intereses rusos y su difusión a través de partidos políticos, como el caso de M5S en Italia).

- Económico: creación de empresas, centros de estudio y organizaciones culturales originarias de los países potencialmente atacantes o con intereses análogos; penetración en terceros países de los actores *oligárquicos*, con lazos en sectores políticos, económicos y en los medios de comunicación locales; recurso a la ayuda externa o sanciones económicas para presionar a un gobierno extranjero.

- Político: diplomacia e inteligencia clásicas, *poder blando*, revelaciones y filtraciones, apoyo a simpatizantes en el exterior, chantajes y represalias.

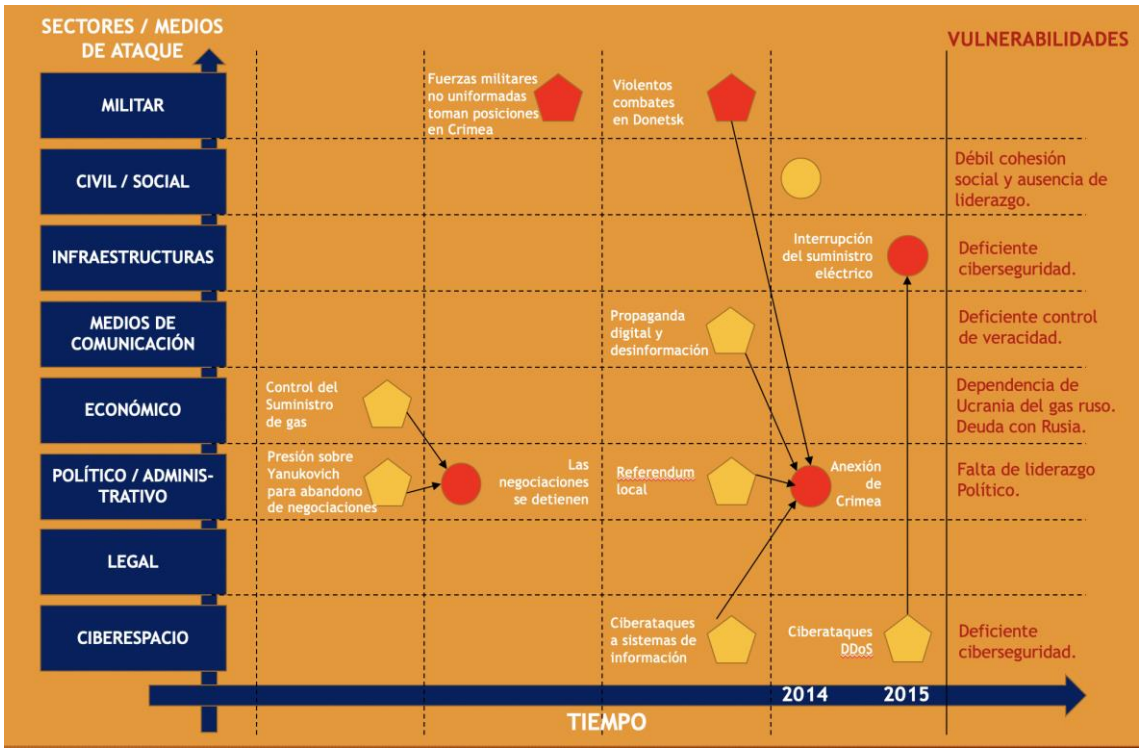
- Normativo: aprovechamiento de las lagunas legales.

[16] Julia Alicia Olmo y Romero, embajadora para las Amenazas Híbridas y la Ciberseguridad, ponencia en la Jornada sobre "Guerra híbrida: nuevas amenazas", Instituto de Seguridad y Cultura, mayo de 2018, Senado de España.

- Ciberespacio: ciberespionaje, ciberdelincuencia o hacktivismo; uso de redes sociales (Twitter, Facebook…), incluidos grupos organizados de publicación de mensajes; revelaciones comprometedoras; desarrollos tecnológicos específicos.

Para su mayor comprensión, las herramientas anteriores se combinan en el modelo gráfico de la Figura 1, en la que se representa el ataque híbrido sobre Ucrania atendiendo a los mecanismos de ataque involucrados, los sectores implicados, la gravedad de las acciones y su impacto.

Figura 1. Modelo de ataques híbridos: aplicación a Ucrania



En la Figura 1 aparecen los sectores y los medios de ataque usados en la columna de la izquierda, lo que da una idea de la intensidad del ataque, y las vulnerabilidades específicas, representadas en la columna de la derecha. En la parte central se identifican acciones y efectos atendiendo a su nivel de criticidad según un código de color: normalidad, crisis o emergencia que se aplican al caso-estudio de Ucrania.[17]

[17] Patrick J. Cullen y Erik Reichborn, "Countering Hybrid Warfare", Multinational Capability Development Campaign (MCDC), enero 2017, pp. 27-28.

Como se refleja en la Figura 1, en la fase inicial del conflicto, Rusia toma medidas para evitar la integración económica y política de Ucrania en la Unión Europea. Para ello aprovechó las vulnerabilidades de la dependencia ucraniana del gas ruso y de su deuda con Rusia para presionar al presidente Viktor Yanukovich para que abandonara las negociaciones de la UE, lo que ocurrió a finales de 2014. Tras el derrocamiento del presidente Yanukovich, Rusia se anexionó el territorio ucraniano de Crimea el 18 de marzo de 2014. En el mes previo a la decisión, Rusia lanzó una campaña híbrida que incluyó operaciones encubiertas, guerra de información, ciberataques y, finalmente, una invasión convencional para tomar el control de la península. Simultáneamente, condujo una campaña en las regiones ucranianas del este de Donetsk y Lugansk con una mezcla de guerra política, apoyo de grupos paramilitares y fuerzas convencionales. El ataque híbrido aprovechó las vulnerabilidades de la falta de liderazgo político y la débil cohesión social en Ucrania para llevar a cabo las operaciones anteriores. Los medios de comunicación pro-Kremlin denominaron a las tropas rusas que se habían trasladado a Crimea "hombrecillos verdes" (*little green men*), "gente educada" e incluso "hombres educados y armados", todo ello pese a que vestían uniformes militares sin identificación y portaban armas. Durante los enfrentamientos en el este de Ucrania, los soldados ucranianos recibieron mensajes de spam en las redes sociales con mensajes como "El comandante de su batallón se ha rendido. Sálvese usted mismo", "No recuperará Donbas. No tiene sentido derramar más sangre" o "Soldado ucraniano: es mejor rendirse con vida que quedarse aquí y morir".

Aspectos legales de la guerra híbrida

Como es sabido, en el Derecho Internacional, el uso de la fuerza por parte de los Estados está regulado por el *ius ad bellum* (derecho *a* la guerra) y su materialización en el *ius in bello* (derecho *en* la guerra), sustentado básicamente en las Convenciones de Ginebra de 1949, sus protocolos adicionales y las normas internacionales consuetudinarias.[18] Por otro lado, el art. 2 de la Carta de las Naciones Unidas prohíbe la amenaza o el uso de la fuerza "contra la integridad territorial o la independencia política de cualquier Estado o de cualquier otra forma incompatible con los Propósitos de las Naciones Unidas" (párrafo 4) y reafirma el principio de no intervención en asuntos que se encuentren esencialmente dentro de la jurisdicción interna de cualquier Estado (párrafo 7). Finalmente, la Resolución 2625 (XXV) de la Asamblea General de las Naciones Unidas, de 24 de octubre de 1970, reafirma la prohibición de amenazas o uso de la fuerza y el principio de no intervención. También enfatiza que "los Estados tienen el deber de evitar la propaganda de guerras de agresión".

El derecho de legítima defensa, asentado en el Derecho Internacional consuetudinario, se activa por un ataque armado. Si la intensidad de las operaciones de un adversario híbrido no alcanza el nivel necesario o se limita a la amenaza de la fuerza, no se puede invocar el derecho a responder utilizando la fuerza en legítima defensa. En el caso Nicaragua contra Estados Unidos, la Corte Internacional de Justicia (CIJ) reafirmó que

[18] Aunque los Convenios de Ginebra todavía mencionan el término "guerra", éste se ha reemplazado en la doctrina del Derecho Internacional y los instrumentos jurídicos por el de "conflicto armado" (véase, en particular, la Convención de La Haya de 1954 para la Protección de los Bienes Culturales en el caso de Conflicto Armado y sus dos Protocolos de 1954 y 1999).

el derecho de legítima defensa solo puede ejercerse en respuesta a un "ataque armado" —que fue interpretado a la luz del artículo 3, párrafo g, de la definición de *agresión* anexa a la Resolución 3314 (XXIX) de la Asamblea General de la ONU de 1974—. Aunque la práctica internacional ha aceptado que el derecho de legítima defensa también se extiende a ataques armados que emanan de actores no estatales, la CIJ ha declarado que este derecho no debería usarse si el ataque se origina desde dentro del propio territorio del objetivo, ya que se pondría en juego la integridad territorial del otro Estado. Esto facilita que los Estados agresores se apoyen en *intermediarios* para realizar sus ataques, porque será más difícil para el Estado objetivo atribuir violencia a su adversario y aplicar a la guerra híbrida las leyes aplicables a los conflictos armados internacionales[19] al negar u ocultar aquellos su participación directa en dichos conflictos armados.

De todo ello podemos extraer las siguientes conclusiones sobre el uso de la fuerza y los ataques híbridos:

- En caso de conflicto armado, incluida una guerra híbrida, se aplica tanto el DIH como el Derecho Internacional propiamente dicho.

- El Tribunal Europeo de Derechos Humanos (TEDH) ha aclarado que, en circunstancias excepcionales, el Convenio Europeo de Derechos Humanos puede aplicarse extraterritorialmente en casos de conflictos armados fuera de la zona geográfica del Consejo de Europa.[20] Sin embargo, la aplicación de la ley de derechos humanos está limitada por el DIH, que opera como *lex specialis*.[21]

- Cuando se producen violaciones del DIH, los Estados tienen la obligación de enjuiciar a los presuntos delincuentes con arreglo a la legislación nacional. Además de esto, tales violaciones también pueden ser procesadas por los tribunales penales internacionales, aunque, como ha señalado el Consejo de Europa (el mencionado Doc. 14.253), el DIH presenta significativas lagunas legales, así como un débil mecanismo de aplicación.

Aspectos legales de las amenazas híbridas

Si algo define las amenazas híbridas desde el punto de vista jurídico es, precisamente, la asimetría legal que existe entre el atacante y sus víctimas. Los agentes de las acciones híbridas, por regla general, niegan su responsabilidad en las operaciones y tratan de escapar de las consecuencias jurídicas de sus acciones valiéndose, además, de la complejidad del ordenamiento jurídico y sus lagunas, bordeando los límites legales,

[19] No se entra en recordar que un conflicto armado puede ser de carácter internacional (IAC) o no internacional (NIAC). El IAC se define en el artículo 2, común, de los Convenios de Ginebra y en el artículo 1, sección 4, del Protocolo Adicional I y establece que un IAC es una "guerra declarada o (…) cualquier otro conflicto armado que pueda surgir entre dos o más Estados". Los NIAC se definen en el artículo 3, común, y en el artículo 1, sección 1, del Protocolo Adicional II.

[20] Ver casos del TEDH sobre operaciones militares internacionales en Irak (Al-Saadoon y Mufdhi contra Reino Unido, n.º 61498/08) o en Irán (Pad y otros contra Turquía, 60167/00).

[21] "Legalidad de la amenaza de las armas nucleares", opinión consultiva de la CIJ de 8 de julio de 1996, *ICJ Reports*, 1996, párr. 25.

operando por espacios no regulados y sin sobrepasar nunca los umbrales legales, lo que les posibilita la realización de acciones difícilmente perseguibles por la vía legal/penal y generan toda la confusión y ambigüedad que les permiten enmascarar sus acciones. Lo anterior no implica que exista un vacío legal, sino que es difícil aplicar a los agentes de las amenazas híbridas la legislación nacional o internacional pertinente, incluido el Derecho Internacional Humanitario.

Por ejemplo, la existencia de un marco legal básico permite afirmar con rotundidad que, si en el contexto de una guerra híbrida un Estado recurre al uso de la fuerza contra otro Estado, este último puede invocar el derecho de legítima defensa sobre la base del artículo 51 de la Carta de las Naciones Unidas y aplicar las normas del Derecho Internacional Humanitario (DIH). Sin embargo, en la práctica, los agentes de las amenazas híbridas evitan el uso de esa dimensión de la fuerza que podría alcanzar el umbral requerido para activar la aplicación de las normas anteriores, con lo que se crea así un área legal gris. Si los adversarios híbridos se abstienen del uso de medios militares, sus acciones deben examinarse a la luz del Derecho Penal nacional y, de ser necesario y atendiendo a la situación concreta, de los instrumentos jurídicos internacionales pertinentes que cubran áreas políticas específicas (tales como el Derecho del Mar y las normas para combatir el ciberdelito, el terrorismo, el discurso de odio o el blanqueo de dinero). Por su parte, el Grupo de Expertos Gubernamentales de las Naciones Unidas emitió en 2013 un informe en el que declara que el Derecho Internacional también se aplica al ciberespacio. Dos años más tarde, prosiguió con un informe consensuado sobre las normas, reglas y principios del comportamiento responsable de los Estados en el ciberespacio, incluido un compromiso con la "no intervención en los asuntos internos de otros Estados".[22]

En el entorno europeo, el Convenio sobre la Ciberdelincuencia de 2001 es el único instrumento internacional vinculante en estas materias que, estando abierto también a Estados no miembros, constituye una guía para cualquier país que pretenda desarrollar legislación nacional integral contra el ciberdelito y como marco para la cooperación internacional.[23] En el caso de acciones hostiles no militares a gran escala, como las campañas de desinformación, es posible invocar el artículo 17 del Convenio Europeo de Derechos Humanos, que prohíbe el abuso de los derechos garantizados por el Convenio. Por consiguiente, un Estado miembro puede presentar una demanda contra otro Estado miembro ante el TEDH en virtud del artículo 33 del Convenio, aunque este artículo no podría ser invocado contra aquellos que, usando tácticas híbridas, fueran meros "intermediarios" de los adversarios. En el caso de los ciberataques, la Asamblea Parlamentaria del Consejo de Europa ha señalado que no está claro cómo se aplica en el ciberespacio la legislación vigente y cómo deben responder los Estados a estos ciberataques, para los que ni siquiera hay una definición uniformemente aceptada en su mencionado Doc. 14.253.

[22] "Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/68/98, de 24 de junio de 2013, y A/70/174, de 22 de julio de 2015.

[23] Consejo de Europa (ETS n.º 185), más conocido como Convenio de Bucarest.

(cont.)

En lo que respecta a la OTAN y al derecho a la autodefensa colectiva, es necesario mencionar, aun de forma sucinta, el *Manual de Tallin 2.0*, publicado en febrero de 2017, sobre el Derecho Internacional aplicable a las ciberoperaciones.[24] El manual no es vinculante ni representa la posición oficial, sino la de un grupo de 19 expertos en Derecho Internacional para codificar su aplicación al ciberespacio. La mayoría de los autores del manual opinaron que se necesitaba, al menos, un daño funcional (por ejemplo, un desabastecimiento de energía eléctrica) para considerar una ciberoperación como un "ataque" en el marco del DIH. En caso de ataque armado contra un miembro de la OTAN, debe aplicarse el artículo 5 del Tratado del Atlántico Norte, que permite una respuesta colectiva. Esta disposición también se extiende a los ataques terroristas desde el exterior dirigidos contra un Estado aliado. Las amenazas híbridas que no alcanzan el umbral de un ataque armado pueden abordarse sobre la base del artículo 4 del tratado, que estipula que los miembros de la OTAN pueden consultarse cada vez que la integridad territorial, la independencia política o la seguridad de cualquiera de ellos se vea amenazada. En general, los Estados deberán ser capaces de contrarrestar las amenazas híbridas mediante el uso de contramedidas proporcionales (represalias adecuadas).

Respecto a la autodefensa frente a un ataque híbrido, el artículo 42, párrafo 7, del TUE contiene una cláusula de asistencia mutua en caso de agresión armada, aunque su alcance sigue sin estar claro, ya que muchos de sus Estados miembros prefieren activar la autodefensa en el marco de la OTAN.[25] También carece de competencia en este ámbito el Consejo de Europa, ya que los "asuntos de defensa nacional" quedan excluidos del alcance de sus actividades sobre la base del artículo 1.d) de su Estatuto. Según algunos autores, como el mencionado Sari, contrarrestar los desafíos legales implica tres tareas que, hasta ahora, no han sido exploradas por la OTAN y la UE: desarrollar una definición de la dinámica jurídica de las amenazas híbridas, comprender las vulnerabilidades legales y fortalecer la preparación, la disuasión y la defensa en el dominio legal.

De todo ello podemos extraer las siguientes conclusiones:

- Los adversarios híbridos explotan las lagunas en la ley y la complejidad legal, operan a través de límites legales y espacios no regulados, explotan los umbrales legales que limitan las respuestas y están preparados para cometer violaciones sustanciales de la ley al amparo de la ambigüedad legal y fáctica.

- Los agresores niegan sus operaciones híbridas para crear una zona gris legal dentro de la cual pueden operar libremente. La regulación legal de las amenazas híbridas siempre es un desafío, puesto que una de las partes intenta evadir deliberadamente sus responsabilidades legales.

[24] "Tallin Manual 2.0 on the International Law Applicable to Cyber Operations", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

[25] El Parlamento Europeo ha reflexionado sobre las implicaciones en "Cybersecurity in the EU Common Security and Defence Policy", PE 603.175, mayo de 2017.

- Los problemas relacionados con los derechos humanos derivados de la lucha contra las amenazas híbridas pueden abordarse siguiendo el enfoque que viene aplicándose a las medidas de lucha contra el terrorismo.

- Las respuestas de los Estados a las amenazas híbridas deben estar sustentadas en la ley y ser proporcionales. En caso de duda, los Estados europeos siempre pueden solicitar la experiencia de la Comisión Europea para la Democracia a través del Derecho (Comisión de Venecia) sobre determinados proyectos de legislación.

- En cuanto a la libertad de expresión, se pueden imponer algunas restricciones para controlar el contenido de las noticias (especialmente para combatir el discurso de odio), pero no deben ser discriminatorias ni llevar a una censura general.

- No siempre es posible identificar al adversario híbrido y atribuir la responsabilidad de las amenazas híbridas a un país específico.

- Fenómenos como las campañas de desinformación también pueden implicar un conflicto entre ciertos derechos humanos y libertades fundamentales, como la libertad de expresión, por un lado, y el derecho a la información y a elecciones libres (como se garantiza en el artículo 3 del Protocolo n.º 1).

Medidas de seguridad frente a derechos humanos

Es innegable que, en muchas ocasiones, existe una enorme dificultad para armonizar los derechos humanos con la adopción de medidas que contrarresten las amenazas híbridas, aunque la experiencia de los Estados en los esfuerzos antiterroristas puede servir de orientación para identificar las limitaciones impuestas por el Derecho Internacional a las medidas para contrarrestar las amenazas de guerra híbrida. Si bien el artículo 15 del Convenio Europeo de Derechos Humanos (ETS n.º 5) permite a los Estados establecer excepciones a ciertas obligaciones “en tiempo de guerra u otra emergencia pública que amenace la vida de la nación”, debe hacerse bajo la premisa de que toda derogación de los derechos consagrados en ella se hará de acuerdo con ciertos requisitos sustantivos y de procedimiento. Para contrarrestar las amenazas híbridas, los Estados parte en la Convención también pueden invocar la seguridad nacional como un objetivo legítimo para limitar ciertos derechos, pero toda restricción de los derechos debe ser “prescrita por la ley” y proporcionada.[26]

En este sentido, el TEDH ha examinado numerosos casos en los que los Estados han invocado la “seguridad nacional” para restringir ciertos derechos humanos, aunque este término no está claramente definido ni se interprete igual en todos los Estados, que lo han aplicado a casos relacionados con la protección de la seguridad del Estado y la

[26] Entre ellos, el derecho al respeto por la vida privada y familiar (Artículo 8), la libertad de expresión (Artículo 10)[26], la libertad de reunión y asociación (Artículo 11), la libertad de circulación (Artículo 2.3 del Protocolo No. 4 al Convenio (ETS No. 46) y las garantías procesales en caso de expulsión de extranjeros (Artículo 1.2 del Protocolo No. 7 del Convenio (ETS No. 117). Francia, Ucrania y Turquía han llevado a efecto derogaciones bajo el artículo 15 del Convenio.

democracia constitucional y contra el espionaje, el terrorismo, el apoyo al terrorismo, el separatismo y la incitación a violar la disciplina militar. En la actualidad, el TEDH pide a los organismos nacionales que verifiquen que cualquier amenaza invocada tenga una base razonable, se sustente en una norma jurídica previa y se module la necesidad de intervención y su proporcionalidad a la amenaza contra la seguridad nacional.

Tabla 1. Casos en los que se suele invocar la "seguridad nacional"

Vigilancia secreta:

- El TEDH considera que las leyes en las que se basa dicha intervención no solo serán "accesibles" y "previsibles", sino también muy detalladas, que demuestren que existen garantías adecuadas y efectivas contra eventuales abusos.[27]

Libertad de expresión:

- En la jurisprudencia del TEDH existe una tendencia a no encontrar violaciones del artículo 10 en casos que impliquen la prohibición de llamamientos a la violencia claros e inequívocos. El derecho a la libertad de expresión no es un derecho a incitar a la violencia.[28]

- El TEDH tiende a excluir de su protección, en virtud del artículo 17 de la Convención, situaciones que puedan constituir discurso de odio y negación de los valores fundamentales de la Convención.[29]

- El TEDH también ha reconocido la importancia de Internet cuando las personas ejercen su derecho a la libertad de recibir e impartir información y ha examinado las medidas que bloquean el acceso a Internet.[30]

- En Stankov y UMO Ilinden contra Bulgaria, sobre la prohibición de las asambleas organizadas por la asociación solicitante para "el reconocimiento de la minoría macedonia en Bulgaria", las autoridades invocaron, entre otras cosas, la seguridad nacional para justificar la medida impugnada. El TEDH declaró que "las modificaciones territoriales esgrimidas en los discursos y manifestaciones no representan necesariamente una amenaza para la integridad territorial y la seguridad nacional".[31]

- En un documento temático sobre "El Estado de Derecho en Internet y en el mundo digital", el comisario del Consejo de Europa para los Derechos Humanos concluyó que "los Estados que deseen interferir en los derechos fundamentales sobre la base de una supuesta amenaza para la seguridad nacional deben demostrar que la amenaza no puede tratarse con el Derecho Penal ordinario, incluidas las leyes antiterroristas especiales que satisfacen las normas internacionales en materia de derecho y procedimiento penal". Esto también es válido para acciones estatales que afectan a Internet y las comunicaciones electrónicas. El TEDH sostiene que el incumplimiento del requisito anterior "viola el Estado de Derecho internacional".[32]

[27] Entre otros casos, Roman Zakharov v. Russia (47143/06); Big Brother Watch and Others v. the UK (58170/13); Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (62322/14); y Human Rights Organisations and Others v. the UK (24960/15).

[28] Zana v. Turkey, demanda 18954/91, sentencia de 25 de noviembre de 1997, para. 60.

[29] Seurot v. France, demanda 57383/00, decisión sobre su admisibilidad de 18 de mayo de 2004.

[30] Ahmet Yildirim v. Turkey, demanda 311/10, sentencia de 18 de diciembre de 2012, y Cengiz and Others v. Turkey, demandas 48226/10 y 14017/11, sentencia de 1 de septiembre de 2015.

[31] Stankov and the United Macedonian Organisation Ilinden v. Bulgaria, demandas 29221/95 y 29225/95, sentencia de 2 de octubre de 2001, para. 97.

(cont.)

La Asamblea Parlamentaria del Consejo de Europa ya ha considerado el problema de las restricciones a los derechos humanos y las libertades fundamentales impuestas en interés de la seguridad nacional y la seguridad pública en el contexto de la lucha contra el terrorismo con plena observancia de los derechos humanos y, en general, el Estado de Derecho.[33]

Lecciones aprendidas y respuestas

La presencia constante de acciones híbridas en los últimos años nos ha permitido aprender algunas cuestiones esenciales, a saber:

1. La guerra híbrida implica el uso sincronizado de medios (militares y no militares) contra vulnerabilidades concretas del adversario (víctima/oponente) con el objetivo de alcanzar los efectos deseados por el atacante.

2. Los medios utilizados pueden aumentar o disminuir en número o intensidad dependiendo del momento y del objetivo perseguido, que puede ser una entidad, un sector o todo un país.

3. La guerra híbrida amplía el *campo de batalla* tradicional y sus resultados no son siempre predecibles.

4. Un "ataque híbrido" puede tener efectos lineales (previsibles) y efectos no lineales.

5. Las amenazas híbridas permiten a sus agentes, al menos al comienzo de las operaciones, actuar por debajo del umbral de detección y respuesta del objetivo (víctima), lo que dificulta la atribución de las acciones y, además, causa daños significativos antes de que el oponente pueda responder, o incluso detectar, un ataque híbrido.

6. La ambigüedad inherente a las acciones híbridas redefine conceptos tales como la coerción, la agresión, el conflicto y la guerra.

7. El nuevo contexto geoestratégico, las tecnologías de la información y la comunicación (TIC) y las nuevas formas organizativas sugieren que esta forma de agresión persistirá y evolucionará en el futuro.

8. Hay muchos actores con experiencia en amenazas híbridas: Rusia, Daesh, al-Qaeda y otros muchos se están preparando para ello.

Por lo que toca a la respuesta legal, hay una máxima hipocrática que exige "evitar hacer daño". Aunque las "sociedades abiertas y democráticas" son, *per se*, más vulnerables

[32] Stankov and the United Macedonian Organisation Ilinden v. Bulgaria, demanda 29225/95 y sentencia de 2 de octubre de 2001, para. 97.

[33] Resoluciones 1840 sobre "Human rights and the fight against terrorism" de 6 de octubre de 2011 y 2014 sobre "National security and access to information", de 2 de octubre de 2013, respectivamente.

que las sociedades cerradas o autoritarias, no pueden ponerse en peligro los atributos fundamentales de tales sociedades: los derechos fundamentales de sus ciudadanos. Es imprescindible, por tanto, mantener indemnes tales derechos, especialmente la libertad de expresión y la privacidad. Por otro lado, parece necesario ampliar los análisis de riesgos a todos los sectores implicados en una acción híbrida, no solo al ciberespacio, aunque sin duda es un elemento decisivo a la hora de perpetrar acciones híbridas. Además, es imprescindible alcanzar una cooperación plena y efectiva entre los sectores público y privado.

Finalmente, una respuesta adecuada será aquella que se sustente en un profundo conocimiento de la situación, en inteligencia fiable, en análisis de calidad y en los esfuerzos de contrainteligencia. Esta exigencia ha requerido modificar la legislación para otorgar a los servicios de inteligencia más autoridad para recopilar información, tanto dentro como fuera del país, en países como Estados Unidos, Alemania o Francia, entre otros.

Respuestas de la Unión Europea

La UE ha adoptado, entre otras medidas, una Comunicación sobre "La lucha contra las amenazas híbridas" con 22 propuestas de acciones que se actualizan periódicamente[34]. Para desarrollarlas, algunos Estados miembros han creado un Centro de Excelencia para las Amenazas Híbridas en Finlandia (HybridCoE, del que España es país fundador), y el Servicio Europeo de Acción Exterior (SEAE) ha creado una célula (EU Hybrid Fusion Cell) dentro de su Centro de Situación e Inteligencia para atender las situaciones de crisis. La Comisión Europea desarrolla medidas para profundizar en la respuesta europea y presenta informes periódicos sobre la aplicación general del marco común relativo a la lucha contra las amenazas híbridas.

En el último[35], la Comisión ha identificado algunos sectores en los que deben adoptarse medidas adicionales:

- Conciencia situacional: La EU Hybrid Fusion Cell precisa disponer de conocimientos especializados para poder hacer frente al amplio espectro de riesgos que comportan estas amenazas. Para ello, este órgano debe ampliarse con componentes especializados en materia química, biológica, radiológica y nuclear (QBRN), contrainteligencia y ciberanálisis.

- Comunicación estratégica: Partiendo de la experiencia previa, debe continuarse con el desarrollo de las capacidades de comunicación estratégica de la UE y asegurar la interacción sistemática entre las estructuras existentes.

- Desarrollo de la resiliencia y la disuasión: La UE ha propuesto diversos medios para reforzar las capacidades y luchar contra las ciberamenazas, tales como la propuesta de un marco de certificación de la ciberseguridad, el mandato para la

[34] Comunicación sobre la "Lucha contra las amenazas hibridas", JOIN(2016)18 de 6 de abril.

[35] Informe sobre "Ejecución desde julio de 2017 a junio de 2018", JOIN(2018)14, de 13 de junio.

ampliación y la modernización de la Agencia de Ciberseguridad de la Unión Europea (ENISA), las pautas sobre cooperación entre los Estados miembros y las agencias de la UE en caso de ataque y un conjunto de instrumentos de ciberdiplomacia. Considera necesario acelerar la actividad dirigida a concluir las negociaciones sobre el Reglamento de Ciberseguridad y llegar a un acuerdo sobre las nuevas normas de recopilación de pruebas electrónicas. Además, se está construyendo una plataforma específica de formación y educación para coordinar la formación en materia de ciberdefensa.

- Desarrollo de la resiliencia frente a las actividades de inteligencia hostiles: La coordinación entre los Estados miembros y entre estos y otras organizaciones internacionales, en particular la OTAN, es crucial. El SEAE y la Comisión aplicarán medidas prácticas que sustenten y amplíen la capacidad interactiva de la UE para repeler la actividad hostil de inteligencia dirigida contra las instituciones.

Respuestas del Consejo de Europa

Fuera de la UE, la Asamblea Parlamentaria del Consejo de Europa elabora recomendaciones para sus Estados miembros[36]:

1. Abstenerse de recurrir a las acciones híbridas en las relaciones internacionales y respetar plenamente las disposiciones del Derecho Internacional, en particular los principios de soberanía, integridad territorial e inviolabilidad de las fronteras, de acuerdo con su objeto y fin, sin explotar abusivamente las lagunas o ambigüedades percibidas.

2. Intensificar la cooperación internacional para identificar adversarios híbridos y todo tipo de amenazas de guerra híbridas, y establecer el marco legal aplicable.

3. Mantener intercambios de información sobre las agresiones híbridas en Europa y compartir experiencias y buenas prácticas para contrarrestar tales amenazas.

4. Tomar medidas para aumentar la conciencia de los ciudadanos sobre las amenazas híbridas y su capacidad para reaccionar rápidamente ante tales amenazas.

5. Firmar, ratificar e implantar —en caso de que no se haya hecho— el Convenio sobre la Delincuencia de Budapest y promover su ratificación por parte de Estados no miembros.

6. Mantener y reforzar las medidas adoptadas por la Unión Europea y la Organización del Tratado del Atlántico del Norte (OTAN) para contrarrestar las amenazas híbridas, y reforzar la cooperación en este ámbito.

[36] Resolución sobre "Legal challenges related to hybrid war and human rights obligations", 2217(2018) de 6 de abril.

7. Hacer un llamamiento a todos los Estados miembros del Consejo de Europa que, simultáneamente, sean miembros de la Unión Europea y la OTAN para que compartan sus mejores prácticas para contrarrestar las amenazas híbridas con otros Estados miembros que puedan verse afectados por este fenómeno.

8. En relación con las medidas destinadas a contrarrestar la guerra híbrida, la Asamblea recuerda su Resolución 1840 (2011) sobre derechos humanos y lucha contra el terrorismo. Además, hace un llamamiento a los Estados miembros para que velen por que tales medidas respeten los requisitos derivados del Convenio Europeo de Derechos Humanos, de conformidad con la jurisprudencia del Tribunal Europeo de Derechos Humanos. En particular, en lo que respecta a los derechos sujetos a restricciones en virtud del Convenio, cualquier limitación debe basarse en la ley, ser proporcional al objetivo legítimo perseguido (por ejemplo, la seguridad nacional) y "necesario en una sociedad democrática".

Esta incesante actividad europea en relación con las amenazas híbridas va a exigir de nuestro país un mayor esfuerzo desde la dirección del Consejo Nacional de Ciberseguridad y que seguramente tendrá su primera oportunidad en la nueva Estrategia de Ciberseguridad Nacional, que actualizará nuestro texto estratégico de 2013.

Conclusiones

De todo lo anterior podemos concluir que las amenazas híbridas, en cualquiera de sus variantes y pese a no constituir en sí mismas realidades nuevas, sí que poseen componentes novedosos asociados a las tácticas que vienen utilizándose para su despliegue. La más importante de todas ellas es el uso del ciberespacio. Cualquier acción hostil, cuando se apoya o se desarrolla en el ciberespacio, adquiere una nueva dimensión, extraordinariamente peligrosa, que exige de los Estados y de sus instituciones competentes en materia de ciberseguridad un esfuerzo adicional y sostenido contra lo que ya constituye uno de los riesgos más representativos de nuestro siglo.

Es de esperar que el desarrollo de la tecnología abrirá nuevas oportunidades a las amenazas híbridas y que nuevos agentes tratarán de aprovechar el creciente poder de manipulación del ciberespacio. La mayor facilidad para suplantar identidades en audio y vídeo incrementará el volumen de *fake news* y dificultará la tarea de atribuir responsabilidades, por lo que será necesario potenciar los mecanismos de identificación electrónica, así como la regulación aplicable a las redes sociales (y a los medios de comunicación en materia de "verificación de los hechos narrados") y, seguramente, incrementar las posibilidades legales de recabar información de los servicios de inteligencia.

Las amenazas híbridas son una "cuestión de Estado", afectan a la sociedad entera, y no pueden ser tratadas aisladamente ni por medios territorialmente limitados. Para prevenir sus efectos, se necesita conocer en profundidad las vulnerabilidades de nuestra sociedad y nuestros sistemas de información en los sectores antes mencionados, para lo que es necesario potenciar el *conocimiento compartido*, lo que significa dotar a los

servicios de inteligencia de más medios y de mayor habilitación legal para recopilar información (interior y exterior). Es necesario implicar, conjuntamente, al sector público y al sector privado, puesto que muchas de las infraestructuras críticas están en manos privadas, así como incrementar la responsabilidad de las redes sociales por los contenidos difundidos a través de ellas.

Es necesario estudiar las nuevas formas de acción, elaborar una doctrina para su empleo y disponer del adiestramiento adecuado, contando con los desarrollos tecnológicos que permitan el combate, y todo ello con una disuasión efectiva y la debida anticipación. Asimismo, se debe regular el concepto de "agresión" para facilitar la respuesta de las nuevas herramientas, así como los medios tecnológicos, para lo que resultarán imprescindibles las certificaciones de seguridad e incorporar los principios éticos al desarrollo de *software* (modelos éticos en los sistemas de inteligencia artificial, por ejemplo) y de sistemas de información.

En concreto, para su aplicación en España, cabría formular las siguientes propuestas más inmediatas:

1. Estratégicamente, parece necesario contemplar las amenazas híbridas en el contexto de la nueva Estrategia de Ciberseguridad Nacional que sustituirá a la de 2013. Comoquiera que ciertas manifestaciones de tales amenazas —muy especialmente, las *fake news* o la desinformación— pueden desarrollarse al margen del ciberespacio, parece apropiado que la nueva Estrategia de Ciberseguridad Nacional, sin olvidar la globalidad del marco en el que se desenvuelven, se concentre en aquellas amenazas que se materializan o pueden materializarse en sistemas de información, ya sean grandes (como los sistemas de seguimiento de satélites o plantas de energía) o pequeños (como un marcapasos), o usen el ciberespacio como elemento propagador de la amenaza.

2. Operativamente, parece necesaria la creación de una Unidad de Tratamiento de las Amenazas Híbridas, a ser posible dentro de alguno de los organismos actuales con competencias en ciberseguridad nacional.

3. Jurídicamente, se debe actualizar la legislación nacional definiendo con precisión lo que se debe entender por "amenazas híbridas" y su encaje legal en nuestro ordenamiento jurídico, especialmente en el orden penal, así como su regulación en materia de medios de comunicación y redes sociales.

4. Culturalmente, se debe fomentar la comunicación estratégica con la sociedad para prevenir y mitigar los efectos de las amenazas híbridas.

5. Finalmente, es necesario reforzar la cooperación internacional con organismos competentes en la materia, muy especialmente con la UE y la OTAN.