New Direction

DESINFORMACIÓN Y EL AUGE DE LAS AMENAZAS HÍBRIDAS EN LA UNIÓN EUROPEA

GUILLERMO PÉREZ

newdirection.online @europeanreform

New Direction

Founded by Margaret Thatcher in 2009 as the intellectual hub of European Conservativism, New Direction has established academic networks across Europe and research partnerships throughout the world.

newdirection.online **@europeanreform** **@europeanreform**

New Direction is registered in Belgium as a not-for-profit organisation and is partly funded by the European Parliament.
REGISTERED OFFICE: Rue du Trône, 4, 1000 Brussels, Belgium. **EXECUTIVE DIRECTOR:** Witold de Chevilly.

ÍNDICE

1

INTRODUCCIÓN

El único consenso internacional que existe con respecto a la idea de guerra híbrida es que "nadie la entiende, pero todo el mundo está de acuerdo, incluidas la OTAN y la Unión Europea, en que es un problema"[1]. Este comentario, aunque pueda resultar paradójico, es pertinente, pues los conceptos de amenazas y guerra híbrida son problemáticos y no hay consenso entre académicos, expertos y profesionales sobre qué constituye una amenaza híbrida o las características de una guerra híbrida[2].

Sin embargo, como punto de partida, ambos conceptos son importantes en el análisis de la seguridad y la defensa internacional, ya que se trata de términos ampliamente empleados en la actualidad y que por tanto, a pesar de sus limitaciones definitorias, tienen utilidad en tanto en cuanto contribuyen a que todas las autoridades europeas tengan en consideración la seguridad en el ejercicio de sus funciones y tomen medidas al respecto[3].

La primera dificultad a la hora de analizar las amenazas híbridas, entre las que se encuentra la desinformación, es el uso indistinto que se da a los términos amenazas híbridas y guerra híbrida (*hybrid warfare*). La OTAN, por ejemplo, utiliza ambos de forma intercambiable en sus documentos y no ofrece claridad conceptual[4].

Weissmann, por su parte, resuelve esta cuestión conceptualizando ambas ideas como dos caras de una misma moneda, que constituyen dos fases del mismo fenómeno: la guerra (*warfare*) híbrida se refiere a las medidas activas llevadas a cabo por un actor hostil, mientras que las amenazas pueden ser tanto activas como pasivas[5].

Contexto

Los conceptos de amenazas híbridas y guerra híbrida surgen en el contexto post-Guerra Fría. Ya en los años 90 del pasado siglo XX muchos elementos actualmente identificados en el marco de la guerra híbrida aparecían en las discusiones sobre guerras de cuarta generación (*Fourth-Generation Warfare*)[6].

Dicho elemento sganan relevancia, especialmente a partir del año 2000, con autores como Frank Hoffman, para describir las características de los conflictos contemporáneos en los que métodos convencionales e irregulares se emplean juntos e indistintamente tanto por actores estatales como no estatales[7].

Antes de que la guerra híbrida alcanzase su prominencia actual en 2014, según los analistas el conflicto que mejor se ajustaba a este concepto era la guerra entre Israel y Hezbolá de 2006, en la que Hezbolá habría empleado tácticas convencionales e irregulares y utilizado las nuevas tecnologías de

1 Cullen and Reichborn-Kjennerud (2017), p. 3.

2 Weissmann (2021), p. 63.

3 Fiott and Parkes (2019), p. 8.

4 Weissmann (2021), p. 63.

5 Ibid.

6 Wither (2016), p. 78.

7 Wither (2016), p. 75.

la información para su propaganda, operaciones psicológicas y comunicación estratégica[8].

Sin embargo, la relevancia actual que tiene el concepto de guerra híbrida no se puede entender sin considerar la invasión rusa de Ucrania en 2014, de ahí que se trate de un punto de inflexión comúnmente reconocido en todos los foros en los que se aborda la cuestión de la guerra híbrida.

En dicha invasión, las fuerzas armadas rusas hicieron uso integrado de herramientas militares y no militares, acciones políticas, coacción económica, operaciones cibernéticas y una intensa campaña de desinformación[9]. Es a partir de la experiencia y acciones rusas en Ucrania cuando el concepto de guerra híbrida se convierte en una idea omnipresente en los ámbitos políticos, militares y periodísticos de Occidente.

En el contexto actual, además de aumentar sus despliegues militares de la OTAN en Europa del Este, los gobiernos europeos están teniendo que hacer frente a campañas de desinformación —que van mucho más allá de las llamadas *fake news*— y ciberataques.

Uno de los hombres clave en esta nueva Rusia hostil es el general Valeri Gerasimov, jefe del Estado Mayor de las Fuerzas Armadas rusas. Tal es su importancia que su conceptualización de la ciencia de la guerra y su doctrina de guerra híbrida han llevado a Rusia a ocupar la posición más amenazante para la OTAN y Occidente desde el final de la Guerra Fría[10].

En su ensayo más influyente, de febrero de 2013, Gerasimov indicaba que en el siglo XXI hay una tendencia que desdibuja las delimitaciones entre guerra y paz y que la conducta actual de la guerra sigue patrones desconocidos. Dicha conducta incluye acciones como el uso de fuerzas especiales y elementos de oposición política para crear un nuevo frente de guerra dentro del territorio del enemigo, así como operaciones de información e influencia. Esta visión de un campo de batalla híbrido en el que predominan elementos políticos, económicos, informativos, humanitarios y otros aspectos no militares fue profética después de la invasión de 2014, cuando soldados rusos vestidos con uniformes sin insignias ni distintivo alguno, los denominados *pequeños hombres verdes*, aparecieron en Crimea para materializar la anexión a Rusia después de protestas populares previamente orquestadas por agentes rusos[11].

Conceptos

Después de las acciones rusas en Ucrania, cuyas consecuencias se mantiene hoy día, muchos analistas empezaron a hablar de la *Doctrina Gerasimov* en el contexto de las guerras híbridas y ésta ha llegado a tomarse como un plan de acción detallado de los objetivos rusos.

Sin embargo, otros expertos ven el ensayo de Gerasimov como una explicación de las acciones de Occidente contra Rusia, no como un plan estratégico para Rusia[12]. Este es un punto clave, pues muestra la complejidad del debate sobre amenazas y guerra híbrida y la diversidad de perspectivas que se encuentran tanto dentro de Occidente como entre los analistas rusos y occidentales.

Cabe recordar, además, que guerra y amenazas híbridas son dos conceptos occidentales. En Rusia, los analistas utilizan ideas como guerra de nueva generación y guerra no lineal (*new generation warfare* y *non-linear war*) para referirse a las características de los conflictos modernos y a la estrategia empleada por Rusia[13].

Así pues, el debate se fija, por una parte, entre Rusia y Occidente, enfrentados por quién está usando la guerra híbrida contra quién; y, por otra, en el seno mismo de Occidente, con una división entre expertos sobre la utilidad y validez de los conceptos de amenazas y guerra híbrida que, por otro lado, han sido plenamente adoptados por la OTAN y los principales países para elaborar estrategias y defensas contra las operaciones rusas y de otros actores.

En este sentido, para algunos observadores la preocupación con la guerra híbrida es una moda en el mejor de los casos y un ejercicio de apatía intelectual en el peor[14]. Además, se menciona la politización del término como una etiqueta útil para englobar todo lo que no se entiende sobre los conflictos contemporáneos[15]. Así, el hecho de que el concepto se utilice en Occidente para referirse a actores tan diversos como Rusia, Daesh, Hezbolá o China podría servir como indicativo de esa politización y falta de coherencia intelectual[16].

Es por culpa de estos problemas que no existe un consenso sobre la definición de los conceptos[17]. En cualquier caso, a pesar de las limitaciones que puedan tener, dichos conceptos son relevantes y útiles no sólo porque estén siendo empleados por políticos, militares y expertos, sino porque se refieren a una realidad tangible como son los ataques protagonizados por actores como Rusia y Daesh y sus entornos, así como al nuevo carácter de la guerra.

De hecho, se puede afirmar que lo que verdaderamente otorga valor analítico a los conceptos de amenazas y guerras híbridas es precisamente esta novedad de métodos y amenazas que ha generado sobre todo el desarrollo de tecnologías de la información y su integración con diferentes instrumentos militares y no-militares[18].

La seriedad de la realidad que hay presente detrás de los conceptos de amenazas y guerras híbridas se puede constatar a través de la respuesta que la OTAN y los Estados miembro de la Unión Europea han dado a dichos fenómenos. Además de la fuerza militar[19], se ha perseguido una idea holística de resiliencia, por la cual todos los niveles de la seguridad nacional (no sólo los tradicionalmente asociados a la seguridad y defensa) deben ser capaces de prever, prevenir y gestionar amenazas y ataques[20].

Institucionalmente, la UE creó en 2015 la East StartCom Task Force con el cometido de combatir la desinformación[21]. Uno de sus productos más útiles de cara al público es la página web www.euvsdisinfo.eu/, que hace frente directamente a casos de desinformación rusa.

Además, la UE estableció en 2016 un marco común para combatir amenazas híbridas, que, entre otras cosas, creaba una unidad de análisis en el Centro de Inteligencia y de Situación de la Unión Europea (EU INTCEN). Por último, la UE publicó en 2016 su estrategia global de seguridad y defensa para proteger Europa a través de la gestión de crisis, la protección de fronteras, y esfuerzos para combatir el extremismo, los ciberataques y la desinformación[22].

Por otro lado, en colaboración con la OTAN, la UE estableció en 2017 el *European Centre of Excellence for Countering Hybrid Threats*, que funciona como organismo de coordinación entre Estados miembro y como *think tank* independiente[23]. Este organismo es el que ha producido la definición de amenaza híbrida más completa y que mejor se ajusta a la visión del concepto por las instituciones gubernamentales occidentales. Según el Hybrid CoE, una amenaza híbrida se caracteriza por:

- Acción coordinada y sincronizada que ataca deliberadamente las vulnerabilidades sistémicas e institucionales de los estados democráticos a

8 Ibid.

9 Wither (2016), p. 76.

10 Foy (2017) https://www.ft.com/content/7e14a438-989b-11e7-a652-cde3f882dd7b.

11 Ibid.

12 Ibid.

13 Wither (2016), p. 80.

14 Giegerich (2016), p. 67.

15 Ibid.

16 Giegerich (2016), p. 68.

17 Weissmann (2021), p. 63.

18 Wither (2016), p. 75; Cullen and Reichborn-Kjennerud (2017), p. 3.

19 Pindják (2014)

20 Giegerich (2016), p. 69.

21 Fiott and Parkers (2019), p. 7.

22 https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

23 https://www.hybridcoe.fi/.

través de una gran variedad de métodos (políticos, económicos, militares, civiles e informativos).

- Actividades que explotan los umbrales de detección y atribución, así como la delimitación entre guerra y paz.

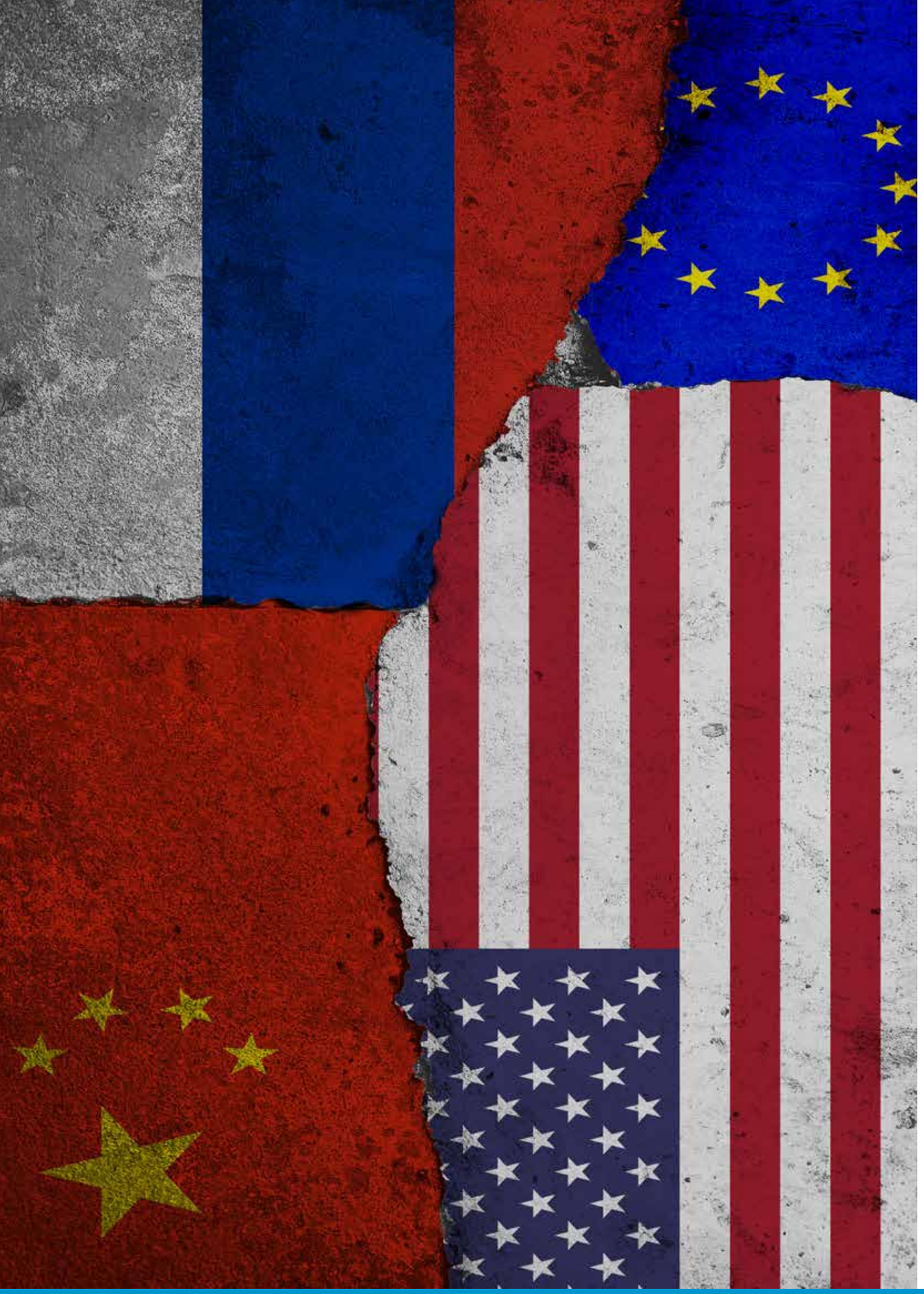
- Tiene el objetivo de influenciar procesos de decisión gubernamental a distintos niveles (local, regional, estado o institucional) para favorecer los intereses estratégicos del atacante y minar o debilitar al receptor.

Weissmann sintetiza las definiciones del Hybrid CoE y de otras organizaciones como The International Institute for Strategic Studies (IISS) en cinco características principales que comparten todas las acciones híbridas: son multidimensionales, coordinadas y sincronizadas, parte de una campaña integrada con objetivos estratégicos, buscan el engaño y buscan explotar la frontera entre guerra y paz[24].

Para concluir, el propósito final de estas campañas híbridas, especialmente de la parte de operaciones de información e influencia, se pudo ver claramente en las acciones desarrolladas por Rusia en Ucrania, que exacerbaron las vulnerabilidades sociales y debilitaron las instituciones gubernamentales ucranias para favorecer los intereses rusos[25]. Esta experiencia demuestra que la opinión pública es uno de los centros de gravedad más importantes en los conflictos contemporáneos.

24 Weissmann (2021), p. 65

25 Wither (2016), p. 77.



2

LOS PRINCIPALES ACTORES RUSIA ABRE CAMINO, CHINA LO EXPLOTA, CUALQUIERA AMENAZA

Incluso desde antes de la actual crisis del coronavirus, que como se verá posteriormente ha servido a China para desplegar una nueva forma de llevar a cabo su política exterior, Pekín venía siendo un actor cada vez más importante en el uso de capacidades híbridas y en la generación de amenazas híbridas[26]. Este creciente enfoque híbrido chino se puede observar sobre todo en sus acciones marítimas en el Mar de la China Meridional (MCM), en la diplomacia y en la doctrina de ciberguerra de Pekín.

Por un lado, China ha mejorado sustancialmente la Armada del Ejército Popular de Liberación en los últimos 20 años y ahora posee capacidades y doctrina marítimas que le otorgan unas herramientas formidables a la hora de promover sus intereses regionales. Entre estos intereses destacan los objetivos geopolíticos chinos de extender su alcance geopolítico por todo el Mar de la China Meridional.

Sin embargo, a la hora de conseguir este objetivo clave de su política exterior, China no depende sólo de su creciente flota, sino también de una milicia irregular marítima (*haishang mingbing*), cuyo propósito es acosar, hostigar y atacar a los buques de otras naciones que navegan por esas aguas. Esta milicia también es conocida como *little blue men* (pequeños hombres azules), en referencia directa a los *little green men* (pequeños hombres verdes) rusos que tomaron Crimea, y representa el símbolo por excelencia de la doctrina híbrida china. Estas fuerzas son empleadas tanto en operaciones convencionales en tándem con la Armada china, como en operaciones no convencionales camufladas como pescadores, en función de las necesidades militares de cada momento[27].

Este ejemplo muestra cómo China hace uso de métodos híbridos a nivel táctico, pero en el contexto marítimo las amenazas híbridas chinas también se extienden al nivel estratégico. Por ejemplo, Pekín utiliza operaciones no lineales para lentamente ir consiguiendo más territorios. La construcción progresiva de islas artificiales en el Mar de la China Meridional se enmarca en este enfoque estratégico, que está pensado para conseguir objetivos políticos sin provocar una escalada de tensiones descontrolada.

26 Miracola (2018), https://www.ispionline.it/it/pubblicazione/chinese-hybrid-warfare-21853.

27 Ibid.

Arrecife Travesura , islas Spartly, tomadas por China en 1994. ASIA MARITIME TRANSPARENCY INITIATIVE

Estas acciones estratégicas se pueden entender también desde el conceto de la Guerra Fría de la *táctica del salami*, pero la novedad híbrida consiste en que estas acciones van más allá del ámbito militar.

Desde 2003, China introdujo en su doctrina militar un documento titulado *Political Work Guidelines of the People's Liberation Army* en el que se describe la utilización de tres tipos de guerra (*warfare*) válidos tanto para tiempos de paz como de conflicto abierto: el primero es la guerra psicológica, dirigida a socavar la voluntad de luchar de los enemigos de China; el segundo es la guerra de opinión o informativa, que incluye la manipulación mediática y la desinformación para influenciar al público global y doméstico; el tercero es la guerra legal (*lawfare*), que contempla la explotación de todas las normas internacionales para asegurar los objetivos chinos y perjudicar a otros países en los foros internacionales[28].

China ya ha aplicado estos tipos de guerra (*warfare*) como parte de sus acciones en el Mar de la China Meridional, pero también en Taiwán. En lo relacionado con el MCM, China se ha movido históricamente entre las operaciones convencionales y las irregulares para dominar el ámbito psicológico de sus adversarios, por ejemplo en el conflicto con Filipinas por el atolón de Scarborough en 2012. Al mismo tiempo, ha llevado a cabo operaciones de influencia en el ámbito internacional y doméstico para reforzar su narrativa con respecto al MCM.

Siguiendo esta misma estrategia, China ha atacado a Taiwán, amenazando reiteradamente con una invasión militar si la isla declara formalmente su independencia. En este contexto, Pekín realiza operaciones de influencia y desinformación en la isla constantemente para socavar los apoyos al Gobierno de Tsai Ing-wen y conseguir que la población de Taiwán apoye la reunificación con China.

El último componente clave de la guerra híbrida china es su enfoque holístico de la ciberguerra. En línea con su pasado revolucionario y con sus doctrinas de guerra popular y fusión civil-militar, el Gobierno chino ha creado unidades de ciberguerreros compuestas por estudiantes universitarios y civiles, lo que proporciona una mayor flexibilidad y alcance, además de utilizar sus grandes corporaciones como Huawei como una extensión de las Fuerzas Armadas[29].

28 Ibid.

29 Ibid.

Entre otras acciones, China ha estado llevando a cabo una campaña de vigilancia online masiva en numerosos países a través de una empresa privada vinculada a los servicios de inteligencia chinos, recopilando los datos privados de un total de 2,4 millones de personas en todo el mundo[30].

Irán

Otros actores internacionales han seguido el ejemplo de Rusia y China para plantear amenazas en el ámbito híbrido y utilizar estas herramientas para conseguir sus objetivos políticos. Irán es un claro ejemplo de éstos.

La versión iraní de guerra híbrida y guerra no lineal aplicada desde 2003 tiene muchas similitudes con las acciones desplegadas por Rusia desde 2014. Las estrategias rusa e iraní pueden ser descritas como actos de imperialismo preventivo destinados a establecer nuevas esferas de influencia y seguridad regional. En el caso iraní, estas esferas de influencia tienen como objetivo principal las comunidades chiíes en su entorno[31].

Irán empleó su equivalente de los *little green men* rusos tanto en Irak, después de la invasión estadounidense, como contra Israel en 2006[32]. En los últimos años, Teherán ha extendido su presencia a otros escenarios como la guerra de Yemen y Siria, además de presentar nuevas amenazas híbridas al tránsito de petróleo por el Estrecho de Ormuz[33].

Los ataques a petroleros y la incertidumbre generada en el mercado mundial del petróleo por las acciones iraníes son un claro ejemplo del enfoque indirecto iraní en su conflicto con EEUU, que busca el desgaste de sus enemigos y la capacidad de negar su involucración en esas acciones.

De todas las redes de influencia y *proxies* iraníes en la región, destaca especialmente Hezbolá, que algunos autores consideran el arquetipo de actor no estatal que emplea métodos híbridos[34]. Su combinación de tácticas militares convencionales e irregulares fusionadas con sus estructuras civiles, así como su aparato propagandístico, hacen de Hezbolá un importante actor híbrido que presenta serias amenazas a países como Israel.

Daesh

Por último, otro actor importante estos últimos años que también ha sido clasificado como un actor híbrido es Daesh. El grupo yihadista destaca por su presencia en internet y su uso del ciberespacio como campo de guerra con fines psicológicos, además del tradicional uso de internet para propaganda y reclutamiento[35].

En general, Daesh destaca como actor híbrido por sus aspiraciones transnacionales, su fusión de tácticas convencionales con tácticas irregulares, su estructura flexible y adaptable y su uso del terror y de la violencia política para tener impacto a nivel psicológico y social[36]. Todas ellas características demostradas durante su intento de creación de un Califato entre Siria e Irak.

Su principal diferenciación con Al Qaeda, entre otras cosas al aspirar a gobernar tanto territorio como fuese posible, y la naturaleza novedosa de su amenaza al mundo llevó a Barack Obama a usar el concepto *híbrido* para diferenciar a *Daesh* de las redes terroristas tradicionales[37] y advertir sobre su peligro.

30 https://www.theguardian.com/world/2020/sep/14/zhenhua-data-full-list-leak-database-personal-details-millions-china-tech-company: https://www.abc.net.au/news/2020-09-14/chinese-data-leak-linked-to-military-names-australians/12656668.

31 Gardner (2015), p. 1. https://www.files.ethz.ch/isn/195396/rp_123.pdf.

32 Ibid., pp. 1 y 6.

33 Cordesman (2019) https://www.csis.org/analysis/strategic-threat-iranian-hybrid-warfare-gulf.

34 Piotrowski (2015), p. 1. https://www.files.ethz.ch/isn/188946/Bulletin%20PISM%20no%2024%20(756)%202%20March%202015.pdf.

35 LSE Ideas (2017): pp. 2 y 6. https://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-Hybrid-Warfare-in-the-Middle-East.pdf.

36 Jasper y Moreland (2014) https://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter.

37 Ibid.

3

DE 2016 A 2020, EL TRIUNFO DEL TERROR HÍBRIDO.

De Estados Unidos...

El Informe Mueller determina en su primer párrafo que "el Gobierno de Rusia interfirió en las elecciones presidenciales de 2016 de forma indiscriminada y sistemática"[38]. Con la publicación de este informe quedaba así demostrada la injerencia rusa durante la campaña electoral de 2016 en EEUU, así como múltiples casos de actividad criminal por parte del entorno de Donald Trump[39].

Entre otras cosas, Mueller establece que Rusia llevó a cabo una campaña de guerra informativa (*information warfare*) a través de las redes sociales que favoreció a Trump y perjudicó a Hillary Clinton, al tiempo que colaboró con Wikileaks para *hackear* bases de datos de la campaña de Clinton y filtrar materiales comprometedores, una táctica clara de *hack and leak*[40].

Mueller también encontró numerosos vínculos entre la campaña de Trump y el Gobierno ruso y que desde el entorno de la campaña de Trump mostraron interés por cualquier información que pudiese perjudicar a Clinton[41].

A pesar de que es imposible determinar el impacto exacto en términos de votos que tuvo esta campaña de injerencia rusa[42], sí está claro que se consiguió el principal objetivo de perjudicar a Clinton, pues la revelación de los e-mails del Partido Demócrata fue devastadora[43] para la candidata.

También parece evidente que Rusia logró condicionar la Presidencia de Donald Trump, ya sea de forma directa o indirecta, polarizando la sociedad estadounidense y socavando la autoridad de la administración Trump, de la que tuvieron que dimitir o ser destituidos un total de 40 altos cargos sólo durante los dos primeros años, muchos de ellos por las investigaciones sobre la llamada trama rusa[44].

El éxito de Rusia en esta campaña de injerencia en EEUU, como también reconoce el informe del *Intelligence and Security Committee* del Parlamento británico[45], fue el punto de inflexión para que muchos países como Reino Unido tomaran muy en cuenta la amenaza rusa a los procesos electorales occidentales. Así pues, es primero el caso de Ucrania y después la injerencia en EEUU lo que hace sonar todas las alarmas en Europa acerca de los intereses geopolíticos rusos, su determinación para conseguirlos y sus métodos híbridos.

38 Vallés (2019), p. 15; https://www.justice.gov/archives/sco/file/1373816/download.

39 https://www.acslaw.org/projects/the-presidential-investigation-education-project/other-resources/key-findings-of-the-mueller-report/.

40 https://www.acslaw.org/projects/the-presidential-investigation-education-project/other-resources/key-findings-of-the-mueller-report/.

41 https://www.acslaw.org/projects/the-presidential-investigation-education-project/other-resources/key-findings-of-the-mueller-report/.

42 Vallés (2019), p. 17.

43 Vallés (2019), p. 22.

44 Vallés (2019), p. 26.

45 ISC (2020), p. 13.

… a Europa

El modelo ruso empleado en Ucrania y EEUU ha sido replicado parcial o totalmente en muchos países europeos, sirviendo algunos como campo de prácticas para acciones posteriores. Ejemplos paradigmáticos son Georgia, el Brexit, los países bálticos y el este de Europa, pero también se ha podido identificar actividad rusa en el norte de Europa, Alemania, Francia, Holanda, Italia e incluso España.

En Europa, uno de los casos más importantes de injerencia rusa en procesos electorales fue el de las elecciones presidenciales francesas de 2017, acción con la que Rusia buscó favorecer a Marine Le Pen y evitar la victoria de Emmanuel Macron[46].

El candidato francés fue objetivo de una operación de desinformación durante la campaña electoral, en la que los medios asociados al Kremlin se esforzaron en mostrarle como una marioneta estadounidense, le acusaron de tener cuentas bancarias en paraísos fiscales e incluso difundieron rumores falsos sobre una relación extramarital homosexual[47]. En este caso, la acción más agresiva llevada a cabo por los rusos fue la operación de *hack and leak* del partido de Macron.[48]

Además de estas acciones durante la campaña, en Francia hay partidos que se han mostrado cercanos a Moscú en todo el espectro político. Sin embargo, ha sido el Frente Nacional el que ha tenido más vínculos con Rusia, hasta el punto de que tiene un acuerdo de cooperación con Rusia Unida, el partido de Vladimir Putin [49].

Marine Le Pen no sólo ha mostrado opiniones prorrusas en temas de política exterior y viajado a Moscú para entrevistarse con Putin[50], sino que su partido recibió nueve millones de euros en financiación de bancos vinculados al Kremlin. Además del Frente Nacional francés, hay partidos importantes con acuerdos de cooperación con Rusia Unida en Austria, Hungría, Italia y Alemania.

En el resto de Europa, los países nórdicos, por ejemplo, han sido objetivo de propaganda poniéndolos como ejemplo de la degradación moral de Occidente, aunque la desinformación rusa dentro de estos países ha sido menos efectiva que en otros gracias, entre otras cosas, a la buena calidad de su sistema educativo[51]. El hecho de ser además países fronterizos con Rusia juega de alguna manera a favor de que tanto los instrumentos de estos estados como la propia población tengan una mayor predisposición a la alerta frente a la injerencia de Moscú.

Más allá, los Países Bajos también han recibido campañas de desinformación rusas durante procesos electorales y, especialmente, en todo aquello relacionado con Ucrania y el derribo del vuelo MH17 de Malaysia Airlines, en el que más de la mitad de los pasajeros eran holandeses y fallecieron justo al resto del pasaje y tripulación por el disparo de un misil tierra-aire desde territorio ucraniano controlado por milicias prorrusas[52].

Por último, en Italia los partidos populistas tanto de izquierda (Movimiento Cinco Estrellas) como de derecha (Ligar Norte) mantienen visiones prorrusas en política exterior y han tenido vínculos con la redes de desinformación rusas y con Rusia Unida[53], el partido de Putin. Algunos expertos sospechan incluso que la Liga Norte pudo haber recibido financiación rusa. El sector energético italiano también es vulnerable a la influencia rusa, especialmente a través de la empresa energética ENI, que es un socio de Gazprom en el proyecto estratégico Nord Stream 2[54].

46 Committee on Foreign Relations U.S. Senate (2018), p. 121.

47 Ibid.

48 Intelligence and Security Committee (2020), p. 5.

49 Committee on Foreign Relations U.S. Senate (2018), p. 50.

50 Ibid., p. 122.

51 Ibid. pp. 109-111.

52 Ibid., p. 113-114.

53 Ibid., p. 137.

54 Ibid., p. 138.

El Brexit

A pesar de la clara presencia hostil e intereses rusos en Reino Unido, es importante comenzar reconociendo que el impacto exacto de cualquier injerencia en procesos políticos como el referéndum del *Brexit* es muy difícil de estimar y evaluar con precisión[55]. Este hecho es reconocido por el *Intelligence and Security Committee* (ISC) del Pqrlamento británico en su informe de 2020 sobre la presencia y acciones rusas en Reino Unido y es una limitación que hay que tener en cuenta en cualquier análisis sobre injerencia rusa en Occidente.

Dicho esto, la presencia hostil rusa en la política europea y occidental, así como los intereses rusos en Reino Unido están más que demostrados. Entre otras cosas, desde 2014, Rusia ha llevado a cabo actividad maliciosa en el ámbito cibernético con la intención de influir en procesos electorales como la campaña presidencial francesa de 2017[56].

Aunque el informe público y sin clasificar del ISC, que además tiene partes censuradas, no recoge evidencia secreta ni contiene conclusión fehaciente algunas sobre la injerencia rusa en el referéndum de 2016, sí que se hace eco (aunque con cautela) de los numerosos informes, artículos y estudios producidos con fuentes abiertas que atestiguan la campaña rusa en redes sociales tanto en el referéndum de 2014 sobre la independencia de Escocia como en el referéndum del *Brexit* de 2016[57].

El informe explora además los numerosos intereses económicos rusos en Reino Unido y las redes de influencia que estos influjos masivos de inversión rusa han generado entre la élite política y empresarial británica[58].

Parte de esta evidencia basada en fuentes abiertas está compuesta por varios estudios académicos que han estimado en hasta 150.000 las cuentas de Twitter y Facebook controladas por los servicios de inteligencia rusos durante la campaña del referéndum de 2016[59]. Lo que además es evidente es el interés ruso en desestabilizar a la Unión Europea[60], algo que se pudo ver en el tratamiento que los medios RT y Sputnik (controlados por el Estado ruso) dieron a la campaña del referéndum del *Brexit*, con una postura sistemáticamente a favor de los partidarios de la ruptura[61].

Esta presencia mediática y la proliferación de *fake news* en redes sociales se ha mantenido incluso después del referéndum, como se pudo ver en la campaña de desinformación rusa que alentó el sentimiento anti musulmán después del atentado del puente de Westminster de 2017 y que logró tener eco en tabloides como *The Sun* y *Mail Online*[62].

La entonces primera ministra británica, Theresa May, advertía en 2017 sobre las actividades hostiles que Rusia estaba llevando a cabo en todo Occidente, aunque sin mencionar el impacto que éstas podían haber tenido en procesos electorales británicos. Otros políticos de primera línea británicos sí se han mostrado más preocupados por ese potencial impacto[63].

Por último, el informe de 2018 del Senado estadounidense sobre injerencia rusa en Europa sí considera que Rusia ha intentado desestabilizar el Reino Unido a través de desinformación, ciberataques y corrupción[64]. Dicho informe recoge las actitudes prorrusas de Nigel Farage, líder del UKIP y uno de los principales impulsores del *Brexit*. Además,

55 Intelligence and Security Committee of Parliament (2020), “Russia Report”, p. 12.

56 Ibid., p. 5.

57 Ibid., pp. 12 y 13.

58 Ibid., pp. 15 y 16.

59 Hern (2017). https://www.theguardian.com/world/2017/nov/15/russian-troll-factories-researchers-damn-twitters-refusal-to-share-data

60 Committee on Foreign Relations U.S. Senate (2018), p. 116.

61 Wintour (2018), https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

62 Booth, Weaver, Hern, Smith y Walker (2017), https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.

63 Mason (2017), https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news.

64 Committee on Foreign Relations U.S. Senate (2018), p. 116.

muestra preocupación por la influencia que las redes económicas rusas en Reino Unido tienen en partidos políticos, el conjunto de la sociedad civil y *think tanks*, además de las facilidades que las leyes británicas sobre financiación de campañas ofrecen para que el dinero opaco ruso termine ayudando a actores políticos británicos[65].

Las conclusiones que se pueden sacar de esta breve exploración es que los intereses rusos por desestabilizar la UE y tener influencia en la política británica son evidentes y que hay indicios que apuntan, por un lado, a campañas de desinformación en redes y, por otro, a dinero ruso fluyendo por los círculos de poder británicos. Sin embargo, actualmente es difícil —de hecho, imposible según el Parlamento británico— esclarecer el impacto exacto y las consecuencias que estas acciones han tenido en la última década en la política británica.

Alemania

En los últimos años, Rusia ha buscado extender su poder en Alemania a través de proyectos energéticos, injerencia política, desinformación y ciberataques[66]. Esto se ha manifestado en campañas de desinformación dirigida hacia procesos electorales como el de 2017 y en los fuertes lazos que mantienen partidos populistas como Die Linke y la Alternative für Deutschland (AfD).[67] Además, según el centro EUvsDisinfo, Alemania es, con diferencia, el país de la Unión Europea que más casos de desinformación rusa ha registrado desde 2015[68].

Unos factores muy importantes en el caso de Alemania son que hay una relación cercana con Rusia en todos los ámbitos, que una parte importante del *establishment* político y empresarial está altamente vinculado a Rusia (los *Russlandversteher*) y que hay una tradición política de pragmatismo hacia Moscú que se remonta a la *Ostpolitik* de la época de Willy Brandt[69].

Por todas estas razones, Alemania es un país especial en el análisis de las amenazas híbridas rusas, hasta el punto de que Rusia podría incluso considerar a Alemania no como un objetivo de dominación, sino como un socio estratégico[70]. Incluso, en el contexto post 2014, sigue habiendo en Alemania un conjunto de intereses políticos y económicos, así como un conjunto de factores sociales como el legado de Alemania del Este y la inmigración rusa, que generan peso social y poder suficiente como para que la canciller Angela Merkel, moderadamente considerada una halcón, haya apoyado hasta el día de hoy un proyecto como Nord Stream 2, a pesar de la amenaza de sanciones por parte de EEUU y de la oposición de muchos países de la UE[71].

El factor más importante en el análisis de Alemania es precisamente este polémico proyecto energético Nord Stream 2, que desde principios de los años 2000 ha estado promovido por un grupo de intereses empresariales y políticos liderado por Gerhard Schröder, predecesor de Angela Merkel en la Cancillería alemana.

Schröder tiene mucha relación con el poder político y económico ruso, hasta el punto de que es presidente del Consejo de Administración de Nord Stream AG, empresa subsidiaria de Gazprom y principal socio en el proyecto de Nord Stream[72]. No es sólo eso, sino que posteriormente se ha unido a la petrolera rusa Rosneft también como presidente del Consejo de Administración[73]. Quien fuera no sólo un líder de Alemania, sino un puntal en las relaciones del conjunto de la Unión Europea entre 1998 y 2005 —recordemos que la entrada de numerosos países del Este y las repúblicas bálticas en la UE se produjo estando él aún al frente de la Cancillería— juega ahora un papel relevante en los intereses rusos energéticos.

Por otro lado, además de recibir financiación rusa (según *Bild*), los medios propagandísticos rusos como RT han apoyado sistemáticamente a la AfD. Estos medios también han participado en campañas más amplias de desinformación dirigidas contra Merkel y asuntos como la crisis de los refugiados sirios[74].

En este sentido, el conocido como *caso Lisa* —una joven germano-rusa de 13 años denunció haber sido secuestrada y violada por un grupo de inmigrantes aunque posteriormente reconoció que todo era una invención— es un ejemplo paradigmático de cómo las redes de desinformación rusas pueden difundir manipulaciones y mentiras para perjudicar a un Gobierno occidental, en esta ocasión incitando el miedo hacia los migrantes en el contexto de las políticas de refugiados abanderadas por el Gobierno de Angela Merkel[75].

Por último, Alemania también ha sido víctima de ciberataques rusos, como el que sufrió el *Bundestag* en 2015, calificado como "escandaloso" por la canciller Merkel, que apuntó directamente a Rusia; así como los hackeos al propio partido de Merkel, la CDU y sus fundaciones asociadas[76].

Cataluña

En España hay una larga tradición de presencia criminal rusa con vínculos directos con altos cargos del régimen de Vladimir Putin y una historia paralela de lucha contra estos grupos criminales por parte de las autoridades[77]. El informe del Senado de EE UU pone énfasis en la presencia de estos grupos criminales en Cataluña y sus redes de influencia en la política regional.

El caso de Xavier Crespo ejemplifica hasta qué punto los grupos criminales rusos han tenido influencia en Cataluña. En 2013, Crespo, político de Convergència i Unió, fue propuesto como secretario de Seguridad de la Generalitat de Cataluña, pero se paralizó su nombramiento cuando los servicios de inteligencia españoles alertaron que estaba involucrado en una trama de sobornos y blanqueo de capitales rusos[78]. Según el informe del Senado estadounidense, su partido, CiU, que se disolvió dos años después, también habría estado recibiendo fondos de organizaciones criminales rusas[79].

Además de esta presencia criminal rusa en Cataluña, hay un creciente número de análisis y evidencias que demuestran la injerencia rusa en la crisis independentista de 2017 a través de campañas desinformación en redes sociales y contactos entre el Gobierno catalán y personas en la órbita del Gobierno ruso[80].

El referéndum de independencia del 1 de octubre de 2017 le dio la oportunidad a Rusia de volver a intentar debilitar a un importante Estado miembro de la Unión Europea. Como mínimo, el Kremlin estuvo involucrado a través de sus órganos de propaganda RT y Sputnik, que lanzaron una importante campaña de desinformación durante las fechas del referéndum y la posterior declaración de independencia[81].

También hay estudios que indican que, entre el 29 de septiembre y el 5 de octubre de 2017, de los cinco millones de mensajes en redes sociales que hubo sobre Cataluña, un 30% provenía de cuentas anónimas que compartían exclusivamente contenido de RT y

65 Ibid., p. 117; Wintour (2018), https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

66 Committee on Foreign Relations U.S. Senate (2018), p. 127.

67 Ibid., p. 128.

68 https://euvsdisinfo.eu/villifying-germany-wooing-germany/.

69 Mankoff (2020), https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect.

70 Mankoff (2020); https://euvsdisinfo.eu/villifying-germany-wooing-germany/.

71 Mankoff (2020).

72 Committee on Foreign Relations U.S. Senate (2018), p. 127.

73 Ibid. P. 128.

74 Ibid., pp. 128 y 129.

75 Ibid.

76 Ibid., p. 130.

77 Committee on Foreign Relations U.S. Senate (2018), p. 133-134.

78 Ibid., p. 134; https://okdiario.com/espana/un-ex-diputado-de-cdc-es-condenado-a-nueve-anos-y-medio-de-inhabilitacion-por-soborno-y-prevaricacion-18960.

79 Ibid.

80 Committee on Foreign Relations U.S. Senate (2018), p. 133.

81 Ibid., p. 134-135.

Sputnik, un 25% provenía de *bots* y un 10% de las cuentas oficiales de estos dos medios de propaganda rusa[82]. Justo antes del referéndum, numerosas cuentas de Twitter a favor del Kremlin aumentaron sus menciones sobre la crisis catalana en un 2.000%[83].

El País, el periódico generalista de mayor tirada de España, informaba en 2017 sobre la existencia de más de 4.800 *bots* en las fechas del referéndum que se dedicaban a compartir contenido de RT y Sputnik. Por ejemplo, estos *bots* consiguieron que dos mensajes superaran cada uno más de medio millón de impactos potenciales[84].

Por su parte, el grupo de expertos creado por la Unión Europea para combatir la propaganda rusa también detectó en los últimos meses de 2017 un aumento de la injerencia propagandística rusa en Cataluña con mensajes dirigidos a desestabilizar a España y a la Unión Europea[85].

Las razones que explican la presencia y el interés ruso en Cataluña las presenta el periodista David Alandete (uno de los principales expertos en este episodio en España): por un lado, Rusia buscaría legitimar su anexión de la península de Crimea creando paralelismos con casos como el de Cataluña y, por otro, ahondaría en su interés último de debilitar a la Unión Europea a través del fenómeno del independentismo[86] y añadiendo tensión a un Estado miembro. Unas tensiones que se mantienen cinco años después con un "autoproclamado presidente de la Generalitat en el exilio", Carles Puigdemont, residiendo en Waterloo y varios políticos independentistas catalanes presos por acciones ilegales cometidas precisamente en torno al referéndum del 1 de octubre.

Por si fuera poco, la injerencia rusa también tiene una parte de injerencia venezolana, pues en los meses de la crisis de Cataluña de 2017 los medios rusos RT y Sputnik se valieron de un elevado número de cuentas en redes sociales del entorno del chavismo y Venezuela para propagar una imagen negativa de España. Esta red de cuentas controladas por Rusia y el chavismo llegó a lograr que se impusiera una determinada interpretación de la crisis catalana en la conversación global en redes sociales[87].

Pero más allá de esta injerencia a través de la difusión de campaña de desinformación en redes sociales y por sus medios de propaganda, Rusia ha estado presente en Cataluña a través de contactos directos que han tenido personas cercanas al poder en Barcelona y Moscú. Un ejemplo es la visita que hizo el ministro de facto de asuntos exteriores de la República de Osetia del Sur (satélite ruso) a Cataluña en octubre de 2017 pare reunirse con empresarios y abrir una oficina de interés en Barcelona[88].

Más preocupantes resultan los indicios de la presencia de un operativo del GRU (inteligencia militar rusa) en Cataluña en los meses previos y posteriores al referéndum de 2017. De hecho, este individuo, Denis Sergeev, también podría haber estado involucrado en el caso Skripal[89], un agente doble ruso que fue envenenado junto a su hija Yulia en Reino Unido en 2018, que derivó en una importante crisis diplomática entre Reino Unido y Rusia y que se amplió a otros Estados miembros de la UE y aliados de los británicos.

También hay noticias sobre los encuentros en Rusia de un enviado de Puigdemont, Víctor Terradellas, ex responsable de relaciones internacionales de Convergència Democràtica de Catalunya —partido que junto a Unió Democràtica de Catalunya configuraba Covèrgencia i Unió–, con un exdiputado ruso para obtener el apoyo de Moscú en caso de que se produjera una declaración unilateral de independencia[90].

82 Ibid.

83 Ibid.

84 Galán, Abad y Alameda (2017), https://elpais.com/politica/2017/12/04/actualidad/1512389091_690459.html; https://elpais.com/internacional/2018/03/05/estados_unidos/1520277454_983401.html.

85 https://www.elconfidencial.com/espana/cataluna/2017-11-10/independencia-cataluna-injerencia-rusia_1475857/.

86 Alandete (2019), p. 44.

87 Alandete (2017), https://elpais.com/politica/2017/11/10/actualidad/1510341089_316043.html.

88 https://elpais.com/politica/2017/10/25/actualidad/1508958307_955473.html.

89 https://www.vozpopuli.com/espana/espia-ruso-Sergei-Fedotov-Cataluna_0_1302471121.html

90 https://www.vozpopuli.com/internacional/Exdiputado-reconoce-Moscu-Puigdemont-Cataluna_0_1302770811.html.

Los contactos del círculo de Puigdemont con Rusia no acaban ahí, y además en los último tiempos Puigdemont se ha ido acercando progresivamente el entorno ruso a través de numerosas apariciones en medios de comunicación en las que ataca a la Unión Europea, pese a formar parte de sus instituciones como eurodiputado, y apoya las posiciones rusas en temas tan polémicos como el de Crimea[91].

Todos estos contactos e indicios de injerencia rusa —la llamada *trama rusa* del 1-O— están siendo investigados por la Justicia española como parte de la causa sobre la red criminal creada por Puigdemont para sufragar su *exilio*.[92] Estas investigaciones, por las que ya se ha detenido a varias personas, incluyen la sospecha que, días antes de la Declaración Unilateral de Independencia, Rusia ofreció a Puigdemont trasladar 10.000 soldados a Cataluña[93].

Ojo: La información aparecida en los medios españoles sobre la llegada de 10 mil soldados rusos a Cataluña está incompleta. Hace falta añadir dos ceros al número de soldados y lo más impactante de toda esta conspiración: las tropas deberían ser transportadas por aviones "Mosca" y "Chato" ensamblados en Cataluña durante la Guerra Civil y escondidas en un lugar seguro de la Cierra Catalana hasta recibir a través de estas publicaciones la orden cifrada de actuar.

Mensaje publicado en Twitter por la cuenta de la Embajada rusa en España el 28 de octubre de 2020[94].

Como suele ser su práctica habitual, Rusia ha negado cualquier injerencia y contactos con líderes independentistas catalanes y rechazó categóricamente a finales de 2020 las acusaciones de la Justicia española, considerándolas "propaganda antirrusa"[95]. Anteriormente, la única respuesta oficial de Rusia sobre estas acusaciones había sido una mofa a través de Twitter[96].

Esta actitud rusa de burla y descalificación de las acusaciones sobre sus actividades en Occidente es una estrategia establecida y demostrada. Tiene un propósito claro de cuestionar la veracidad de las acusaciones y sembrar dudas entre la población a través del ridículo. Esto se ha podido observar anteriormente en el *caso Skripal*, en el que la cuenta de Twitter de la embajada rusa en Londres hizo burla en repetidas ocasiones de los graves hechos que las autoridades británicas imputaban al Gobierno ruso[97].

91 https://www.vozpopuli.com/espana/putin-financiacion-bitcoin-anotaciones-puigdemont_0_1300670215.html; https://www.vozpopuli.com/elliberal/Puigdemont-deja-querer-Kremlin_0_1295270953.html.

92 https://www.elperiodico.com/es/politica/20191113/juez-investiga-trama-rusa-independencia-catalunya-puigdemont-7733376; https://elpais.com/espana/catalunya/2020-10-28/el-juez-investiga-al-circulo-de-puigdemont-por-sus-contactos-con-el-kremlin.html; https://www.abc.es/espana/catalunya/politica/abci-juez-cree-rusia-ofrecio-puigdemont-10000-soldados-202010281620_noticia.html.

93 https://www.elperiodico.com/es/politica/20201028/el-juez-senala-la-vinculacion-de-rusia-con-el-proces-8178454.

94https://twitter.com/EmbajadaRusaES/status/1321529417609420803?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1321529417609420803%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.lavozdeasturias.es%2Fnoticia%2Factualidad%2F2020%2F10%2F29%2Fembajada-rusia-mofa-informaciones-sobre-llegada-10000-soldados-rusos-cataluna-faltan-dos-ceros%2F00031603968921270492671.htm.

95 https://www.elperiodico.com/es/politica/20201029/moscu-guarda-silencio-sobre-la-supuesta-trama-rusa-8179802.

96 https://elpais.com/espana/catalunya/2020-10-28/la-embajada-rusa-se-burla-del-supuesto-envio-de-10000-soldados-a-cataluna.html.

97 https://www.bbc.com/news/world-europe-46567364.

Mensaje publicado en Twitter por la cuenta de la Embajada rusa en Londres el 18 de marzo de 2018.

Los países del Este

El informe del Senado de EEUU sobre injerencia rusa en Europa recoge múltiples ejemplos de los países del este de Europa, aunque, sin duda alguna, el caso más paradigmático es el de **Ucrania**. Este país ha sido el objetivo de la campaña híbrida más completa desarrollada por Rusia con el objetivo de convertir el país en un Estado fallido[98]. De especial importancia fue la operación de información estratégica (desinformación) que explotó las vulnerabilidades sociales existentes, debilitó al Gobierno e instituciones estatales y erosionó la legitimidad del Estado ucraniano, además de crear justificaciones para la invasión rusa[99]. Ucrania ha sufrido, además, una invasión militar convencional complementada por asesinatos selectivos, ciberataques, uso de la energía como arma y corrupción[100].

Prácticamente todos los sectores de la sociedad y de la economía ucranianas (medios, finanzas, transporte, Fuerzas Armadas, instituciones, políticos, sistema electoral e infraestructura energética) han sido víctimas de ciberataques rusos en los últimos años[101]. Por ejemplo, entre 2015 y 2016 hubo dos importantes ciberataques rusos a la red eléctrica ucraniana.

Pero no es sólo Ucrania, sino toda la antigua órbita soviética en Europa la que está sufriendo la injerencia rusa. Según el Senado estadounidense, hay varios factores comunes que tienen la mayoría de estos países y que explican la agresividad rusa:

- En primer lugar, la mayoría tienen sectores de su población que son receptivos a la propaganda del Kremlin o incluso tienen poblaciones de rusos étnicos dentro de sus fronteras.

98 Giegerich (2016), p. 66; Committee on Foreign Relations U.S. Senate (2018), p. 67.

99 Wither (2017), p. 77.

100 Committee on Foreign Relations U.S. Senate (2018), p. 67.

101 Ibid., p. 68.

- En segundo lugar, estos países poseen en general instituciones gubernamentales y sociedad civil débiles y altos niveles de corrupción que los vuelven vulnerables a acciones rusas.

- Por último, Rusia ataca especialmente a los países que han mostrado su intención de unirse a la Unión Europea o la OTAN, pues considera que esto atenta contra la zona de influencia que merece como gran potencia. Las acciones rusas en Georgia, Ucrania y Montenegro son las que más evidencian esta preocupación geopolítica[102].

Georgia fue invadida por Rusia en 2008 para garantizar la independencia de las repúblicas de Abjasia y Osetia del Sur, con una campaña militar que estuvo complementada en todo momento por ciberataques[103]. Desde entonces, Rusia ha mantenido una red mediática propagandística y ha apoyado a partidos políticos y grupos civiles dentro de Georgia[104].

Montenegro, por su parte, también ha sufrido la intervención directa de Rusia dentro de sus fronteras. En 2016, Rusia intensificó su presencia en el país para evitar, infructuosamente, que Montenegro se uniese a la OTAN. Esta campaña incluyó propaganda y apoyo a ONG y partidos políticos, y culminó con un intento de golpe de Estado patrocinado, supuestamente, por Rusia[105].

En cuanto a **Bulgaria**, Rusia mantiene fuertes lazos culturales y religiosos, además de importantes inversiones económicas sobre todo en el sector energético. También tiene influencia en los partidos políticos búlgaros y relación con sus Fuerzas Armadas por la dependencia de éstas del equipamiento ruso[106]. En general, Rusia mantiene un importante *poder blando* en Bulgaria.

En lo que respecta a **Hungría** es, probablemente, el país europeo cuyo Gobierno tiene mejor relación con el Kremlin. Además de las típicas redes de propaganda, corrupción y apoyo a organizaciones políticas y grupos extremistas, el Gobierno ruso mantiene una relación muy cercana con el húngaro y Viktor Orbán es posiblemente el líder que más apoya a Vladimir Putin, su estilo de liderazgo y su visión general del mundo. El Gobierno de Orbán ve positivamente la propaganda rusa antieuropea, antiestadounidense y xenófoba porque está alineada con su visión política. Además, la visión de democracia iliberal que ha perseguido Orbán desde 2010 es muy similar a la visión rusa de democracia soberana[107].

Por último, es importante considerar la influencia rusa en los países bálticos a través de intimidación militar, dependencia energética, lazos comerciales, lazos culturales, corrupción, desinformación y ciberataques. **Letonia** y **Estonia** son especialmente vulnerables por su proximidad geográfica a Rusia y por su población de rusos étnicos. **Estonia**, por ejemplo, lleva desde 2007 sufriendo ciberataques y campañas de desinformación rusas, así como involucración directa de políticos y diplomáticos rusos en el debate público estonio. Las campañas de desinformación rusas están especialmente dirigidas a los rusos étnicos de esos países y se han intensificado desde que la OTAN desplegase tropas. Por ejemplo, en 2017 medios prorrusos difundieron la historia falsa de una violación a una niña de 13 años por parte de soldados alemanes de la OTAN[108]. Tienen como objetivo que se perciba a los países bálticos como estados fracasados, sacudidos por la inmigración y la pobreza, y dirigidos por una élite siniestra con afinidades fascistas y vendida a Occidente[109].

102 Committee on Foreign Relations U.S. Senate (2018), p. 65.

103 Ibid., pp. 73-74.

104 Ibid., pp. 74-75.

105 Ibid., pp. 77.

106 Ibid., pp. 89.

107 Ibid., pp. 94-96.

108 https://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870.

109 Committee on Foreign Relations U.S. Senate (2018), pp. 99-101.

El coronavirus

La crisis provocada por la pandemia de Covid-19 ha puesto de manifiesto las actividades de Rusia y de China en el ámbito de la desinformación. A pesar de la predominancia rusa en este ámbito a lo largo de la última década, durante la pandemia China hatomado la iniciativa en este terreno[110].

Por un lado, Rusia ha continuado con sus campañas disruptivas con el objetivo de socavar, desorientar, agitar, polarizar o neutralizar estratégicamente a sus adversarios y rivales. China, por su parte, tiene un planteamiento más ambicioso y de largo alcance y está apostando por la búsqueda de la supremacía narrativa y el control del relato[111].

Pekín ha aprovechado los errores de los países europeos y la propia UE en la gestión de la crisis del coronavirus para cambiar el relato predominante sobre la pandemia y encubrir su responsabilidad en el origen del virus en Wuhan[112].

Desde principios de 2020, China ha estado manipulando la realidad y difundiendo deliberadamente información falsa para sembrar dudas en la opinión pública mundial sobre los orígenes del virus, poner énfasis en los errores de otros, especialmente las democracias, y promover el liderazgo mundial de China[113].

Hay una gran cantidad de evidencia que demuestra que China ha estado sumida en una guerra informativa durante la pandemia, dirigiendo todo su aparato propagandístico, que en tiempos normales se centraba en el ámbito doméstico, hacia el mundo entero[114].

Los actores chinos involucrados en esta guerra informativa han sido los portavoces oficiales del Gobierno en Pekín, los ministerios e instituciones chinas, sus medios de comunicación domésticos e internacionales, los diplomáticos en sus comunicados oficiales y en redes sociales, y todas las redes de miles de cuentas en redes sociales que han servido para amplificar todos los mensajes[115]. En resumen, ha habido un esfuerzo coordinado de todo el aparato estatal y social chino para emplazar su desinformación en la narrativa mundial sobre la pandemia.

Para asegurar el éxito en la difusión de sus mensajes, China ha copiado los métodos rusos: ha usado un gran número de cuentas falsas (*trolls* y *bots*) en redes sociales e incluso ha hecho uso de las redes de *proxies* del Kremlin para propagar su desinformación[116].

Los medios y políticos rusos, e incluso los iraníes, no han dudado en sumarse a la difusión de las conspiraciones chinas sobre el origen del virus[117]. También hay indicios de las actividades de los servicios de inteligencia chinos en EEUU para promover el pánico entre la población usando aplicaciones de mensajería móvil[118].

Además, en claro contraste con su actitud antes de la pandemia y con la narrativa del *ascenso pacífico* de China, diplomáticos chinos en todo el mundo han participado en estas campañas difundiendo información falsa y apoyándose en los medios de comunicación chinos en el exterior para promover los mensajes de Pekín.

Los niveles de agresividad y beligerancia demostrados por estos diplomáticos les han valido el sobrenombre de *wolf warriors*[119]. Esta nueva postura diplomática china ya ha provocado varios incidentes diplomáticos con países como Australia, Canadá y Francia[120].

Según algunos expertos, esto presagia una nueva era para la presencia china en el mundo, que sería mucho más activa y conflictiva, acuñando incluso el término *wolf warrior diplomacy*. Esta nueva política exterior, que viola las normas y convenciones diplomáticas, reflejaría la creencia en China de que el liderazgo occidental del mundo está en declive y China ya no tiene que mantener relaciones amistosas con el mundo[121].

Este análisis se refuerza considerando el apoyo que los medios propagandísticos y tabloides chinos están dando a la beligerancia de sus diplomáticos. Además, China no está siguiendo la *wolf warrior diplomacy* sólo en lo relacionado con la pandemia, sino que se está viendo también en temas como la represión de los Uigures y en Taiwán[122].

Por su parte, además del apoyo que le ha dado a China, Rusia ha llevado a cabo una campaña de desinformación en redes sociales, Internet y medios propagandísticos dirigida contra las vacunas occidentales. Atacando vacunas como la de Pfizer y difundiendo mentiras sobre su efectividad y efectos secundarios, Rusia pretende erosionar la gestión de la pandemia de los países occidentales y, por tanto, su legitimidad y prestigio.

Además, junto a su campaña a favor de la vacuna rusa Sputnik V, pretende impulsar las ventas y el prestigio de su capacidad científica[123]. China e Irán también parecen estar involucrados en campañas para denigrar las vacunas occidentales.[124]

De igual manera, merece la pena recordar la campaña de ayuda llevada a cabo por Rusia en el peor momento de la pandemia en Italia, en un momento en el que la respuesta de la Unión Europea y los Estados miembros a la crisis que vivía Italia dejaba mucho que desear. A finales de marzo de 2020, Rusia envió 15 aviones con suministros para ayudar al país transalpino, un gesto que tuvo un gran impacto mediático, especialmente por el contraste que supuso ver los camiones rusos circulando por las autopistas italianas frente al abandono de Italia a su suerte por parte de Europa[125].

Teniendo en cuenta que, según el diario *La Stampa*, el 80% del material enviado por los rusos terminó siendo inútil[126], el objetivo de Rusia era claramente aprovechar espontáneamente la crisis del Covid-19 y la negligente repuesta europea a la solicitud de ayuda italiana para mejorar su imagen, a la vez que amplificr la grave pérdida de prestigio de la UE.

La ayuda china a Italia en esos mismos días[127] también puede entenderse como un gesto propagandístico espontáneo, en este caso para desviar la atención de la responsabilidad china en la difusión de la pandemia y su problemática gestión.

Como conclusión, es necesario destacar que no son sólo las grandes potencias globales las que han aprovechado la crisis para impulsar sus objetivos políticos. En España, sin ir más lejos, se ha visto cómo el nacionalismo catalán ha continuado su implacable campaña de desprestigio y ataque contra España durante la pandemia. El 19 de marzo de 2020, al inicio de la crisis, el entonces presidente de la Generalitat, Quim Torra, concedió una entrevista a la BBC con el objetivo de criticar la gestión española, deslegitimar la democracia española e internacionalizar el proceso separatista[128].

Numerosos líderes e instituciones separatistas catalanes han hecho uso de las redes sociales durante la pandemia para difundir mentiras e información

110 https://www.independent.co.uk/news/world/americas/us-politics/covid-conspiracy-shows-vast-reach-of-chinese-disinformation-chinese-beijing-ap-pew-research-center-twitter-b1802255.html.

111 de Pedro (2020), p. 4.

112 Ibid., p. 5.

113 Kurlantzick (2020), https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic.

114 https://www.dw.com/en/china-disinformation-campaign-clouds-covid-origins/av-56576257.

115 https://www.dw.com/en/china-disinformation-campaign-clouds-covid-origins/av-56576257.

116 Kurlantzick (2020); https://www.independent.co.uk/news/world/americas/us-politics/covid-conspiracy-shows-vast-reach-of-chinese-disinformation-chinese-beijing-ap-pew-research-center-twitter-b1802255.html

117 https://www.independent.co.uk/news/world/americas/us-politics/covid-conspiracy-shows-vast-reach-of-chinese-disinformation-chinese-beijing-ap-pew-research-center-twitter-b1802255.html.

118 Kurlantzick (2020), https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic.

119 Twigg y Allen (2021), https://www.bbc.com/news/56364952.

120 Cheung y Wilhelm (2021), https://www.worldpoliticsreview.com/trend-lines/29554/china-s-wolf-warrior-diplomacy-is-here-to-stay.

121 Ibid.

122 Ibid.; Gorman (2021), https://www.ft.com/content/7e508af8-0b35-4610-b52d-8c9e3e888a91.

123 Gordon y Volz (2021), https://www.wsj.com/articles/russian-disinformation-campaign-aims-to-undermine-confidence-in-pfizer-other-covid-19-vaccines-u-s-officials-say-11615129200.

124 Ibid.; Griffiths (2021), https://edition.cnn.com/2021/01/26/asia/xi-jinping-china-vaccine-intl-hnk/index.html; Wang (2021), https://www.hrw.org/news/2021/03/04/chinas-dangerous-game-around-covid-19-vaccines.

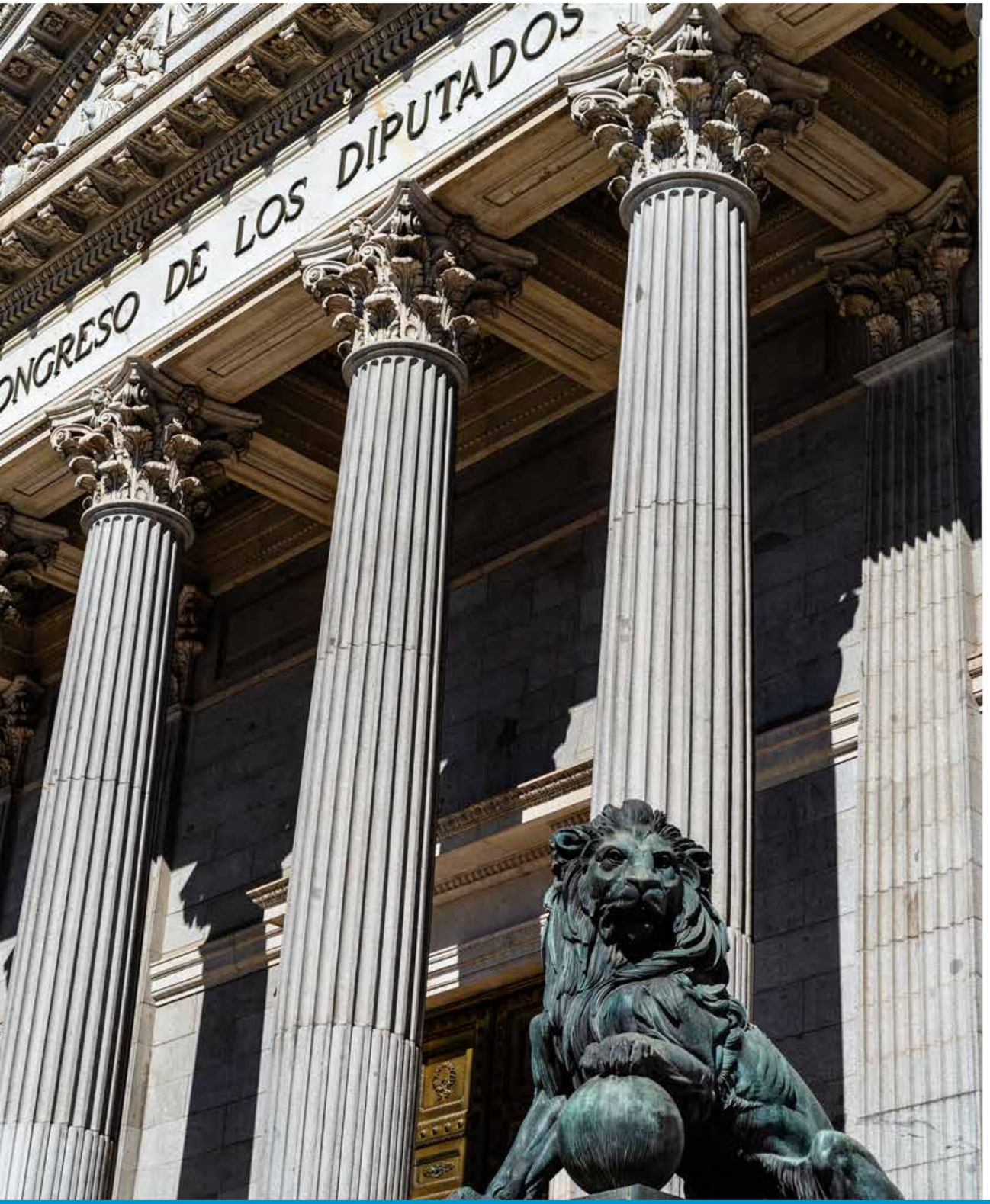
125 Cristiani (2020), https://jamestown.org/program/russian-motives-behind-helping-italys-coronavirus-response-a-multifaceted-approach/.

126 Ibid.

127 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_600.

128 de Pedro (2020), p. 5.

hostil con la excusa del coronavirus con la idea de que el coronavirus "viene y es culpa de Madrid" como eje central[129]. En este sentido, este esfuerzo para crear una narrativa insidiosa de tono conspirativo que cale en la sociedad catalana tiene similitudes con las campañas rusa y china.



4

LOS RETOS DE LA GESTIÓN DE UNA AMENAZA INCONTROLABLE.

Desde que las amenazas híbridas han conseguido una posición de prominencia en los círculos políticos, militares y académicos de Europa y la OTAN, los países europeos y la Unión Europea han adoptado varias medidas dirigidas a defender a Europa frente a las amenazas híbridas y la desinformación, así como a hacer frente a los actores hostiles que emplean estos métodos.

La Unión Europea

Desde 2015, la Unión Europea, a través de sus diferentes instituciones, identifica las amenazas híbridas como una realidad con potencial de perjudicar a Europa. Ese año, tanto el Consejo de Asuntos Exteriores como el Consejo Europeo ordenaron al Alto Representante de la Unión trabajar con la Comisión, la Agencia Europea de Defensa y los Estados miembros para desarrollar un Marco Común para contrarrestar las amenazas híbridas, que se adoptó formalmente a principios de 2016[130].

Este Marco Común identifica a los Estados miembros como los principales actores que deben hacer frente a las amenazas híbridas y vulnerabilidades en cada contexto específico, pero al mismo tiempo indica que hay amenazas comunes en las que la UE puede ser un mejor instrumento así como una plataforma para multiplicar y reforzar los esfuerzos nacionales.

El Marco Común recoge las políticas y estrategias existente en el ámbito de la seguridad, ciberdefensa y seguridad marítima, y propone 22 acciones operacionales dirigidas a aumentar la concienciación, construir resiliencia, prevenir, responder y recuperarse de las crisis y aumentar la cooperación entre la UE y la OTAN.

De forma específica, estas acciones tienen impacto sobre la ciberseguridad, las infraestructuras críticas, el sistema financiero, los programas de lucha contra la radicalización, el intercambio de información entre agencias y administraciones, etcétera. Por ejemplo, creando una célula de análisis de amenazas híbridas dentro del Centro de Inteligencia y de Situación de la Unión Europea (EU INTCEN)[131].

Sin duda alguna, una de las iniciativas estrella de la Unión Europea ha sido la creación en 2015 de la *East Stratcom Task Force*, un equipo del Servicio de Acción Exterior diseñado específicamente para contrarrestar las acciones hostiles rusas. Entre otras cosas, esta *Task Force* diseña campañas de comunicación estratégica para difundir los valores y políticas de la Unión Europea en Armenia, Azerbaiyán, Bielorrusia, Georgia, Moldavia y Ucrania[132].

Sin embargo, el trabajo de este equipo que más visibilidad tiene es el proyecto de *EUvsDisinfo*, que se dedica a monitorear, revelar y contrarrestar casos de desinformación rusa en Europa, así como a divulgar contenidos educativos para que los ciudadanos puedan protegerse frente a campañas de desinformación[133].

130 https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250.

131 https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats/; https://www.dsn.gob.es/sites/dsn/files/hybrid_threats_en_final.pdf.

132 https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.

133 https://euvsdisinfo.eu/es/.

Todos los esfuerzos europeos contra la desinformación se enmarcan actualmente dentro del *Plan de Acción contra la Desinformación*, publicado en 2018, que conceptualiza el problema, identifica las amenazas y establece los objetivos de la acción europea[134].

A finales de 2020, la Comisión Europa publicó el *Plan de Acción para la Democracia Europea*, que adopta un enforque más holístico para defender los procesos electorales y los sistemas democráticos europeos de amenazas híbridas como desinformación y los ciberataques[135].

Otras medidas relevantes adoptadas por la Comisión han sido el *Código de buenas prácticas de la Unión en materia de desinformación*[136], el *European Digital Media Observatory*[137] (una red para verificadores y académicos) y la campaña contra la desinformación en el contexto de la pandemia de Covid-19[138].

La desinformación y las amenazas híbridas han continuado siendo asuntos de máxima relevancia en los últimos años[139], pero han adquirido un nuevo grado de urgencia con la pandemia. Actores como Rusia y China han intensificado sus campañas de desinformación, adaptándolas en los últimos meses al contexto de la pandemia para desprestigiar las medidas europeas, así como para sembrar dudas y miedo sobre las vacunas. La Unión Europea es muy consciente de estas campañas[140] y ha adoptado varias medidas, con el objetivo de reforzr los instrumentos de comunicación estratégica que ya poseía[141] e introducir nuevas plataformas para que los ciudadanos puedan obtener datos y corroborar la información[142].

Por otra parte, en lo que respecta a la cooperación de la UE con otros actores, destaca sobre todo la colaboración con la OTAN para crear en Helsinki el Centro de Excelencia Europeo para Contrarrestar Amenazas Híbridas (HybridCoE)[143]. Esta institución independiente fue creada en 2017 con el objetivo de servir como foro y fábrica de ideas para mejorar las capacidades de los participantes a la hora de prevenir y contrarrestar amenazas híbridas[144]. También sirve como plataforma para que la UE y la OTAN puedan mantener discusiones estratégicas y llevar a cabo entrenamiento y ejercicios. Este esfuerzo UE-OTAN común también se ha podido ver en el aumento de la cooperación en ciberdefensa desde 2016[145] y apunta a la manera en que deberían abordarse este tipo de amenazas: con la interlocución, coordinación y sinergia de instituciones supranacionales capaces de aunar esfuerzos de forma efectiva y eficiente.

La OTAN

Por su parte, la OTAN también tiene desde 2015 una estrategia que determina el papel de la Alianza para contrarrestar amenazas híbridas. El papel principal recae sobre cada Estado miembro, pero la OTAN está comprometida en la defensa de todos los aliados. Para ello, su estrategia se estructura en los ejes de preparación, disuasión y defensa.

El primer eje de preparación involucra, entre otros, a la *Joint Intelligence and Security Division*, que identifica y analiza datos, información e indicaciones sobre amenazas y posee una unidad de análisis híbrido equivalente a la del EU INTCEN. La OTAN también comparte conocimiento experto, apoya a los Aliados a la hora de identificar vulnerabilidades nacionales y mejorar su resiliencia e impulsa ejercicios y entrenamiento para los procesos de toma de decisiones[146].

El segundo eje, la disuasión, se consigue, según la OTAN, demostrando la determinación y voluntad política de la Alianza para actuar conjunta y rápidamente allí donde y cuando sea necesario. Por último, la Alianza está comprometida en la defensa colectiva (a través del Artículo 5) de cualquier Aliado si fracasa la disuasión[147].

Además de este enfoque estratégico, la OTAN se ha adaptado al nuevo entorno, por ejemplo, declarando el ciberespacio como nuevo dominio operativo y mejorando la ciberdefensa de los Aliados. En este sentido, en julio de 2018 los líderes de la OTAN aprobaron la creación de equipos de apoyo especializados en contrarrestar acciones híbridas, que están disponibles para todos los países miembros para su preparación y respuesta. El primero de estos equipos se desplegó en noviembre de 2019 en Montenegro[148].

España

En España, la Estrategia de Seguridad Nacional de 2017 identifica las acciones híbridas como amenaza, aunque no se desarrolla ninguna medida para contrarrestar amenazas específicas[149]. La Directiva de Defensa Nacional de 2020, que sustituye a la de 2012, sí que recoge con más detalle los cambios en el panorama internacional y estratégico, y considera a las estrategias híbridas como una amenaza para España[150].

La Directiva de Defensa Nacional ha tenido impacto en la Directiva de Política de Defensa 2020 y el nuevo Ciclo de Planeamiento de la Defensa. Ambos documentos consideran que las amenazas híbridas destacan en la nueva situación estratégica, por lo que la adquisición de nuevas capacidades y la preparación deben reflejar este hecho[151].

En cuanto a medidas concretas, el Gobierno español adoptó a finales de 2020 el Procedimiento de Actuación Contra la Desinformación, enmarcado dentro del Departamento de Seguridad Nacional[152]. Esta medida persigue implementar en España las recomendaciones de la Unión Europea y dotar a nuestro Sistema de Seguridad Nacional de mecanismos equivalentes a los creados por Bruselas.

El Procedimiento establece la necesidad de establecer una acción coordinada y acorde a los valores democráticos de España, que confronte los riesgos y amenazas para nuestra sociedad, el incremento de nuestras capacidades con el objetivo de hacer frente a la desinformación y de reforzar la resiliencia.

No se trata de responder a las *fake news*, ni adentrarse en el debate político, sino que establece los instrumentos necesarios para participar en los mecanismos que la Unión Europea ha puesto a disposición de los Estados miembros para reforzar las capacidades de respuestas coordinadas y conjuntas a las campañas de desinformación e influencia. También busca la colaboración de la sociedad civil y el sector privado. En este ámbito, en España destaca el trabajo realizado sobre amenazas híbridas y desinformación por *think tanks* como el Real Instituto Elcano, el CIDOB y el Instituto de Seguridad y Cultura[153].

Aunque el Procedimiento de Actuación Contra la Desinformación sólo prevé la posibilidad de realizar campañas de comunicación para contrarrestar las noticias falsas, no de censurarlas, fue criticado en su momento bajo acusaciones de dejar en manos del Gobierno la capacidad de decidir qué es desinformación[154].

134 https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf.

135 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250.

136 https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

137 https://edmo.eu/.

138 https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.

139 https://www.consilium.europa.eu/es/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/; https://www.euronews.com/2021/06/16/eu-must-be-more-robust-and-resilient-against-russian-attempts-to-undermine-it-says-borrell.

140 https://www.consilium.europa.eu/es/policies/coronavirus/fighting-disinformation/.

141 https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_es.

142 https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation_es#identificar-las-teoras-conspiratorias.

143 https://www.hybridcoe.fi/.

144 https://www.hybridcoe.fi/who-what-and-how/.

145 https://www.nato.int/cps/en/natohq/news_127836.htm.

146 https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text=What%20are%20the%20hybrid%20threats,and%20use%20of%20regular%20forces.

147 Ibid.

148 https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

149 https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf.

150 https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2020.pdf.

151 https://www.iniseg.es/blog/seguridad/las-amenazas-hibridas-en-el-nuevo-ciclo-de-planeamiento-de-la-defensa-en-espana/#_ftn1.

152 https://www.dsn.gob.es/es/actualidad/sala-prensa/procedimiento-actuaci%C3%B3n-contra-desinformaci%C3%B3n.

153 http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt20-2018-galan-amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones; https://www.cidob.org/es/articulos/anuario_internacional_cidob/2019/la_desinformacion_de_nueva_generacion. https://www.youtube.com/watch?v=43wbKaYsF7Q

154 https://www.abc.es/espana/abci-sanchez-activa-plan-para-controlar-desde-gobierno-desinformacion-202011051208_noticia.html.

Previsiblemente, estas decisiones están basadas en las definiciones y procedimientos de la Unión Europea, pues la realidad es que esta medida del Gobierno español se produjo a instancias de Bruselas y ha sido avalada por la Comisión Europea[155].

5

A MODO DE CONCLUSIÓN: LA PARADOJA HÍBRIDA.

Numerosos analistas y expertos suelen recalcar que la desinformación, quizás la pata más visible y tangible del conjunto de amenazas que se han dado en denominar híbridas resulta un fenómeno casi paradójico pues para que se dé necesariamente debe ser en un contexto garantista de libertades de información, opinión y prensa.

Para ejemplificarlo basta con acudir al modelo contrario: el de aquellos estados capaces de controlar el flujo informativo entre su población aún en una época de potencial pérdida de control por la multiplicación de canales por los que dicha información transita.

China, sin ir más lejos, es el ejemplo perfecto de cómo un régimen puede asegurarse el control de lo que sus ciudadanos perciben y cómo lo hacen aun tratándose de un modelo de país con un desarrollo tecnológico elevado y donde cada vez más ciudadanos tienen acceso a dichos avances. La sociedad china vive rodeada de avances tecnológicos, pero el hecho de que uno de los principales fabricantes de tecnología del mundo haya decidido crear también una red social propia dirigida a sus ciudadanos da buena cuenta de lo muy en serio que se toma el control de la información el régimen chino.

Weibo es a China lo que Facebook, Twitter y otras redes sociales a Occidente, pero con una diferencia importante. El Estado chino controla las entrañas de Weibo mientras que, como se ha evidenciado en numerosas ocasiones, los estados occidentales tienen muy difícil controlar las redes sociales y las plataformas de mensajería, ajenas a legislaciones y jurisdicciones nacionales. Incluso la Justicia de cada Estado debe solicitar la colaboración de estas plataformas para poder acceder a información tan sensible como la relacionada con actos terrorista, y aun así no siempre se consigue el acceso.

En este contexto, esa dificultad de control sobre las herramientas que permiten los flujos libres de información occidentales se ha convertido en el principal activo para todo aquel agente, estatal o no, que quiera poner en marcha campañas de desinformación contra estados, organizaciones o grupos poblacionales concretos.

La paradoja híbrida hace que la desinformación solo sea efectiva allí donde no se puede apagar internet. China, Rusia, Irán o Turquía, entre otros, son conscientes y, ajenos al problema reputacional que pueda suponer para ellos que internacionalmente se les señale como regímenes autoritarios que coartan la libertad de información, opinión y prensa, hacen y deshacen a su antojo en función de su agenda e intereses garantizando un escudo de protección frente a fenómenos que, como se ha visto, ellos mismos patrocinan y ejecutan sobre Occidente.

En el mismo sentido, estos regímenes tienen una característica más en común que supone una mayor garantía de defensa frente a amenazas híbridas y, específicamente, campañas de desinformación y que a su vez establece una relación inversamente proporcional entre ellos y Occidente: la concentración de poder.

El modelo de democracia occidental, basado no solamente en un sistema de representación parlamentaria, sino sobre todo en un marco constitucional de garantías de derechos y libertades de sus ciudadanos, supone el otro gran factor de debilidad frente a las estrategias híbridas.

La separación de poderes, concepto inseparable del de democracia occidental, permite que acciones dirigidas a desestabilizar un Estado o una organización supranacional como la Unión Europea encuentren mayor facilidad a la hora de inyectarse, y a su vez las instituciones de dicho Estado u organización tengan mayores dificultades a la hora de atajar de forma rápida y efectiva la inoculación de dicho veneno social.

A todo esto debe añadirse un tercer elemento: la ruptura del paradigma informativo tradicional. Aquel que establecía un modelo lineal unidireccional en el que un emisor enviaba un mensaje a un receptor. Dicho sistema establecía un flujo informativo sencillo y, por tanto, más difícil de corromper.

Al emisor (medio de comunicación o entidad pública) se le presupone por el mero hecho de tener el monopolio del control del mensaje un argumento de autoridad. Al mismo tiempo, el rol del receptor es meramente pasivo, pues su capacidad de actuación en dicho sistema se reduce a la mera asimilación del mensaje.

Sin embargo, la multiplicación de canales de comunicación y la evolución del sistema de información de este modelo sencillo y lineal a un modelo de nodos en el que se han perdido los referentes de autoridad informativa han derivado en un universo en el que la capacidad de intoxicar, y por tanto desinformar, se ha convertido en una posibilidad muy real, como ha podido verse en Occidente en los últimos años.

Las amenazas híbridas buscan desestabilizar a un adversario a través de la generación de desconfianza en sus sociedades, de ahí que la desinformación sea la más clara y evidente en este sentido. Aunque el uso de la propaganda no es en absoluto un fenómeno novedoso, el contexto anteriormente descrito sí que ha generado un nuevo paradigma en el que las campañas de desinformación encuentran el ecosistema perfecto para desarrollarse con efectividad.

Como señala Torres Soriano[156], Internet ha dado un nuevo impulso a las operaciones de desinformación debido a cuatro factores:

- Ha disminuido radicalmente el coste en tiempo, dinero y esfuerzo, con lo que ha ampliado la capacidad de poner en marcha este tipo de campañas a un número de actores casi infinito.

- Ha laminado el rol de los medios de comunicación como instrumentos de autentificación de la información, desapareciendo con ello su capacidad de filtrado y convirtiéndoles además en vulnerables a dichas campañas.

- El modelo de economía de la atención de algunas redes sociales alinea sus intereses con los de los manipuladores, pues éstas potencian los mecanismos de gamificación y viralización al tener como primer objetivo el aumentar el nivel de implicación de los usuarios de estas redes.

- El potencial que tiene internet ha generado ya un cambio radical en los modelos de persuasión política, especialmente en relación con el uso de la Inteligencia Artificial, como se está poniendo de manifiesto con las herramientas automatizadas de edición de vídeo o voz capaces de suplantar identidades y que se están viralizando en muchas redes sociales.

En suma, una tormenta perfecta, como señala el propio Torres Soriano, en gran medida incentivada por las características de las sociedades occidentales y los modelos garantistas en los que se sustentan. Ante dicha tormenta perfecta, no debe caerse en la tentación de valorar la posibilidad de reducir o recortar estas garantías del sistema de democracia occidental, pues a la postre supondría el triunfo último de aquellos actores, estatales o no, que están utilizando estrategias híbridas para desestabilizar a Occidente.

156 Torres (2019), p. XI-XVI.

BIBLIOGRAFÍA

- Torres Soriano, Manuel R. "A modo de introducción: la tormenta perfecta". IX-XVII." En *#Desinformación: Poder y manipulación en la era digital*, editado por Manuel R. Torres, 43-56. Granada: Editorial Comares, 2019.
- Alandete, David. "Guerra mundial en internet. Cómo la desinformación agravó la crisis de la independencia catalana." En *#Desinformación: Poder y manipulación en la era digital*, editado por Manuel R. Torres, 43-56. Granada: Editorial Comares, 2019.
- Alandete, David. "La trama rusa empleó redes chavistas para agravar la crisis catalana." *El País*, 11 de noviembre, 2017.
- https://elpais.com/politica/2017/11/10/actualidad/1510341089_316043.html.
- Alandete, David. "Putin alienta la independencia con un enviado a Cataluña." *El País,* 26 de octubre, 2017.
- https://elpais.com/politica/2017/10/25/actualidad/1508958307_955473.html.
- Albalat, Jesús G. "El juez investiga una trama rusa de apoyo a la DUI." *El Periódico de Cataluña*, 13 de noviembre, 2019.
- https://www.elperiodico.com/es/politica/20191113/juez-investiga-trama-rusa-independencia-catalunya-puigdemont-7733376.
- Albalat, Jesús G. "El juez cree que Rusia ofreció a Carles Puigdemont 10.000 soldados y pagar la deuda catalana." *El Periódico de Cataluña*, 28 de octubre, 2020. https://www.elperiodico.com/es/politica/20201028/el-juez-senala-la-vinculacion-de-rusia-con-el-proces-8178454.
- American Constitution Society. "Key Findings of the Mueller Report." Recuperado el 1 de mayo de 2021. https://www.acslaw.org/projects/the-presidential-investigation-education-project/other-resources/key-findings-of-the-mueller-report/.
- Associated Press. "COVID conspiracy shows vast reach of Chinese disinformation." *The Independent*, 15 de febrero, 2021.
- https://www.independent.co.uk/news/world/americas/us-politics/covid-conspiracy-shows-vast-reach-of-chinese-disinformation-chinese-beijing-ap-pew-research-center-twitter-b1802255.html.
- Booth, Robert, Weaver, Matthew, Hern, Alex, Smith, Stacee y Walker, Shaun. "Russia used hundreds of fake accounts to tweet about Brexit, data shows." *The Guardian*, 14 de noviembre, 2017. https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.
- Cheung, Rachel y Wilhelm, Benjamin. "Why China's 'Wolf Warriors' Won't Back Down." *World Politics Review,* 7 de abril, 2021. https://www.worldpoliticsreview.com/trend-lines/29554/china-s-wolf-warrior-diplomacy-is-here-to-stay.
- Committee on Foreign Relations. "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." *U.S. Senate*, 2018. https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.
- Cordesman, Anthony H. "The Strategic Threat from Iranian Hybrid Warfare in the Gulf." *Center for Strategic and International Studies*, 13 de junio, 2019. https://www.csis.org/analysis/strategic-threat-iranian-hybrid-warfare-gulf.
- Cristiani, Dario. "Russian Motives Behind Helping Italy's Coronavirus Response: A Multifaceted Approach." *The Jamestown Foundation*, 8 de abril, 2020. https://jamestown.org/program/russian-motives-behind-helping-italys-coronavirus-response-a-multifaceted-approach/.
- Cullen, Patrick y Reichborn-Kjenneru, Erik. "Understanding Hybrid Warfare." *Multinational Capability Development Campaign Countering Hybrid Warfare Project*, 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.
- De Pedro. "Desinformación rusa contra la Unión Europea." En *#Desinformación: Poder y manipulación en la era digital*, editado por Manuel R. Torres, 29-42. Granada: Editorial Comares, 2019.
- Deutsche Welle. "China disinformation campaign clouds COVID origins." *DW*, 15 de febrero, 2021. https://www.dw.com/en/china-disinformation-campaign-clouds-covid-origins/av-56576257.
- Durán, Gonzaga. "Un ex diputado de CDC es condenado a nueve años y medio de inhabilitación por soborno y prevaricación." *OKDiario*, 6 de noviembre, 2015. https://okdiario.com/espana/un-ex-diputado-de-cdc-es-condenado-a-nueve-anos-y-medio-de-inhabilitacion-por-soborno-y-prevaricacion-18960.
- EC. "La UE detecta un aumento de la injerencia rusa en relación con Cataluña." *El Confidencial*, 11 de octubre, 2017. https://www.elconfidencial.com/espana/cataluna/2017-11-10/independencia-cataluna-injerencia-rusia_1475857/.
- El Liberal. "Puigdemont se deja querer por el Kremlin." *VozPópuli,* 28 de octubre, 2019. https://www.vozpopuli.com/elliberal/Puigdemont-deja-querer-Kremlin_0_1295270953.html.
- European Commission Press Release. "Coronavirus: Chinese aid to the EU delivered to Italy." *European Commission*, 6 de abril, 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_600.
- European External Action Service. "Shared Vision, Common Action: A Stronger Europe." Recuperado el 1 de mayo de 2021.
- https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf
- EUvsDisinfo. "Vilifying Germany; Wooing Germany." Recuperado el 1 de mayo de 2021. https://euvsdisinfo.eu/villifying-germany-wooing-germany/.
- Fiott, Daniel y Parkes, Roderick. "Protecting Europe: the EU's response to hybrid threats." *Chaillot Paper/151* (abril 2019): 1-48.
- https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf
- Foy, Henry. "Valery Gerasimov, the general with a doctrine for Russia." *Financial Times*, 17 de septiembre, 2017. https://www.ft.com/content/7e14a438-989b-11e7-a652-cde3f882dd7b
- Galán, Javier, Abad, José Manuel y Alameda, David. "Los 4.800 bots que jalearon el 'procés'." *El País*, 10 de diciembre, 2017.
- https://elpais.com/politica/2017/12/04/actualidad/1512389091_690459.html.
- García, Jesús y Carranco, Rebeca. "El juez investiga al círculo de Puigdemont por sus contactos con el Kremlin." *El País*, 28 de octubre, 2020. https://elpais.com/espana/catalunya/2020-10-28/el-juez-investiga-al-circulo-de-puigdemont-por-sus-contactos-con-el-kremlin.html.
- Gardner, Hall. "Hybrid Warfare: Iranian and Russian Versions of 'Little Green Men' and Contemporary Conflict." *Research Paper (Research Division, NATO Defense College)*, no. 123 (diciembre 2015): 1-16. https://www.files.ethz.ch/isn/195396/rp_123.pdf.
- Giegerich, Bastian. "Hybrid Warfare and the Changing Character of Conflict." *Connections* 15, no. 2 (primavera 2016): 65-72.
- https://www.jstor.org/stable/10.2307/26326440.
- Gordon, Michael R. y Volz, Dustin. "Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other Covid-19 Vaccines, U.S. Officials Say." *Wall Street Journal*, 7 de marzo, 2021. https://www.wsj.com/articles/russian-disinformation-campaign-aims-to-undermine-confidence-in-pfizer-other-covid-19-vaccines-u-s-officials-say-11615129200.
- Gorman, Lindsay. "Do China's 'wolf warrior' diplomats really have any bite?." *Financial Times*, 14 de abril, 2021. https://www.ft.com/content/7e508af8-0b35-4610-b52d-8c9e3e888a91.
- Griffiths, James. "Xi Jinping touts coronavirus cooperation as China persists with vaccine disinformation push." *CNN*, 26 de enero, 2021. https://edition.cnn.com/2021/01/26/asia/xi-jinping-china-vaccine-intl-hnk/index.html.

- Hern, Alex. "Russian troll factories: researchers damn Twitter's refusal to share data." *The Guardian*, 15 de noviembre, 2017.

- https://www.theguardian.com/world/2017/nov/15/russian-troll-factories-researchers-damn-twitters-refusal-to-share-data.

- Hierro, Jesús. "El juez cree que Rusia ofreció a Puigdemont 10.000 soldados tras el 1-O." *ABC*, 30 de octubre, 2020. https://www.abc.es/espana/catalunya/politica/abci-juez-cree-rusia-ofrecio-puigdemont-10000-soldados-202010281620_noticia.html.

- Hurst, Daniel, Kuo, Lily y Graham-McLay, Charlotte. "Zhenhua Data leak: personal details of millions around world gathered by China tech company." *The Guardian*, 14 de septiembre, 2020. https://www.theguardian.com/world/2020/sep/14/zhenhua-data-full-list-leak-database-personal-details-millions-china-tech-company.

- Intelligence and Security Committee. "Russia." *House of Commons*, 2020. https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.

- Jasper, Scott y Moreland, Scott. "The Islamic State is a Hybrid Threat: Why Does That Matter?" *Small Wars Journal*, 12 de febrero, 2014.

- https://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter.

- Kurlantzick Joshua. "How China Ramped Up Disinformation Efforts During the Pandemic." *Council on Foreign Relations*, 10 de septiembre, 2020. https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic.

- LSE Ideas. "GLOBAL STRATEGIES. Hybrid Warfare in the Middle East." *LSE Ideas*, febrero, 2017. https://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-Hybrid-Warfare-in-the-Middle-East.pdf.

- Mankoff, Jeffrey. "Russian Influence Operations in Germany and Their Effect." *Center for Strategic and International Studies*, 3 de febrero, 2020. https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect.

- Marginedas, Marc. "Moscú afirma que las acusaciones del juez Aguirre «exceden el absurdo." *El Periódico de Cataluña,* 28 de octubre, 2020. https://www.elperiodico.com/es/politica/20201029/moscu-guarda-silencio-sobre-la-supuesta-trama-rusa-8179802.

- Mars, Amanda. "RT y Sputnik fueron los mayores difusores de noticias sobre Cataluña por redes." *El País*, 6 de marzo, 2018. https://elpais.com/internacional/2018/03/05/estados_unidos/1520277454_983401.html.

- Mason, Rowena. "Theresa May accuses Russia of interfering in elections and fake news." *The Guardian*, 14 de noviembre, 2017.

- https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news.

- Miracola, Sergio. "Chinese Hybrid Warfare." *Instituto per gli Studi di Politica Internazionale*, 21 de diciembre, 2018.

- https://www.ispionline.it/it/pubblicazione/chinese-hybrid-warfare-21853.

- Mueller, Robert S. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." *U.S. Department of Justice*, 2019.

- https://www.justice.gov/archives/sco/file/1373816/download.

- Ochoa, Liliana, Calleja, Tono y Requeijo, Alejandro. "«Putin», «financiación» y «bitcoin»: el manuscrito que vincula a Puigdemont con Rusia." *VozPópuli*, 15 de noviembre de 2019. https://www.vozpopuli.com/espana/putin-financiacion-bitcoin-anotaciones-puigdemont_0_1300670215.html.

- Piotrowski, Marcin Andrzej. "Hezbollah: The Model of a Hybrid Threat." *PISM Bulletin*, No. 24 (756), (March 2015): 1-2.

- https://www.files.ethz.ch/isn/188946/Bulletin%20PISM%20no%2024%20(756)%202%20March%202015.pdf.

- Pindják, Peter. "Deterring hybrid warfare: a chance for NATO and the EU to work together?" *NATO Review*, 18 de noviembre, 2014.

- https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html.

- Piñols, Àngels. "La Embajada de Rusia se burla del supuesto envío de 10.000 soldados a Cataluña." *El País*, 29 de octubre, 2020. https://elpais.com/espana/catalunya/2020-10-28/la-embajada-rusa-se-burla-del-supuesto-envio-de-10000-soldados-a-cataluna.html.

- Proby, Andrew y Doran, Matthew. "China's 'hybrid war': Beijing's mass surveillance of Australia and the world for secrets and scandal." *ABC News*, 14 de septiembre, 2020. https://www.abc.net.au/news/2020-09-14/chinese-data-leak-linked-to-military-names-australians/12656668.

- Requeijo, Alejandro y Calleja, Tono. "Tras la pista de Sergei Fedotov, el espía ruso cuyo rastro se extiende hasta Cataluña el 1-O." *VozPópuli*, 22 de noviembre, 2019. https://www.vozpopuli.com/espana/espia-ruso-Sergei-Fedotov-Cataluna_0_1302471121.html.

- Robinson, Olga. "How Putin's Russia turned humour into a weapon." *BBC*, 15 de diciembre, 2018. https://www.bbc.com/news/world-europe-46567364.

- Rumer, Eugene y NG, Nicole. "The West Fears Russia's Hybrid Warfare. They're Missing the Bigger Picture." *Carnegie Endowment for International Peace*, 3 de julio, 2019. https://carnegieendowment.org/2019/07/03/west-fears-russia-s-hybrid-warfare.-they-re-missing-bigger-picture-pub-79412.

- Rusia en España (@EmbajadaRusaES). "Ojo: La información aparecida en los medios españoles sobre la llegada de diez mil soldados rusos a Cataluña está incompleta." Twitter, 28 de octubre, 2020.

- https://twitter.com/EmbajadaRusaES/status/1321529417609420803?s=20.

- Schultz, Teri. "Why the 'fake rape' story against German NATO forces fell flat in Lithuania." *Deutsche Welle*, 23 de febrero, 2017. https://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870.

- The European Centre of Excellence for Countering Hybrid Threats. "Hybrid CoE." https://www.hybridcoe.fi/

- Twigg, Krassi y Allen, Kerry. "The disinformation tactics used by China." *BBC*, 12 de marzo, 2021. https://www.bbc.com/news/56364952.

- Vallés, Vicente. "La injerencia rusa. Putin contra Occidente." En *#Desinformación: Poder y manipulación en la era digital*, editado por Manuel R. Torres, 15-28. Granada: Editorial Comares, 2019.

- VozPópuli. "Un exdiputado ruso reconoce que se reunió en Moscú con un emisario de Puigdemont y que enviaron agentes secretos a Cataluña." *VozPópuli*, 22 de noviembre, 2019. https://www.vozpopuli.com/internacional/Exdiputado-reconoce-Moscu-Puigdemont-Cataluna_0_1302770811.html.

- Wang, Yaqiu. "China's Dangerous Game Around Covid-19 Vaccines." *Human Rights Watch*, 4 de marzo, 2021. https://www.hrw.org/news/2021/03/04/chinas-dangerous-game-around-covid-19-vaccines.

- Weissmann, Mikael. "Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone." En *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, edited by Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm, 61-82. Londres: Bloomsbury, 2021.

- Wintour, Patrick. "Russian bid to influence Brexit vote detailed in new US Senate report." *The Guardian*, 10 de enero, 2018.

- Wither, James K. "Making Sense of Hybrid Warfare." *Connections* 15, no. 2 (primavera 2016): 73-87. https://www.jstor.org/stable/26326441?seq=1#metadata_info_tab_contents

ANEXOS

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO, AL CONSEJO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES[157]

Plan de Acción contra la desinformación

La libertad de expresión es un valor fundamental de la Unión Europea, consagrado en la Carta de los Derechos Fundamentales de la Unión Europea y en las constituciones de los Estados miembros. Nuestras sociedades democráticas abiertas dependen de la capacidad de los ciudadanos para acceder a una información variada y verificable que les permita formarse una opinión sobre diferentes cuestiones políticas. De este modo, los ciudadanos pueden participar con conocimiento de causa en los debates públicos y expresar su voluntad mediante procesos políticos libres y limpios. Estos procesos democráticos se ven cada vez más cuestionados por la propagación deliberada, a gran escala y sistemática de desinformación.

La desinformación se define como "información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público"[158]. El perjuicio público incluye las amenazas a los procesos democráticos, así como a bienes públicos tales como la salud, el medio ambiente o la seguridad de los ciudadanos de la Unión. La desinformación no incluye los errores involuntarios, la sátira y la parodia, ni las noticias y comentarios partidistas claramente identificados. Las acciones incluidas en el presente Plan de Acción solo se dirigen a los contenidos de desinformación que tienen carácter legal con arreglo a la legislación nacional o de la Unión y se entenderán sin perjuicio de la legislación de la Unión o de cualquiera de los Estados miembros que pueda ser aplicable, incluidas las normas sobre contenidos ilícitos[159].

Tras el ataque con sustancias químicas ocurrido en Salisbury y las conclusiones correspondientes del Consejo Europeo[160], la Comisión y la Alta Representante presentaron una Comunicación conjunta sobre el aumento de la resiliencia frente a las amenazas híbridas[161] que ponía de relieve la comunicación estratégica como ámbito prioritario para seguir trabajando. Posteriormente, el Consejo

157 https://data.consilium.europa.eu/doc/document/ST-15431-2018-INIT/es/pdf

158 Comunicación sobre la lucha contra la desinformación en línea, COM(2018) 236.

159 La Comisión propuso medidas específicas para abordar la propagación de contenidos ilícitos en línea, incluida la Recomendación sobre medidas para combatir eficazmente los contenidos ilícitos en línea [C(2018) 1177]. Véase también la propuesta de Reglamento sobre la prevención de la difusión de contenidos terroristas en línea [COM(2018) 640] así como la revisión de la Directiva de servicios de comunicación audiovisual acordada el 6 de noviembre de 2018.

160 Conclusiones del Consejo Europeo de 22 de marzo de 2018.

161 JOIN(2018) 16.

Europeo invitó "a la Alta Representante y a la Comisión a que, a más tardar en diciembre de 2018, en cooperación con los Estados miembros y en consonancia con las Conclusiones del Consejo Europeo de marzo de 2015, presenten un plan de acción con propuestas concretas para ofrecer una respuesta coordinada de la UE al desafío de la desinformación, en el que se prevean los mandatos oportunos y recursos suficientes para los equipos del Servicio Europeo de Acción Exterior encargados de las comunicaciones estratégicas"[162].

El presente Plan de Acción responde al llamamiento del Consejo Europeo en favor de medidas para "proteger los sistemas democráticos de la Unión y combatir la desinformación, también en el contexto de las próximas elecciones europeas"[163]. Se basa en las iniciativas existentes de la Comisión y en los trabajos del Grupo de Trabajo sobre Comunicación Estratégica del Este del Servicio Europeo de Acción Exterior (SEAE); establece las medidas que deben adoptar la Comisión y la Alta Representante, con la asistencia del SEAE, en cooperación con los Estados miembros y el Parlamento Europeo e incluye las aportaciones de los Estados miembros, en particular a través de los debates en el Consejo[164], los Comités de Representantes Permanentes I y II, en el Comité Político y de Seguridad, los grupos de trabajo pertinentes del Consejo y las reuniones de los directores de comunicación estratégica y los directores políticos de los Ministerios de Asuntos Exteriores. También tiene en cuenta la cooperación con socios clave de la Unión, incluida la Organización del Tratado del Atlántico Norte (OTAN) y el G7[165].

La Comunicación sobre la lucha contra la desinformación en línea ("Comunicación de abril") puso de relieve el papel clave desempeñado por la sociedad civil y el sector privado (en particular, las plataformas de redes sociales) para abordar el problema de la desinformación. Con posterioridad, en septiembre de 2018, las plataformas en línea y el sector de la publicidad acordaron un código de buenas prácticas destinado a aumentar la transparencia en línea y proteger a los ciudadanos, especialmente con vistas a las elecciones al Parlamento Europeo de 2019, pero también con una perspectiva a más largo plazo. Ahora es esencial que estos agentes cumplan los objetivos fijados por la Comisión en abril y que se atengan estrictamente al Código de buenas prácticas[166]. Además, se está desarrollando una red independiente de verificadores de datos para aumentar la capacidad de detectar y exponer la desinformación, y se realizan esfuerzos sostenidos a nivel nacional y de la Unión para apoyar la alfabetización mediática.

El presente Plan de Acción va acompañado de un informe sobre la Comunicación de abril[167] que expone los avances realizados en las distintas acciones, especialmente en lo que se refiere al Código de buenas prácticas; al fomento de un ecosistema en línea seguro, fiable y responsable; a las actividades relacionadas con la sensibilización y la alfabetización mediática; así como al apoyo a unos medios de comunicación independientes y al periodismo de calidad.

En 2015 el Consejo Europeo reconoció por primera vez la amenaza de las campañas de desinformación en línea, al pedir a la Alta Representante que abordara las campañas de desinformación de Rusia. El Grupo de Trabajo sobre Comunicación Estratégica del Este se creó para abordar esta cuestión y sensibilizar al respecto. Además, la Comunicación conjunta sobre la lucha contra las amenazas híbridas[168] creó la Célula de fusión de la UE contra las amenazas híbridas, en el seno del SEAE, para

162 Conclusiones del Consejo Europeo de 28 de junio de 2018.

163 Conclusiones del Consejo Europeo de 18 de octubre de 2018.

164 Véase el debate político sobre «La lucha contra la propagación de la desinformación en línea: retos para el ecosistema de los medios de comunicación» y las Conclusiones del Consejo de 27 de noviembre de 2018.

165 En el compromiso de Charlevoix sobre la defensa de la democracia frente a las amenazas extranjeras, los líderes del G7 se comprometieron a tomar medidas concertadas para responder a los agentes extranjeros que tratan de socavar nuestras sociedades e instituciones democráticas, nuestros procesos electorales, nuestra soberanía y nuestra seguridad.

166 Véanse también las conclusiones del Consejo de 27 de noviembre de 2018.

167 COM(2018) 794.

168 Aunque las definiciones de «amenaza híbrida» varían y deben ser flexibles para responder a su naturaleza cambiante, el concepto abarca el conjunto de actividades intimidatorias y subversivas, métodos convencionales y no convencionales (es decir, diplomáticos, militares, económicos y tecnológicos) que pueden ser utilizados de manera coordinada por agentes estatales o no estatales para alcanzar objetivos específicos, pero que no alcanzan el umbral de una guerra declarada oficialmente. Suelen aprovecharse las vulnerabilidades del objetivo y se genera ambigüedad para obstaculizar los procesos decisorios. Las campañas de desinformación a gran escala a través de las redes sociales para controlar el discurso político o para radicalizar, reclutar y manipular a individuos que actúan como agentes interpuestos, pueden constituir vectores de estas amenazas híbridas. Véase JOIN (2016) 18.

que actuara como centro único de análisis de las amenazas híbridas. También dio lugar a la creación del Centro de excelencia para la lucha contra las amenazas híbridas, que comparte las mejores prácticas y apoya las actividades de la Unión y de la OTAN en este ámbito.

Con vistas a las elecciones al Parlamento Europeo de 2019 y a más de 50 elecciones presidenciales, nacionales, locales o regionales que se celebrarán en los Estados miembros de aquí a 2020, es urgente intensificar los esfuerzos para garantizar unos procesos democráticos libres y limpios. Las amenazas que afectan a la democracia en cualquier Estado miembro pueden perjudicar a la Unión en su conjunto. Además, la desinformación a menudo tiene como objetivo a las instituciones europeas y a sus representantes, y busca socavar el propio proyecto europeo en general. El 12 de septiembre de 2018, la Comisión adoptó medidas[169] para garantizar unas elecciones europeas libres y justas y recomendó aplicar sanciones, si es necesario, incluido en el caso de utilización ilegal de datos personales para influir en el resultado de las elecciones[170]. Además, es urgente que los Estados miembros adopten las medidas necesarias para preservar la integridad de sus sistemas e infraestructuras electorales y que las sometan a prueba antes de las elecciones europeas.

Las campañas de desinformación, en particular por parte de terceros países, suelen formar parte de la guerra híbrida[171], lo que implica ataques informáticos y el pirateo de redes[172]. Las pruebas demuestran que agentes de Estados extranjeros despliegan cada vez más estrategias de desinformación para influir en los debates sociales, crear divisiones e interferir en la toma de decisiones democráticas. Estas estrategias se dirigen no solo a los Estados miembros, sino también a los países socios de la vecindad oriental, así como a los países vecinos meridionales, a los de Oriente Medio y África.

En el contexto de varias elecciones y referendos en la UE[173] se ha detectado desinformación producida o difundida por fuentes rusas. Las campañas de desinformación relacionadas con la guerra en Siria[174], el derribo del vuelo MH-17 en el este de Ucrania[175] y el uso de armas químicas en el ataque de Salisbury[176] están bien documentadas.

COMPRENDER LAS AMENAZAS QUE REPRESENTA LA DESINFORMACIÓN Y REFORZAR LA RESPUESTA EUROPEA

La desinformación es una amenaza cambiante que requiere esfuerzos continuos con respecto a los actores pertinentes, los vectores, las herramientas, los métodos, los objetivos prioritarios y el impacto. Algunas formas, especialmente la desinformación impulsada por el Estado, son analizadas por la Célula de fusión de la UE contra las amenazas híbridas, en cooperación con los Grupos operativos de comunicación estratégica del SEAE y con el apoyo de los servicios de los Estados miembros.

Los agentes que están detrás de la desinformación pueden ser internos, pues actúan desde dentro de los Estados miembros, o externos, incluidos

169 Para un panorama completo de las medidas, véase la Comunicación sobre la garantía de unas elecciones europeas libres y justas, COM(2018) 637 final.

170 Estas sanciones se añaden a las previstas en el Reglamento general de protección de datos [Reglamento (CE) n.º 2016/679].

171 Comunicación conjunta sobre la lucha contra las amenazas híbridas: una respuesta de la Unión Europea, JOIN(2016) 18 final.

172 Estos ataques informáticos pueden incluir intrusiones específicas para hacerse con información sensible para luego filtrarla o con fines similares, el pirateo de cuentas de redes sociales, el control de cuentas en redes sociales mediante ordenadores zombies y la alteración de los sistemas informáticos de, por ejemplo, empresas de radiodifusión o comités electorales.

173 Véase, por ejemplo, el informe del Centro de Análisis, Previsión y Estrategia y del Instituto de Investigación Estratégica de la Escuela Militar de Francia: https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

174 Declaración conjunta de 17 países miembros de la Organización para la Prohibición de las Armas Químicas (OPAQ) sobre los ataques químicos en Duma, Siria: https://www.diplomatie.gouv.fr/en/french-foreign-policy/manipulation-of-information/article/syria-chemical- attacks-in-douma-7-april-joint-statement-by-france-and-16-other.

175 Con respecto a la campaña de desinformación sobre el vuelo MH-17, véase Grupo de trabajo sobre comunicación estratégica del este: https://euvsdisinfo.eu/mh17-time-is-running-out-for-disinformation/ y https://euvsdisinfo.eu/flight-mh-17-three-years-on-getting-the-truth-out-of-eastern-ukraine/, así como la declaración del equipo conjunto de investigación: https://www.om.nl/onderwerpen/mh17-crash/@104053/reaction-jit-to/.

176 https://euvsdisinfo.eu/timeline-how-russia-built-two-major-disinformation-campaigns/. Sobre la manipulación informática rusa dirigida a la OPAQ en La Haya, véase: https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw.

agentes estatales (o patrocinados por Gobiernos) y no estatales. Según determinados informes[177], más de 30 países utilizan desinformación e influyen en actividades de diferentes formas, incluso en sus propios países. El uso de la desinformación por parte de agentes dentro de los Estados miembros es una fuente creciente de preocupación en toda la Unión. También se han notificado casos de desinformación por parte de agentes no estatales en la Unión, por ejemplo en relación con la vacunación[178]. Por lo que se refiere a los agentes externos, las pruebas son sólidas en el caso de Rusia. Sin embargo, otros terceros países también aplican estrategias de desinformación, pues han aprendido rápidamente de los métodos de Rusia.

Según la célula de fusión de la UE contra las amenazas híbridas, la desinformación por parte de Rusia[179] supone la mayor amenaza para la UE pues es sistemática, cuenta con recursos suficientes y tiene una escala diferente a la de otros países. En términos de coordinación, nivel de los objetivos e implicaciones estratégicas, la desinformación procedente de Rusia forma parte de una amenaza híbrida más amplia que utiliza una serie de herramientas, instrumentos y agentes no estatales.

Es probable que las constantes campañas específicas de desinformación contra la Unión, sus instituciones y sus políticas aumenten hasta las elecciones al Parlamento Europeo de 2019. **Esto requiere una actuación urgente e inmediata para proteger a la Unión, a sus instituciones y a sus ciudadanos contra la desinformación.**

Las redes sociales se han convertido en medios importantes para la difusión de desinformación e incluso en algunos casos, como el de Cambridge Analytica, para hacer llegar contenidos de desinformación a usuarios específicos, identificados por el acceso y el uso no autorizados de datos personales, con el objetivo último de influir en los resultados electorales. Datos recientes muestran que los servicios de mensajería privada se utilizan cada vez más para propagar desinformación[180]. Entre las técnicas utilizadas se incluyen la manipulación de vídeos ("falsificaciones profundas") y la falsificación de documentos oficiales; el uso de programas informáticos automatizados en internet (ordenadores zombis) para difundir y amplificar contenidos polémicos y debates en las redes sociales; los ataques de troles contra perfiles de redes sociales; y el robo de información. Al mismo tiempo, métodos más tradicionales como la televisión, los periódicos, los sitios web y los correos electrónicos en cadena siguen desempeñando un papel importante en muchas regiones. Las herramientas y técnicas utilizadas cambian rápidamente por lo que **la respuesta debe evolucionar con la misma rapidez.**

Además de actuar dentro de los Estados miembros y a escala de la Unión, la Unión tiene un gran interés en colaborar con sus socios en tres regiones prioritarias: la vecindad oriental y meridional de la Unión y los Balcanes occidentales. Exponer la desinformación que afecta a los países vecinos de la Unión es complementario a la lucha contra el problema dentro de la Unión.

El SEAE ha creado grupos operativos de comunicación estratégica específicos, compuestos por expertos con competencias lingüísticas y conocimientos pertinentes, para abordar la cuestión y elaborar estrategias de respuesta. Están colaborando estrechamente con los servicios de la Comisión para lograr un enfoque de comunicación coordinado y coherente en las diferentes regiones.

Basándose en el Plan de acción sobre comunicación estratégica, adoptado el 22 de junio de 2015, el mandato del Grupo de Trabajo sobre Comunicación Estratégica del Este comprende tres líneas de acción: i) comunicación eficaz y promoción de las políticas de la Unión para con los países vecinos del este; ii) refuerzo del entorno mediático general en los países vecinos del este y en los Estados miembros, incluido apoyo a la libertad de los medios de comunicación y fortalecimiento de los medios de comunicación independientes; iii) mejora de la capacidad de la Unión para prever, abordar y responder a las actividades de desinformación de Rusia. En respuesta a las Conclusiones del Consejo de diciembre de 2015 y junio de 2017, el SEAE creó dos grupos de trabajo adicionales, uno para los Balcanes occidentales[181] y otro para los países de Oriente Próximo, el norte de África y la región del Golfo[182].

Desde su creación, el Grupo de Trabajo sobre Comunicación Estratégica del Este ha difundido eficazmente información sobre las políticas de la Unión en la vecindad oriental, principalmente a través de campañas. Además, ha catalogado, analizado y puesto en el punto de mira más de 4 500 ejemplos de desinformación por parte de Rusia, descubriendo numerosos casos, incrementado la sensibilización y exponiendo las herramientas, técnicas e intenciones de las campañas de desinformación. El Grupo se centra en los países de la Asociación Oriental y en los medios de comunicación nacionales e internacionales rusos, y su enfoque consiste en exponer, sobre la base de las pruebas recogidas, las tendencias, discursos, métodos y canales utilizados, y en sensibilizar al público al respecto.

Por consiguiente, debe mantenerse el mandato del Grupo de Trabajo sobre Comunicación Estratégica del Este y revisar el mandato de los otros dos grupos de trabajo sobre comunicación estratégica (Balcanes occidentales y países meridionales) a la luz de la creciente escala e importancia de las actividades de desinformación en esas regiones y de la necesidad de concienciar sobre los efectos adversos de la desinformación.

ACCIONES PARA UNA RESPUESTA COORDINADA DE LA UNIÓN A LA DESINFORMACIÓN

La lucha contra la desinformación requiere determinación política y una acción unificada que movilice a todas las ramas de las Administraciones públicas (incluidos quienes se encargan de la lucha contra las amenazas híbridas, la seguridad informática, la inteligencia y la comunicación estratégica, la protección de datos, el sistema electoral, las autoridades policiales y judiciales y las autoridades que rigen los medios de comunicación). Esto debe hacerse en estrecha cooperación con socios afines en todo el mundo así como entre las instituciones de la Unión, los Estados miembros, la sociedad civil y el sector privado, especialmente las plataformas en línea.

La respuesta coordinada a la desinformación presentada en el presente Plan de Acción se basa en cuatro pilares:

1. Mejora de la capacidad de las instituciones de la Unión para detectar, analizar y exponer la desinformación.

2. Refuerzo de las respuestas coordinadas y conjuntas a la desinformación.

3. Movilización del sector privado para combatir la desinformación.

4. Aumento de la sensibilización y la capacidad de respuesta de la sociedad.

PILAR 1: MEJORA DE LA CAPACIDAD DE LAS INSTITUCIONES DE LA UNIÓN PARA DETECTAR, ANALIZAR Y EXPONER LA DESINFORMACIÓN

Para abordar eficazmente la amenaza que supone la desinformación es necesario reforzar los grupos de trabajo sobre comunicación estratégica del SEAE, las Delegaciones de la Unión y la Célula de fusión de la UE contra las amenazas híbridas, asignándoles personal adicional especializado, como expertos en minería de datos y en análisis para tratar los datos pertinentes. También es importante contratar servicios adicionales de seguimiento de los medios de comunicación para abarcar una gama más amplia de fuentes e idiomas, así como investigaciones y estudios adicionales sobre el alcance y el impacto de la desinformación. Además, es necesario invertir en instrumentos analíticos como, por ejemplo, programas informáticos específicos para explotar, organizar y compilar grandes cantidades de datos digitales.

El refuerzo de los equipos de comunicación estratégica del SEAE se hará en dos etapas.

177 Véase https://freedomhouse.org/report/freedom-net/freedom-net-2017.

178 Véanse COM(2018) 245 y COM(2018) 244.

179 La doctrina militar rusa reconoce explícitamente la guerra de la información como uno de sus ámbitos: https://www.rusemb.org.uk/press/2029.

180 Según la Universidad de Oxford, este año las plataformas de mensajería directa han albergado campañas de desinformación en al menos 10 países.

181 Conclusiones del Consejo sobre la ampliación y el proceso de estabilización y asociación, de 15 de diciembre de 2015.

182 Conclusiones del Consejo sobre la lucha contra el terrorismo, de 19 de junio de 2017.

A corto plazo, se espera que el presupuesto para comunicación estratégica se duplique ampliamente[183] en 2019, lo que irá acompañado de un refuerzo de al menos 11 puestos antes de las elecciones europeas. A medio plazo[184], se solicitarán puestos adicionales de funcionarios permanentes para los equipos estratégicos de comunicación y para la Célula de fusión de la UE contra las amenazas híbridas, destinados en la sede, así como nuevos puestos en las Delegaciones en los países vecinos, para totalizar unos 50 a 55 nuevos miembros de plantilla durante los próximos dos años.

Se obtendrán nuevas sinergias entre los servicios de la Comisión y el SEAE, por ejemplo mediante el uso compartido de herramientas o el diseño de las campañas de comunicación.

Los análisis de amenazas y la evaluación de la información confidencial constituyen la base del trabajo en materia de desinformación. La experiencia del Centro de Inteligencia y de Situación de la Unión Europea debe aprovecharse plenamente para analizar el carácter evolutivo de las campañas de desinformación.

Los grupos de trabajo sobre comunicación estratégica colaborarán estrechamente con las Delegaciones de la Unión y la Comisión para luchar contra la desinformación, en particular con la red interna contra la desinformación, creada en el seno de la Comisión a raíz de la Comunicación de abril[185].

Los Estados miembros deben complementar y respaldar las acciones de las instituciones de la Unión incrementando sus capacidades nacionales y apoyando los aumentos de recursos necesarios para las instituciones de la Unión.

Acción 1: Con vistas a las elecciones al Parlamento Europeo de 2019 en particular, pero también con una perspectiva a más largo plazo, la Alta Representante, en cooperación con los Estados miembros, reforzará los grupos de trabajo sobre comunicación estratégica y las Delegaciones de la Unión a través de personal adicional y de los nuevos instrumentos necesarios para detectar, analizar y exponer las actividades de desinformación. Los Estados miembros tendrán, en su caso, que mejorar también su capacidad nacional en este ámbito y apoyar el necesario aumento de recursos para los grupos de trabajo sobre comunicación estratégica y las Delegaciones de la Unión.

Acción 2: La Alta Representante examinará los mandatos de los grupos de trabajo sobre comunicación estratégica para los Balcanes occidentales y los países del sur con objeto de permitirles abordar eficazmente la desinformación en estas regiones.

PILAR 2: REFUERZO DE LAS RESPUESTAS COORDINADAS Y CONJUNTAS A LA DESINFORMACIÓN

Las primeras horas tras la divulgación de la desinformación son fundamentales para detectarla, analizarla y contrarrestarla. Por consiguiente, **se creará un sistema de alerta rápida para alertar instantáneamente sobre campañas de desinformación** a través de una infraestructura tecnológica específica. Esto facilitará la puesta en común de datos y la evaluación, a fin de permitir un conocimiento común de la situación, una atribución y una respuesta coordinada y rápida, y de garantizar la eficiencia en el uso de los recursos.

Con vistas a la creación del sistema de alerta rápida, **cada Estado miembro deberá designar, de acuerdo con su estructura institucional, un punto de contacto, idealmente perteneciente a los servicios encargados de las comunicaciones estratégicas**. Este punto de contacto compartirá las alertas y garantizará la coordinación con todas las demás autoridades nacionales pertinentes, así como con la Comisión y el SEAE, sin perjuicio de las competencias existentes de las autoridades nacionales en virtud de la legislación de la Unión o nacional o de otras partes del presente Plan de Acción. En los casos en que la desinformación se refiera a las elecciones o al funcionamiento de las instituciones democráticas en los Estados miembros, los puntos de contacto nacionales deberán cooperar estrechamente con las redes electorales nacionales[186]. En este caso, el resultado del trabajo del sistema de alerta rápida deberá compartirse con la Red europea de cooperación electoral[187], en particular para el intercambio de información sobre las amenazas pertinentes para las elecciones y para apoyar la posible aplicación de sanciones. Las plataformas en línea deben cooperar con los puntos de contacto en los que se basa el sistema de alerta rápida, en particular durante los períodos electorales, para facilitar información pertinente y oportuna.

El sistema de alerta rápida debe estar estrechamente vinculado a la actual capacidad de respuesta permanente, como la que representa el Centro Europeo de Coordinación de la Respuesta a Emergencias[188] y la Sala de Guardia del Servicio Europeo de Acción Exterior (*situation room*)[189]. La Célula de fusión de la UE contra las amenazas híbridas del Centro de Inteligencia y de Situación de la Unión Europea, así como los grupos de trabajo pertinentes del Consejo, también podrían utilizarse como canales para el intercambio de información. La Comisión y la Alta Representante velarán por el intercambio periódico de información y mejores prácticas con socios clave, incluidos el G7 y la OTAN.

Una rápida reacción mediante una comunicación basada en hechos y eficaz es esencial para contrarrestar y prevenir la desinformación, incluidos los casos de desinformación sobre asuntos y políticas de la Unión. Esto es importante para fomentar un debate abierto y democrático sin manipulación, incluso en el contexto de las próximas elecciones europeas. Las instituciones de la Unión[190] y los Estados miembros deben mejorar su capacidad de reaccionar y comunicar eficazmente. La Comisión ya ha aumentado su financiación para mejorar las actividades de comunicación, aplicadas a través de sus programas de comunicación regionales, incluidos en los países vecinos y en las Delegaciones de la Unión. Todas las instituciones de la Unión se ocupan activamente de la comunicación sobre la acción y las políticas europeas en la Unión; en particular las Representaciones de la Comisión y las Oficinas de Enlace del Parlamento Europeo en los Estados miembros desempeñan un papel clave para difundir mensajes adaptados a nivel local, incluidos instrumentos específicos para hacer frente a los mitos y difundir hechos[191].

Debe reforzarse la cooperación entre los Estados miembros y las instituciones de la Unión, especialmente en lo que se refiere al intercambio de información, el aprendizaje común, la sensibilización, el envío activo de mensajes y la investigación. Es necesario un mayor intercambio de información entre los Estados miembros y las instituciones de la Unión para mejorar el conocimiento de la situación y sus respectivas capacidades de respuesta. La comunicación activa y objetiva sobre los valores y las políticas de la Unión es especialmente eficaz cuando la realizan directamente los Estados miembros. Con este fin, la Comisión y la Alta Representante piden a los Estados miembros que intensifiquen sus esfuerzos de comunicación y que defiendan a la Unión y a sus instituciones contra las campañas de desinformación.

Acción 3: En marzo de 2019, la Comisión y la Alta Representante, en cooperación con los Estados miembros, crearán un sistema de alerta rápida para abordar las campañas de desinformación, en estrecha colaboración con las redes existentes, el Parlamento Europeo, así como la OTAN y el Mecanismo de Respuesta Rápida del G7.

Acción 4: Con vistas a las próximas elecciones europeas, la Comisión, en cooperación con el Parlamento Europeo, intensificará sus esfuerzos de

183 Los actuales debates sobre el presupuesto de 2019 prevén un aumento desde 1,9 millones EUR en 2018 a 5 millones en 2019.

184 Mediante enmiendas al presupuesto de 2019 o en el proyecto de presupuesto de 2020.

185 Esta red incluye a representantes de las Direcciones Generales de la Comisión y de sus Representaciones. La Comisión también ha creado recientemente un grupo de trabajo con el SEAE y el Parlamento Europeo sobre la lucha contra la desinformación con vistas a las elecciones europeas.

186 Véase la Recomendación C(2018) 5949 sobre las redes de cooperación electoral, la transparencia en línea, la protección contra los incidentes de seguridad informática y la lucha contra las campañas de desinformación en el contexto de las elecciones al Parlamento Europeo. Estas redes reunirán a las autoridades electorales nacionales, a los reguladores de los medios audiovisuales, a las autoridades de seguridad informática y a las autoridades de protección de datos, así como a los grupos de expertos pertinentes, por ejemplo, sobre alfabetización mediática. Todos ellos constituyen, junto con las instituciones de la Unión, la Red europea de cooperación electoral, que se convocará por primera vez en enero de 2019.

187 Creada de conformidad con la Recomendación de 12 de septiembre de 2018.

188 El Centro Europeo de Coordinación de la Respuesta a Emergencias fue creado en virtud del artículo 7 de la Decisión 1313/2013/UE relativa a un Mecanismo de Protección Civil de la Unión.

189 La Sala de Guardia del Servicio Europeo de Acción Exterior es un órgano permanente del SEAE, que realiza un seguimiento a escala mundial y analiza la situación en cada momento. Forma parte del Centro de Inteligencia y de Situación de la Unión Europea y actúa como centro de información de todas las partes interesadas de las instituciones europeas.

190 En la Comisión, los miembros del Colegio de Comisarios, el Servicio del Portavoz y las Representaciones de la Comisión mantendrían su papel clave de intervención para replicar en caso de que existan errores en las noticias difundidas por los medios de comunicación.

191 Varias Representaciones de la Comisión han desarrollado herramientas adaptadas a nivel local para contrarrestar la desinformación, tales como Les Décodeurs de l'Europe en Francia, UE Vero Falso en Italia, Euromyty.sk en Eslovaquia, el concurso de dibujos animados para combatir los mitos en torno a la UE en Austria, y una serie de dibujos animados en Rumanía.

comunicación sobre los valores y las políticas de la Unión. Los Estados miembros deben reforzar significativamente sus propios esfuerzos de comunicación sobre los valores y las políticas de la Unión.

Acción 5: La Comisión y la Alta Representante, en cooperación con los Estados miembros, reforzarán las comunicaciones estratégicas en los países vecinos de la Unión.

PILAR 3: MOVILIZACIÓN DEL SECTOR PRIVADO PARA COMBATIR LA DESINFORMACIÓN

Las plataformas en línea, los anunciantes y el sector de la publicidad tienen un papel crucial que desempeñar en la lucha contra el problema de la desinformación, ya que su escala está directamente relacionada con la capacidad de las plataformas para amplificar y difundir mensajes de desinformación de agentes malintencionados, dirigidos o no a objetivos concretos. Habida cuenta de sus anteriores fracasos a la hora de actuar adecuadamente para afrontar este problema, la Comisión les instó en abril de 2018 a que intensificaran sus esfuerzos. En este contexto, el Código de buenas prácticas sobre desinformación se publicó el 26 de septiembre de 2018[192]. Las principales plataformas en línea que firmaron el Código se comprometieron a adoptar medidas concretas antes de las elecciones al Parlamento Europeo de 2019.

La Comisión hace un llamamiento a todos los firmantes del Código de buenas prácticas para aplicar las acciones y los procedimientos identificados en el Código de manera rápida y eficaz a escala de la UE, centrándose en las acciones que son urgentes y pertinentes para garantizar la integridad de las elecciones europeas de 2019. En particular y con carácter inmediato, las grandes plataformas en línea deben: i) garantizar el control de la colocación y la transparencia de la publicidad política, sobre la base de controles eficaces y ágiles de la identidad de quienes la contratan; ii) cerrar cuentas falsas activas en sus servicios; iii) detectar los ordenadores zombis automatizados y etiquetarlos en consecuencia. Las plataformas también deben cooperar con los reguladores audiovisuales nacionales, los verificadores de datos y con investigadores independientes para detectar y señalar las campañas de desinformación, en particular durante los períodos electorales, y velar por que los contenidos verificados sean más visibles y obtengan una mayor difusión.

La Comisión, con la ayuda del Grupo de entidades reguladoras europeas de los servicios de comunicación audiovisual (ERGA, por sus siglas en inglés)[193], supervisará la aplicación de los compromisos por parte de los firmantes del Código de buenas prácticas e informará periódicamente sobre si las plataformas cumplen estos compromisos y en qué medida. Para permitir un seguimiento eficaz y exhaustivo, las plataformas deben facilitar a la Comisión, antes de que finalice el presente año, información actualizada y completa sobre las medidas que hayan adoptado para cumplir estos compromisos. La Comisión publicará esta información en enero de 2019. A partir de ese momento y periódicamente las plataformas también deberán facilitar información completa, en particular respondiendo a peticiones específicas de la Comisión, sobre cómo aplican los compromisos, a fin de permitir un seguimiento específico del cumplimiento del Código antes de las elecciones al Parlamento Europeo. Esta información también se publicará.

Además, el Código de buenas prácticas prevé que los firmantes presenten un informe exhaustivo al cabo de 12 meses que incluirá datos e información completos que permitan a la Comisión realizar una evaluación en profundidad. Sobre esta base, **la Comisión, asistida por expertos independientes y con la ayuda del ERGA, evaluará la eficacia del Código de buenas prácticas**. La Comisión también podrá solicitar la asistencia del Observatorio Audiovisual Europeo.

192 https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation. El 16 de octubre, los firmantes iniciales del Código facilitaron sus suscripciones formales al Código, señalaron los compromisos que cada signatario respetará y presentaron un cuadro en el que se enumeran las mejores prácticas pertinentes de la empresa, así como los hitos para la aplicación general del Código en la UE. Los primeros firmantes incluyen las principales plataformas en línea (Facebook, Google, Youtube, Twitter), los proveedores de programas informáticos (Mozilla), los anunciantes, así como una serie de asociaciones comerciales que representan a las plataformas en línea y a la industria de la publicidad. El Código de buenas prácticas debería crear un ecosistema en línea más transparente, fiable y responsable, y proteger a los usuarios contra la desinformación.

193 El Grupo de entidades reguladoras europeas de servicios de comunicación audiovisual comprende todos los reguladores pertinentes de todos los Estados miembros. Proporciona asesoramiento técnico a la Comisión en una serie de ámbitos relacionados con la aplicación de la Directiva, facilita la cooperación entre las autoridades u organismos reguladores nacionales y entre las autoridades u organismos reguladores nacionales y la Comisión. La revisión de la Directiva de servicios de comunicación audiovisual reforzó aún más el papel de este Grupo, en particular en relación con las plataformas de distribución de vídeos.

La Comisión considera que la eficacia del Código depende de la participación más amplia posible de las plataformas en línea y del sector de la publicidad en línea. Por ello, pide a las demás partes interesadas pertinentes que se adhieran al Código.

Acción 6: La Comisión garantizará un seguimiento estrecho y continuo de la aplicación del Código de buenas prácticas. Cuando sea necesario, y en particular con vistas a las elecciones europeas, impulsará su aplicación rápida y efectiva, procediendo a una evaluación exhaustiva al concluir el período inicial de aplicación del Código, que abarcará 12 meses. En caso de que la aplicación y el impacto del Código resulten insatisfactorios, la Comisión podrá proponer nuevas acciones, incluidas medidas de carácter reglamentario.

PILAR 4: AUMENTO DE LA SENSIBILIZACIÓN Y LA CAPACIDAD DE RESPUESTA DE LA SOCIEDAD

Una mayor sensibilización de la opinión pública es esencial para mejorar la capacidad de respuesta de la sociedad frente a la amenaza que supone la desinformación. El punto de partida es una mejor comprensión de las fuentes de desinformación y de las intenciones, herramientas y objetivos subyacentes a la desinformación, pero también de nuestra propia vulnerabilidad. Una metodología científica sólida puede ayudar a identificar las principales vulnerabilidades de los Estados miembros[194]. Es esencial comprender cómo y por qué los ciudadanos, y a veces comunidades enteras, se dejan convencer por los discursos de desinformación, y definir una respuesta general a este fenómeno.

El desarrollo de la capacidad de respuesta también incluye formación especializada, conferencias y debates públicos, así como otras formas de aprendizaje común para los medios de comunicación. Conlleva asimismo la capacitación de todos los sectores de la sociedad y, en particular, la mejora de la alfabetización de los ciudadanos para comprender cómo detectar y contrarrestar la desinformación.

Una respuesta integral a la desinformación requiere la participación activa de la sociedad civil. **La Comunicación y la Recomendación[195], que forman parte de un conjunto de medidas concebidas para garantizar unas elecciones europeas libres y justas, instan a los Estados miembros a participar, junto con los medios de comunicación, las plataformas en línea, los proveedores de tecnología de la información y otras partes interesadas,** en actividades de sensibilización para aumentar la transparencia de las elecciones y generar confianza en los procesos electorales. En el período previo y en el contexto de las elecciones europeas es necesario un compromiso activo y un seguimiento por parte de los Estados miembros.

Los verificadores de datos y los investigadores independientes desempeñan un papel clave a la hora de fomentar la comprensión de las estructuras que apoyan la desinformación y los mecanismos que determinan cómo se difunde en línea. Además, a través de sus actividades, sensibilizan sobre diversos tipos de amenazas de desinformación y pueden contribuir a mitigar su impacto negativo. Es necesario reforzar su capacidad para detectar y exponer las amenazas de la desinformación y facilitar la cooperación transfronteriza. Sobre la base de las acciones esbozadas en la Comunicación de abril, es preciso ampliar los equipos multidisciplinares nacionales de verificadores de datos e investigadores universitarios independientes con conocimientos específicos sobre los entornos de información locales. Esto requiere el apoyo y la cooperación de los Estados miembros con el fin de facilitar el funcionamiento de la Red europea de verificadores de datos, respetando plenamente la independencia de las actividades de verificación e investigación. En el marco del Mecanismo "Conectar Europa"[196], la Comisión financiará una plataforma digital que reunirá a equipos nacionales multidisciplinares independientes.

Para aumentar la sensibilización y la capacidad de respuesta de los ciudadanos, la Comisión seguirá reforzando su compromiso y sus actividades actuales en relación con la alfabetización mediática, a fin de

194 Este aspecto podría explorarse más detenidamente en el marco del trabajo del Observatorio del pluralismo de los medios de comunicación, un proyecto cofinanciado por la Unión Europea y ejecutado por el Centro para la Libertad y el Pluralismo en los Medios de Comunicación de Florencia.

195 Véase la Recomendación de la Comisión sobre las redes de cooperación electoral, la transparencia en línea, la protección contra incidentes de seguridad informática y la lucha contra las campañas de desinformación en el contexto de las elecciones al Parlamento Europeo, C(2018) 5949.

196 Reglamento (UE) n.º 1316/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, por el que se crea el Mecanismo "Conectar Europa", por el que se modifica el Reglamento (UE) n.º 913/2010 y por el que se derogan los Reglamentos (CE) n.º 680/2007 y (CE) n.º 67/2010.

capacitar a los ciudadanos de la Unión para que puedan identificar y tratar mejor la desinformación[197]. Los Estados miembros deben aplicar rápidamente la disposición de la Directiva de servicios sobre comunicación audiovisual revisada que les exige promover y desarrollar las capacidades de alfabetización mediática[198].

La Comisión ha propuesto financiar el desarrollo de nuevas herramientas para comprender y combatir mejor la desinformación en línea en su propuesta para el programa Horizonte Europa[199]. La Comisión también apoyará, cuando proceda, campañas de información para sensibilizar a los usuarios sobre las tecnologías más recientes (por ejemplo, falsificaciones profundas).

El trabajo de unos medios de comunicación independientes es esencial para el funcionamiento de una sociedad democrática. Por lo tanto, la Comisión[200] seguirá apoyando a los medios de comunicación independientes y a los periodistas de investigación, ya que contribuyen a desenmascarar la desinformación. Además, seguirá llevando a cabo programas específicos relacionados con el apoyo a los medios de comunicación, incluido el apoyo financiero y la profesionalización en los países vecinos[201].

Acción 7: Con vistas, en particular, a las elecciones europeas de 2019, pero también a largo plazo, la Comisión y la Alta Representante organizarán, en cooperación con los Estados miembros, campañas específicas para el público en general y formaciones para que los medios de comunicación y la opinión pública de la Unión y de los países vecinos aumenten la sensibilización sobre los efectos negativos de la desinformación. Se continuarán los esfuerzos para apoyar la labor de los medios de comunicación independientes y el periodismo de calidad, así como la investigación sobre la desinformación, a fin de dar una respuesta general a este fenómeno.

Acción 8: Los Estados miembros, en cooperación con la Comisión, deben apoyar la creación de equipos de verificadores de datos e investigadores independientes multidisciplinares con un conocimiento específico de los entornos de información locales con objeto de detectar y exponer las campañas de desinformación entre las diferentes redes sociales y los medios digitales.

Acción 9: Como parte de la semana de la alfabetización mediática que tendrá lugar en marzo de 2019, la Comisión apoyará, en colaboración con los Estados miembros, la cooperación transfronteriza entre profesionales de la alfabetización mediática, así como la puesta en marcha de herramientas prácticas para promover la alfabetización mediática del público. Los Estados miembros también deben aplicar rápidamente las disposiciones de la Directiva de servicios de comunicación audiovisual que abordan la alfabetización mediática.

Acción 10: Con vistas a las próximas elecciones europeas de 2019, los Estados miembros deben garantizar la aplicación efectiva del conjunto de medidas concebidas para garantizar unas elecciones europeas libres y justas, en particular de la Recomendación. La Comisión supervisará atentamente la aplicación del conjunto de medidas y, en su caso, prestará el apoyo y el asesoramiento pertinentes.

197 Estas actividades incluirán una biblioteca sobre alfabetización mediática y un centro de aprendizaje en línea de la Unión, así como otros instrumentos de alfabetización mediática.

198 Artículo 33 bis de la Directiva de servicios de comunicación audiovisual revisada.

199 COM(2018) 435.

200 En caso de que sea adoptado, el programa Europa Creativa ayudará a reforzar el sector de los medios de comunicación europeos, la diversidad y el pluralismo de los contenidos periodísticos, así como un enfoque crítico con respecto al contenido de los medios de comunicación a través de la alfabetización mediática, COM(2018) 438.

201 La Comisión financia el proyecto "Centro abierto de medios de comunicación" con el fin de: i) dotar a los periodistas de los países vecinos de las competencias necesarias para la redacción de noticias independientes y objetivas; ii) mejorar las competencias del personal editorial; iii) reforzar la red de profesionales de los medios de comunicación y periodistas en los países vecinos. Por lo que se refiere a los Balcanes occidentales, la Comisión facilita ayuda financiera para la creación de una red de asociaciones de periodistas, el establecimiento de relaciones de confianza en los medios de comunicación y el refuerzo de los sistemas judiciales para defender la libertad de expresión. En este ámbito, la Comisión también apoya a los medios de comunicación de servicio público, a los nuevos medios de comunicación independientes y a la mejora de la calidad y la profesionalidad del periodismo.

CONCLUSIONES

La desinformación es un reto importante para las democracias y las sociedades europeas, y la Unión debe abordarla permaneciendo fiel a las libertades y los valores europeos. La desinformación socava la confianza de los ciudadanos en la democracia y en las instituciones democráticas y contribuye además a la polarización de las opiniones públicas e interfiere en los procesos democráticos de toma de decisiones. También puede utilizarse para socavar el proyecto europeo, lo que puede tener importantes efectos negativos sobre la sociedad en toda la Unión, en particular en el período previo a las elecciones al Parlamento Europeo de 2019.

Es necesario un compromiso firme y acciones rápidas para preservar el proceso democrático y la confianza de los ciudadanos en las instituciones públicas, tanto a nivel nacional como de la Unión. El presente Plan de Acción contempla acciones clave para hacer frente a la desinformación mediante un enfoque coordinado de las instituciones de la Unión y los Estados miembros. También pone de relieve las medidas que deben tomar con carácter prioritario los diferentes agentes antes de las elecciones al Parlamento Europeo de 2019. Los Estados miembros deben reforzar su solidaridad y defender a la Unión contra los ataques híbridos, incluidos los ataques que se valen de la desinformación.

Al mismo tiempo, y a largo plazo, el objetivo es que la Unión y sus países vecinos tengan más capacidad de respuesta frente a la desinformación. Esto requiere esfuerzos continuos y sostenidos para apoyar la educación y la alfabetización mediática, al periodismo, a los verificadores de datos, a los investigadores y a la sociedad civil en su conjunto.

Por consiguiente, la Comisión y la Alta Representante:

- recuerdan que todos los agentes institucionales pertinentes, así como el sector privado, en particular las plataformas en línea, y la sociedad civil en su conjunto deben actuar conjuntamente para abordar de manera eficaz todos los diferentes aspectos de la amenaza que supone la desinformación;

- piden al Consejo Europeo que respalde el presente Plan de Acción;

- piden a los Estados miembros que cooperen para llevar a cabo las acciones establecidas en el presente Plan de Acción;

- piden a todos los agentes relevantes que apliquen con carácter prioritario las medidas urgentes y pertinentes en el período previo a las próximas elecciones europeas de mayo de 2019.

ORDEN PCM/1030/2020, DE 30 DE OCTUBRE, POR LA QUE SE PUBLICA EL PROCEDIMIENTO DE ACTUACIÓN CONTRA LA DESINFORMACIÓN APROBADO POR EL CONSEJO DE SEGURIDAD NACIONAL[202]

El Consejo de Seguridad Nacional, en su reunión del día 6 de octubre de 2020, ha aprobado el Procedimiento de actuación contra la desinformación. Para general conocimiento se dispone su publicación en el «Boletín Oficial del Estado» como anejo a la presente Orden.

Madrid, 30 de octubre de 2020.– La Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes y Memoria Democrática, Carmen Calvo Poyato.

ANEJO

Procedimiento de actuación contra la desinformación

1. CONTEXTO

El acceso a información veraz y diversa es uno de los pilares que sustentan a las sociedades democráticas y que deben asegurar las instituciones y administraciones públicas, porque se conforma como el instrumento que permite a los ciudadanos formarse una opinión sobre los distintos asuntos políticos y sociales. Además, la información permite a la ciudadanía adquirir conciencia y fundamento para participar en los debates públicos y, entre otros derechos democráticos, en los procesos electorales. Por este motivo, la libertad de expresión y el derecho a la información se consagran como derechos fundamentales en nuestra Constitución. Sin embargo, estos procesos de participación democrática se ven cada vez más amenazados por la difusión deliberada, a gran escala y sistemática de desinformación, que persiguen influir en la sociedad con fines interesados y espurios.

En este sentido, la Comisión Europea, en su *Flash Eurobarometer 464* de abril de 2018: *Fake news and disinformation online*, expone que el 88 % de los ciudadanos consideran que la desinformación es un problema en España, y el 66% afirma encontrarse con información falsa o que malinterpreta la realidad al menos una vez a la semana según los datos del *Special Eurobarometer 503* de la de Comisión Europea de marzo 2020 *Attitudes towards the impact of digitalisation on daily lives*.

Por su parte, en la Comunicación sobre la lucha contra la desinformación en línea, COM (2018) 236, la Comisión Europea define la desinformación como la «información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público», e incluye en este perjuicio público las amenazas a los procesos democráticos y a bienes públicos tales como la salud, el medio ambiente o la seguridad, entre otros.

En la lucha contra la desinformación, los ciudadanos consideran que los medios de comunicación, las autoridades públicas y las plataformas de medios sociales son los principales responsables de frenar la divulgación de noticias falsas.

Para hacer frente a este fenómeno, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) estableció un Plan de Acción para la lucha contra la desinformación, presentado y aprobado en el Consejo Europeo de los días 13 y 14 de diciembre de 2018. El Plan tiene como objetivos principales el desarrollo de capacidades en el seno de la Unión, y fortalecer la cooperación entre sus Estados miembros; e incluye un paquete de medidas destinado a hacer frente a la desinformación durante los procesos electorales europeos, así como los nacionales y locales que se celebraron en los Estados Miembros en 2019.

202 https://www.boe.es/eli/es/o/2020/10/30/pcm1030/con

Por otro lado, tal y como indica la Comisión en la Comunicación Conjunta al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones- La lucha contra la desinformación acerca de la COVID-19: contrastando los datos, la crisis de la COVID19 - la desinformación puede estar presente y afectar a cualquier campo, y en los tiempos actuales se ha observado de manera directa en la actual pandemia, viéndose acompañada de una «infodemia» sin precedentes.

Tomando como punto de partida el Plan de Acción contra la Desinformación de 2018, es necesaria una actuación más coordinada y acorde a nuestros valores democráticos que haga frente a los riesgos para las sociedades abiertas. Nuestras instituciones democráticas y nuestros valores comunes –la libertad de expresión y la libertad y pluralidad de los medios de comunicación, entre otros– son el fundamento de la resiliencia de nuestras sociedades frente a los desafíos.

Por ello, a fin de incrementar las capacidades de los Estados miembros y con el objetivo de atajar la desinformación y reforzar la resiliencia de las sociedades europeas, el nuevo impulso europeo se materializa a través del *European Democracy Action Plan*, con las siguientes líneas estratégicas: 1) Incrementar la integridad electoral y garantizar que los sistemas electorales sean libres y justos; 2) fortalecer la libertad de expresión y el debate democrático, examinando la libertad y pluralismo de los medios de comunicación, así como el papel de la sociedad civil y, por último; 3) abordar la desinformación de manera coherente, considerando la necesidad de examinar los medios que se utilizan para interferir los sistemas democráticos, basándose en las acciones sobre la lucha contra la desinformación relacionada con la COVID-19.

Esta situación sugiere la necesidad de un reajuste de este marco de actuación y, a tal efecto, se desarrolla la actualización de este procedimiento, que ha servido de base para la creación de un Sistema Nacional para la prevención, detección, alerta, seguimiento y respuesta cuyas causas, medio y/o consecuencias están relacionadas con la desinformación.

Además, se establecen los instrumentos necesarios para participar en los mecanismos que la Unión Europea ha puesto a disposición de los Estamos miembros y se refuerzan las capacidades de respuestas coordinadas y conjuntas a las campañas de desinformación, incrementando así el intercambio de información con los órganos y organismos con competencias en esta materia, a través de la Comisión Permanente contra la desinformación.

Por último, se revisan las funciones de la Comisión, a fin de responder a la necesidad de elaborar una propuesta de Estrategia Nacional de Lucha contra la desinformación.

2. PROPÓSITO Y OBJETIVOS

Dado el rápido progreso del entorno digital, el uso intensivo de los medios digitales y la complejidad de la temática abordada, establecer medios de funcionamiento y mecanismos dirigidos a evaluar de manera continua el fenómeno de la desinformación a nivel global y particularmente para España resulta imprescindible.

Por tanto, y con la finalidad de dar cumplimiento a los requerimientos establecidos por la Unión Europea e implementar a nivel nacional las políticas y estrategias promulgadas en el ámbito de la lucha contra la desinformación, urge redefinir los aspectos implicados mediante la identificación de los órganos, organismos y autoridades que forman el sistema, y marcar el procedimiento sus actuaciones. Para ello, se desarrolla el actual documento obteniendo así respuestas a las necesidades detectadas en este contexto.

Las acciones y procesos recogidos en este procedimiento ayudarán a mejorar y aumentar la transparencia con respecto al origen de la desinformación y a la manera en la que se produce y difunde, además de evaluar su contenido.

Por otro lado, dichas acciones apoyarán el fomento de la información veraz, completa y oportuna que provenga de fuentes contrastadas de los medios de comunicación y las Administraciones en el marco de la comunicación pública. Por último, este procedimiento incluye un aspecto de sensibilización de los organismos públicos y privados implicados, así como la colaboración entre ellos.

Por todo ello, se establecen los siguientes objetivos para este procedimiento:

- Identificar y definir los órganos, organismos y autoridades del sistema.

- Establecer los niveles para la prevención, detección, alerta temprana, análisis, respuesta, y evaluación.

- Describir los cometidos específicos implicados para los niveles establecidos en la lucha contra la desinformación.

- Definir los mecanismos establecidos para el intercambio de información en los niveles estratégico, operacional y técnico.

- Determinar los mecanismos de evaluación de la implementación y funcionamiento del procedimiento.

- Definir una metodología para la identificación, análisis y gestión de eventos desinformativos.

- Proponer el marco y la composición de un equipo de trabajo ad hoc para la elaboración y revisión de una Estrategia Nacional de Lucha contra la Desinformación.

3. ÓRGANOS, ORGANISMOS Y AUTORIDADES RESPONSABLES

Acorde con los órganos y organismos que conforman el Sistema de Seguridad Nacional, se establece una composición específica para la lucha contra la desinformación. La estructura está constituida por los siguientes componentes:

- El Consejo de Seguridad Nacional. Al Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, le corresponde asistir al Presidente del Gobierno en la dirección de la política de Seguridad Nacional.

- El Comité de Situación. El Comité de Situación regulado por Orden PRA/32/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, tiene carácter único para el conjunto del Sistema de Seguridad Nacional y actuará, apoyado por el Departamento de Seguridad Nacional, de acuerdo con las directrices político-estratégicas dictadas por el Consejo de Seguridad Nacional en materia de gestión de crisis. El Comité podrá apoyarse en una Célula de Coordinación de lucha contra la desinformación activada *ad hoc* por el Director del Departamento de Seguridad Nacional.

- La Secretaría de Estado de Comunicación. La Secretaría de Estado de Comunicación es la responsable de la coordinación de la política informativa del Gobierno y de la elaboración de los criterios para su determinación, así como del impulso y de la coordinación de la política de comunicación institucional del Estado, por otro lado, es la responsable de la gestión de la comunicación en situaciones de crisis y punto único de contacto con la Unión Europea en el ámbito de la lucha contra la desinformación.

- Comisión Permanente contra la desinformación. La Comisión Permanente contra la desinformación (el funcionamiento y modo de actuación se desarrolla en el anexo II) se establece para facilitar la coordinación interministerial a nivel operacional en este ámbito. Coordinada por la Secretaría de Estado de Comunicación y dirigida por el Departamento de Seguridad Nacional, se compone de aquellos órganos y organismos con responsabilidades operativas en este ámbito. Además, es el órgano al que corresponde asistir a los organismos anteriormente mencionados sobre aspectos relativos a la valoración técnica y operativa de posibles campañas de desinformación.

Secretaría de Estado de Comunicación en coordinación con:

De la Presidencia del Gobierno:

– Departamento de Seguridad Nacional.

Del Ministerio de Defensa:

– Centro Nacional de Inteligencia.

Del Ministerio del Interior:

– Gabinete de coordinación y estudios Secretaría de Estado de Seguridad.

Del Ministerio de Asuntos Exteriores, UE y Cooperación:

– Dirección General de Comunicación, Diplomacia Pública y Redes.

Ministerio de Asuntos Económicos y Transformaclón Digital:

– Secretaría de Estado de Transformación Digital e Inteligencia Artificial (SEDIA). Dirección del Gabinete de la SEDIA

Los organismos que componen la Comisión Permanente designarán, para para cada nivel, el órgano u organismo de su ámbito de competencia que les represente.

Autoridades públicas competentes. El marco institucional de la lucha contra la desinformación se complementa con las autoridades públicas competentes en la materia, estos son:

– Secretaria de Estado de Comunicación.

– Presidencia del Gobierno (DSN).

– Centro Nacional de Inteligencia.

– Gabinetes de comunicación de Ministerios, y otros organismos relevantes.

Sector privado y sociedad civil. Los medios de comunicación, las plataformas digitales, el mundo académico, el sector tecnológico, las organizaciones no gubernamentales y la sociedad en general juegan un papel esencial en la lucha contra la desinformación, con acciones como la identificación y no contribución a su difusión, la promoción de actividades de concienciación y la formación o el desarrollo herramientas para su evitar su propagación en el entorno digital, entre otras.

En este sentido, las autoridades competentes podrán solicitar la colaboración de aquellas organizaciones o personas cuya contribución se considere oportuna y relevante en el marco de la lucha contra el fenómeno de la desinformación.

4. NIVELES

El procedimiento establece cuatro niveles diferentes de activación que sirven tanto para detección de campañas de desinformación y su análisis ante unos posibles impactos en la Seguridad Nacional, como para el apoyo en la gestión de situaciones de crisis donde pudiera haber una afectación derivada de dichas campañas.

- Nivel 1: Nivel con capacidad para actuar a nivel técnico de detectar, realizar la alerta temprana y notificar según su comunidad de referencia.

- Nivel 2: Nivel con capacidad para apoyar la coordinación, sincronizar y priorizar todos los esfuerzos en la lucha contra la desinformación

- Nivel 3: Nivel en el que se adoptan decisiones y marcan objetivos de carácter político-estratégico con el objeto de hacer frente a una campaña de desinformación.

- Nivel 4: Nivel de gestión política en el marco del sistema de seguridad nacional.

A continuación, y para cada uno de los niveles establecidos, se establecen las siguientes actuaciones (el funcionamiento y modo de actuación se desarrolla en el anexo I):

Nivel 1.

1. Monitorización y vigilancia: detección, alerta temprana, notificación y análisis.

2. Participación en el Sistema de Alerta Rápida de la Unión Europea (RAS) y activación de los protocolos.

3. Investigación del posible origen, el propósito y seguimiento de su actividad.

4. Decisión sobre su elevación o finalización.

Nivel 2.

1. Convocatoria, seguimiento y evaluación de la alerta por parte de la Comisión

Permanente contra la desinformación.

2. Análisis de la situación y apoyo a la definición de propuestas de actuación.

3. Activación, en su caso, de una célula de Coordinación contra la desinformación activada *ad hoc* por el Director del Departamento de Seguridad Nacional.

4. Decisión sobre su elevación o la realización de una campaña de comunicación pública dirigida por la Secretaría de Estado de Comunicación en función de

la naturaleza de la campaña de desinformación.

Nivel 3.

1. Información al nivel político-estratégico por parte de la Secretaria de Estado de Comunicación.

2. Seguimiento y evaluación de la alerta por parte del Comité de Situación o Comunicación pública acordada según orientaciones del Comité de Situación.

Nivel 4.

1. Coordinación de la respuesta a nivel político por parte del Consejo de Seguridad Nacional en caso de atribución pública de una campaña de desinformación a un tercer Estado.

5. GESTIÓN EN EL MARCO DE LA UNIÓN EUROPEA

Nivel 1: Nacional. Se funcionará según el nivel 1 establecido para el ámbito nacional a fin de detectar campañas de desinformación de bajo impacto que puedan estar relacionadas con información relativa a la Unión Europea.

Colaboración con los StratComs en la identificación y análisis de eventos desinformativos, sobre todo, de aquellos que tengan estrecha vinculación con España, o le afecten de forma evidente.

Intercambio de buenas prácticas y procedimientos en la detección y análisis de campañas de desinformación con el resto de países miembros en el marco de los grupos de trabajo de la Unión.

Nivel 2: Intercambio de información que apoyen en la gestión de campañas de desinformación utilizando el Sistema de Alerta Rápida de la Unión Europea (RAS) a través de la Secretaria de Estado de Comunicación, como punto único de contacto con la Unión Europea para este ámbito. Se valorará, previa aprobación por la Comisión, la elevación al RAS de los informes elaborados.

Nivel 3: Intercambio de información a fin de apoyar la toma de decisiones a nivel político a través de la Secretaria de Estado de Comunicación.

Nivel 4: Toma de decisiones y coordinación a nivel político del Consejo de Seguridad Nacional.

6. APROBACIÓN Y PUESTA EN PRÁCTICA

El procedimiento descrito debe ser probado y entrenado, tanto en ejercicios nacionales como en ejercicios y simulacros realizados conjuntamente con otros países e instituciones de la Unión Europea.

La puesta en práctica de este procedimiento permitirá su mejora y adaptación a la evolución de las campañas de desinformación, incluyendo el establecimiento de un sistema de lecciones aprendidas.

NOTES