

Capítulo tercero

Türkiye y su seguridad interna: insurgencia, terrorismo y ciberespacio

Manuel J. Gazapo Lapayese

Resumen

Turquía o Türkiye, por su posición geoestratégica, es una potencia regional que está amenazada por fenómenos de diferente naturaleza. Su capacidad de proyectar poder y ejercer influencia depende de la estabilidad de su seguridad interior. Desde el fallido golpe de Estado de 2016 hasta la actualidad, Ankara ha reordenado su arquitectura securitaria derivando hacia un modelo hiperpresidencialista que identifica tres amenazas estratégicas interconectadas: el PKK, el Daesh y el ciberespacio. El PKK se presenta como un conflicto endémico cuya insurgencia violenta ha justificado tanto la militarización interna como la proyección militar en Siria e Irak, y cuyo anuncio de disolución en 2025 abre un escenario de posconflicto cargado de incertidumbres. El terrorismo de etiología salafista yihadista de Daesh se perpetua como un fenómeno descentralizado con capacidad de poner en crisis toda la seguridad del Estado. Los últimos atentados y las recientes detenciones demuestran que la amenaza continúa evolucionando. El ciberespacio emerge como un dominio central que amplifica las amenazas tradicionales y genera nuevos retos para la unidad nacional. Del análisis de estas amenazas, se extrae la idea de que la Türkiye de Erdoğan ha reforzado notablemente sus

capacidades operativas y tecnológicas, pero advierte que la securitización permanente, los déficits democráticos y la ausencia de soluciones políticas de fondo pueden reproducir, a medio y largo plazo, las mismas amenazas que el Estado pretende neutralizar.

Palabras clave

Türkiye, Erdoğan, Seguridad, Terrorismo, Ciberespacio.

Türkiye and its internal security: insurgency, terrorism and cyberspace

Abstract

Türkiye, due to its geostrategic position, is a regional power exposed to threats of different natures. Its ability to project power and exert influence depends on the stability of its internal security. From the failed coup attempt in 2016 to the present, Ankara has reorganized its security architecture, moving toward a hyper-presidential model that identifies three interconnected strategic threats: the PKK, Daesh, and cyberspace. The PKK is presented as an endemic conflict whose violent insurgency has justified both internal militarization and military projection into Syria and Iraq, and whose announcement of dissolution in 2025 opens a post-conflict scenario marked by significant uncertainty. Terrorism of salafi-jihadist origin associated with Daesh persists as a decentralized phenomenon capable of putting the entire security of the state under strain. Recent attacks and successive arrest operations demonstrate that the threat continues to evolve. Cyberspace has emerged as a central domain that amplifies traditional threats and generates new challenges to national unity. From the analysis of these threats, it follows that Erdoğan's Türkiye has significantly strengthened its operational and technological capabilities, while warning that permanent securitization, democratic deficits, and the absence of substantive political solutions may reproduce, in the medium and long term, the very threats the state seeks to neutralize.

Keywords

Türkiye, Erdoğan, Security, Terrorism, Cyberspace.

Introducción

Turquía —en adelante Türkiye, en referencia al nuevo nombre oficial del país ante las Naciones Unidas— es una potencia media con vocación de actor global. Este país euroasiático es un jugador geopolítico singular cuya posición internacional no puede comprenderse sin atender a su seguridad interna. Situada en el cruce estratégico entre Europa, Oriente Medio, el Cáucaso y el Mediterráneo Oriental, Türkiye controla el estrecho del Bósforo y actúa como frontera exterior tanto de la OTAN como de la Unión Europea (Pierini y Siccardi, 2025). Con más de 85 millones de habitantes, unas Fuerzas Armadas entre las más numerosas del mundo y una economía que figura entre las veinte mayores del planeta, Ankara proyecta influencia como potencia regional emergente y como intermediario diplomático entre Oriente y Occidente. Sin embargo, esta capacidad de proyección exterior está profundamente condicionada por dinámicas internas.

En Türkiye, lo endógeno y lo exógeno, lo doméstico y lo internacional no son esferas separadas, sino dimensiones que se retroalimentan de manera constante. En este sentido, la capacidad de Ankara para actuar como potencia regional está intrínsecamente ligada a la estabilidad de su frente doméstico. Así, es vital comprender que, desde hace más de una década, la seguridad interior turca no es un asunto aislado, sino el pilar sobre el que descansa su rol geopolítico regional y su aspiración global (Mourenza, 2025).

Tras el golpe de Estado fallido del año 2016, Recep Tayyip Erdoğan purgó las instituciones gubernamentales, reorganizó la estructura del Estado y apostó por un sistema de poder caracterizado por el hiperpresidencialismo (Cerbone, 2021). Diez años después, a nivel interno ya no se tiene miedo a un nuevo golpe militar, sino a un atentado en Estambul, a un ataque informático al gasoducto TANAP o a una manifestación que las redes sociales logren convertir en revuelta.

Por lo tanto, en pleno 2026, puede afirmarse que la capacidad que tiene Türkiye de proyectar su poder regionalmente depende de su capacidad para contener los tres riesgos que considera primarios en sus documentos estratégicos: en primer lugar, la amenaza estructural asociada a la insurgencia violenta del Partido de los Trabajadores del Kurdistán (PKK); en segundo lugar, el terrorismo de etiología salafista yihadista de Daesh, y, en tercer lugar, la guerra híbrida que se libra en el ciberespacio mediante

campañas de desinformación y ciberataques a infraestructuras críticas.

Visión gubernamental: tres documentos estratégicos

Entre 2016 y 2026, la percepción turca de la amenaza interna ha experimentado una transformación cualitativa que no altera el repertorio de riesgos, pero sí su jerarquización, su tratamiento doctrinal y los instrumentos empleados para su contención. Si se analiza la documentación estratégica oficial turca procedente del Ministerio del Interior, del Consejo de Seguridad Nacional y de la Estrategia Nacional de Ciberseguridad subyacen las siguientes ideas:

En primer lugar, según el Consejo de Seguridad Nacional, el terrorismo constituye la principal amenaza existencial a la seguridad estatal, la estabilidad interna y la unidad nacional (R.T. Consejo de Seguridad Nacional, 2025a). Este organismo subraya que los colectivos vinculados a FETÖ (Bayrakli *et al.*, 2018), las milicias kurdas de las Unidades de Protección Popular o YPG (Malet *et al.*, 2025), el PKK o el Daesh materializan atentados con efectos muy graves y severos para la estabilidad interna del país. Además, si se analiza minuciosamente el archivo de comunicaciones disponibles en la página web de la Secretaría General del Consejo de Seguridad Nacional se puede observar cómo durante 2024 y 2025 se han ido incorporando referencias cada vez más numerosas y preocupantes relativas a la guerra informativa (Espona, 2023), la manipulación digital y el ciberespacio. Este último despierta un especial interés dentro de los análisis de seguridad de las autoridades en tanto se interpreta como un ámbito de ataque, un vector de desestabilización, y una amenaza para infraestructuras críticas y orden público. En los comunicados más recientes, el ciberespacio ya no recibe únicamente un tratamiento técnico, sino que es gestionado como una cuestión transversal a toda la seguridad del Estado al estar ligado a problemáticas como la desinformación, el sabotaje, la vulneración de infraestructuras críticas o el propio terrorismo en sus múltiples formas y dimensiones.

«El Consejo fue informado sobre las actividades realizadas contra todas las amenazas y peligros a nuestra unidad nacional primariamente de las organizaciones terroristas PKK/KCK-PYD/YPG, FETÖ e ISIS [...] en consonancia con el objetivo de una «Türkiye libre de terrorismo», se discutieron los esfuerzos multidimensionales encaminados a la terminación completa y permanente del terrorismo y al fortalecimiento

de nuestra unidad y solidaridad nacionales; se enfatizó que no hay lugar para ninguna manifestación de terrorismo y violencia en el futuro de nuestra región» (R.T. Consejo de Seguridad Nacional, 2025b).

En segundo lugar, según el Plan Estratégico 2024-2028 (R.T. Ministerio del Interior, 2024), la seguridad interior, de forma coincidente, se ve afectada por la insurgencia radical del PKK, por el terrorismo de Daesh y por las amenazas procedentes del ciberespacio, una dimensión que condiciona la estabilidad del orden público y el control de la información. En este documento institucional, se expone que Ankara no concibe la amenaza terrorista como residual, sino como un factor estructural que condiciona la organización territorial y logística del Estado. Además, entienden que el terrorismo no es un fenómeno aislado, sino permeado por lo que ocurre en el plano digital, social e informacional. El texto del Ministerio expone que el Estado trabaja de forma simultánea en el espacio terrestre (*Kara Vatan*), en el espacio marítimo (*Mavi Vatan*) y en el ciberespacio (*Siber Vatan*) para garantizar que ninguna de estas amenazas escapa a su control y gestión de riesgos.

«El Ministerio del Interior, en consonancia con la visión de «La paz de Türkiye», cumple su labor día y noche con gran convicción, determinación y firmeza para garantizar la tranquilidad y la seguridad de nuestro país, con 600.000 efectivos desplegados en la Patria Terrestre, la Patria Azul y la Patria Cibernética» (R.T. Ministerio del Interior, 2024: 9).

En tercer lugar, según la Estrategia Nacional de Ciberseguridad 2024-2028 (R.T. Ministerio de Transporte e Infraestructuras, 2024), el ecosistema digital que constituye el ciberespacio se consolida como una amenaza en sí misma y, simultáneamente, como multiplicador transversal de todos los riesgos que afectan a la seguridad interna de Türkiye. El texto advierte del poder desestabilizador de las ciberamenazas, señalando no solo su capacidad de causar víctimas, sino también su potencial para erosionar la autoridad del Estado, fracturar la cohesión social y condicionar la toma de decisiones políticas. En esta lógica, un atentado de Daesh puede generar conmoción puntual, pero una campaña digital sostenida que cuestione la competencia o la legitimidad del Gobierno puede producir efectos sistémicos mucho más duraderos.

Este desplazamiento del foco explica la aprobación de la Ley n.º 7545, conocida como la Ley de Ciberseguridad de 2025

(República de Türkiye, 2025), que amplía de manera significativa el margen de intervención del Estado sobre el espacio informacional. Al tipificar como delito la difusión de información considerada falsa sobre filtraciones o fallos en infraestructuras críticas y habilitar a la Autoridad de Tecnologías de la Información y la Comunicación (*Bilgi Teknolojileri ve İletişim Kurumu – BTK*) para bloquear plataformas sin orden judicial en caso de peligro para la seguridad pública nacional, Ankara institucionaliza una lectura del ciberespacio como frente interno prioritario, equiparable a los escenarios clásicos de seguridad.

Visión gubernamental: tres amenazas estratégicas

Del marco conceptual y normativo configurado por los tres documentos gubernamentales referenciados, se extraen las siguientes ideas coincidentes: en relación con el PKK, pese a las declaraciones recientes de abandono de la lucha armada en determinados contextos, este no desaparece como amenaza estratégica. Desde la perspectiva institucional turca, el criterio de evaluación no es el discurso político, sino la capacidad remanente, la proyección transfronteriza y la persistencia de un ecosistema organizativo que sigue siendo percibido como un desafío directo a la unidad nacional y a la supervivencia del Estado (*beka*). La continuidad entre el plano interno y los teatros sirio-iraquíes refuerzan la lectura del PKK como una amenaza estructural, susceptible de mutar en intensidad, pero no de desaparecer. De ahí que Ankara mantenga una lógica de contención permanente —operaciones internas, proyección militar exterior, vigilancia ISR (Nieto y Mateo, 2014) y presión sostenida sobre espacios de refugio— coherente con la idea de que el riesgo puede adaptarse y replegarse, pero no extinguirse (CFR, 2025).

En relación con el terrorismo yihadista, se afirma que Daesh ocupa un lugar específico y diferenciado dentro de la arquitectura de amenazas por el alto valor simbólico y psicológico que tienen sus atentados. La desarticulación en 2024 de una célula que planeaba atentarse contra la estación central de Ankara el Día de la República; el ataque de enero de 2025 en la iglesia de Santa María de Estambul; la detención de más de un centenar de sospechosos de Daesh en redadas simultáneas a nivel nacional en diciembre de 2025 y la operación contraterrorista llevada a cabo en Yalova (Ferreira, 2025) a pocos días de comenzar 2026, confirman la persistencia de actores auto-radicalizados y la expansión de microcélulas con capacidad de acción autónoma. Estos

episodios refuerzan la percepción estatal de que el yihadismo no ha sido derrotado, sino descentralizado, desplazándose hacia formas menos visibles y más imrededibles (Tuysuz y Tawfeeq, 2025).

En relación con el ciberespacio, la centralidad del dominio digital no sustituye a las amenazas tradicionales, sino que las reconfigura y amplifica, convirtiéndolo en el vector a través del cual estas pueden multiplicar su impacto.

En conjunto, la convergencia de estas tres amenazas —PKK, terrorismo yihadista y ciberespacio— no es accidental ni coyuntural. La política de seguridad turca no solo identifica estos riesgos como prioritarios, sino que los trata como interdependientes; constituyen el núcleo duro de la percepción de riesgo interno turco hacia 2026 y los años posteriores. El PKK representa la amenaza estructural y territorial; el yihadismo, la violencia episódica de alto impacto simbólico y el ciberespacio, el multiplicador transversal que permite a ambas erosionar la estabilidad estatal sin necesidad de control físico del territorio.

Teniendo la certeza de que Türkiye es un caso paradigmático de cómo la seguridad interna condiciona el devenir de la proyección estratégica de una potencia regional más allá de sus fronteras inmediatas, a continuación, se analizan las tres amenazas y sus efectos disruptivos en el desarrollo del país.

1 PKK: presente y futuro del conflicto endémico de Türkiye

El Partido de los Trabajadores del Kurdistán (PKK) ha sido, durante más de cuarenta años, la principal amenaza a la seguridad interna turca (Robinson, 2023). Esta insurgencia kurda, iniciada en 1984, convirtió la cuestión kurda en un asunto central de la agenda política y de seguridad de Türkiye. El conflicto ha costado la vida a más de cuarenta mil personas desde los años 1980 (ICG, 2025) provocando una militarización del Estado en la que las Fuerzas Armadas y los servicios de inteligencia (MİT) asumieron un rol protagonista y justificaron medidas excepcionales en nombre de la unidad nacional. Hace más de una década Ankara catalogó oficialmente al PKK como organización terrorista y como la principal amenaza para la integridad del país (Ministerio de Asuntos Exteriores, 2025). La lucha contra el PKK ha moldeado la doctrina militar turca y ha condicionado hasta la actualidad su política exterior.

El legado de este prolongado conflicto, que ha marcado y afectado a numerosas generaciones, conlleva desafíos profundos de seguridad y gobernanza. Las campañas militares continuas y la imposición de estados de emergencia durante años en el sureste de Anatolia debilitaron la confianza en las instituciones y tensionaron la cohesión social. El Estado turco, bajo el principio constitucional de una patria indivisible restringió durante mucho tiempo los derechos culturales y lingüísticos de la minoría kurda en pro de la unidad nacional.

«The Kurds are believed to number around 30 million and are widely believed to be the largest group of stateless people in the world. [...] The Kurds do not have a single common language, but the most widely spoken Kurdish dialect. [...] Likewise, the Kurds do not share a common religion. Most are Sunni Muslims. [...] Other Kurds follow Alevism, an unorthodox form of Shi'ite Islam, as well as the indigenous Kurdish faith of Yezidism. There are minor communities of Kurdish Jews, Christians and Baha'is [...] From the start, expressions of Kurdish identity were discouraged, and the Kurds were compelled to behave in accordance with the norms of the countries in which they now found themselves. In time, military incursions into Kurdish regions became common occurrences, with comprehensive attempts made to forcibly dissipate Kurdish networks in border areas and stamp out the notion of a separate Kurdish identity» (Yildiz y Muller, 2008: 4).

Este enfoque de seguridad del Estado versus derechos humanos ha sido objeto de duras críticas internacionales: la persecución de políticos prokurdos, la ilegalización de partidos, el encarcelamiento de líderes del Partido Democrático de los Pueblos (HDP) y la sustitución sistemática de alcaldes elegidos por administradores estatales ilustran una deriva que prioriza la estabilidad sobre la democracia (U.S. Department of State, 2022). Observadores internacionales señalan que Türkiye ha experimentado una profunda involución democrática, evidenciada por la clasificación de Freedom House (2023) como país «no libre» desde 2018, atribuida en parte al prolongado conflicto interno y al uso político del mismo para reforzar el poder ejecutivo¹.

¹ Véase: Freedom House (2023), *Freedom in the World 2023*, donde se evalúa la situación en Türkiye: «Turkey. Not Free: Political Rights 16/40. Civil Liberties 16/60. Last Year's Score Status: 32/100. Overview: President Recep Tayyip Erdoğan and his Justice and Development Party (AKP), which have ruled Turkey since 2002, have

1.1 Dimensiones transnacionales y estrategia de externalización

A pesar de periodos de alto el fuego y negociaciones en el pasado, la insurgencia kurda no ha desaparecido; por el contrario, su carácter transnacional obliga a Ankara a operar en un teatro complejo que combina lo interno y lo externo: Por un lado, el PKK mantiene la capacidad de ejecutar esporádicamente atentados y ataques dentro de Türkiye, especialmente en las provincias de mayoría kurda del sureste, aunque también ha perpetrado ataques terroristas en grandes urbes cuando ha podido. Informes de inteligencia turcos y occidentales señalan que el PKK ha sido históricamente responsable de más de cuarenta mil muertes desde 1984 (CFR, 2025), ilustrando el enorme coste humano y la persistencia de esta amenaza. Incluso en fechas recientes, en 2023 y 2024, atentados mortales atribuidos al PKK o a facciones vinculadas sacudieron Türkiye. Un ejemplo que muestra que el peligro subsiste pese a la presión militar es el ataque suicida frente al Ministerio del Interior en octubre de 2023 (RTVE, 2023).

Por otro lado, Ankara ha externalizado el conflicto kurdo más allá de sus fronteras. El grueso de su infraestructura logística y sus santuarios se sitúan fuera del territorio turco: en las montañas del norte de Irak, en la región de Kandil, y en zonas bajo control kurdo en el norte de Siria. Esta dualidad hace que Türkiye justifique y lleve a cabo operaciones militares más allá de sus fronteras como parte de su estrategia de seguridad. Desde 2016 se han sucedido operaciones como Escudo del Éufrates (2016-2017), Rama de Olivo (2018), Fuente de Paz (2019) y las más recientes de la serie Garra (*Pençe*) en territorio iraquí. Todas estas operaciones e intervenciones militares estaban orientadas a golpear a milicias kurdas sirias aliadas del PKK, como las Unidades de Protección Popular (YPG) y a combatir los focos remanentes del Daesh en la franja fronteriza sirio-iraquí.

La percepción estratégica de Ankara es que permitir la emergencia de una entidad kurda armada autónoma en Siria o Irak supondría un riesgo existencial para su seguridad, al estimular las aspiraciones separatistas dentro de su propio territorio. Erdoğan ha reiterado en numerosas ocasiones que no permitirán la creación

become increasingly authoritarian in recent years, consolidating significant power through constitutional changes and by imprisoning opponents and critics. A deepening economic crisis and the upcoming elections in 2023 have given the government new incentives to suppress dissent and limit public discourse».

de un «corredor terrorista en su frontera sur» (Euronews, 2016), enfatizando que Türkiye apoyará al Gobierno de Damasco para evitar que una hipotética fragmentación de Siria pudiera beneficiar al PKK/YPG (SWI, 2025b). Esta postura firme explica la continuidad de la presencia militar turca más allá de sus fronteras: hoy en día, contingentes turcos siguen desplegados en una zona *buffer* de seguridad de aproximadamente 30 km de profundidad en el norte de Siria. Ese área de amortiguación permite a las fuerzas de Erdoğan controlar el territorio que se extiende entre Afrin, Jarabulus y Ras al-Ain. Igualmente, Ankara mantiene decenas de bases en el Kurdistán iraquí, desde las cuales hostigan a militantes del PKK.

Con relación a estos despliegues, es necesario señalar que, aunque los aliados occidentales de Türkiye reconocen formalmente al PKK como organización terrorista, la comunidad internacional ha expresado preocupación ante estas intervenciones unilaterales que el Gobierno de Erdoğan defiende como autodefensa preventiva legítima frente al terrorismo (European Commission, 2016).

1.2 El anuncio de paz de 2025 y sus incertidumbres

El año 2025 marcó un hito en este conflicto endémico. En mayo, durante un congreso extraordinario, el PKK anunció el cese definitivo de la lucha armada y la disolución de su estructura militar, atendiendo a un llamamiento histórico de su líder encarcelado Abdullah Öcalan. Esta decisión tomada en su XII Congreso puso fin a cuarenta años de insurgencia declarada. En octubre, los militantes del PKK comenzaron a retirarse del territorio turco hacia sus bastiones en el norte de Irak, escenificando ceremonias simbólicas de desarme (Al Jazeera, 2025b). El presidente Erdoğan, que en 2024 inició el proyecto «Türkiye libre de terrorismo», calificó el momento como «un nuevo capítulo histórico» reconociendo la trascendencia de la paz alcanzada y celebrando que «un país poderoso que se libera del terrorismo» (Reuters, 2025).

«The project Terror-free Türkiye targets the transformation of the Turkish political perspective at two different levels. At the national level, it aims to «consolidate the national front, » as explained by Turkish officials. The main objective of the project is to get rid of one of the most active political fault lines, the Kurdish problem, in the country. At the regional level, it intends to eradicate terrorism from the Middle East

to create a terror-free region, as the PKK and its branches are active not only in Türkiye but in several regional countries» (Ataman, 2025).

Ahora bien, el posconflicto presenta incertidumbres significativas. La transición del PKK de las armas a la política se está llevando a cabo de forma opaca y sin un debate público transparente, lo que despierta recelos (Hamza y Toye, 2025). Si el proceso de desarme, desmovilización y reintegración (DDR) no se gestiona con inclusividad y respeto a la justicia transicional, existen riesgos latentes que pueden estallar en cualquier momento: la fragmentación del movimiento kurdo, la aparición de facciones disidentes o vacíos de seguridad en el sureste anatolio que podrían ser explotados por otros grupos violentos. Analistas internacionales advierten que, sin transparencia ni participación ciudadana, esta oportunidad de paz podría malograrse y «replicar fracasos del pasado, provocando un retorno a la violencia» (Cahid, 2025). Además, quedan cabos sueltos en el tablero regional: la influencia sobre las milicias kurdas de Siria y la respuesta del Estado turco en materia de reformas políticas. El PKK ha condicionado su disolución a pasos concretos de Ankara —amnistías, garantías para la participación democrática kurda, mejoras en las condiciones carcelarias de Öcalan— que aún están por materializar (Al Jazeera, 2025a).

En suma, aunque el conflicto armado con el PKK parece llegar a su fin, el reto de Türkiye para este 2026 y los próximos años será consolidar una paz duradera que aborde las causas políticas subyacentes, preserve la seguridad sin una militarización excesiva y fortalezca la cohesión entre turcos y kurdos tras décadas de desconfianza.

2 Terrorismo yihadista: Daesh en el panorama de seguridad turco

La amenaza del terrorismo yihadista en Türkiye se intensificó con la guerra civil siria y la aparición de Daesh en 2014. Debido a su posición geográfica colindante con Siria e Irak, Türkiye se convirtió tanto en un blanco de atentados como en un país de tránsito para miles de combatientes extranjeros que se unieron a Abu Bakr al-Baghdadi (Neuman *et al.*, 2025). Entre 2015 y 2017, miembros de la organización llevaron a cabo ataques terroristas de gran magnitud en territorio turco. Entre los más graves destacan el doble atentado suicida de Ankara de octubre de 2015, que

causó ciento tres muertos —la peor masacre terrorista en la historia reciente de Türkiye— y varios ataques en Estambul contra zonas turísticas e infraestructuras críticas, destacando el atentado en el aeropuerto internacional Atatürk en junio de 2016, que dejó 45 fallecidos. Estas acciones evidenciaron la capacidad del yihadismo para golpear en cualquier espacio del territorio urbano sembrando el pánico e insuflando incertidumbre e inestabilidad en la vida nacional.

En un inicio, Ankara mostró reticencia a confrontar abiertamente a Daesh porque las prioridades estratégicas eran distintas: el régimen sirio o los kurdos tenían mayor peso en su cálculo estratégico. Sin embargo, tras verse directamente atacada en 2015, Türkiye modificó drásticamente su postura. En julio de 2015, el Gobierno turco autorizó el uso de la base aérea de Incirlik por la coalición internacional liderada por EE. UU. contra Daesh, y poco después inició sus propias operaciones de contraterrorismo. La Operación Escudo del Éufrates (2016-2017) supuso el primer despliegue militar turco directo en Siria contra objetivos de Daesh, logrando expulsar a los milicianos radicales de importantes enclaves fronterizos como Jarabulus o Al-Bab, entre otros. En el transcurso de esa campaña, las fuerzas turcas neutralizaron a más de dos mil combatientes yihadistas, mostrando el compromiso de Ankara en dismantelar el califato territorial de la organización terrorista que reivindicaba sus atentados a través de Amaq News Agency y Al Hayat Media Center (Hasnain, 2019).

Desde entonces, Türkiye ha mantenido una presión constante sobre redes yihadistas en su territorio: la policía y el MİT han detenido a centenares de sospechosos, desarticulando tanto células durmientes como tramas logísticas de captación y financiación. A nivel internacional (U.S. Department of State, 2025), Türkiye coopera estrechamente con aliados occidentales —incluidos sus socios europeos— intercambiando inteligencia para la detección temprana de terroristas internacionales y retornados. A este respecto, cabe tener presente dos ejemplos: en primer lugar, que la Comisión Europea y el Gobierno de Erdoğan mantienen de manera periódica diálogos de alto nivel sobre migración y seguridad en los que se trabaja de manera intensiva la cooperación en la lucha contra el terrorismo y el crimen organizado (SWI, 2023). Y, en segundo lugar, que en el marco de la coalición global contra Daesh, las fuerzas de seguridad turcas y españolas han colaborado (Departamento de Seguridad Nacional de España, 2016) activamente en la identificación y detención

de yihadistas con conexiones transnacionales (Presidencia del Gobierno de España, 2018).

2.1 Las redes de captación y la autopista yihadista

El análisis detallado de redes de captación de Daesh dentro de Türkiye revela infraestructuras clandestinas que se fueron construyendo desde 2014. Estas redes no se limitaron a reclutar simpatizantes; también crearon pisos francos, rutas de tránsito hacia Siria, sistemas *hawala* de financiación informal (El Qorchi, Munzele y Wilson, 2025) y centros de adoctrinamiento encubiertos. Eran redes flexibles, con nodos autónomos insertos en comunidades marginadas donde el Estado tenía presencia limitada. Los «dinamizadores de contenido» (Gazapo, 2018), los captadores y los reclutadores utilizaban mezquitas no oficiales, bibliotecas, centros deportivos, asociaciones caritativas y círculos de estudio religioso para identificar jóvenes vulnerables: desempleados, desplazados internos, inmigrantes, refugiados o individuos con baja integración social, cultural y económica. El informe «The financing of the Islamic State in Iraq and Syria (ISIS)» del Parlamento Europeo evidenciaba esta red de actores que facilitaban pagos y compraventas de armas de Daesh a través de Türkiye:

«The Iraqi Central Bank took action by establishing a blacklist of 142 exchange offices suspected of allowing IS money throughout territory under its control. According to an investigative report published by the Wall Street Journal, three primary routes are used for such money transfers, two of which are in Türkiye and another in Jordan. International organizations are striving to neutralize such sources of financing, which often transfer funds through small-denomination banknotes [...] IS forces source most of the products used in the manufacture of weapons and ammunition from the Turkish domestic market. CAR's findings continuously reinforce evidence that the group operates a major acquisition network in Türkiye and has a direct line of supply from Türkiye, through Syria, to the Mosul area» (European Parliament, 2017: 11-15).

Cabe destacar que Şanlıurfa y otras ciudades fronterizas situadas en el sureste de Türkiye, se convirtieron en nudos logísticos esenciales para estas redes de captación yihadista a razón de su proximidad a los pasos fronterizos con Siria, su mezcla

demográfica y la debilidad de Ankara a la hora de proyectar allí el monopolio de la fuerza estatal. Desde esas ciudades partían caravanas, se falsificaban documentos y se distribuían fondos hacia las zonas controladas por Daesh. La permisividad institucional del Estado turco durante 2014 y 2015, centrado entonces en derrocar a Assad y contener al PKK, permitió que Daesh consolidara estructuras que después se demostrarían sumamente difíciles de destruir: «The Islamic State has also cultivated looser networks of cells, operatives, and sympathizers in Europe, Asia, Africa, and United States. Its networks in Türkiye facilitated the flow of fighters, weapons, resources and even oil exports» (USIP, 2017: 17).

Francesco Siccardi, subdirector de Carnegie Europe, centro regional de Carnegie Endowment for International Peace, expuso con detalle cómo la política inicial de Türkiye hacia Siria desempeñó un papel clave —aunque involuntario— en la expansión territorial y logística de Daesh durante los primeros años del conflicto. Desde 2011, Ankara adoptó una estrategia centrada en la caída del régimen de Bashar al-Assad. Bajo este enfoque, el Gobierno turco relajó el control de sus fronteras para proveer de apoyo logístico y humano a grupos opositores sirios sin establecer una distinción clara entre facciones moderadas e insurgencias islamistas radicales (Siccardi, 2021). El informe del Carnegie detalla que esta combinación de permisividad, relajación del control fronterizo y fragmentación de la insurgencia siria facilitó la aparición de una autopista yihadista que conectaba Europa, Türkiye y Siria.

El experto en terrorismo Kyle W. Orton (2017) coincide en el diagnóstico y señala que entre 2012 y 2014 miles de combatientes extranjeros utilizaron rutas turcas para entrar a zonas controladas por Daesh, aprovechando pasos fronterizos poco vigilados, redes de contrabando y espacios de gobernanza frágil en la frontera sur. Türkiye no actuó deliberadamente para favorecer a Daesh, pero sí creó, mediante decisiones estratégicas erróneas, un entorno operativo donde el grupo pudo expandirse y consolidar su estructura organizativa. El efecto *boomerang* de esta política se manifestó entre 2015 y 2017, cuando Türkiye sufrió los ya referenciados atentados de Daesh en Ankara y Estambul. Estos episodios, que corresponden a los ataques terroristas más mortíferos de la historia reciente de Türkiye, revelaron de forma trágica cómo la porosidad fronteriza previa y la apuesta turca por un cambio de régimen en Siria habían propiciado condiciones que luego fueron explotadas por la organización yihadista. La posterior construcción del muro fronterizo, el refuerzo militar

y los cambios doctrinales en la política exterior turca pasaron a ser correcciones tardías a una etapa inicial marcada por excesiva permisividad y subestimación del riesgo.

2.2 Combatientes retornados, radicalización doméstica y contranarrativa institucional

El International Crisis Group (ICG) profundizó en 2020 en una dimensión crítica: los combatientes retornados. El *think tank* liderado actualmente por la doctora Comfort Ero, señaló que Türkiye debía gestionar entre cinco mil y nueve mil ciudadanos que, tras combatir en las filas del Daesh, regresaron o intentaron regresar. El ICG destacó que Ankara había mejorado el intercambio de información e inteligencia con sus aliados europeos, y con ello logrado encarcelar a cientos de radicales y congelar activos financieros. Sin embargo, el informe subrayaba una limitación estructural: la ausencia de programas de desradicalización y reintegración. Türkiye había optado por un enfoque eminentemente punitivo, que podía neutralizar la amenaza a corto plazo, pero dejaba sin atender el riesgo de que los liberados reincidieran o creasen nuevas células clandestinas (ICG, 2020).

El ICG también alertó de un factor geopolítico que consistía en que cientos de combatientes turcos que habían jurado lealtad a Daesh estaban detenidos en cárceles del norte de Siria, bajo control kurdo. Dado que Türkiye no cooperaba con estas milicias, su futuro era incierto: si estallaba un nuevo conflicto, muchos podrían escapar y reactivar redes transfronterizas.

«Türkiye has to deal with thousands of citizens who travelled to join ISIS and have now returned. Of the few convicted, many will soon be released from jail. Others are under surveillance. The fate of the rest is murky [...] At the same time, Turkish state institutions have only recently begun contemplating what they call «de-radicalisation» or «rehabilitation» efforts -broadly speaking, policies designed to move former militants away from jihadist ideology and violence. For the most part, the authorities rely on surveillance -monitoring those they believe may pose a threat-, combined with short detentions designed to scare anyone whom they think is poised to join militant circles away from doing so» (ICG, 2020).

Si se atiende al Global Terrorism Index del Institute for Economics & Peace, se observa que Türkiye se sitúa en el puesto 32 de los

países más afectados por la amenaza del terrorismo. Aunque lejos de los niveles de impacto alcanzados en el pico de violencia de mediados de la década de 2010, el país controlado por Erdoğan todavía ocupa una posición preocupante al estar dentro del grupo de países con afectación significativa por terrorismo (IEP, 2025). Es decir, la amenaza yihadista ha disminuido en intensidad, pero no ha desaparecido. Los acontecimientos de 2025 confirman este diagnóstico: el 16 de abril de 2025, el ministro del Interior Ali Yerlikaya anunció la detención de 89 sospechosos vinculados a Daesh en operaciones coordinadas en diecisiete provincias, incluida Estambul; pocos meses después, entre el 5 y el 12 de septiembre de 2025, las autoridades informaron de una nueva ofensiva que se saldó con 161 detenidos en 38 provincias, incautando armas, documentación y material digital del grupo (Xinhua News, 2025). Estas cifras muestran que el Estado turco sigue afrontando una red yihadista activa y que el terrorismo salafista forma parte central del cálculo de seguridad interna.

La radicalización doméstica constituye otro pilar de preocupación. Diversos estudios indican que más de 2100 ciudadanos turcos se unieron como combatientes extranjeros a grupos yihadistas en Siria o Irak evidenciando un caldo de cultivo interno no gestionado ni neutralizado por Erdoğan o el MİT (Bingol, 2023). Ante este escenario, las autoridades han desplegado campañas de contranarrativa a través de la *Diyanet İşleri Başkanlığı* o Dirección de Asuntos Religiosos con el fin de promover un islam suní moderado para desacreditar la ideología salafista y ofrecer un marco identitario alternativo para jóvenes vulnerables. Sin embargo, profesores expertos en esta área como Ihsan Yılmaz e Ismail Albayrak advierten que esta contranarrativa puede fracasar si es reactiva y politizada. La instrumentalización política de la religión erosiona su legitimidad y genera rechazo, en especial, entre minorías kurdas, alevíes o secularistas. Cuando un Estado combate el extremismo únicamente endureciendo la coerción o manipulando la religiosidad oficial, corre el riesgo de producir más radicalización. Además, el hacinamiento carcelario tras las purgas de 2016 genera temor de que las prisiones se conviertan en viveros de extremismo si no se implementan programas efectivos de desradicalización.

«AKP with the help of Diyanet, merged the concepts of democracy and jihad. Thus, it is no surprise that Erdoğan has called the failed coup 'a gift from God'. [...] The events have allowed him to strengthen his conspiracy filled narra-

tive with the aid of the 'divine' authentication of the narrative by Diyanet [...] Diyanet and AKP evolved and moved towards Islamism and authoritarianism together. Strategizing a congenial relationship between politics and religious rhetoric, state and mosque have transitioned from promoters of Islamic democratic conservatism to outright Islamist authoritarianism» (Yılmaz y Albayrak, 2022).

2.3 Securitización del Estado y costes democráticos

En 2014, en pleno ascenso del Daesh y en un momento crítico de la guerra civil siria, el Gobierno turco aprobó la Ley n.º 6532 (República de Türkiye, 2014), conocida por la reforma que afectó a la Organización Nacional de Inteligencia. Esta norma modificó la estructura y competencias del MİT ampliando sus facultades para operar tanto en el interior como en el exterior del país. Antes de esta reforma, requería autorización judicial estricta para interceptar comunicaciones, acceder a datos privados o realizar actividades encubiertas. La Ley 6532 eliminó buena parte de estas restricciones, otorgando al MİT inmunidad funcional, ampliando sus poderes de recopilación de datos y permitiéndole llevar a cabo operaciones encubiertas sin supervisión judicial efectiva.

Si bien la ley fue muy beneficiosa para los funcionarios del ámbito de la seguridad y la defensa, Human Rights Watch (HRW) denunció ese mismo año que la medida debilitaba las garantías democráticas esenciales, pues aprobaba la interceptación de comunicaciones, el acceso a registros personales y la protección legal de los agentes incluso si actuaban sin orden judicial. Aunque la intención oficial era reforzar la lucha contra amenazas como Daesh, la reforma evidenciaba una tendencia clara: Türkiye comenzaba a securitizar profundamente su aparato estatal. Esta securitización implicaba que la amenaza moldeaba su evolución legal, gubernamental y judicial.

«A new law on Türkiye's National Intelligence Agency greatly increases its surveillance powers while threatening journalists who expose its abuses with prison terms. The law would decrease state accountability, media freedom, and the right to privacy. Several of its key provisions should be amended without delay because they violate Türkiye's obligations under international human rights law and domestic laws. Under the law, journalists and editors who publish leaked

intelligence material are liable to jail terms of up to nine years» (HRW, 2014).

En 2017, la Comisión de Venecia del Consejo de Europa alertó que los decretos de emergencia de Türkiye tras el golpe de 2016 tuvieron efectos adversos en las capacidades de contraterrorismo del Estado. Se reforzó el control político, pero se erosionó la resiliencia institucional y operacional al purgar de manera masiva la policía, el ejército y la judicatura. La Comisión advirtió que un Estado que concentra poder sin controles aumenta su vulnerabilidad a largo plazo. Esta llamada de atención resulta esencial para comprender los límites de las políticas ultraagresivas de Türkiye: si las herramientas de seguridad se aplican e implementan de manera desproporcionada y sin rendición de cuentas, el resultado siempre será más inestabilidad. Tal y como alertó Mateusz Chudziak (2016), investigador del Centre for Eastern Studies, la eliminación de personal experto en seguridad, justicia e inteligencia, bajo el pretexto de la lucha antiterrorista, mermó temporalmente la eficacia del Estado frente a la amenaza terrorista.

«Following the failed *coup d'état* of 15 July 2016, which was immediately condemned by the President of the Venice Commission, the Turkish Government declared the state of emergency and started legislating through emergency decree laws [...] It is particularly worrying that, through emergency legislation, the central authorities are enabled, in the framework of the fight against terrorism, to appoint unelected mayors, vicemayors and members of local councils, and exercise, without judicial control, discretionary control over the functioning of the concerned municipalities» (Venice Commission, 2017: 3-21).

A pesar de la centralización del poder y de la hiperpresidencialización llevada a cabo por Erdoğan, las medidas represivas posteriores adolecieron de ineficacia y mostraron límites importantes: la experiencia comparada y los análisis publicados hace ya una década advertían a Türkiye que unas políticas demasiado coercitivas, basadas únicamente en la represión, podían resultar contraproducentes, generando más radicalización entre hombres, mujeres y niños. Cuando la acción estatal se percibe como indiscriminada o excesivamente punitiva, los grupos extremistas explotan esa narrativa para reclutar nuevos seguidores. La creciente islamización de la esfera pública bajo el AKP, sumada a la represión de disidentes laicos, alevíes o kurdos, refuerzan de

forma indirecta la propaganda yihadista que se presenta como defensora auténtica del islam frente a un Estado turco percibido como autoritario (Taş, 2018).

Tras levantar el estado de emergencia en 2018, el Gobierno turco aprobó una nueva ley antiterrorista que, en palabras de la oposición, equivale a un «estado de emergencia permanente» bajo la excusa de la lucha contra el terror como sostienen desde HRW (2018). Esta ley extendió de cuatro a doce días el período de detención preventiva sin cargos, amplió los motivos para prohibir manifestaciones y permitió retirar el pasaporte tanto a funcionarios destituidos tras el golpe como a sus familiares. Además, otorgó a los servicios de inteligencia una casi total impunidad legal, quedando sus operaciones internas «fuera de cualquier escrutinio público» (HRW, 2018: 560). Estos cambios normativos consolidaron la securitización del disenso: las autoridades disponen ahora de herramientas legales para criminalizar actividades opositoras bajo tipificaciones vagas de terrorismo y amenaza a la seguridad nacional.

Existen varios casos que ilustran el uso discrecional de las normas de seguridad para penalizar el disenso político y muestran que, en la Türkiye contemporánea, las leyes antiterroristas se utilizan habitualmente para procesar a periodistas, académicos, activistas y políticos opositores, con cargos genéricos como «propaganda terrorista» o «pertenencia a organización armada» que a menudo carecen de fundamento real (Freedom House, 2023). Por ejemplo, en 2023, un tribunal condenó a una veintena de dirigentes kurdos a largas penas de prisión por publicar en redes sociales contenidos relativos a las protestas de Kobane 2014. Los posts fueron interpretados *ex post facto* como incitación terrorista (HRW, 2024). En 2025, la detención del alcalde de Estambul, Ekrem İmamoğlu (Amnesty International, 2025b), desencadenó una ola de protestas multitudinarias en todo el país. Una declaración conjunta de Amnistía Internacional y ARTICLE 19 entre otras organizaciones denunciaron el uso abusivo de las leyes de orden público y antiterroristas para restringir la libertad de reunión y expresión, reclamando al Gobierno que cesara los ataques contra manifestantes pacíficos, periodistas y voces críticas. Posteriormente, un informe específico de Amnistía Internacional sobre la represión de las protestas de marzo halló patrones de uso ilícito de la fuerza —gases lacrimógenos, proyectiles de impacto cinético, cañones de agua y malos tratos bajo custodia— que, en algunos casos, «podrían equivaler a tortura u otros tratos crueles, inhumanos o degradantes» (2025b: 2).

3 Ciberespacio: control y securitización del dominio informativo

El panorama de ciberamenazas, a nivel global, refleja un incremento tanto en volumen como en complejidad técnica de los ataques, lo que puede acarrear efectos devastadores para cualquier actor del panorama internacional. En el caso particular de Türkiye, el país se enfrenta a una creciente sofisticación de ciberataques que provocan interrupciones en servicios esenciales, pérdidas económicas significativas y merma de la confianza ciudadana en la economía digital (SETA, 2025). Además, su rápida transformación digital y su importancia regional han atraído la atención de grupos *hackers* y actores estatales hostiles.

El *National Cyber Security Index* (NCSI) elaborado por la *e-Governance Academy* de Estonia, ubica a Türkiye en el lugar 50.º de 126 países en su *ranking* de 2025. La precisión de este diagnóstico revela una valoración baja en capacidad de gestión de crisis cibernéticas (22 %), en contraste con una alta puntuación en ciberdefensa militar (67 %) y de lucha contra el cibercrimen (81 %) (NCSI, 2025). Esta particular asimetría refleja que la robusta capacidad defensiva de Ankara coexiste con una limitada preparación de cara a gestionar crisis de gran escala. Esta valoración se explica por la implementación parcial de la Estrategia Nacional 2024-2028 (Presidencia de la República de Türkiye, 2024) y por la aplicación fragmentada de políticas de ciberseguridad por parte de la Autoridad de Tecnologías de la Información y la Comunicación. Aunque en apartados posteriores se comentará con mayor detalle la arquitectura legal a nivel cibernético, resulta de interés señalar que la BTK, como organismo regulador encargado de supervisar las telecomunicaciones y el uso de Internet, ha intentado construir una defensa cibernética nacional más robusta a través de medidas concretas como la *Tedbir 581.4*, relativa a la inteligencia de amenazas mediante IA y *big data* o la difusión intersectorial de protocolos para proteger infraestructuras críticas durante emergencias.

Empresas de monitorización de ciberamenazas como ThreatMoN dibujan un panorama preocupante de estas amenazas emergentes, donde los ciberataques y las actividades en la dark web plantean riesgos crecientes. El uso delincencial de la *dark web*, la expansión de los *ransomware* y la diversificación de las amenazas avanzadas persistentes (APT) conforman un triángulo de riesgo creciente para Ankara. Y no se deben obviar otras vulnerabilidades

de alto nivel como la venta de datos médicos sensibles turcos con información personal, el secuestro de credenciales militar con acceso a redes gubernamentales o el intento de venta del dominio «.gov» del Gobierno:

«Türkiye is rapidly transforming into a critical player in the global digital landscape. However, this advancement comes with heightened cybersecurity risks. The 2025 National Cyber Threat Report provides a comprehensive analysis of the growing threats and regulatory changes shaping Türkiye’s cybersecurity environment. Dark web marketplaces continue to be a hotbed for the sale of sensitive Turkish data, including personal information and government access credentials. High-profile incidents include the sale of data from a Turkish nursery and unauthorized access to a retail company’s internal systems. The attempted sale of a .gov domain controller further underscores the need for stronger defense measures» (ThreatMoN, 2025).

Según el análisis de ThreatMon los ataques de *ransomware* se han intensificado, afectando a sectores clave como la industria tecnológica, la manufactura, la sanidad y las finanzas. Grupos criminales identificados como *RansomHub*, *Hellcat* y *FunkSec* han llevado a cabo intrusiones que paralizaron operaciones empresariales y comprometieron datos sensibles, contando entre sus víctimas a destacadas compañías turcas de software y alimentación. Del mismo modo, cibercriminales y piratas asociados a terceros Estados han incrementado el uso de APT y ampliado las campañas de ciberespionaje contra infraestructuras críticas. Se ha detectado una actividad creciente de grupos vinculados a Estados como *Promethium*, piratas informáticos iraníes y colectivos prrusos, como «Cozy Bear» (*APT29/Nobelium*), «Fancy Bear» (*APT28/Sofacy*) que focalizan sus ataques en sectores estratégicos como la administración pública, la energía o el aeroespacial (Yuldoshkhujaev *et al.*, 2025). Estos sujetos emplean técnicas sofisticadas para sustraer información sensible o sabotear capacidades, en consonancia con las tensiones geopolíticas de la región.

3.1 Desinformación y amenazas digitales

Desde instancias de la Unión Europea en general y desde el Parlamento Europeo en particular han advertido que actores extranjeros realizan con asiduidad campañas de manipulación

o *Foreign Information Manipulation Interference* (FIMI), destinadas a difundir narrativas manipuladoras en el entorno informativo turco y así provocar pérdidas de cohesión democrática² (European Commission, 2025). Por ejemplo, en marzo de 2025, el Servicio Europeo de Acción Exterior hacía énfasis en que la operación *Doppelgänger*³, campaña FIMI atribuida a Rusia y activa desde 2022, operaba en el idioma turco para generar caos, división y polarización social (European External Action Service, 2025). Desde la perspectiva del gobierno local, esta problemática de carácter híbrido y cibernético se percibe como una cuestión de seguridad nacional de primer orden y han enfatizado el riesgo que representan las campañas de desinformación masiva. En la cumbre STRATCOM21, organizada por la Dirección de Comunicaciones de la Presidencia, Erdoğan exponía su visión al respecto:

«La desinformación se ha convertido en un problema de seguridad global. Las democracias desarrolladas del mundo están en alerta máxima ante el creciente fascismo digital y la ola de noticias falsas. La desinformación ha trascendido el concepto de seguridad nacional y se ha convertido en un problema de seguridad global. [...] Las redes sociales, descritas como un símbolo de la libertad cuando surgieron, se han convertido en una de las principales fuentes de amenaza para la democracia actual» (Erdoğan, citado en Özkan, 2021).

Desde 2021, en Ankara sostienen que actores malintencionados están explotando el ecosistema digital para polarizar a la sociedad turca, difundir propaganda extremista o sembrar caos

² Véase: European Commission (2025), *Türkiye 2025 Report*, donde se exponen las preocupaciones de la UE: «The EU's serious concerns about the continued deterioration of democratic standards, the rule of law, the independence of the judiciary and respect for fundamental rights were not addressed. The arrests of and charges brought against elected officials, opposition figures, political activists, civil society and business representatives, journalists, and others since the beginning of 2025, gave rise to increasing questions regarding Türkiye's adherence to its democratic tradition, and deepened concerns about the independence of the judiciary».

³ Véase: European External Action Service (2025), *3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations*, donde se señala que «Doppelgänger is a FIMI campaign attributed to Russia, active since mid-2022. According to data collected by the EEAS, it consists of 228 domains and 25,000 CIB networks operating across nine languages: English, German, French, Spanish, Turkish, Polish, Arabic, Hebrew and Italian. The campaign has a prominent presence within the Russian FIMI infrastructure and has been linked to 60 documented incidents in the analyzed sample».

durante procesos políticos críticos, como elecciones o referéndums: «Intentamos proteger a nuestro pueblo, en especial a los sectores vulnerables de nuestra sociedad, de las mentiras y la desinformación sin violar el derecho de nuestros ciudadanos a recibir información precisa e imparcial» (Erdoğan, citado en Independent, 2021). Tiempo después, en 2023, en la cumbre STRATCOM23 el presidente de la república turca hacía un nuevo llamamiento a luchar contra la desinformación: «Necesitamos librar una lucha integral contra los efectos destructivos de la desinformación que corrompe la democracia y atenta contra los derechos y las libertades individuales» (Erdoğan, 2023). El lema de esa cumbre fue la «lucha global contra las amenazas híbridas», haciéndose evidente que el país había adoptado ya un enfoque cada vez más vigilante y proactivo en el control de la información.

El problema estaba en que, bajo el argumento de proteger a la población de las amenazas digitales, la desinformación y las *fake news*, el aparato del Estado estaba comenzando a desplegar un conjunto de instrumentos que hacían inviable lograr un equilibrio entre la seguridad informativa y la libertad de los medios de comunicación. Y, tal y como se advierte desde instancias europeas, eso constituye el desafío más complejo al que se enfrenta Türkiye:

«With regard to hybrid threats, in the context of international conflicts and crises, the circulation of false information and propaganda on social and mainstream media was observed also in the Turkish information environment. Türkiye did not restrict the operations of Russian media outlets in the context of the Russian aggression against Ukraine. In addressing disinformation, it is crucial that Türkiye does not restrict further the freedom of media, but that it implements, in an objective and proportionate manner, any legal framework aimed at preventing the spread of false information» (European Parliament, 2022).

3.2 Marco legal y lucha contra la desinformación

Ante el panorama disruptivo que emana del ciberespacio, Türkiye ha adoptado medidas legales específicas para responder a las amenazas híbridas en el campo de la información y controlar el espacio virtual y digital. En 2022, fue aprobada la Ley N.º 7418, conocida como la Ley de Lucha contra la Desinformación (República de Türkiye, 2022), mediante la cual se tipificó como

delito penado con tres años de cárcel la difusión de «información falsa» que amenace la seguridad, el orden público o la salud pública. Además, como apuntan desde el despacho Elig Gurkaynak (2022), se reforzó el control gubernamental sobre los sitios de noticias en línea y las redes sociales, obligando a las plataformas digitales con más de un millón de usuarios a establecer representación legal en Türkiye —exigencia ya introducida en 2020— y a acatar órdenes de retirada de contenido y entrega de datos de usuarios, bajo pena de severas sanciones (Amnistía Internacional, 2022)

En 2024, el Gobierno elabora la *National Cyber Security Strategy and Action Plan 2024-2028* (R.T. Ministerio de Transportes e Infraestructuras, 2024) y se establecen las prioridades nacionales en materia de ciberseguridad: protección de infraestructuras críticas, capacidades de respuesta a incidentes, gobernanza digital, cooperación internacional. La Estrategia hace una diagnosis de la situación geopolítica y de la vulnerabilidad cibernética del país: «Due to its geopolitical importance, economic structure and the leaps in the field of technology especially it has made in recent years, our country is an attraction point for cyber threat actors» (R.T. Ministerio de Transportes e Infraestructuras, 2024: 7). En la introducción, el presidente habla de la necesidad de generar disuasión cibernética y de que Türkiye no solo sea un país que use tecnología, sino que también la produzca.

«The key issue is to have a strong cyber defense on a national scale [...] With the increase in cyber threat actors and attack vectors, threats have become increasingly complex, and the emergence of hybrid threats that include cyber threats reveals that the approach to cyber defense to counter these forces must be developed simultaneously and proportionately» (R.T. Ministerio de Transportes e Infraestructuras, 2024: 6-18).

El documento publicado por el Ministerio de Transportes e Infraestructuras en 2024 identifica nueve metas operativas, entre las que destaca la cuarta, enfocada en potenciar la ciberseguridad y proyectar la confianza del usuario. Esta meta articula un conjunto de medidas concretas que incluyen: la creación de una mesa de coordinación diaria, integrada por la Presidencia de Ciberseguridad, la Organización Nacional de Inteligencia, el regulador bancario y los principales operadores de infraestructuras críticas; la expansión anual del Centro Nacional de Respuesta a Incidentes con el despliegue de sensores basados en inteligencia

artificial y plataformas de análisis de grandes volúmenes de datos, capaces de procesar más de tres millones de eventos diarios y la obligatoriedad de que los equipos provinciales de respuesta a incidentes conocidos como *SOME* obtengan la certificación de seguridad emitida por el Instituto Turco de Estándares, además de intercambiar indicadores de compromiso en tiempo real a través de la Red de Inteligencia de Amenazas Turca. El plan contempla, asimismo, la elaboración de la normativa secundaria que regule la firma electrónica remota; la aprobación de un protocolo de emergencia y gestión de crisis cibernéticas que garantice la recuperación de infraestructuras críticas en menos de veinticuatro horas y el desarrollo de campañas de ciberhigiene. Todo ello contribuye a consolidar la supervisión del espectro radioeléctrico, la seguridad de las redes de quinta generación y la confianza en el comercio electrónico, bajo una arquitectura de respuesta integrada y de funcionamiento continuo.

En 2025, consciente del desafío cibersecuritario, Erdoğan decidió establecer la «Dirección de Ciberseguridad» bajo el control de su presidencia, lo que demuestra su intención de ser un actor decisivo en el ámbito digital (Kizilaslan, 2025). Meses después, Türkiye aprobó la Ley N.º 7545 o Ley de Ciberseguridad (República de Türkiye, 2025), mediante la cual se declara la ciberseguridad como una prioridad nacional. Entre sus ejes principales, destacan la protección de infraestructuras críticas y datos sensibles, la promoción de soluciones nacionales en ciberdefensa, y la mejora continua de políticas y capacidades de seguridad. Su ámbito de aplicación es excepcionalmente amplio, aplicándose a autoridades públicas, instituciones, personas naturales y jurídicas, y entidades sin personalidad jurídica que existan, operen o presten servicios en ciberespacio, definido este último como un entorno que abarca todos los sistemas de información conectados directa o indirectamente a Internet, comunicaciones electrónicas o redes informáticas.

Tal y como queda reflejado en el artículo 9 de la Ley N.º 7545, su aprobación trae consigo la creación del «Consejo de Ciberseguridad», que será el encargado de establecer la política nacional, determinar infraestructuras críticas, resolver conflictos de competencia y aprobar la hoja de ruta tecnológica nacional. Asimismo, se fortalece la Presidencia de Ciberseguridad como autoridad central encargada de hacer cumplir la ley, realizar auditorías, coordinar equipos de respuesta a incidentes y gestionar la inteligencia de amenazas cibernéticas, incluyendo la cooperación internacional (TRT Haber, 2025).

La nueva normativa también impone exigentes requisitos de seguridad y notificación a las organizaciones: deberán realizar evaluaciones de riesgo periódicas, implementar medidas de protección adecuadas en sus sistemas de información y reportar con prontitud cualquier incidente al órgano competente (Kizilaslan, 2025). Asimismo, empresas y agencias deben establecer equipos internos de respuesta a incidentes y usar productos de seguridad certificados por la Presidencia de Ciberseguridad. Las sanciones por incumplimiento se han endurecido notablemente, incluyendo penas de prisión para delitos informáticos graves. La ley hace referencia a casos diversos entre los que se contempla la difusión no autorizada de datos relacionados con servicios públicos esenciales, que puede conllevar de tres a cinco años de cárcel, mientras que los ciberataques que comprometan la seguridad nacional podrían penarse con diez a quince años de prisión.

3.3 Vigilancia estatal y control del flujo de información

Desde la reforma de 2014 a la Ley de Inteligencia, y amparándose en la lucha contra amenazas terroristas e híbridas, Türkiye ha intensificado las capacidades de seguimiento electrónico y ha ensamblado un marco normativo que convierte la vigilancia masiva en una política de Estado (Freedom House, 2025). Un ejemplo es que el MIT tiene ahora potestad para intervenir líneas y recolectar metadatos sin supervisión judicial efectiva. Ante este escenario, el Parlamento Europeo ha advertido que Türkiye se ha convertido en el país con el marco legal más restrictivo para el periodismo digital de la zona euroasiática, un punto que ya había sido denunciado en 2023 cuando instituciones europeas dijeron que la Ley de Desinformación constituía una amenaza para la libertad de expresión del país.

«A highly concentrated and government-controlled media environment can lead to an informational autocracy, where the state or malign foreign actors can easily exert influence through the manipulation of information [...] Denounces signs of Turkish interference and persecution of political activists, opposition leaders and minorities within the EU; condemns Türkiye's new Disinformation Law proposal, which poses a threat to the freedom of speech in the country» (European Parliament, 2023).

La aplicación de la actual legislación turca se traduce en bloqueos de Internet cada vez que estalla una crisis política: En 2016,

durante el intento de golpe de Estado de 2016, se cortó Twitter, YouTube y Wikipedia; En 2020, mientras los incendios forestales arrasaban el Mediterráneo turco, las autoridades redujeron el ancho de banda de Twitter e Instagram durante veinticuatro horas para contener las críticas a la escasa respuesta estatal. En 2021, Signal sufrió un bloqueo selectivo de veintitrés horas tras ser utilizado por estudiantes universitarios para coordinar protestas contra el nombramiento de un rector afín al Gobierno en el Bósforo. En 2025, durante las protestas desencadenadas por la detención del alcalde de Estambul, el Gobierno recurrió de nuevo a cortar el ancho de banda y los habitantes de Estambul experimentaron redes sociales prácticamente inaccesibles durante 42 horas seguidas (Amnistía Internacional, 2025a). Tal y como apuntan desde el Open Observatory of Network Interference OONI (2025), Twitter/X, Instagram, TikTok, YouTube, WhatsApp y Signal fueron reducidos al 8 % de su capacidad, mientras que Telegram quedó completamente inaccesible para los usuarios de las redes TNET y Turkcell Superonline. En paralelo, se exigió a la plataforma fundada por Jack Dorsey la suspensión de cuentas de opositores políticos sin mandamiento judicial, como parte de la respuesta a dichas protestas. Expertos legales turcos denunciaron el carácter arbitrario de estas medidas extrajudiciales, señalando que se adoptaron bajo la pretensión de evitar supuestas noticias falsas, pero en ausencia de base legal transparente. Como denuncia Yaman Akdeniz, profesor y director de Türkiye's Freedom of Expression Association —İfade Özgürlüğü Derneği (İFÖD)—, Türkiye avanza hacia un «Estado de vigilancia», donde las herramientas digitales se emplean para la censura preventiva y el control social.

«There was no court decision behind the bandwidth reduction or the bid to block X accounts. These measures were put in place arbitrarily [...] We are moving towards a surveillance state [...] By law, the BTK can only keep the data collected for two years. However, we have seen data going back 10 years being provided to prosecutors during the investigation into the Istanbul mayor. This data retention, despite the law, for purposes which are unknown, opens the way for arbitrary practices. With facial recognition the government is trying to discourage people from joining demonstrations, while hindering their mobilization through social networks» (Akdeniz, 2025).

El control no se limita al corte de canales, ya que el Estado también ha desplegado una infraestructura de vigilancia de miles de

cámaras equipadas con algoritmos de reconocimiento facial que convierten la calle en una extensión del espacio digital y que ha alcanzado niveles orwellianos tal y como señala la periodista de investigación Ylenia Gostoli (2025): «Türkiye is not hiding its ambitions to expand AI-driven security». En las protestas de 2025, el tejido de videovigilancia identificó a un ingente número de manifestantes en solo cuarenta y ocho horas, permitiendo detenciones selectivas durante la noche siguiente. En este contexto de control estatal, İFÖD junto con otras organizaciones publicaba en mayo de 2025 una carta abierta a las empresas de redes sociales sobre la censura en Türkiye⁴ (IFOD *et al.*, 2025).

La Dirección General de Seguridad, con sus unidades especializadas en ciberdelincuencia y análisis de redes sociales, completa el denominado círculo de control y monitorización: tiene capacidad de procesar millones de publicaciones de Twitter, Instagram o TikTok para generar mapas de influencia y marcar usuarios con «potencial de radicalización», una información que luego cruza con los historiales de navegación que la autoridad de tecnologías BTK conserva durante diez años, violando el límite legal de dos años previsto en la Ley 5651. El resultado es un archivo acumulativo que permite construir causas penales por publicaciones de hace una década. Esta atmósfera de censura generalizada, donde cada clic queda registrado y puede ser utilizado retroactivamente, convierte cualquier manifestación en un laboratorio de identificación masiva: a diferencia de lo que ocurrió en las protestas de Gezi en 2013 cuando los activistas dominaban las redes, hoy cada rostro visible puede ser registrado, vinculado a una identidad, una dirección y, por ende, acusado penalmente.

«Türkiye's scale of censorship staggers: by the end of 2024, the total number of websites and domain names blocked in the past years reached 1,264,506, as documented by Dr. Yaman Akdeniz of the Freedom of Expression Association (İFÖD). İFÖD's latest report shows that 5,740 news articles scraped last year were based on 803 court orders. Amid the crackdown, some persist in pushing back» (Inform, 2025).

Frente a este escenario, la sociedad civil ha tejido redes de resistencia que combinan tecnología y autoorganización. Si se estudian los informes de Freedom House, MLSA, NetBlocks, Access

⁴ Véase: IFOD *et al.* (2025). Carta dirigida a Mark Zuckerberg, Chief Executive Officer, Meta; Shou Zi Chew, Chief Executive Officer, TikTok; Neal Mohan, Chief Executive Officer, YouTube; Linda Yaccarino, Chief Executive Officer, X.

Now, Top10VPN o ProtonMail se puede visualizar que entre 2020 y 2024, el uso de redes privadas virtuales o VPN en Türkiye experimentó un crecimiento significativo, especialmente coincidiendo con episodios de bloqueo de redes sociales y restricciones informativas. Informes de proveedores de servicios y de organizaciones de monitorización de Internet indican que, durante los cierres de marzo y septiembre, el tráfico asociado a VPN se multiplicó varias veces respecto a los niveles habituales, situando a Türkiye entre los países con mayores picos de uso de estas herramientas en contextos de censura digital (Migliano, 2025).

En las calles, los manifestantes han recuperado el pañuelo y la gorra como barrera facial, pero también experimentan con maquillaje antirreconocimiento y gafas cuyos patrones desorientan a las cámaras de vigilancia y sus algoritmos de identificación; colectivos como *DigitalMask* difunden plantillas de «rostros adversariales» que reducen el éxito de la tasa de identificación (SWI, 2025a). En los tribunales, la asociación İFÖD y el Colegio de Abogados de Estambul (Istanbul Bar Association) han presentado más de sesenta demandas de inconstitucionalidad contra la Ley de Ciberseguridad y los bloqueos de 2025, cuyos fallos están aún pendientes⁵.

El Gobierno, sin embargo, mantiene la línea marcada por el presidente y multiplica frentes. Cuando la censura técnica no basta, recurre a la desinformación oficial: durante las protestas de 2025, el presidente Erdoğan acusó a los manifestantes de «sembrar el terror», cometer vandalismo y profanar mezquitas, afirmaciones que a pesar de ser desmentidas por imágenes de vídeo lograron deslegitimar la movilización ante sectores conservadores (Mourenza, 2025). Esta contrainsurgencia narrativa⁶ (Amnesty International, 2021) funciona como extensión de la censura técnica: si no es posible impedir la protesta, al menos se erosiona su legitimidad. El resultado es un círculo cerrado en el que la ley habilita la vigilancia, la tecnología identifica, la censura silencia y la desinformación desacredita, colocando a Türkiye en el puesto 159/180 del *ranking* de libertad de prensa de Reporteros Sin Fronteras (2025).

Desde el Palacio Blanco (*Ak Sarayı*) se defiende la necesidad de regular el ecosistema digital para proteger a la ciudadanía frente a la avalancha de bulos y campañas malintencionadas. Altos

⁵ Véase: Amnesty International (2025c).

⁶ Véase: Amnesty International (2021).

cargos, incluido el presidente Erdoğan, rechazan las acusaciones de deriva autoritaria y enfatizan en cambio «el perjuicio disruptivo de la desinformación» en la sociedad contemporánea como apuntaba Fahrettin Altun (2023), director de Comunicaciones de la Presidencia de Türkiye durante el periodo 2018-2025. Burhanettin Duran, actual director de Comunicaciones, mantiene la misma línea señalando incluso que muchos países occidentales están legislando contra las *fake news* y alegando que Türkiye tiene el derecho soberano a hacer lo propio para salvaguardar su democracia (Dayly Sabah, 2025). Eso no impide que observadores independientes subrayen que la clave estará en cómo se interprete y ejecute la ley: usada con prudencia podría atajar campañas maliciosas, pero usada de forma partidista podría estrechar aún más el espacio de debate público (Hassan, 2025). Inquieta y preocupa como este conjunto de arquetipos legales se utilizarán para cercar el debate público meses antes de las elecciones presidenciales de 2028.

Conclusiones

A lo largo de los últimos diez años, la forma en la que Türkiye ha percibido y gestionado sus riesgos ha ido evolucionando conforme se han transformado los fenómenos que afectan a su seguridad. El análisis de las tres amenazas objeto de estudio, entendidas como los principales riesgos a la estabilidad y la unidad nacional de Türkiye, demuestran que el país liderado por Erdoğan es tan poderoso como estable es su seguridad interior. Así, la política exterior y la política interior están interconectadas, demostrando que es correcto afirmar que la capacidad de proyección regional y global de Ankara está plenamente condicionada por la evolución de la insurgencia, el terrorismo y la ciberseguridad a nivel interno.

En torno a Türkiye y su estrategia contraterrorista

En el tiempo transcurrido de 2016 a 2026, Türkiye se ha consolidado como una potencia regional y ha revolucionado con notable éxito su estrategia contraterrorista. A la par que ha hecho frente al PKK tanto en su territorio como fuera de él, en Siria e Irak, Ankara ha adaptado sus tácticas operativas y sus capacidades de inteligencia para gestionar de manera preventiva y proactiva la amenaza del terrorismo. Como razona Murat Yeşiltaş (2025), director de Política Exterior de la Fundación SETA, las mejoras

que se han visto en la estrategia contraterrorista implementada por Türkiye se deben, por un lado, al cambio de paradigma y entendimiento de la amenaza, y por otro, a las transformaciones tácticas y operacionales a la hora de combatir a los diferentes grupos terroristas sobre el terreno.

En relación con el cambio de paradigma y entendimiento de la amenaza, Erdoğan ha ido integrando y sincronizando esfuerzos políticos, securitarios, económicos y tecnológicos para reforzar la capacidad global del Estado a la hora de neutralizar ataques terroristas, intervenir sus comunicaciones, frenar su financiación y desbaratar sus procesos de captación y reclutamiento. Si en 2016 la estrategia contraterrorista turca se basaba en un plan de acción-reacción y, en consecuencia, era cortoplacista y unidimensional, en 2026 el prisma ha cambiado por completo y los esfuerzos destinados al contraterrorismo se conciben desde una perspectiva multidimensional y a largo plazo. Antes, parecía limitarse a reaccionar ante ataques terroristas contra objetivos estratégicos militares, especialmente en el sureste del país. Ahora, la estrategia contraterrorista apuesta por operaciones militares y de seguridad constantes y preventivas.

Según el terrorismo evolucionaba y se transformada en un fenómeno más líquido, reticular y resiliente, Türkiye transformaba su concepción del fenómeno en cuestión y pasó a interpretarlo como una amenaza estructural que requería de nuevos enfoques y capacidades: Ankara ahora trabaja simultáneamente en el espacio físico y en espacio virtual, combina sutiles operaciones de inteligencia con notorias operaciones policiales y militares, actúa en grandes centros urbanos y en aisladas zonas rurales y aplica su *hard power* en plena conexión con su *soft power* y su *sharp power*.

En relación con las transformaciones tácticas, debe señalarse que la razón del éxito de las últimas actuaciones policiales en las que se detuvieron a más de trescientos cincuenta terroristas vinculados al yihadismo salafista se haya en la innovación operativa y la actualización tecnológica (Pluvinet, 2025). Desde la purga posterior al golpe de Estado hasta el presente año 2026, se ha visto con claridad cómo Türkiye ha dedicado una gran cantidad de recursos a su capacitación tecnológica y a los programas de entrenamiento de los diferentes cuerpos de seguridad destinados hacer frente a las organizaciones terroristas identificadas en su «Estrategia de Seguridad Nacional 2024-2028». Las reformas efectuadas bajo la batuta de Erdoğan y el empoderamiento de

estaba sufriendo ataques cibernéticos que afectaban a las infraestructuras críticas, a la gobernanza y a la opinión pública. Cabe destacar las advertencias emitidas desde el Servicio Europeo de Acción Exterior relativas a la campaña FIMI DOPELGÄNGER atribuida a Rusia, las operaciones detectadas por ThreatMon relativas a los sabotajes e injerencias efectuados por grupos ciber criminales como *RansomHub*, *Hellcat* y *FunkSec*, o el uso intensivo del ciberespacio por parte de organizaciones terroristas como Daesh o el PKK. A ello se suman el robo de información de millones de ciudadanos por parte de piratas informáticos (Yinanç, 2016) y la continua violación de datos de decenas de millones de personas, señalada por el experto en seguridad virtual Minhac Çelik (2025). Estas y otras muchas acciones dañinas recurrentes, han evidenciado la vulnerabilidad cibernética turca.

Por todo ello, Erdoğan ha decidido incorporar plenamente el dominio digital a su arquitectura de seguridad nacional, integrándolo de forma explícita en una concepción ampliada de soberanía que articula el *Kara Vatan*, el *Mavi Vatan* y el *Siber Vatan* como espacios interdependientes, tal y como sostiene el Plan Estratégico 2024-2028. Desde una perspectiva estrictamente operativa, tal y como explicó el Gobierno turco en la cumbre STRATCOM23, Ankara ha demostrado una creciente capacidad para identificar, atribuir y responder a ciberataques, amenazas híbridas y campañas de desinformación procedentes de rivales endógenos y exógenos como organizaciones terroristas, grupos opositores insurgentes o terceros estados. La aprobación concatenada de cuatro Estrategias Nacionales de Ciberseguridad (2013-2014, 2016-2019, 2020-2023 y 2024-2028), el desarrollo del *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028* como Plan de Acción plenamente integrado, el impulso de la primera norma integral y específica de ciberseguridad materializado en la Ley de Ciberseguridad de 2025 (Ley N.º 7545), la aplicación de la Ley de Lucha contra la Desinformación (Ley N.º 7418), la creación de la Presidencia de Ciberseguridad por decreto presidencial, el reporte directo de todas las estructuras y agencias al presidente Erdoğan y el impulso de la industria nacional para el desarrollo de cibercapacidades tecnológicas propias, demuestran continuidad política, maduración técnica progresiva y consolidación de la resiliencia cibernética del Estado frente a un entorno informativo crecientemente hostil.

Si bien todas estas acciones de medio y largo alcance son positivas y necesarias, diversos organismos y entidades han alzado la voz

determinados ministerios, organismos y entidades como el MİT o la BTK han hecho posible que Ankara controle la práctica totalidad del dominio operacional y, por ende, incrementa su capacidad de dismantelar las redes establecidas por los diferentes grupos terroristas que actúan en su zona de influencia.

En este momento, tal y como se desprende del Panorama Geopolítico de los Conflictos 2025 (Sánchez, 2025: 119), Türkiye está combinando de manera efectiva la experiencia en combate acumulada durante más de cuatro décadas por parte de sus efectivos policiales y militares, con el desarrollo de punteras capacidades tecnológicas gracias al trabajo de entidades como Tübitak Sage y de empresas como Aselsan, Havelsan, TAI, Roketsan, Baykar o MKE. En relación con el ámbito tecnológico y la industria de la defensa aplicada al contraterrorismo y la contrainsurgencia, hay que destacar el proyecto Steel Dome o *Çelik Kubbe* impulsado desde 2024 por el Comité Ejecutivo de la Industria de Defensa (SSİK); los UAV Anka-III, Aksungur y Super Şimşek desarrollados por TAI; los UAV Bayraktar TB2, TB3, Akinci y el Kizilelma, diseñados por Baykar y los sistemas de guerra electrónica, videovigilancia, reconocimiento facial e inteligencia artificial desarrollados por Aselsan y Havelsan. Así, las tecnologías aplicadas a la vigilancia y monitoreo de redes sociales y espacios públicos, las nuevas tácticas y estrategias contraterroristas, las mejoras en los entrenamientos, la actualización de los ciclos de inteligencia y la mejora de los mecanismos de colaboración e intercambio de información con países europeos han ayudado de manera indudable a prevenir nuevos ataques terroristas.

Ahora bien, el escenario también presenta retos, preocupaciones e incertidumbres. A pesar de los avances operativos y tecnológicos, los logros alcanzados son frágiles, reversibles y profundamente dependientes de factores estructurales no resueltos. La potencia regional liderada por Erdoğan ha demostrado una capacidad notable para neutralizar amenazas inmediatas, pero no ha logrado desactivar las condiciones que las generan. En este sentido, el posconflicto kurdo, la mutación del yihadismo y las amenazas híbridas del ciberespacio configuran un triángulo de riesgos estructurales que podrían desencadenar una nueva ola de violencia o una crisis de legitimidad estatal en el medio o largo plazo.

En torno a Türkiye y el PKK

Si se atiende al PKK, queda claro que se habla de un conflicto enquistado y cronificado donde destaca una perpetua espiral de

violencia terrorista que trasciende fronteras. El anuncio de disolución difundido por parte de la organización en 2025 no transmite demasiada confianza si se recuerdan las múltiples e infructuosas declaraciones de alto al fuego comunicadas en 2002, 2006, 2009 o 2013. Por otro lado, el citado anuncio no ha venido acompañado, al menos por el momento, de un proceso de paz inclusivo, transparente y con participación civil significativa. Tampoco le ha acompañado un proceso de desarme, desmovilización o reintegración de combatientes (DDR). El hecho de que no se hayan efectuado reformas políticas concretas o no se hayan abordado aún las demandas históricas del movimiento kurdo, genera recelo. Y al igual que ocurre en otros conflictos a lo largo del planeta, eso trae implícito un incremento del riesgo de fractura interna dentro del propio movimiento, donde facciones más radicales podrían romper el alto al fuego si perciben que la vía política está bloqueada.

Además, la influencia del PKK sobre las YPG en Siria sigue siendo un factor de tensión geopolítica, ya que Türkiye no puede negociar con ellas, pero tampoco puede ignorar su presencia en una zona fronteriza clave. Esto deja abierta la puerta a nuevas operaciones militares unilaterales, que alimentarán el ciclo de violencia.

Por todo ello, y a pesar de los anuncios de abandono de la lucha armada, el Estado turco no puede ni debe dejar de identificar al PKK como un desafío directo a la unidad nacional, como un reto a la supervivencia del Estado y como una amenaza estratégica a su seguridad. Al igual que ocurre con cualquier tipo de violencia armada de carácter étnico o nacionalista, el PKK es susceptible de mutar en intensidad y visibilidad, pero no de desaparecer completamente. De ahí que a Ankara le convenga mantener una lógica de contención permanente en el plano securitario y una lógica de diálogo constante en el plano político y social.

La resolución del conflicto kurdo es un requisito forzoso para que Türkiye pueda, desde el punto de vista operacional, actuar como una potencia regional y aspirar a ser un actor global en un futuro. Su capacidad de proyectar su poder en el exterior depende de cuán estable y segura sea su dimensión interna.

En torno a Türkiye y el Daesh

Si se atiende al terrorismo de etiología yihadista salafista de Daesh, es pertinente recordar que el descenso en el número de atentados no equivale a una derrota ideológica ni a un desmantelamiento estructural. La desarticulación de células en 2024 y

2025 confirman que el yihadismo no ha sido derrotado, sino descentralizado. Tal y como se destila del artículo *The Islamic State Is 'Back.'* *In Reality, It Never Went Away* de Clara Broekaert y Colin P. Clarke (2025), el Daesh ha ido desplazándose hacia formas menos jerárquicas y más autónomas e impredecibles.

Durante la última década, el yihadismo en Türkiye ha evolucionado hacia formas más difusas y digitales, con micro células que no dependen de una jerarquía central, sino de ideología, financiación y redes de reclutamiento que siguen activas en el ciberespacio y en barrios marginales. La radicalización *online*, la criminalización de la pobreza y la falta de programas de desradicalización convierten al país en un caldo de cultivo para una nueva generación de extremistas, especialmente entre jóvenes turcos y refugiados sirios que no ven salidas económicas ni sociales. Aunque la respuesta punitiva de las autoridades turcas sea cada vez más efectiva a la hora de desarticular células, no aborda las causas profundas de la amenaza tal y como advierte Peter Neumann (2025), director del Centre for the Study of Radicalisation.

Estas ideas son las que permiten afirmar que, a pesar de las notables mejoras descritas en los primeros párrafos de estas conclusiones, la política de seguridad turca ha generado una dinámica de retroalimentación negativa: la prioridad otorgada a la lucha contra el PKK ha limitado la cooperación con actores kurdos clave en Siria e Irak, dificultando el control de redes yihadistas. Y, al mismo tiempo, el endurecimiento del marco antiterrorista frente al yihadismo ha reforzado una narrativa securitaria que reduce el espacio político kurdo, alimentando tensiones que perpetúan el conflicto como sostiene Francesco Siccardi (2021), subdirector de Carnegie Europe. Türkiye encarna, por tanto, un dilema securitario que consiste en cómo contener la amenaza del terrorismo sin que el propio Estado se convierta en factor de inestabilidad. Ankara ha construido su arquitectura de seguridad sobre una base que reproduce los problemas que pretende resolver. La Ley 6532, que otorgaba inmunidad funcional al MİT, sumada a las purgas institucionales y a la securitización de la *Diyanet* han ayudado a combatir a Daesh y al PKK, pero también erosionan la confianza ciudadana, fragmentan la resiliencia social y generan nuevos reclutas para el extremismo.

En torno a Türkiye y el ciberespacio

Si se atiende al ámbito cibersecuritario, durante la última década se ha evidenciado que Türkiye, por su posición geoestratégica,

preocupados, porque el exceso de control merma las libertades de los ciudadanos turcos. La Unión Europea y actores no gubernamentales como el Comité para la Protección de los Periodistas, Human Rights Watch, ARTICLE19 o IFOD han denunciado estas políticas emprendiendo acciones legales y emitiendo comunicados conjuntos dirigidos a las grandes empresas tecnológicas como META y X para que no caigan en la censura gubernamental implementada por el Gobierno: «Under the United Nations Guiding Principles on Business and Human Rights (UNGPR), social media companies have a responsibility to respect human rights, which includes resisting government pressure to restrict freedom of expression in ways that violate international human rights law» (IFOD *et al.*, 2025).

La represión digital que sufre Türkiye continúa aumentando y es especialmente intensa tras el arresto Ekrem Imamoglu, alcalde de Estambul en marzo 2025, momento en el que plataformas como X o Bluesky acataron las órdenes judiciales turcas y cerraron sus dominios (Reci, 2025). Voces críticas con la implementación de la Ley de Ciberseguridad indican que prima el control de la seguridad por encima de los derechos, y que el texto legal se usa para silenciar la discrepancia o la información legítima contraria al hiperpresidencialismo de Erdoğan.

Como apunta Byung-Chul Han (2022), filósofo ganador del Premio Princesa de Asturias de Comunicación y Humanidades 2025, el poder de un Estado del siglo XXI reside en su capacidad de acceso a la información de sus ciudadanos para ejercer una vigilancia psicopolítica. Türkiye, con sus instrumentos actuales, tiene acceso a todo el flujo de datos que generan sus más de 85 millones de habitantes. Por un lado, eso le otorga el conocimiento y el poder para anticiparse de manera cada vez más ágil a los ciberataques y amenazas híbridas que ponen en riesgo se seguridad. Por otro lado, le otorga la capacidad de vigilar y controlar a los ciudadanos, condicionar los discursos, alterar los relatos, anular el disenso, reducir la pluralidad social y religiosa, y fragmentar la oposición política. En el medio plazo, este uso del poder derivado del dominio del *Siber Vatan* será útil para que Erdoğan controle el devenir de la voluntad política del país de cara a las elecciones presidenciales de 2028, pero a largo plazo reproducirá con más virulencia las amenazas que pretende enfrentar.

Bibliografía

- Akdeniz, Y. (2025). In Türkiye, new technologies reinforce repression [en línea]. *France24*. París. [Consulta: 22 enero 2026]. Disponible en: <https://www.france24.com/en/live-news/20250330-in-turkey-new-technologies-reinforce-repression>
- Al Jazeera. (2025a). PKK's jailed leader Ocalan says armed struggle against Türkiye over [en línea]. *Al Jazeera*. Doha, Qatar. [Consulta: 22 enero 2026]. Disponible en: <https://www.aljazeera.com/news/2025/7/9/pkks-ocalan-says-armed-struggle-against-turkiye-over>
- . (2025b). Kurdish PKK announces it is withdrawing fighters from Türkiye to Iraq [en línea]. *Al Jazeera*. Doha, Qatar. [Consulta: 22 enero 2026]. Disponible en: <https://www.aljazeera.com/news/2025/10/26/kurdish-pkk-announces-its-withdrawing-fighters-from-turkiye-to-iraq>
- Altun, F. (2023). Truth Is a Human Right: Türkiye's Stance on the Fight against, Disinformation [en línea]. *Insight Turkey*. 25(1). [Consulta: 22 enero 2026]. Disponible en: <https://www.jstor.org/stable/48720511>
- Amnesty International. (2021). Türkiye: Weaponizing counter-terrorism. Türkiye exploits terrorism financing assessment to target civil society [en línea]. Londres, Amnesty International. [Consulta: 22 enero 2026].
- . (2022). Türkiye's «disinformation law» tightens government control and curtails freedom of expression [en línea]. Londres, Amnesty International. [Consulta: 22 enero 2026].
- . (2025a). Türkiye: Massive escalation in ongoing crackdown including arrest of Istanbul mayor. (March 2025) [en línea]. Londres, Amnesty International. [Consulta: 22 enero 2026]. Disponible en: <https://www.amnesty.org/en/latest/news/2025/03/turkiye-massive-escalation-in-ongoing-crackdown-including-arrest-of-istanbul-mayor/>
- . (2025b). Türkiye: «I cannot breathe» allegations of torture and other ill-treatment in the context of mass protests between 19 - 26 march must be investigated [en línea]. Londres, Amnesty International. [Consulta: 22 enero 2026].
- . (2025c). Türkiye: Proceedings against Istanbul Bar Association board a «direct assault» on independence of legal profession [en línea]. Londres, Amnesty International. [Consulta: 22 enero 2026].

- Ataman, M. (2025). Challenges Facing Terror-free Türkiye Project [en línea]. Ankara, SETA. [Consulta: 22 enero 2026]. Disponible en: <https://www.setav.org/en/challenges-facing-terror-free-turkiye-project>
- Bayrakli, E., Boyraz, H. y Güngörmez, O. (2018) The Gülenist terror organization (FETÖ) in the United Kingdom [en línea]. Ankara, SETA. [Consulta: 22 enero 2026]. Disponible en: <https://media.setav.org/en/file/2018/07/the-gulenist-terror-organization-feto-in-the-united-kingdom.pdf>
- Bingol, O. (2023). *Foreign fighters and Türkiye's problem* [en línea]. Berlín. [Consulta: 22 enero 2026]. Disponible en: https://www.researchgate.net/publication/369189668_Foreign_Fighters_and_Türkiye's_Problem
- Broekaert, C. y Clarke, C. (2025). The Islamic State is 'back.' In reality, it never went away [en línea]. *World Politics Review*. Washington D.C. [Consulta: 22 enero 2026]. Disponible en: <https://www.worldpoliticsreview.com/islamic-state-isis-terrorist-attacks/>
- Cahid Cingi, M. (2025). Terror-free Türkiye: A homegrown peace reshaping the region [en línea]. *Al Jazeera*. Doha, Qatar. [Consulta: 22 enero 2026]. Disponible en: <https://www.aljazeera.com/opinions/2025/10/24/terror-free-turkiye-a-homegrown-peace-reshaping-the-region>
- Çelik, M. (2025). Türkiye's cybersecurity problem: Governance, culture and coordination [en línea]. *Balkan Insight*. [Consulta: 22 enero 2026]. Disponible en: <https://balkaninsight.com/2025/12/29/turkeys-cybersecurity-problem-governance-culture-and-coordination/>
- Cerbone, P. (2021). El hiperpresidencialismo como resultado de la interacción entre presidencialismo fuerte y populismo [en línea]. *RIPS: Revista de Investigaciones Políticas y Sociológicas*. Universidad de Santiago de Compostela. 20(1). [Consulta: 22 enero 2026]. Disponible en: <https://revistas.usc.gal/index.php/rips/article/view/7676/10917>
- CFR. (2025). Conflict between Türkiye and armed Kurdish groups [en línea]. Washington D.C., Council on Foreign Relations. [Consulta: 22 enero 2026]. Disponible en: <https://www.cfr.org/global-conflict-tracker/conflict/conflict-between-turkey-and-armed-kurdish-groups>
- Chudziak, M. (2016). From purges to a «new Türkiye». The final stage of the state's reconstruction [en línea]. Varsovia,

- OSW - Centre for Eastern Studies. [Consulta: 22 enero 2026]. Disponible en: <https://www.osw.waw.pl/en/publikacje/osw-commentary/2016-12-07/purges-to-a-new-turkey-final-stage-states-reconstruction>
- Dayly Sabah. (2025). Communications directorate counters rising disinformation in Türkiye [en línea]. *Daily Sabah*. Estambul, Türkiye. [Consulta: 22 enero 2026]. Disponible en: https://www.dailysabah.com/turkiye/communications-directorate-counters-rising-disinformation-in-turkiye/news?gallery_image=undefined#big
- Erdoğan, R. T. (2023). STRATCOM '23. Cumbre Internacional de Comunicación Estratégica 2023 [en línea]. Presidencia de la República de Türkiye. [Consulta: 22 enero 2026]. Disponible en: https://www.iletisim.gov.tr/images/uploads/dosyalar/Stratcom2023_TR.pdf
- Departamento de Seguridad Nacional (DSN). (2016). España/Türkiye – Terrorismo yihadista [en línea]. Departamento de Seguridad Nacional. [Consulta: 22 enero 2026]. Disponible en: <https://www.dsn.gob.es/eu/node/3770>
- El Qorchi, M., Munzele, S. y Wilson, J. F. (2025). Sistemas informales de transferencias de fondos [en línea]. Washington D.C., International Monetary Fund. [Consulta: 22 enero 2026]. Disponible en: <https://www.imf.org/external/pubs/nft/op/222/>
- Espona, Rafael J. de. (2023). Acción estratégica de la defensa sobre el ámbito cognitivo: Los centros de gravedad del ámbito cognitivo [en línea]. *Documento Opinión 19/2023*. Madrid, Instituto Español de Estudios Estratégicos (IEEE). [Consulta: 22 enero 2026]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEEO19_2023_RAFESP_Cognitivo.pdf
- Euronews. (2016). Erdoğan asegura que no permitirá que se cree un corredor del terror en la frontera con Siria [en línea]. Euronews. [Consulta: 22 enero 2026]. Disponible en: <https://www.youtube.com/watch?v=uXHqsIX9MT4>, <https://es.euronews.com/2016/09/02/erdogan-asegura-que-no-permitira-que-se-cree-un-corredor-del-terror-en-la>
- European Commission. (2016). Key findings of the 2016 report on Türkiye [en línea]. Bruselas, European Commission. [Consulta: 22 enero 2026]. Disponible en: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_16_3639/MEMO_16_3639_EN.pdf

- (2025). Türkiye 2025 report. November 2025 [en línea]. Bruselas, European Commission. [Consulta: 22 enero 2026]. Disponible en: https://enlargement.ec.europa.eu/document/download/4bb4ddd1-4f20-4ee0-92db-926996ec8dd1_en?filename=t%C3%BCrkiye-report-2025.pdf
- European External Action Service. (2025). 3rd EEAS report on foreign information manipulation and interference threats exposing the architecture of FIMI operations [en línea]. Bruselas, European External Action Service. [Consulta: 22 enero 2026]. Disponible en: <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>
- European Parliament. (2017). The financing of the «Islamic State» in Iraq and Syria (ISIS) [en línea]. Estrasburgo, European Parliament. [Consulta: 22 enero 2026]. Disponible en: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/603835/EXPO_IDA\(2017\)603835_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/603835/EXPO_IDA(2017)603835_EN.pdf)
- (2022). 2022 Report on Türkiye [en línea]. Estrasburgo, European Parliament. [Consulta: 22 enero 2026]. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0320_EN.html
- (2023). Foreign interference in all democratic processes in the European Union, including disinformation [en línea]. Estrasburgo, European Parliament. [Consulta: 22 enero 2026]. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219_EN.html
- Ferreira, S. (2025). Türkiye detains 357 suspected IS members in nationwide raids [en línea]. *BBC*. Londres. [Consulta: 22 enero 2026]. Disponible en: <https://www.bbc.com/news/articles/c4g5gq19n9zo>
- Freedom House. (2023). Freedom in the World 2023: Türkiye. [en línea]. *Freedom House*. Washington D.C. [Consulta: 22 enero 2026]. Disponible en: <https://freedomhouse.org/country/turkey/freedom-world/2023>
- (2025). Freedom in the world 2025 Türkiye [en línea]. *Freedom House*. Washington D.C. [Consulta: 22 enero 2026]. Disponible en: <https://freedomhouse.org/country/turkey/freedom-world/2025>
- Gazapo, M. J. (2018). *Daesh: Terrorismo global y local a medio camino entre lo físico y lo virtual* [en línea]. Universidad Complutense de Madrid. [Consulta: 22 enero

- 2026]. Disponible en: <https://docta.ucm.es/entities/publication/7b42f534-affa-406b-bbca-679f6a65868f>
- Gostoli, Y. (2025). Türkiye's AI-powered protest crackdown [en línea]. *New Lines Magazine*. [Consulta: 22 enero 2026]. Disponible en: <https://newlinesmag.com/spotlight/turkeys-ai-powered-protest-crackdown/>
- Gurkaynak, E. (2022). Law No. 7418 on amendment of press law and certain laws is published [en línea]. *Gurkaynak Avukatlik Burosu*. Estambul. [Consulta: 22 enero 2026]. Disponible en: <https://www.gurkaynak.av.tr/Content/dosya/1507/law-no-7418-on-amendment-of-press-law-and-certain-laws-is-published-32865-17977.pdf>
- Hamza, A. y Toye, A. (2025). The secret peace in Türkiye: How aging leaders are ending a war [en línea]. *War on the Rocks*. Washington D.C. [Consulta: 22 enero 2026]. Disponible en: <https://warontherocks.com/2025/07/the-secret-peace-in-turkey-how-aging-leaders-are-ending-a-war/>
- Han, B.-C. (2022). *Infocracia: La digitalización y la crisis de la democracia*. Madrid, Taurus.
- Hasnain, J. (2019). Why Syria safe zones? [en línea]. *Daily Sabah*. Estambul. [Consulta: 22 enero 2026]. Disponible en: <https://www.dailysabah.com/op-ed/2019/11/20/why-syria-safe-zones>
- Hassan, T. (2025). Türkiye world report 2025 [en línea]. Nueva York, Human Rights Watch. [Consulta: 22 de enero de 2026]. Disponible en: <https://www.hrw.org/world-report/2025/country-chapters/turkiye>
- HRW. (2014). Türkiye: Spy agency law opens door to abuse [en línea]. Nueva York, Human Rights Watch. [Consulta: 22 enero 2026]. Disponible en: <https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse>
- . (2018). Türkiye: «Emergency» measures become permanent law [en línea]. Nueva York, Human Rights Watch. [Consulta: 22 enero 2026]. Disponible en: https://www.hrw.org/sites/default/files/world_report_download/201801world_report_web.pdf
- . (2024). Türkiye: Kurdish politicians convicted in unjust masstrial [en línea]. Nueva York, Human Rights Watch. [Consulta: 22 enero 2026]. Disponible en: <https://www.hrw.org/news/2024/05/16/turkiye-kurdish-politicians-convicted-unjust-mass-trial>
- ICG. (2020). Calibrating the response: Türkiye's ISIS returnees [en línea]. International Crisis Group. [Consulta: 22

- enero 2026]. Disponible en: <https://www.crisisgroup.org/rpt/europe-central-asia/turkiye/258-calibrating-response-turkeys-isis-returnees>
- . (2025). Türkiye's PKK conflict: A visual explainer [en línea]. International Crisis Group. [Consulta: 22 enero 2026]. Disponible en: <https://www.crisisgroup.org/visual-explainers/turkiyes-pkk-conflict-visual-explainer>
- İFÖD. (2025). Joint open letter to social media companies on censorship in Türkiye [en línea]. *İfade Özgürlüğü Derneği*. Estambul. [Consulta: 22 enero 2026]. Disponible en: <https://ifade.org.tr/en/press-releases-announcements/joint-open-letter-to-social-media-companies-on-censorship-in-turkiye/>
- IEP. (2025). Global terrorism index [en línea]. Sídney, Institute for Economics & Peace. [Consulta: 22 enero 2026]. Disponible en: <https://www.economicsandpeace.org/global-terrorism-index/>
- Independent. (2021). Presidente turco: Redes sociales atentan contra la democracia [en línea]. *Independent*. [Consulta: 22 enero 2026]. Disponible en: <https://www.independentespanol.com/ap/presidente-turco-redes-sociales-atentan-contra-democracia-b1974392.html>
- Inform. (2025). Global freedom of expression, Columbia University: Newsletter, 27 November 2025 [en línea]. Nueva York, Columbia University. [Consulta: 22 enero 2026]. Disponible en: <https://inform.org/2025/11/28/global-freedom-of-expression-columbia-university-newsletter-27-november-2025/>
- Kizilaslan, M. (2025). Cybersecurity doctrine: Türkiye as a preventive hybrid actor [en línea]. *Daily Sabah*. Estambul. [Consulta: 22 enero 2026]. Disponible en: <https://www.dailysabah.com/opinion/op-ed/cybersecurity-doctrine-turkiye-as-a-preventive-hybrid-actor>
- Malet, D., Farrell-Molloy, J. y Young, J. (2025). Foreign fighter mobilization: YPG volunteers in their own words [en línea]. *Terrorism and Political Violence*. 37(1), pp. 93-110. [Consulta: 22 enero 2026]. Disponible en: <https://www.tandfonline.com/doi/full/10.1080/09546553.2023.2275055>
- Migliano, S. (2025). VPN demand surges around the world [en línea]. TOP10VPN. [Consulta: 22 enero 2026]. Disponible en: <https://www.top10vpn.com/research/vpn-demand-statistics/#vpn-demand-surges-in-2021>

- Mourenza, A. (2025). Cientos de detenidos en las protestas en Türkiye contra el gobierno de Erdoğan [en línea]. *El País*. Madrid. [Consulta: 22 enero 2026]. Disponible en: <https://elpais.com/internacional/2025-03-22/cientos-de-detenidos-en-las-protestas-en-turquia-contra-el-gobierno-de-erdogan.html>
- NCSI. (2025). Türkiye 2025 [en línea]. National Cyber Security Index. [Consulta: 22 enero 2026]. Disponible en: <https://ncsi.ega.ee/country/tr/>
- Neumann, P. R., Breuer, N. y Hauser, Z. L. (2025). IS Khorasan: The Türkiye nexus [en línea]. *Studies in Conflict & Terrorism*. [Consulta: 22 enero 2026]. Disponible en: <https://www.tandfonline.com/doi/pdf/10.1080/1057610X.2025.2554451>
- Nieto, R. A. y Mateo, E. D. (2014). La aplicación del concepto inteligencia, vigilancia y reconocimiento (ISR) en espacios no tradicionales [en línea]. *El impacto de las nuevas tecnologías y las formas de hacer guerra en el diseño de las Fuerzas Armadas*. Madrid, Centro Superior de Estudios de la Defensa Nacional. [Consulta: 22 enero 2026]. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=4784310>
- OONI. (2025). Open observatory of network interference. Throttling of social media in Türkiye during protests: An analysis of OONI data [en línea]. OONI. [Consulta: 22 enero 2026]. Disponible en: <https://ooni.org/post/2025-turkiye-throttling-social-media/>
- Orton, K. (2017). *The forgotten foreign fighters: The PKK in Syria* [en línea]. Londres, Henry Jackson Society. [Consulta: 22 enero 2026]. Disponible en: <https://henryjacksonsociety.org/wp-content/uploads/2017/08/3053-PYD-Foreign-Fighter-Project-1.pdf>
- Özkan, B. (2021). Presidente Erdoğan: La desinformación se ha convertido en un problema de seguridad global [en línea]. *Anadolu Ajansı*. Ankara. [Consulta: 22 enero 2026]. Disponible en: <https://www.aa.com.tr/tr/gundem/cumhurbaskani-erdogan-dezenformasyon-kuresel-bir-guvenlik-sorunu-halini-almistir/2444770>
- Pierini, M. y Siccardi, F. (2025). Türkiye's ambivalence is a threat to European security [en línea]. Bruselas, Carnegie Europe. [Consulta: 22 enero 2026]. Disponible en: <https://carnegieendowment.org/posts/2025/04/turkeys-ambivalence-is-a-threat-to-european-security?lang=en>

- Pluvinet, M. (2025). Türkiye detiene a 357 sospechosos del grupo Estado Islámico tras operaciones nacionales [en línea]. *France24*. París. [Consulta: 22 enero 2026]. Disponible en: <https://www.france24.com/es/medio-oriente/20251230-turqu%C3%ADa-detiene-a-357-sospechosos-del-grupo-estado-isl%C3%A1mico-tras-operaciones-nacionales>
- Presidencia de la República de Türkiye. (2024). Dirección de Estrategia, Plan 2024-2028 [en línea]. Presidencia de la República de Türkiye. [Consulta: 22 de enero de 2026]. Disponible en: https://www.sbb.gov.tr/wp-content/uploads/2023/11/On-Ikinci-Kalkinma-Plani_2024-2028_17112023.pdf
- Presidencia del Gobierno de España (2018). Rajoy destaca la contribución de Türkiye a la seguridad europea [en línea]. Madrid, La Moncloa. [Consulta: 22 enero 2026]. Disponible en: <https://www.lamoncloa.gob.es/presidente/actividades/Paginas/2018/240418-ruedaturquia.aspx?galv2r=2>
- R.T. Consejo de Seguridad Nacional. (2025a). MGK: Milli Güvenlik Kurulu [en línea]. Ankara, Consejo de Seguridad Nacional. [Consulta: 22 enero 2026]. Disponible en: <https://www.mgk.gov.tr/index.php/milli-guvenlik-kurulu/genel-bilgi>
- . (2025b). MGK: Milli Güvenlik Kurulu. Reunión de fecha 26 de noviembre de 2025 [en línea]. Ankara, Consejo de Seguridad Nacional. [Consulta: 22 enero 2026]. Disponible en: <https://www.mgk.gov.tr/index.php/milli-guvenlik-kurulu/mgk-toplantisi-basin-aciklamalari/son-toplantinin-basin-aciklamasi>
- R.T. Ministerio de Asuntos Exteriores (2025). PKK [en línea]. Ankara, Ministerio de Asuntos Exteriores de la República de Türkiye. [Consulta: 22 enero 2026]. Disponible en: <https://www.mfa.gov.tr/pkk.en.mfa>
- R.T. Ministerio del Interior (2024). Plan estratégico 2024-2028 [en línea]. Ankara, Ministerio del Interior. [Consulta: 22 enero 2026]. Disponible en: https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/strateji/raporlar/stratejik-planlar/ICISLERI_BAKANLIGI_2024_2028_STRATEJIK_PLANI.pdf
- R.T. Ministerio de Transporte e Infraestructuras (2024). Estrategia y Plan Nacional de Ciberseguridad 2024-2028 [en línea]. Ankara, Ministerio de Transporte e Infraestructuras. [Consulta: 22 enero 2026]. Disponible en: <https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028>.

pdf/ <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2024-2028.pdf>

- Reci, M. (2025). Digital rights review: Governments and Big Tech 'enabling' online violations [en línea]. Balkan Insight. [Consulta: 22 enero 2026]. Disponible en: <https://balkaninsight.com/2025/05/28/digital-rights-review-governments-and-bigtech-enabling-online-violations/>
- Reporteros Sin Fronteras. (2025). Clasificación mundial de la libertad de prensa RSF [en línea]. Reporteros Sin Fronteras. [Consulta: 22 enero 2026]. Disponible en: <https://rsf-es.org/clasificacion-mundial-de-la-libertad-de-prensa-rsf-2025-el-debilitamiento-economico-de-los-medios-constituye-una-de-las-principales-amenazas-para-la-libertad-de-prensa/>
- República de Türkiye (2022). Ley n.º 7418, de 18 de octubre de 2022, por la que se modifican la Ley de Prensa y otras leyes. Resmî Gazete, n.º 31987 [en línea]. Ankara, Gran Asamblea Nacional. [Consulta: 22 enero 2026]. Disponible en: <https://www.resmigazete.gov.tr/eskiler/2022/10/20221018-1.htm>
- . (2014). Ley n.º 6532, de 17 de abril de 2014. Resmî Gazete, n.º 28983 [en línea]. Ankara, Gran Asamblea Nacional. [Consulta: 22 enero 2026]. Disponible en: <https://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm>
- . (2025). Ley n.º 7545, de 19 de marzo de 2025. Resmî Gazete, n.º 32846 [en línea]. Ankara, Gran Asamblea Nacional. [Consulta: 22 enero 2026]. Disponible en: <https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm>
- Reuters. (2025). Türkiye's Erdogan heralds «new phase» in PKK peace process [en línea]. *Reuters*. Londres. [Consulta: 22 enero 2026]. Disponible en: <https://www.reuters.com/business/media-telecom/turkeys-erdogan-heralds-new-phase-pkk-peace-process-2025-11-05/>
- Robinson, K. (2023). Türkiye's growing foreign policy ambitions [en línea]. Washington D.C., Council on Foreign Relations. [Consulta: 22 enero 2026]. Disponible en: <https://www.cfr.org/backgrounders/turkeys-growing-foreign-policy-ambitions>
- RTVE. (2023). Türkiye mueren dos terroristas en Ankara en un atentado suicida contra el Ministerio del Interior turco [en línea]. *RTVE*. [Consulta: 22 enero 2026]. Disponible en: <https://www.rtve.es/noticias/20231001/ankara-turquia-explasion-parlamento/2457267.shtml>

- Sánchez, P. (2025). *Panorama Geopolítico de los Conflictos 2025* [en línea]. Madrid, Instituto Español de Estudios Estratégicos. [Consulta: 28 enero 2026]. Disponible en: <https://www.defensa.gob.es/ceseden/-/panorama-geopol%C3%ADtico-de-los-conflictos-2025>
- SETA. (2025). SETA security radar. Uncertainties Türkiye's geopolitical landscape in 2025 [en línea]. Ankara, SETA. [Consulta: 22 enero 2026]. Disponible en: <https://www.setav.org/en/seta-security-radar-turkiyes-geopolitical-landscape-in-2025>
- Siccardi, F. (2021). How Syria changed Türkiye's foreign policy [en línea]. Washington D.C., Carnegie Endowment for International Peace. [Consulta: 22 enero 2026]. Disponible en: <https://carnegieendowment.org/es/research/2021/09/how-syria-changed-turkeys-foreign-policy>
- SWI. (2023). Bruselas y Türkiye acuerdan reforzar la cooperación en la lucha contra el terrorismo [en línea]. *Swissinfo*. Berna. [Consulta: 22 enero 2026]. Disponible en: <https://www.swissinfo.ch/spa/bruselas-y-turqu%C3%ADa-acuerdan-reforzar-la-cooperaci%C3%B3n-en-la-lucha-contra-el-terrorismo/49005294>
- . (2025a). Las nuevas tecnologías ayudan a reforzar la represión en Türkiye [en línea]. *Swissinfo*. Berna. [Consulta: 22 enero 2026]. Disponible en: <https://www.swissinfo.ch/spa/las-nuevas-tecnolog%C3%ADas-ayudan-a-reforzar-la-represi%C3%B3n-en-turqu%C3%ADa/89086448>
- . (2025b). Erdoğan asegura que Türkiye apoyará al gobierno sirio para evitar una desestabilización [en línea]. *Swissinfo*. Berna. [Consulta: 22 enero 2026]. Disponible en: <https://www.swissinfo.ch/spa/erdogan-asegura-que-turqu%C3%ADa-apoyar%C3%A1-al-gobierno-sirio-para-evitar-una-desestabilizaci%C3%B3n/89169010>
- Tas, H. (2018). The 15 July abortive coup and post-truth politics in Türkiye [en línea]. *Southeast European and Black Sea Studies*. 18(1), pp. 1-19. [Consulta: 22 enero 2026]. Disponible en: <https://www.tandfonline.com/doi/full/10.1080/14683857.2018.1452374#d1e152>
- ThreatMon. (2025). Türkiye's Cybersecurity Outlook: Key insights from the 2025 National Cyber Threat Report [en línea]. ThreatMon. [Consulta: 22 enero 2026]. Disponible en: <https://threatmon.io/turkiyes-cybersecurity-outlook-key-insights-from-the-2025-national-cyber-threat-report/>

- TRT Haber. (2025). Siber güvenlik kanunu meclisten geçti (Ley de ciberseguridad se aprueba en el Parlamento) [en línea]. *TRT Haber*. Ankara. [Consulta: 22 enero 2026]. Disponible en: <https://www.trthaber.com/haber/gundem/siber-guvenlik-kanunu-yasalasti-900579.html>
- Tuysuz, G. y Tawfeeq, M. (2025). Türkiye detains 115 ISIS suspects in nationwide raids ahead of Christmas, New Year [en línea]. *CNN*. Atlanta. [Consulta: 22 enero 2026]. Disponible en: <https://edition.cnn.com/2025/12/25/world/turkey-detains-115-isis-suspects-ahead-of-holidays-intl-latam>
- U.S. Department of State. (2022). 2022 Country Report on Human Rights Practices: Türkiye (Türkiye) [en línea]. Washington D.C., U.S. Department of State. [Consulta: 22 enero 2026]. Disponible en: <https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/turkey/>
- . (2025). Meeting of the Global Coalition to Defeat ISIS Small Group (Nota de prensa, 27 de junio de 2025) [en línea]. Washington D.C., U.S. Department of State. [Consulta: 22 enero 2026]. Disponible en: <https://www.state.gov/releases/office-of-the-spokesperson/2025/06/meeting-of-the-global-coalition-to-defeat-isis-small-group>
- USIP. (2017). *The jihadi threat. ISIS, al-Qaeda, and beyond* [en línea]. Washington D.C., United States Institute of Peace. [Consulta: 22 enero 2026]. Disponible en: <https://www.usip.org/sites/default/files/The-Jihadi-Threat-ISIS-Al-Qaeda-and-Beyond.pdf>
- Venice Commission. (2017). Türkiye – Opinion on the provisions of the emergency decree law No. KHK/696 of 2017 [en línea]. Estrasburgo, Consejo de Europa. [Consulta: 22 enero 2026]. Disponible en: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2017\)021-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2017)021-e)
- Xinhua News. (2025). Türkiye detains 298 suspected ISIS members in anti-terror operations [en línea]. *Xinhua News*. Pekín. [Consulta: 22 enero 2026]. Disponible en: <https://english.news.cn/20250521/6640b7e602d14a85b47a3351ea542402/c.html>
- Yesiltas, M. (2025). Making sense of Türkiye's new counter-terrorism strategy [en línea]. *Politics Today*, Internet. [Consulta: 22 de enero de 2026]. Disponible en: <https://politicstoday.org/making-sense-of-turkeys-new-counter-terrorism-strategy/>
- Yildiz, K. y Muller, M. (2008). *The European Union and Turkish accession. Human rights and the Kurds* [en línea]. Londres,

- Pluto Press. [Consulta: 22 enero 2026]. Disponible en: https://api.pageplace.de/preview/DT0400.9781849644013_A24191659/preview-9781849644013_A24191659.pdf
- Yılmaz, İ. y Albayrak, I. (2022). Redefining Diyanet in the AKP era [en línea]. En: Yılmaz, İ. y Albayrak, I. (ed.). *Populist and Pro-Violence State Religion*. [Consulta: 22 de enero de 2026]. Disponible en: https://www.researchgate.net/publication/357937287_Redefining_Diyanet_in_the_AKP_Era
- Yinanç, B. (2016). Awareness on information security low in Türkiye [en línea]. *Hurriyet Daily News*. Estambul. [Consulta: 22 enero 2026]. Disponible en: <https://www.hurriyetdailynews.com/awareness-on-information-security-low-in-turkey-97595>
- Yuldoshkhujayev, S. *et al.* (2025). A decade-long landscape of advanced persistent threats: Longitudinal analysis and global trends [en línea]. arXiv. [Consulta: 22 enero 2026]. Disponible en: <https://arxiv.org/pdf/2509.07457v1>