uc3m | Universidad Carlos III de Madrid

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

***Coordinadora Curso:* -Profª (PhD) María Nieves de la Serna Bilbao**

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

TEMA 10: CIBERSEGURIDAD Y AMENAZAS HÍBRIDAS

IV. LAS AMENAZAS HÍBRIDAS

Elaborado por Profs. Dr. Carlos Galán Pascual (PhD) y Carlos Galán Cordero
Profesores Área Derecho Administrativo// Departamento de Derecho Público
Profesores Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz
Universidad Carlos III de Madrid

SUMARIO:

IV. LAS AMENAZAS HÍBRIDAS

4.1 Definiciones y conceptos concordantes: amenazas híbridas y guerra híbrida

4.2 ¿Qué persiguen y por qué existen las amenazas híbridas?

4.3 Los elementos novedosos de las amenazas híbridas

A. Information warfare

B. Ciberataques

4.4 Los aspectos legales de la guerra y las amenazas híbridas

4.5 Buenas prácticas y propuestas concretas

IV. LAS AMENAZAS HÍBRIDAS

Desde hace unos años, los términos "amenazas híbridas", "guerra híbrida", *fake news*, "posverdad", "desinformación", etc., han venido incorporándose 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 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 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, aislando sus elementos constituyentes y acotando sus límites -si ello, como se verá, es posible-, analizar 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.

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 la capacidad que desarrollan 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 la guerra y la paz y, con ello, por ejemplo, impedir la activación del compromiso de "asistencia mutua" recogido en el art. 5 del Tratado de la OTAN[1].

[1] El artículo 5 del Tratado de Washington, texto jurídico fundacional de la Alianza Atlántica, suscrito el 4 de abril de 1949 en la capital norteamericana, señala: "*Artículo 5. Las partes convienen en que un ataque armado contra una o contra varias de ellas, acaecido en Europa o*

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.

4.1 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.

Utilizaremos las siguientes definiciones:

Amenaza Híbrida ***(Hybrid Threat)***	Fenómeno resultante de la convergencia e interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional[2].
Conflicto Híbrido ***(Hybrid Conflict)***	Situación en la cual las partes se abstienen del uso abierto de la fuerza (armada), confiando sus acciones a una combinación de acciones de intimidación militar (sin llegar a un ataque convencional) y la explotación

en América del Norte, se considerará como un ataque dirigido contra todas ellas y, en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas, asistirá a la parte o partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer y mantener la seguridad en la región del Atlántico Norte.
Todo ataque armado de esta naturaleza y toda medida adoptada en consecuencia se pondrán, inmediatamente, en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las medidas necesarias para restablecer y mantener la paz y la seguridad internacionales."

[2] European Parliament Research Service (EPRS): At a Glance: Understanding Hybrid Threats. (Junio, 2015)

	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)[3].

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"[4].

Según el European Parlamientary Research Service (EPRS), las amenazas híbridas pueden comprender varias situaciones, incluidos los actos terroristas (de Boko Haram, Al-Queda 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.)

En todo caso, las amenazas híbridas pueden partir tanto de Estados como de agentes no estatales y pueden 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 su consecuencia, se activa la aplicación del Derecho Internacional Humanitario (DIH)[5].

---

[3] Numerosos especialistas conciben la "guerra híbrida" como un tipo de amenazas intrínsecamente nuevas. La proliferación de la guerra híbrida 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, integrándolos con el uso 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.

[4] Consejo de Europa - Asamblea Parlamentaria. Committee on Legal Affairs and Human Rights. Legal challenges related to the hybrid war and human rights obligations. (Report). (Draft resolution and recommendation adopted unanimously by the committee on 14 March 2018.)

[5] Derecho Internacional Humanitario (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 o que han decidido dejar de participar en el enfrentamiento, y restringir y regular los medios y métodos de guerra a disposición de los combatientes; regulando la conducta en los conflictos armados (*ius in bello*). Se compone de una serie de

El concepto "guerra híbrida" combina capacidades cinéticas convencionales (acciones armadas no encubiertas) con tácticas irregulares, tales como el terrorismo, crímenes transnacionales, especialmente cuando son cometidos por actores que, aparentemente patrocinados o dependientes por un estado, dan la impresión de no encontrarse bajo su autoridad. Estas acciones suelen también recurrir al empleo de otros medios: los ciberataques, la desinformación y la propaganda, dirigidas a poblaciones enteras o incluso a minorías nacionales u otras minorías significativas, medios entre los que se incluyen la corrupción de agentes esenciales mediante uso de dinero negro o la habilitación de presupuestos paralelos.

4.2 ¿Qué persiguen y por qué existen las amenazas híbridas?

Como hemos señalado, las amenazas híbridas persiguen alcanzar sus objetivos estratégicos, influyendo en la toma de decisiones de sus víctimas, socavando sus valores, su estructura social y la confianza de la población.

Es general, las amenazas híbridas han venido persiguiendo, entre otros objetivos[6]:

- 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, por ejemplo) o de las organizaciones internacionales (como 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).

Como se ha señalado, 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, 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 en los demás sus creencias, actitudes, preferencias, opiniones, expectativas, emociones y/o predisposiciones para

---

normas, en su mayoría reflejadas en los Convenios de Ginebra de 1949 y sus protocolos adicionales. (Wikipedia).

[6] Fuente: Ponencia de Alejandro Alvargonzalez, Secretario Gral. Adjunto OTAN. Jornada "Guerra híbrida: nuevas amenazas”. Instituto Seguridad y Cultura. Mayo, 2018. Senado de España.

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, posibilitando que los 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 del juego nacionales e internacionales aún están en su infancia. No podemos considerar el ciberespacio como una frontera, sino como un verdadero ámbito operativo que representa un desafío a la idea tradicional de seguridad.

Por otro lado, si cambiante es el orden mundial no lo es menos el ecosistema de la información pública y el panorama de los medios de comunicación.

Efectivamente, 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.

Como decimos, la información 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. ¿Resultado?: la confianza, uno de los pilares fundamentales de las sociedades, se está erosionando.

La naturaleza cambiante de conceptos tan tradicionales como los conflictos armados o la guerra también ha sido señalado 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 conflicto armado convencional o 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. Ambas características han venido dirigiendo muchas de las decisiones políticas en materia de seguridad. Con posterioridad, la globalización, poniendo el acento en los conceptos de "integración" e "interdependencia", supuso una nueva forma de entender el mundo y las relaciones entre sus habitantes. Producto de todo ello, las nuevas generaciones, sustentadas en lo digital y en el ciberespacio, presentan dos características contradictorias: el cosmopolitismo y los neonacionalismos, consecuencias, en ocasiones, de la manipulación política de acontecimientos históricos.

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 contra-protestas en relación con una mezquita en Houston, acciones en estos casos presuntamente orquestadas por elementos rusos[7], constituyen solo unos pocos ejemplos de lo que sin duda constituyen las amenazas híbridas del Siglo XXI.

4.3 Los elementos novedosos de las amenazas híbridas

Dicho lo anterior, en la actualidad, podemos mencionar dos elementos nuevos y diferenciadores: Information Warfare y los Ciberataques.

Veámoslos por separado.

A. Information warfare

Podemos definir este concepto como: "El conflicto entre dos o más grupos, en el ámbito de la información"[8], pretendiendo imponer un punto de vista específico a una determinada población[9].

---

[7] Un análisis de la German Marshall Fund's Alliance for Securing Democracy (https://securingdemocracy.gmfus.org) señaló que el gobierno ruso había utilizado ciberataques, desinformación e influencia financiera para penetrar en los asuntos internos de, al menos, 27 países europeos y norteamericanos desde 2004 (EE.UU., Francia, Reino Unido (Brexit), Alemania, España (caso catalán), etc.)

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

[9] 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, University of Helsinki, 2016, p.11.

Se trata de una combinación de guerra electrónica (cyberwarfare, incluidas las contramedidas electrónicas) y las 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)[10].

En relación con la desinformación, han venido apareciendo los denominados Online *Trolls*, personas y actores no estatales, semi-organizados, que expresan opiniones afines a la agenda política de un Estado en particular, creando 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[11].

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 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 (2010/13 / UE) y del Convenio Europeo del Consejo de Europa sobre Televisión Transfronteriza (STE Nº 132)[12].

B. Ciberataques

Como han venido señalado los anuales Informes de Amenazas y Tendencias del Centro Criptológico Nacional, en los últimos años varios países, incluyendo ex-repúblicas de la URSS (Estonia, Georgia, Lituania y Ucrania), así como países occidentales (Finlandia, Alemania, Holanda, el Reino Unido o los Estados Unidos) han denunciado haber sido víctimas de ciberataques rusos.

---

[10] Dichas campañas parecen tener más éxito en regiones que ya son inestables. Las campañas de desinformación rusas, por ejemplo, cayeron en terreno fértil en Crimea y en la región de Donbas, donde una parte de la población ya estaba inclinada a aceptar la narrativa rusa de los acontecimientos. En su informe "Sobre las consecuencias políticas del conflicto en Ucrania", la Comisión de Asuntos Políticos y Democracia del Consejo de Europa describió la participación de Rusia con amplias operaciones de información y su guerra de propaganda como "tan peligrosa como la guerra".

[11] Véase: Amnesty international, "Dangerously Disproportionate, the Ever-Expanding National Security State in Europe", Report, January 2017.

[12] Consejo de Europa, Asamblea Parlamentaria. Resolution 2217 (2018). Legal challenges related to hybrid war and human rights obligations.

Como respuesta, algunos países europeos han aprobado leyes antiterroristas que pueden utilizarse contra tales amenazas, aunque algunas de estas medidas podrían llegar a violar los derechos humanos[13].

He aquí algunos ejemplos de tales medidas:

- En mayo de 2017, el presidente de Ucrania, Petro Poroshenko, firmó 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.
- En enero de 2018, el presidente francés Macron anunció que estaba analizando la posibilidad de una ley especial para combatir las "noticias falsas".

Como decimos, muchas de las reflexiones en torno a posibles medidas a aplicar podrían suscitar 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 (acciones cinéticas), enfrentando a las sociedades, no a los ejércitos. La distinción entre combatientes y ciudadanos, borrosa durante décadas, se desmorona casi por completo.

4.4 Los aspectos legales de la guerra y las amenazas híbridas

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 por el *ius in bello* (derecho *en* la guerra), sustentado básicamente por las Convenciones de Ginebra de 1949 y sus protocolos adicionales, así como por las normas internacionales consuetudinarias[14].

[13] Swedish Defence University – Center for Asymetric Threat Studies – The European Centre of Excellence for Countering Hybrid Threats: Addressing Hybrid Threats. (2018).

[14] Aunque los Convenios de Ginebra aún mencionan el término "guerra", ha sido reemplazado en la doctrina del Derecho Internacional y los instrumentos jurídicos por el término "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).

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 encuentran esencialmente dentro de la jurisdicción interna de cualquier Estado (párrafo 7).

Finalmente, la resolución 2625 de la Asamblea General de las Naciones Unidas de 25 de octubre de 1970 reafirma la prohibición de la amenaza o el 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*".

Como viene siendo conocido, 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 vs. Estados Unidos, la Corte Internacional de Justicia (CIJ) reafirmó que el derecho de legítima defensa solo puede ejercerse en respuesta a un "ataque armado" (que fue interpretado a la luz del Artículo 3, el párrafo (g) de la Definición de agresión anexa a la Resolución 3314 (XXIX) de la Asamblea General de la ONU de 1974)[15].

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[16]. Esto significa que si un Estado se hace ayudar de “intermediarios” será más difícil para el Estado objetivo atribuir violencia a su adversario[17].

---

[15] Consejo de Europa - Asamblea Parlamantaria. Committee on Legal Affairs and Human Rights. Legal challenges related to the hybrid war and human rights obligations. (Report).

[16] Véase: Corte Internacional de Justicia: Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion of 9 July 2004, paragraph 139.

[17] No entramos ahora a 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, mientras que los NIAC lo está en el Artículo 3 común y en el Artículo 1 Sección 1 del Protocolo Adicional II. El artículo común 2 de los Convenios de Ginebra establece que un IAC es una "guerra declarada o ... cualquier otro conflicto armado que pueda surgir entre dos o más Estados”. Lógicamente, si una guerra híbrida se califica como IAC, las cuestiones relativas a la atribución, bajo el DIH y las leyes de derechos humanos, son más directas. Como el umbral para la aplicabilidad de la ley de IAC es bajo, es probable que un adversario híbrido niegue su participación en dicho conflicto armado o evite la participación directa en operaciones de combate. Si las hostilidades son inevitables, al adversario le conviene utilizar tácticas híbridas para usar sustitutos a fin de ocultar su propia participación.

El uso de la ley en apoyo de la guerra no es una novedad (por ejemplo, para la CE[18] la invasión japonesa de Manchuria en 1931 presenta muchas similitudes con la anexión rusa de Crimea en 2014).

De todo ello podemos extraer las siguientes conclusiones:

- En caso de conflicto armado, incluida una "guerra híbrida", se aplica tanto el DIH como el derecho internacional, propiamente dicho.
- El TEDH ha aclarado que, en circunstancias excepcionales, la Convención puede aplicarse extraterritorialmente, incluso en casos de conflictos armados fuera de la zona geográfica del Consejo de Europa[19]. Sin embargo, la aplicación de la ley de derechos humanos está limitada por el DIH, que opera como *lex specialis*[20].
- 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[21], el DIH presenta significativas lagunas legales, así como un débil mecanismo de aplicación.

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.

Efectivamente, los agentes de las acciones híbridas, por regla general, niegan su responsabilidad en las operaciones, tratando de escapar de las consecuencias jurídicas de sus acciones, valiéndose, además, de la complejidad del ordenamiento jurídico y sus lagunas, bordeando los límites legales, 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, generando al tiempo la confusión y ambigüedad que les permite enmascarar sus acciones.

Pese a lo dicho, conviene remarcar que los agentes de las amenazas híbridas no operan en un vacío legal, porque, en cualquier caso, siempre resulta de

---

[18] Consejo de Europa - Asamblea Parlamantaria. Committee on Legal Affairs and Human Rights. Legal challenges related to the hybrid war and human rights obligations. (Report).
[19] Ver casos del TEDH sobre operaciones militares internacionales en Irak: Al-Sadoon & Mufdhi v. Reino Unido, demanda no. 61498/08, sentencia de 2 de marzo de 201; Al-Skeini y otros v. Reino Unido, demanda no. 61498/08, y Al-Jedda v. El Reino Unido, demanda no. 55721/07, Sentencias de 7 de julio de 2011 (Gran Sala). Véase también un caso relativo a la intervención de soldados turcos en Irán: Pad y otros v. Turquía, demanda no. 60167/00, sentencia de 28 de junio de 2007.
[20] Véase CIJ, Legalidad de la amenaza de las armas nucleares, Opinión Consultiva, 8 de julio de 1996, ICJ Reports 1996, párr. 25. Véase también Noam Lubell, Desafíos en la aplicación de las leyes de derechos humanos a los conflictos armados, Revista Internacional de la Cruz Roja, vol. 87/860, diciembre de 2005.
[21] Consejo de Europa - Asamblea Parlamentaria. Committee on Legal Affairs and Human Rights. Legal challenges related to the hybrid war and human rights obligations. (Report).

aplicación la legislación nacional o internacional pertinente, incluido el derecho internacional humanitario, aunque, efectivamente, la atribución de la autoría resulte ser siempre la labor más complicada.

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, aplicándose 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, creándose así un área legal gris[22].

En el otro lado, en los casos en que un adversario híbrido se abstiene 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, a los instrumentos jurídicos internacionales pertinentes que cubran áreas políticas específicas (tales como el derecho del mar, las normas para combatir el ciberdelito, el terrorismo, el discurso del odio o el blanqueo de dinero).

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 la Convención. 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 ciberataques, la CE[23] ha señalado que no está claro cómo se aplica la legislación vigente en el ciberespacio y cómo deben responder los Estados a estos ciberataques, para los que ni siquiera hay una definición uniformemente aceptada[24].

En 2013, el Grupo de Expertos Gubernamentales de las Naciones Unidas emitió 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 o principios del comportamiento

[22] Consejo de Europa: Provisional versión. Committee on Legal Affairs and Human Rights. Legal challenges related to the hybrid war and human rights obligations. (14.03.2018).
[23] Consejo de Europa - Asamblea Parlamentaria. Committee on Legal Affairs and Human Rights. Legal challenges related to the hybrid war and human rights obligations. (Report).
[24] Por ejemplo, El Comité Internacional de la Cruz Roja (ICRC), define *ciberataque* como cualquier acción hostil de un adversario contra un enemigo concreto diseñada para “descubrir, alterar, destruir, interrumpir o transferir, manipular o transmitir datos almacenados en un sistema de información”. Ver https://www.icrc.org/en/document/cyber-warfare

responsable de los Estados en el ciberespacio, incluido un compromiso con la "no intervención en los asuntos internos de otros Estados"[25].

Como es sabido, la Convención sobre la Ciberdelincuencia del Consejo de Europa de 2001 (CETS No.185) 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[26].

Llegado este punto conviene detenernos un instante para mencionar, aun de forma sucinta, el Manual de Tallin.

En febrero de 2017, se publicó el Manual de Tallin 2.0 sobre el derecho internacional aplicable a las ciberoperaciones.

Elaborado por un grupo de 19 expertos en derecho internacional bajo los auspicios del Cooperative Cyber Defence Centre of Excellence de la OTAN (con sede en Tallin, Estonia), es una iniciativa no-vinculante para codificar la aplicación del derecho internacional al ciberespacio.

Pese a su importancia, representa sin embargo los puntos de vista de sus autores (y no la posición oficial de la OTAN). Un ejemplo: los expertos no pudieron ponerse de acuerdo sobre cómo se aplica el derecho internacional a situaciones específicas (por ejemplo, sobre la presunta acción rusa al Comité Nacional Demócrata de EE. UU. en 2016).

Aunque el DIH prohíbe los ataques directos contra la población y objetivos civiles, su aplicación no excluye todo tipo de ciberataques contra ellos. La mayoría de los autores del Manual 2.0 de Tallin opinaron que, al menos, se necesitaba un daño funcional (por ejemplo, un desabastecimiento de energía eléctrica) para considerar una ciberoperación como un "ataque" en el marco del DIH. Según el Comité Internacional de la Cruz Roja (CICR), la definición de "ataque" del DIH se aplica a los ciberataques, pero esta opinión sigue suscitando polémica entre los juristas internacionales, sin que esté claro en qué situaciones un Estado puede invocar el derecho de autodefensa en caso de un ciberataque[27].

Según algunos autores[28], contrarrestar los desafíos legales implica tres tareas (que, hasta ahora, no han sido exploradas por la OTAN y la UE), a saber:

---

[25] Véase: UN, 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, 24 June 2013, and A/70/174, 22 July 2015.
[26] Véase: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[27] Véase: https://ccdcoe.org/cycon/2012/proceedings/d3r1s1_schmitt.pdf
[28] Véase: A. Sari, Hybrid Warfare, Law and the Fulda Gap, University of Exeter, Law School, 2017.

1) Desarrollar una definición de la dinámica jurídica de las amenazas híbridas,

2) Comprender las vulnerabilidades legales y

3) Fortalecer la preparación, la disuasión y la defensa en el dominio legal.

Con respecto a las vulnerabilidades y los desafíos legales, debe recordarse que, contra las acciones equivalentes a un ataque armado, el Estado objetivo puede usar la fuerza en defensa propia. El Consejo de Europa carece claramente de competencia en este ámbito, ya que los "asuntos de defensa nacional" quedan excluidos del alcance de sus actividades sobre la base del artículo 1.d) de su Estatuto.

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[29].

Las amenazas híbridas que no alcanzan el umbral de un ataque armado pueden abordarse sobre la base del Artículo 4 del Tratado del Atlántico Norte, 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).

Los párrafos 1 y 2 del artículo 42 del Tratado de la Unión Europea (TUE) estipulan que "*la política común de seguridad y defensa debe formar parte integrante de la política exterior y de seguridad común*" e "*incluirán el encuadre progresivo de una política común de defensa de la Unión*" (cuyo establecimiento necesita una decisión del Consejo Europeo). Por su parte, 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.

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.
- Niegan sus operaciones híbridas para crear una zona gris legal dentro de la cual pueden operar libremente. La regulación legal de las

[29] Véase: https://www.nato.int/cps/ic/natohq/news_18553.htm?selectedLocale=en

amenazas híbridas siempre es un desafío puesto que una de las partes intenta evadir deliberadamente sus responsabilidades legales.

- 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 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 el derecho a elecciones libres (como se garantiza en el Artículo 3 del Protocolo no. 1).

4.5 Buenas prácticas y propuestas concretas

De todo lo anterior podemos deducir un conjunto elemental de buenas prácticas, a saber:

1. Las AH son una “cuestión de Estado”. Implican a la sociedad entera y no pueden ser tratadas aisladamente ni por medios territorialmente limitados.
2. Es necesario conocer en profundidad las vulnerabilidades de nuestra sociedad y nuestros sistemas de información en los sectores antes mencionados.
3. Lo más novedoso: el ciberespacio es el instrumento de ataque más significativo, eficaz y peligroso en el despliegue de las AH.
4. Es necesario implicar, conjuntamente, al Sector Público y al Sector Privado (puesto que muchas de las Infraestructuras Críticas están en manos privadas).

5. 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).
6. Es necesario incrementar la responsabilidad de las redes sociales por los contenidos difundidos a su través.
7. Es necesario estudiar las "nuevas formas de acción"[30], hay que 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 anticipación debida.
8. Es necesario regular:
    - Respecto de los medios tecnológicos (definir lo que "debe" hacer un ordenador ", para lo que resultarán imprescindibles las "certificaciones de seguridad").
    - Extendiendo el concepto de "agresión" a estas nuevas herramientas (igual que sucedió con las armas químicas en su momento o, más tarde, con las armas nucleares), incorporando estas cuestiones a la Carta de Naciones Unidas y al resto de la legislación nacional.
    - Para incorporar los principios éticos al desarrollo de software (modelos éticos en los sistemas de inteligencia artificial, por ejemplo) y de sistemas de información.

Cabe, por tanto, formular las siguientes **propuestas** más inmediatas:

1. A nivel estratégico: Parece necesario **contemplar las amenazas híbridas en el contexto de la Estrategia de Ciberseguridad Nacional**. Como quiera que ciertas manifestaciones de tales amenazas (muy especialmente, las fake news o la desinformación) pueden desarrollarse al margen del ciberespacio, parece apropiado que el desarrollo de dicha estrategia, 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 se se use el ciberespacio como elemento propagador de la amenaza. (En este contexto, un pen-drive también constituye un elemento del ciberespacio).
2. Análisis y coordinación: Así las cosas, 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. A nivel jurídico: Es necesario **actualizar la legislación nacional**, definiendo jurídicamente con precisión lo que debe entender por AH y su

[30] Félix Sanz Roldán. Secretario de Estado Director del CNI. Jornada "Guerra híbrida: nuevas amenazas". Instituto Seguridad y Cultura. Mayo, 2018. Senado.

encaje legal en nuestro ordenamiento jurídico (especialmente, en el orden penal) así como la introducción de las AH en la legislación en materia de medios de comunicación y redes sociales.

4. Formación y concienciación: Estas actividades, desplegadas a nivel nacional, resultan absolutamente necesarias para contribuir en el conocimiento y formación de criterio.
5. A nivel externo: Incrementar la cooperación internacional con organismos competentes en la materia, muy especialmente con la UE y la OTAN.

De todo lo anterior podemos concluir que las amenazas híbridas, en cualquiera de sus variantes, y pese a no constituir por sí mismas realidades nuevas, sí 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.