INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

VI CURSO DE COMANDO E DIREÇÃO POLICIAL

Trabalho Individual Final

Ameaças Híbridas: Um Desafio Multidimensional à Segurança Interna

Auditor

Fortunato Miguel Ribeiro de Paiva

Lisboa, 03 de outubro de 2025

Agradecimentos

Começo por gradecer à Polícia de Segurança Pública e ao Instituto Superior de Ciências Policiais e Segurança Interna pela oportunidade e pelos ensinamentos proporcionados ao longo da formação, destacando o empenho e o trabalho dos Docentes e de todos os Profissionais que colaboram na realização deste curso.

Agradeço aos Ilustres Camaradas do VI Curso de Comando e Direção Policial, em especial à Turma A, pela partilha de experiências, companheirismo, apoio e por tornarem o percurso académico muito mais estimulante.

Por fim, agradeço aos Senhores Superintendente-Chefe Luís Elias, Superintendente Roberto Fernandes e Subintendente David Pereira pela disponibilidade demonstrada e pelas valiosas reflexões críticas que contribuíram para a realização deste trabalho.

A todos, o meu sincero bem-haja.

Resumo

As ameaças híbridas constituem um dos fenómenos mais complexos e disruptivos da atualidade, caracterizando-se pela utilização coordenada de instrumentos convencionais e não convencionais com o intuito de explorar vulnerabilidades políticas, sociais, económicas e tecnológicas. O presente trabalho analisou de que modo estas ameaças afetaram a segurança interna em Portugal, atendendo à crescente dependência digital, à relevância das infraestruturas críticas e à inserção do país em organismos internacionais de segurança e defesa.

Procurou-se compreender as dimensões do fenómeno, identificar os vetores mais relevantes – como os ciberataques, a desinformação, a instrumentalização de fluxos migratórios, a radicalização e as vulnerabilidades das infraestruturas críticas – e avaliar o seu impacto na prevenção e segurança, na ordem pública e na investigação criminal.

Demonstrou-se que as ameaças híbridas não se circunscreveram ao domínio da defesa, afetando diretamente a segurança interna, exigindo uma resposta integrada e multidimensional. Identificaram-se ainda os principais instrumentos, órgãos e serviços nacionais que lidam com este fenómeno, salientando-se a relevância da cooperação interinstitucional, da capacitação tecnológica e da resiliência para garantir uma resposta mais eficaz face aos desafios emergentes.

Palavras-chave: Ameaças híbridas, Segurança Interna, Cibersegurança, Desinformação e Infraestruturas Críticas.

Abstract

Hybrid threats represent one of the most complex and disruptive phenomena of the present time, characterized by the coordinated use of conventional and non-conventional instruments aimed at exploiting political, social, economic, and technological vulnerabilities. This study examined the ways in which such threats have affected internal security in Portugal, considering the country's growing digital dependence, the strategic importance of its critical infrastructures, and its integration within international security and defense frameworks.

The analysis sought to understand the dimensions of the phenomenon, to identify its most relevant vectors – such as cyberattacks, disinformation, the instrumentalization of migratory flows, radicalization, and vulnerabilities in critical infrastructures – and to assess their impact on prevention and security, public order, and criminal investigation.

It was demonstrated that hybrid threats were not confined to the domain of defense but directly affected internal security, thereby requiring an integrated and multidimensional response. The main national instruments, bodies, and services addressing this phenomenon were also identified, highlighting the importance of interinstitutional cooperation, technological capacity-building, and resilience as key factors in ensuring a more effective response to emerging challenges.

Keywords: Hybrid Threats, Internal Security, Cybersecurity, Disinformation, Critical Infrastructures.

Índice

… se um homem não domina as suas circunstâncias, acabará por ser dominado por elas.

(Towles, 2016, p. 24)

1. Introdução

A crescente complexidade do sistema internacional, marcada pela intensificação da competição estratégica entre potências globais, pela rápida transformação tecnológica e pela fragilidade das instituições multilaterais, tem originado novas formas de instabilidade e insegurança. As ameaças híbridas assumem um papel de destaque, não apenas pela sua capacidade de desestabilizar os Estados e fragilizar as sociedades democráticas, mas também pela dificuldade em serem identificadas, atribuídas e combatidas.

A edição do Relatório de Riscos Globais 2025 revela um cenário cada vez mais fragmentado, com crescentes ameaças à estabilidade e ao progresso. A dois anos surgem como principais riscos a desinformação e informação falsa, a polarização social, a ciberespionagem e guerra cibernética, a desigualdade e a migração ou deslocação involuntária, riscos que se repetem numa prospeção a dez anos (Fórum, 2025).

A última edição da Avaliação da Ameaça da Criminalidade Grave e Organizada da União Europeia (UE) refere que "a criminalidade grave e organizada também desestabiliza cada vez mais a UE através da colaboração entre redes criminosas e agentes de ameaça híbrida" (Europol, 2025, p. 2).

Eventos recentes como a pandemia de COVID-19 e o conflito entre a Rússia e a Ucrânia, vieram demonstrar a exposição a riscos globais, geradores de incerteza e altamente complexos, de modo que "a externalização da segurança interna e da justiça é hoje um elemento fundamental de forma a fazer face à criminalidade transnacional e a uma miríade de novos fenómenos crimonógenos" (Elias, 2022, p. 220), permitindo que as ameaças análogas sejam "abordadas de forma mais eficaz através de uma resposta coordenada a nível da UE" (Europeia, 2016, p. 2). A segurança é a "base da proteção pessoal, mas protege também direitos fundamentais e constitui os alicerces da confiança e do dinamismo da nossa economia, da nossa sociedade e da nossa democracia [na medida em que] a proteção, a prosperidade e o bem-estar dos cidadãos dependem da segurança" (Europeia, 2020, p. 2).

Portugal, enquanto Estado-Membro da UE e da Organização do Tratado do Atlântico Norte (NATO) e com uma posição geoestratégica relevante no Atlântico, não está imune a estas dinâmicas. Pelo contrário, a crescente dependência de infraestruturas digitais e tecnológicas, a exposição de setores críticos como energia, transportes e comunicações, bem como a centralidade dos cabos submarinos que ligam a Europa ao resto do mundo,

evidenciam a pertinência de analisar a temática das ameaças híbridas no contexto da segurança interna[1].

A pertinência do estudo fundamenta-se pela necessidade de compreender o conceito de ameaças híbridas, dado que o termo continua a ser objeto de debate e de interpretações diversas, pela importância de identificar as principais ameaças que afetam Portugal, tanto no plano tecnológico como social e político, bem como pela necessidade de compreender se essas ameaças se inserem apenas no domínio da defesa nacional ou se também devem ser encaradas como parte integrante da segurança interna. Assim, impõe-se analisar o impacto das ameaças híbridas na segurança interna, considerando a sua influência ao nível da segurança e prevenção, ordem pública e investigação criminal. Finalmente, pela necessidade de conhecer quais os instrumentos e órgãos que tratam do fenómeno, de forma a percecionar o nível de preparação para os desafios atuais e futuros.

O estudo pretende atingir os seguintes objetivos: (i) compreender o conceito de ameaças híbridas; (ii) identificar os principais vetores de ameaça e o seu impacto na segurança interna; (iii) compreender se este é um problema circunscrito à defesa ou também é da segurança interna; (iv) identificar quais os principais instrumentos, órgãos e serviços nacionais que lidam com o fenómeno. A pergunta de partida que orienta a investigação, à qual procuraremos responder durante a nossa explanação pode, assim, ser formulada nos seguintes termos: O que são ameaças híbridas e de que modo afetam a segurança interna de Portugal?

A metodologia adotada assenta numa análise qualitativa de carácter teórico e documental, baseada na revisão de literatura académica especializada, em relatórios estratégicos nacionais e internacionais, bem como em documentos oficiais da UE, da NATO e de Portugal.

Após esta introdução, o capítulo seguinte do trabalho analisa o conceito e as dimensões das ameaças híbridas. Seguidamente centra-se nos principais desafios colocados à segurança interna, procurando identificar os principais vetores de ameaça. O terceiro capítulo aborda a interseção entre segurança interna e defesa, discutindo as zonas cinzentas criadas pelas ameaças híbridas. O quarto capítulo procura identificar os principais

[1] Nos termos do artigo 1.º n.º 1 da Lei n.º 53/2008, de 29 de Agosto, na sua redação atual, "a segurança interna é a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática".

instrumentos, órgãos e serviços que tratam da temática e, por fim, terminamos com algumas conclusões sintetizando as principais reflexões e perspetivas futuras.

Com este estudo esperamos contribuir para uma melhor compreensão das ameaças híbridas em Portugal e para a reflexão crítica no contexto da segurança interna.

2. Ameaças híbridas: conceito e caracterização

2.1 Conceito

A literatura especializada e os relatórios das principais organizações internacionais, como a UE e a NATO, convergem na ideia de que as ameaças híbridas constituem hoje um dos principais desafios à segurança, considerando que "a intensidade destas atividades está a aumentar, suscitando uma crescente preocupação com a possível interferência em atos eleitorais, com campanhas de desinformação e ciberatividades maliciosas" (Europeia, 2017, p. 3).

A definição de ameaça híbrida tem sido alvo de discussão e reflecção, não sendo unanimemente aceite. Veja-se que o próprio termo – híbrida – encerra em si mesma ausência de objetividade. Para a UE o conceito de ameaça híbrida visa envolver a combinação de "atividades coercivas com atividades subversivas, de métodos convencionais com métodos não convencionais (ou seja, diplomáticos, militares, económicos, tecnológicos) que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para atingir objetivos específicos, mantendo-se, no entanto, abaixo do limiar de uma guerra formalmente declarada" (Europeia, 2016, p. 2). O conceito deve permanecer flexível, de forma a "responder à sua natureza evolutiva" (Europeia, 2016, p. 2), caracterizando-se por serem ameaças "multidimensionais, combinando medidas coercivas e subversivas, […] para desestabilizar a parte contrária […] de forma a serem difíceis de detetar ou de atribuir." (Europeia, 2018, p. 2). Considera-se a utilização do Direito como parte de uma campanha híbrida, quando um ator hostil combina e sincroniza ações no domínio jurídico com outras atividades, visando as vulnerabilidades sistémicas de sociedades democráticas (Sari, 2020).

A ambiguidade é uma característica intrínseca das ameaças híbridas. Ao contrário dos conflitos tradicionais, estas não se traduzem num ataque militar aberto e facilmente identificável. Pelo contrário, manifestam-se de forma difusa, diluída no tempo e no espaço, dificultando a sua deteção, a atribuição da responsabilidade e a resposta.

Com efeito, destacamos que "não será pela verificação da concretização de uma ameaça que se poderá determinar estar-se perante ameaças híbridas, mas, antes, pela verificação de diversas ameaças combinadas, de forma sistemática, pelos mesmos perpetradores, na prossecução de um objetivo específico" (Pereira, 2018, p. 9).

2.2 Características

A análise documental permite-nos identificar um conjunto de características que ajudam a compreender a natureza das ameaças híbridas. Em primeiro lugar destacamos a multidimensionalidade, na medida em que as ameaças híbridas atuam em simultâneo em várias dimensões, nomeadamente militar, política, económica, tecnológica, social e cultural (Europeia, 2016; Europeia, 2018; Pereira, 2018; Sari, 2020). A ambiguidade é outra característica relevante, uma vez que as operações ocorrem tipicamente nas designadas zonas cinzentas, dificultando a distinção entre guerra e paz, entre ataque e incidente, entre ação estatal e não estatal, bem como a negação plausível, através da qual autores procuram ocultar ou negar a sua responsabilidade para evitar retaliações (Europeia, 2016; Europeia, 2018; Pereira, 2018; Sari, 2020). As ameaças híbridas procuram explorar vulnerabilidades, sobretudo ao nível das divisões sociais, dependências económicas ou fragilidades tecnológicas (Europeia, 2016; Europeia, 2018; Pereira, 2018; Sari, 2020). Para além dos danos materiais que possam infligir, as ameaças híbridas procuram influenciar perceções, fragilizar a confiança e a instabilidade social, gerando efeitos psicológicos muito significativos, especialmente em sociedades abertas e democráticas, onde a liberdade de informação e de expressão, a transparência e a diversidade política podem ser exploradas por atores hostis (Europeia, 2016; Europeia, 2018; Pereira, 2018; Sari, 2020).

Com efeito, as ameaças híbridas distinguem-se das restantes ameaças através da concomitância da "dificuldade da sua identificação e atribuição da autoria, a sua utilização sistemática, coordenada e sincronizada com um amplo leque de ações hostis" (Pereira, 2018, p. 25). De acordo com o autor, "na eventualidade das características acima mencionadas não se verificarem cumulativamente, dificilmente se poderá considerar estar perante ameaças híbridas" (Pereira, 2018, p. 25).

2.3 Dimensão tecnológica e informacional

Um dos domínios mais críticos das ameaças híbridas é o tecnológico, em especial o ciberespaço. O crescimento exponencial da digitalização das sociedades trouxe benefícios

inegáveis, mas também aumentou as possibilidades para agentes hostis promoverem ataques cibernéticos, com impactos extremamente significativos.

O uso das novas tecnologias e plataformas, incluindo as redes sociais, suscitam questões complexas sobre a aplicação das normas de Direito Internacional, cuja adesão das sociedades mais respeitadoras – em especial os Estados Democráticos –, tem resultado em vulnerabilidades que são exploradas por atores menos respeitadores do Direito Internacional (Sari, 2020). Os autores das ameaças híbridas tendem as explorar os limiares da deteção e autoria, uma vez que "o atual quadro legal internacional, dificulta a aplicação das medidas previstas no Direito Internacional, configurado para situações convencionais, e mina a capacidade de resposta dos países regidos por regimes de Estado de Direito Democrático" (Pereira, 2018, p. 25).

A manipulação da informação ganhou centralidade. As campanhas de desinformação procuram explorar divisões sociais e políticas, amplificar tensões existentes e minar a confiança nas instituições. "A manipulação da informação por parte de agentes estrangeiros é cada vez mais frequente, explorando novas tecnologias como a inteligência artificial. As crianças, os jovens e os idosos são particularmente vulneráveis" (Europeia, 2025, p. 1). Com efeito, verificam-se cada vez mais ações com recurso à utilização de tecnologias emergentes e disruptivas para obterem vantagens estratégicas que visam a "interferência direta nas nossas eleições e nos nossos processos políticos" (Europeia, 2022, p. 11).

A inteligência artificial acrescenta novas dimensões e desafios. A capacidade de criar conteúdos falsos, mas altamente verosímeis, desafia a literacia mediática e coloca em causa a distinção entre realidade e manipulação. Os sistemas de inteligência artificial – chatbots – tendem a refletir o que está mais disseminado *online*, e não necessariamente o mais rigoroso, levando a que falsidades sejam amplamente difundidas e interpretadas como factos reais (Talbat & Olson, 2025).

2.4 Contexto internacional

Ao longo dos últimos anos Portugal "enquanto ator global de pendor universalista, geográfica e politicamente inscrito nos projetos da UE da Organização das Nações Unidas (ONU) e da NATO, beneficiou da disposição securitária interdependente e cooperativa convencionada no pós-Segunda Guerra Mundial" (Fernandes, 2024, p. 2). "A posição geográfica de Portugal, na qualidade de fronteira exterior da UE, converte os assuntos

nacionais de segurança interna em preocupações europeias, acarretando responsabilidades acrescidas para o nosso país" (Lourenço et. al., 2015, p. 49), de modo que as estratégias de segurança, em particular ao nível da segurança interna devem "estar alinhadas com as preocupações e objetivos do Espaço de Liberdade, de Segurança e Justiça da UE" (Lourenço et. al., 2015, p. 49). No contexto europeu, os "Estados-Membros assumem responsabilidades pela segurança interna europeia de modo partilhado" (Lourenço et. al., 2015, p. 49), sendo fundamental existirem mecanismos de coordenação funcionais entre os diversos atores.

Atualmente, as ameaças híbridas representam um desafio para a UE, bem como para outras organizações de referência, nomeadamente para a NATO, sendo primordial garantir o diálogo e coordenação, tanto a nível político como a nível operacional (Europeia, 2016, p. 19). Considerando que a UE e a NATO partilham valores semelhantes, impõe-se uma estreita coordenação e cooperação entre ambas, no sentido de melhorar o conhecimento da situação no que concerne às ameaças híbridas, bem como quanto à comunicação estratégica, à cibersegurança, à prevenção e resposta a situações de crise (Europeia, 2016, p. 19).

A Europol assume um papel central em matéria de segurança, contudo o facto de "o seu atual mandato não abranger novas ameaças à segurança, como a sabotagem as ameaças híbridas ou a manipulação da informação" (Europeia, 2025, p. 5) constitui uma forte limitação no contexto atual. A Bússola Estratégica – que é um plano de ação que define uma visão estratégica comum e objetivos concretos para reforçar a política de segurança e defesa da UE até 2030 –, prevê a criação de equipas de resposta rápida às ameaças híbridas para ajudar os Estados-Membros e os parceiros (Europeia C. d., 2022). A estreita colaboração entre a UE e a NATO permitiu desenvolver o Centro Europeu de Excelência para Ameaças Híbridas (Hybrid CoE)[2], em Helsínquia, em cooperação com a Finlândia, ao qual Portugal aderiu em 2019, evidenciando o reforço do compromisso nacional para com a cooperação internacional.

Os esforços dos Estados refletem a consciência crescente de que as ameaças híbridas não respeitam fronteiras e que a sua mitigação exige cooperação internacional. Para países como Portugal, a integração em organizações multilaterais constitui uma mais-valia, permitindo reforçar a capacidade para enfrentar ameaças híbridas, reforçar a resiliência, beneficiando do trabalho conjunto de análise, prevenção e deteção precoce, promovendo a

[2] O Hybrid CoE é uma organização internacional autónoma e baseada em rede que combate ameaças híbridas, e tem por missão fortalecer a segurança dos Estados participantes, fornecendo conhecimento especializado e treino para combater ameaças híbridas, aprimorando a cooperação UE-NATO (https://www.hybridcoe.fi/).

partilha atempada de informações, bem como treino e mecanismos de resposta, capacidades que dificilmente poderiam ser desenvolvidos de forma isolada (Europeu et. al., 2016).

3. O impacto das ameaças híbridas na Segurança Interna

3.1 Enquadramento

Para compreender o impacto das ameaças híbridas na segurança interna vamos procurar identificar os vetores de ameaça mais relevantes, a fim de perceber a sua influência sobre os diferentes domínios da segurança interna, bem como caracterizar os desafios específicos que se colocam às forças e serviços de segurança. Embora Portugal surja na sétima posição, enquanto país mais pacífico dos 163 Estados analisados – de acordo com o Global Peace Index 2025 –, não devemos obliterar o aumento dos níveis de militarização de muitos países, num contexto de crescentes tensões geopolíticas, intensificação de conflitos, desagregação de alianças tradicionais e aumento da incerteza económica, cujos fenómenos híbridos manifestam-se de forma cada vez mais evidente, criando vulnerabilidades que podem afetar tanto a perceção de segurança da população como a capacidade do Estado em garantir a proteção de pessoas, bens e instituições (Peace, 2025b).

A globalização e a digitalização intensificaram a interdependência, uma vez que as "pessoas dependem de infraestruturas essenciais na sua vida quotidiana para se deslocar, trabalhar, beneficiar de serviços públicos essenciais, como hospitais, transportes, fornecimentos de energia, ou para exercer os seus direitos democráticos" (Europeia, 2020, p. 6), cujas vulnerabilidades podem ser exploradas por atores hostis. Neste quadro, as ameaças híbridas não se limitam ao campo da defesa militar, mas interferem diretamente na esfera da segurança interna, na qual os efeitos se materializam.

3.2 Cibersegurança e ciberataques

Entre os principais vetores de ameaça híbrida encontram-se os ciberataques. "A vida quotidiana e as nossas economias dependem cada vez mais de tecnologias digitais" (Europeia, 2018, p. 10), expondo instituições e cidadãos a riscos que no passado eram residuais. A sociedade portuguesa, tal como a europeia, depende de redes de comunicações, de sistemas de pagamentos eletrónicos e de plataformas digitais que, em caso de disrupção, podem paralisar serviços essenciais. Na mesma lógica, "o aparecimento de casas e equipamentos inteligentes […] bem como a digitalização crescente do sistema energético,

implicam igualmente uma maior vulnerabilidade a ciberataques" (Europeia, 2016, p. 12-13).

Em Portugal, nos últimos anos, registaram-se incidentes significativos – conforme demonstram os Relatórios anuais de Cibsersegurança, tema Riscos e Conflitos, do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS) –, os quais afetaram tanto a continuidade de serviços como a confiança dos cidadãos[3]. Estes episódios demonstram que os ciberataques não são apenas questões técnicas, têm implicações diretas na segurança interna, uma vez que perturbam a vida quotidiana das pessoas, afetam setores críticos e exigem a mobilização de recursos policiais garantir a segurança e a investigação.

Considerando que a "segurança começa com uma antecipação eficaz" (Europeia, 2025, p. 3), a prevenção assume especial destaque, exigindo a monitorização constante de redes e sistemas, com vista à deteção precoce de intrusões. Ao nível da segurança e ordem pública, ciberataques a serviços como telecomunicações, energia ou transportes podem gerar perturbações sociais significativas, colocando em causa a segurança de pessoas e bens. No domínio da investigação criminal, colocam-se desafios acrescidos, dada a transnacionalidade destes crimes e a sofisticação dos métodos utilizados, requerendo cooperação internacional e elevada especialização técnica, atendendo aos "desafios da recolha de prova digital" (Europeia, 2025, p. 3).

3.3 Desinformação e manipulação informacional

Outro vetor central das ameaças híbridas é a desinformação, pois "prejudica as nossas democracias, uma vez que impede os cidadãos de tomar decisões fundamentadas e de participar no processo democrático (Europeia, 2019, p. 5). Os autores de ameaças híbridas podem efetuar campanhas sistemáticas de desinformação, "nomeadamente através dos meios de comunicação social" (Europeia, 2016, p. 5), bem como recorrendo às novas tecnologias, as quais podem "ser utilizadas para divulgar desinformações a uma escala e um ritmo sem precedentes, com um direcionamento específico, de modo a semear a desconfiança e criar tensões sociais" (Europeia, 2019, p. 5).

[3] De acordo com a 6.ª edição do Relatório de Cibersegurança, tema Riscos e Conflitos (Cibersegurança, 2025), publicado em setembro de 2025, destacam-se, a título de exemplo, os seguintes ataques ocorridos em 2024:
- agosto e setembro: *Leak* de milhares de credenciais da adm. pública, operadores de serviços essenciais e prestadores de serviços digitais;
- outubro: *Ransomware* contra entidade pertencente à administração pública central;
- novembro: Infeção de *ransomware* no setor da educação;
- dezembro: Infeção de *ransomware* na defesa nacional.

Numa fase em que cada vez mais as redes sociais são as plataformas preferenciais para consumir informação, as notícias falsas "podem influenciar a opinião pública em benefício de alguns indivíduos, organizações ou governos [… com] o objetivo mais vasto de semear a confusão nas nossas sociedades e de desacreditar os governos democráticos e as nossas estruturas, instituições e eleições" (Europeia, 2017, p. 5).

O impacto da desinformação na segurança interna é substancial, na medida em que mina a confiança nas instituições democráticas, podendo criar divisões sociais e alimentar teorias da conspiração, desencadeando, em alguns casos, comportamentos hostis contra representantes políticos, autoridades em geral e forças policiais em particular[4]. As campanhas de manipulação, "a polarização da sociedade, as discriminações reais ou percebidas e outros fatores psicológicos e sociológicos podem aumentar a vulnerabilidade das pessoas face ao discurso radical" (Europeia, 2020, p. 16), incitando protestos, gerando clivagens sociais ou intensificando tensões em comunidades locais, resultando em problemas de segurança e ordem pública. O facto de muitos destes conteúdos serem difundidos a partir do estrangeiro, gera, uma vez mais, dificuldades ao nível da investigação criminal. A liberdade de expressão, característica típica dos Estados Democráticos, pode vista como oportunidade e ser malevolamente explorada por atores hostis.

3.4 Migrações e instrumentalização geopolítica

A questão das migrações tem ganho relevância no debate sobre ameaças híbridas, sobretudo a partir de casos registados em alguns países europeus, onde fluxos migratórios foram, aparentemente, instrumentalizados por Estados terceiros, com o objetivo de exercer pressão política sobre a UE. Na fronteira externa da UE com a Rússia e a Bielorrússia, verifica-se "um ataque híbrido por parte de Estados hostis que pretendem desestabilizar a região através da guerra de agressão contra a Ucrânia, ao mesmo tempo que usam a migração como arma" (Europeia, 2024, p. 6). A instrumentalização da migração materializa-se por parte dos atores hostis "facilitando e incentivando continuamente os migrantes a chegarem às fronteiras terrestres orientais externas da União, com a intenção de exercer pressão sobre os Estados-Membros e a União" (Europeia, 2024, p. 8).

[4] Em Lisboa, no ano e 2012, decorram manifestações violentas anti Troika, provocando alterações da ordem pública, motivando a intervenção policial, sobre as quais foram alegadas desinformações sobre a existências de Polícias à paisana infiltrados com o objetivo de instigarem a desordem, situação refutada pelo Governo através do Ministro da Administração Interna (Lusa, 2012).

Embora Portugal não tenha enfrentado, até ao momento, situações semelhantes, a possibilidade não pode ser descartada. A localização atlântica e o papel do país como ponto de entrada na Europa, enquanto fronteira externa da UE, fazem de Portugal um território suscetível a pressões.

O impacto na segurança interna traduz-se em múltiplas dimensões, desde logo considerando que a chegada repentina de fluxos migratórios significativos pode gerar pressões sobre serviços sociais, aumentar perceções de insegurança e alimentar narrativas populistas ou xenófobas, resultando em problemas ao nível da contestação social, da ordem pública e do sentimento de segurança. Do ponto de vista da investigação criminal, no que respeita aos crimes conexos à imigração ilegal, torna-se complexo distinguir entre movimentos legítimos de migração e tentativas de instrumentalização para fins políticos ou criminosos.

3.5 Extremismo e radicalização

O fenómeno da radicalização constitui outro vetor híbrido de relevo, "embora os atos terroristas e o extremismo violento não sejam, por si só, de natureza híbrida, os autores de ameaças híbridas podem visar e recrutar os membros mais vulneráveis da sociedade" (Europeia, 2016, p. 15). Apesar de Portugal apresentar índices insignificativos de atividade terrorista – de acordo com o *Global Terrorism Index 2025: Measuring The Impact of Terrorism* (Peace, 2025) –, não está imune à influência de redes transnacionais que utilizam o espaço digital para recrutar e mobilizar indivíduos, cujos impactos potenciais justificam a nossa atenção. A radicalização *online* constitui um risco para a segurança interna, uma vez que são difundidas ideologias extremistas, que incitam a violência e promovem a polarização, destacando-se que o "recrutamento de jovens é uma preocupação crescente" (Europeia, 2025, p. 20). "A radicalização religiosa e ideológica, […] as ameaças de intervenientes solitários, as novas vias de radicalização – potencialmente também no contexto da crise migratória –, o aumento do extremismo de direita (incluindo a violência contra os migrantes) e os riscos de polarização" (Europeia, 2017, p. 15) devem ser tidos em conta.

A prevenção do extremismo e da radicalização constitui um enorme desafio, considerando que a monitorização reveste enorme exigência e carece de meios específicos e especializados. As eventuais manifestações de violência inspiradas por ideologias extremistas podem gerar distúrbios e afetar a coesão social, bem como resultar em

problemas de segurança graves, exigindo uma resposta de elevada complexidade e perigosidade por parte da segurança interna.

3.6. Infraestruturas críticas e dependências estratégicas

As infraestruturas críticas representam ativos de importância estratégica, mas também potenciais vulnerabilidades, "(por exemplo, as cadeias de aprovisionamento energético e os transportes), uma vez que um ataque não convencional, por autores de ameaças híbridas, a qualquer «alvo vulnerável» poderá conduzir a graves perturbações económicas ou sociais" (Europeia, 2016, p. 6). Destacamos que "ataques híbridos a infraestruturas de transporte (tais como, aeroportos, infraestruturas rodoviárias, portos e caminhos de ferro) podem ter consequências graves, conducentes a perturbações das deslocações e das cadeias de abastecimento" (Europeia, 2016, p. 8).

A sabotagem ou disrupção de um cabo submarino poderia comprometer gravemente comunicações, serviços financeiros e operações governamentais, na medida em que "muitas infraestruturas críticas dependem de uma informação de tempo exata para sincronizar as suas redes (por exemplo, energia e telecomunicações) ou indicar a hora das operações (por exemplo, mercados financeiros)" (Europeia, 2016, p. 9). Do mesmo modo, ataques a centrais elétricas ou redes de distribuição de energia podem impactar diretamente na vida quotidiana e na segurança das pessoas – veja-se o impacto do apagão de 28 de abril de 2025[5] (ERSE, 2025). A dependência energética surge como instrumento de pressão política, especialmente por parte de Estados fornecedores, uma vez que "a produção e distribuição de energia sem perturbações revestem-se de importância vital, [… sendo que um] elemento essencial da luta contra as ameaças híbridas consiste em diversificar as fontes energéticas, os fornecedores e os itinerários de aprovisionamento" (Europeia, 2016, p. 7).

Ao nível da prevenção, torna-se essencial reforçar a proteção física e digital destas infraestruturas, implementando planos de segurança integrados. No domínio da segurança e ordem pública, uma falha em larga escala poderia gerar perturbações sociais, pânico e perda de confiança na capacidade do Estado, culminando em ações de protesto, pilhagens e outras manifestações criminais e violentas altamente complexas.

[5] No dia 28 de abril de 2025 os sistemas de energia de Portugal e Espanha sofreram um apagão cuja investigação final ainda está em curso (ERSE, 2025). Contudo, os impactos comprovaram a vulnerabilidade dos nossos sistemas, da sociedade e das instituições.

4. Segurança Interna e Defesa: interseções e desafios

4.1 Enquadramento

A separação entre segurança interna e defesa nacional tem raízes constitucionais e históricas, refletindo o princípio democrático da distinção de missões entre forças e serviços de segurança. Tipicamente a segurança interna ocupa-se da proteção de pessoas e bens no território nacional e as Forças Armadas da defesa contra agressões externas. Todavia, o surgimento e intensificação das ameaças híbridas têm vindo a desafiar esta fronteira habitual.

A natureza ambígua das ameaças híbridas, frequentemente situadas na designada «zona cinzenta» entre paz e guerra, gera situações em que não é claro se estamos perante um problema de defesa nacional ou de segurança interna. Os "atos de sabotagem dirigidos às infraestruturas críticas, fogo posto, ciberataques, ingerência eleitoral, manipulação da informação e ingerência por parte de agentes estrangeiros, incluindo a desinformação, e instrumentalização da migração" (Europeia, 2025, p. 12) são exemplos de incidentes que podem simultaneamente assumir uma dimensão externa e interna.

4.2 Previsão constitucional e legal

A Constituição da República Portuguesa (CRP) estabelece no artigo 272.º que a polícia tem por funções "defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos", cuja competência de desenvolve, tipicamente, dentro das fronteiras nacionais. Porém, a Lei de Segurança Interna (LSI), aprovada pela Lei n.º 53/2008, de 29 de agosto, na sua redação atual, no artigo 4.º n.º 2 prevê que:

> As forças e os serviços de segurança podem atuar fora do espaço referido no número anterior [espaço sujeito aos poderes de jurisdição do Estado Português], em cooperação com organismos e serviços de Estados estrangeiros ou com organizações internacionais de que Portugal faça parte, tendo em vista, em especial, o aprofundamento do espaço de liberdade, segurança e justiça da União Europeia. (República, 2008)

Os artigos 273.º e seguintes da CRP regem a defesa nacional e as Forças Armadas, as quais têm por missão a defesa militar da República contra agressões externas, competindo-lhes garantir a soberania e a integridade territorial. A LSI e a Lei de Defesa

Nacional – Lei Orgânica n.º 1-B/2009, de 07 de julho, na sua redação atual –, materializam esta separação, clarificando competências e estabelecendo mecanismos de coordenação em situações de exceção.

Apesar desta delimitação formal, colocam-se questões práticas sobre a aplicabilidade destas fronteiras rígidas, dada a "natureza das ameaças atuais e a ligação intrínseca entre a segurança interna e externa" (Europeia, 2025, p. 1).

4.3 A «zona cinzenta»

As ameaças híbridas situam-se frequentemente abaixo do limiar da guerra declarada, explorando as fragilidades jurídicas e institucionais dos Estados, pese embora seja cada vez mais "difícil distinguir entre ameaças híbridas e guerra aberta" (Europeia, 2025, p. 1). Por exemplo, um ciberataque contra sistemas governamentais portugueses pode ser conduzido a partir do um Estado estrangeiro, envolvendo competências de defesa, mas os seus efeitos são sentidos no território nacional, afetando serviços essenciais e exigindo a resposta das forças e dos serviços de segurança. A «zona cinzenta» resulta, assim, da dificuldade em classificar os incidentes, uma vez que contrariam a "tradicional separação paradigmática, política e orgânica entre as dimensões interna e externa da segurança consagrada pelo legado realista" (Brandão, 2015, p. 5).

Com efeito, "a segurança interna é hoje largamente afetada pelo exterior e as fronteiras físicas têm vindo a diluir-se. O carácter interno ou externo da segurança corresponde, essencialmente, à materialização geográfica das ameaças" (Silva, 2022, p. 29), não se coadunando com as ameaças híbridas. A ambiguidade que caracteriza as ameaças híbridas tem diversas implicações, desde logo no plano jurídico, uma vez que levanta dúvidas sobre a entidade responsável pela resposta imediata. No plano operacional, exige coordenação entre instituições com culturas organizacionais diferentes e com missões legalmente distintas, assim como no plano estratégico, diplomático e político, seja ao nível da comunicação pública, da atribuição de responsabilidade ou da preservação da confiança dos cidadãos.

4.4 Cooperação entre forças

A cooperação entre os "serviços de polícia, os serviços de segurança e cibersegurança, a proteção militar e civil e os operadores privados é essencial para antecipar, detetar, prevenir e responder eficazmente a ameaças" (Europeia, 2025, p. 12).

Considerando o carácter difuso das ameaças híbridas e das suas consequências multinível a resposta "parece necessitar, cada vez mais, do empenho tanto das Forças de Segurança como da Forças Armadas" (Silva, 2022, p. 29), na medida em que a "prevenção, reação, contenção e investigação das ameaças […] exige a implementação de um modelo integrado e pluridisciplinar." (Silva, 2022, p. 30). Com efeito, "os limites à ação das forças armadas e das polícias estão em constante redefinição e ajustamento às novas exigências de liberdade e segurança dos cidadãos, [impondo-se cada vez mais a realização de] de missões conjuntas, complementares, flexíveis, adaptáveis e em parceria" (Elias, 2013, p. 16). Portugal necessita de prosseguir com a evolução das políticas de segurança, "nas suas vertentes interna e externa, [uma vez que] têm uma natureza fragmentada, excessivamente normativa e com fortes lacunas ao nível da cooperação e coordenação interministerial e interinstitucional" (Elias, 2013, p. 10).

"Com a globalização, as fronteiras territoriais tornaram-se permeáveis às novas ameaças" (Júnior & Brandão, 2021, p. 6), de modo que a segurança interna assume-se cada vez mais "intercomunitária ou internacional consoante as necessidades e fontes dos perigos e rege-se por cláusulas de cooperação, de coordenação e de solidariedade" (Lourenço et. Al, 2015, p. 49), assumindo particular destaque a cooperação, a formação e capacitação "entre quadros e unidades militares, policiais, de emergência médica, de proteção civil (incluindo exercícios regulares) que ajudem a robustecer e a consolidar uma intervenção integrada em cenários de crise" (Elias, 2013, p. 25).

Ao nível da cooperação internacional, Portugal beneficia da integração na UE e na NATO, na medida em que ambas as organizações têm vindo a desenvolver mecanismos de cooperação entre defesa e segurança interna, no âmbito das ameaças híbridas, como por exemplo a criação do Hybrid CoE, permitindo, assim, beneficiar da partilha de informação, treino conjunto e acesso a recursos que ultrapassam a capacidade nacional, colmatando fragilidades e potenciando sinergias.

5. Instrumentos e órgãos

5.1 Enquadramento

Com o objetivo de procurar compreender de que forma Portugal está capacitado e considera, do ponto de vista estratégico, a necessidade de prevenir e responder a ameaças híbridas, passearemos a enunciar alguns documentos relevantes, bem como alguns órgãos

que integram, designadamente, as forças armadas e as forças e serviços de segurança que, de algum modo, podem relacionar-se diretamente com os desafios emergentes, a fim de permitir conhecer genericamente o sistema nacional. Face às limitações de espaço do presente estudo, não pretendemos aprofundar as missões e o modo de emprego, mas tão-só conhecê-los e formar uma perceção ao nível da resposta organizacional.

5.2 Instrumentos relevantes

O Conceito Estratégico de Segurança da NATO de 2022 refere que a área euro-atlântica já não está em paz, devido ao aumento da competição estratégica, instabilidade e ameaças híbridas, incluindo ciberataques e campanhas de desinformação (NATO, 2022). Na mesma linha, o Relatório do Conselho de Revisão do Conceito Estratégico de Defesa Nacional salienta que "a intensificação das ameaças híbridas, com recurso a um leque alargado de formas de coação, operações de informação e emprego de meios militares de forma não convencional, a par de campanhas de desinformação e de interferências externas, obrigam a um reforço da resiliência dos Estados e da cooperação internacional" (Nacional, 2023, p.15).

Ao nível das principais ameaças à segurança interna, o último Relatório Anual de Segurança Interna (RASI) destaca os conflitos regionais e instabilidade geopolítica, fluxos migratórios, instabilidade económica e social, sabotagem, ciberespionagem e ataques cibernéticos, operações de desinformação e extremismos políticos (Interna, 2025).

A Estratégia Nacional de Segurança do Ciberespaço 2019-2023, aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, visa a segurança do ciberespaço nacional, promovendo uma utilização livre, segura e eficiente por cidadãos, empresas e entidades públicas e privadas, bem como garantir a proteção das infraestruturas críticas e dos serviços vitais de informação (Ministros, 2019). Ainda no domínio da cibersegurança, destaca-se a relevância da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro – Diretiva NIS2 –, cujo objetivo é reforçar a cibersegurança na União Europeia, aumentando a resiliência de organizações públicas e privadas contra incidentes e ameaças híbridas (Europeu & Europa, 2022). A Proposta de Lei n.º 7/XVII/1.ª (GOV) aprovada em 19SET2025 pela Assembleia da República, autoriza o Governo a transpor a referida diretiva (Assembleia da República, 2025), aguardando-se a sua publicação.

O Decreto-Lei n.º 22/2025, de 19 de março, estabelece um quadro jurídico robusto para a identificação, designação e reforço da resiliência das entidades críticas em Portugal e de importância europeia, atribuindo ao Secretário-Geral do Sistema de Segurança Interna um conjunto relevante de competências (Ministros, 2025).

5.3 SIRP, SIED e SIS

A Lei n.º 9/2007, de 19 de fevereiro, na sua redação atual, define a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa (SIRP), do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS). Nos termos do artigo 3.º, "ao Secretário-Geral incumbe dirigir superiormente, através dos directores do SIED e do SIS, no respeito da Constituição e da lei, a actividade de produção de informações necessárias à salvaguarda da independência nacional e dos interesses nacionais e à garantia da segurança externa e interna do Estado Português".

Nos termos do mesmo artigo, o "SIED é o único organismo incumbido da produção de informações que contribuam para a salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português" e o "SIS é o único organismo incumbido da produção de informações destinadas a garantir a segurança interna e necessárias a prevenir a sabotagem, o terrorismo, a espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido".

5.4 Comando de Operações de Ciberdefesa

O Decreto-Lei n.º 19/2022, de 24 de janeiro, estabelece a Lei Orgânica do Estado-Maior-General das Forças Armadas e altera as Leis Orgânicas dos três ramos das Forças Armadas. Com efeito, no artigo 41.º surgem elencadas as atribuições do Comando de Operações de Ciberdefesa (COCiber), destacando-se a responsabilidade por "planear, dirigir, coordenar, controlar e executar operações no e através do ciberespaço em apoio a objetivos militares, garantindo a liberdade de ação das Forças Armadas neste domínio", bem como "no quadro das suas atribuições e em missões conjuntas de natureza operacional, o COCiber relaciona-se diretamente com as estruturas internacionais ligadas à ciberdefesa e à cibersegurança cooperativa, designadamente no âmbito da NATO e da UE".

5.5 Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

O Decreto-Lei n.º 137/2019, de 13 de setembro, na sua redação atual, define a estrutura organizacional da Polícia Judiciária (PJ). O artigo 33.º prevê as atribuições da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), a qual "é a unidade operacional especializada que dá resposta preventiva e repressiva ao fenómeno do cibercrime". Nos termos do mesmo artigo, à UNC3T "compete a prevenção, deteção e investigação de crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos", bem como "elaborar e manter atualizado o Plano Nacional da PJ para a Prevenção e o Combate ao Cibercrime, nomeadamente, em articulação com o Centro Nacional de Cibersegurança", "assegurar o regular funcionamento de um grupo consultivo informal para debate e aconselhamento estratégico, formativo, jurídico, técnico e científico de questões relacionadas com o cibercrime, com a criminalidade tecnológica e a cibersegurança", "testar e desenvolver ferramentas específicas para a investigação do cibercrime, da criminalidade tecnológica e da decifragem de dados", e ainda "recolher, tratar e difundir dados relativos a *ciber-intelligence* para apoio às investigações, à cooperação policial internacional e à prevenção de atos de cibercrime".

5.6 Centro Nacional de Cibersegurança

A Lei n.º 46/2018, de 13 de agosto, estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação. O artigo 7.º define que o Centro Nacional de Cibersegurança (CNCS) tem por missão:

> Garantir que o País usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento da

Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais. (República, 2018)

5.7 Sistema de Segurança Interna

Lei n.º 53/2008, de 29 de agosto, na sua redação atual, aprovou a Lei de Segurança Interna, consubstanciando o próprio Sistema de Segurança Interna (SSI), em especial no Capítulo III. O artigo 11.º diz-nos que "os órgãos do Sistema de Segurança Interna são o Conselho Superior de Segurança Interna, o Secretário-Geral e o Gabinete Coordenador de Segurança". O Secretário-Geral do SSI, previsto no artigo 14.º, é a peça fundamental do sistema e "tem competências de coordenação, direção, controlo e comando operacional", nos termos do artigo 15.º.

Na dependência e sob coordenação do Secretário-Geral do SSI funciona a Unidade de Coordenação Antiterrorismo (UCAT), prevista no artigo 23.º, o Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI), previsto no artigo 23.º-A e a Unidade de Coordenação de Fronteiras e Estrangeiros (UCFE), prevista no artigo 23.º-B, sendo estas Unidades fundamentais para a partilha de informação ao nível interno e para a cooperação internacional, as quais têm evoluído e tornando-se mais robustas e capacitadas, destacando-se a passagem dos Gabinetes da Europol e da Interpol da PJ para o PUC-CPI.

5.8 Polícia de Segurança Pública

As atribuições da PSP surgem no artigo 3.º da lei orgânica – Lei n.º 53/2007, de 31 de agosto, na redação atual, destacando-se "garantir as condições de segurança que permitam o exercício dos direitos e liberdades e o respeito pelas garantias dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de direito", bem como "garantir a ordem e a tranquilidade públicas e a segurança e a proteção das pessoas e dos bens".

O Despacho n.º 1168/2024, de 31 de janeiro, define as unidades orgânicas flexíveis da Direção Nacional da PSP, sublinhando-se as atribuições da Divisão de Análise, Cibercriminalidade, Coordenação e Cooperação Internacional (DACCCI), do Departamento de Investigação Criminal, as quais surgem elencadas no artigo 15.º. De entre a diversas atribuições destaca-se "garantir a ligação com várias entidades externas, para agilizar a partilha de informação", "garantir o esforço de pesquisa dedicado à exploração

dos vários mecanismos de partilha de informação ao nível da cooperação policial internacional", "coordenar a utilização dos canais de cooperação e a troca de informação policial, com entidades externas nacionais e entre as subunidades" e "representar a PSP em organizações e grupos de trabalho de âmbito nacional e internacional relativos à prevenção e investigação da cibercriminalidade, bem como aqueles destinados à partilha de informação e cooperação policial no âmbito da cibercriminalidade".

No que concerne à Estratégia 2025-2027 da PSP, salientamos a referência a "num tempo de incertezas e crescente complexidade do ambiente operacional, onde emergem continuamente novos riscos e ameaças, a incorporação de tecnologias emergentes e processos inovadores torna-se imprescindível" (DNPSP, 2025 p. 20), bem como o objetivo de "participar ativamente, no plano internacional, em projetos e missões, alinhada com a estratégia do Ministério da Administração Interna, reforçando o seu papel nas agências europeias e organizações internacionais, como a EUROPOL, INTERPOL e EUROJUST" (DNPSP, 2025 p. 24).

6. Conclusão

O conceito de ameaças híbridas não é consensual, porém, na nossa perspetiva, mais relevante do que a definição é compreender como se caracterizam e materializam e qual o seu impacto na sociedade. Os "autores das ameaças híbridas tendem a explorar os limiares da deteção e autoria, operando, frequentemente, nas zonas de indefinição, explorando, também, os limites da paz e da guerra" (Pereira, 2018, p. 25). Trata-se de um fenómeno multidimensional e complexo, que combina instrumentos convencionais e não convencionais, procurando explorar vulnerabilidades políticas, sociais, económicas e tecnológicas, dificultando a aplicação do Direito Internacional e a reação dos Estados de Direito Democrático.

Procuramos identificar os principais vetores de ameaça, em particular ciberataques, desinformação, instrumentalização de fluxos migratórios, radicalização e vulnerabilidades associadas a infraestruturas críticas. O estudo procura demonstrar que as ameaças híbridas não estão limitadas à esfera da defesa. A segurança interna tem uma ação direta, evidenciando-se a "necessidade do envolvimento dos diversos operadores para a obtenção de uma resposta multissetorial, coerente, coordenada e integrada" (Silva, 2022, p. 30), designadamente entre as Forças e Serviços de Segurança, os Serviços de Informações e as

Forças Armadas. A necessidade de coordenação e cooperação estende-se além-fronteiras, cujo "desafio consistirá em melhorar os mecanismos de cooperação policial e judicial internacional, de forma a garantir a segurança, a realização da justiça, com o fim último de, não só manter, mas de aprofundar a liberdade" (Elias, 2022, p. 223). As ameaças híbridas incidem frequentemente na «zona cinzenta». Por exemplo, uma ciberameaça pode ser um ato de guerra, se perpetrado por um Estado, requerendo uma resposta militar, contudo pode ter origem num grupo criminoso, requerendo uma resposta da segurança interna, pese embora a autoria possa ter interferência dissimulada por parte de um ator Estatal.

No plano da segurança interna, procuramos demostrar que as ameaças híbridas afetam dimensões essenciais, designadamente ao nível da prevenção e segurança, uma vez que exigem a monitorização constante, em especial do espaço digital, da vigilância e deteção de sinais de radicalização e de fluxos informacionais anómalos. Por outro lado, as ameaças híbridas têm o potencial de desestabilizar o funcionamento da sociedade, quer através da interrupção de serviços críticos por ciberataques ou ataques diretos, quer por campanhas de desinformação capazes de gerar protestos, polarização social e sérios problemas de ordem pública e de insegurança. A desinformação tem o poder "interferir no planeamento e gestão dos incidentes, comprometendo a eficácia da atuação policial e a segurança das populações" (Fernandes, 2025, p. 48), sendo este vetor "uma das armas mais relevantes e de longo alcance" (Fernandes, 2025, p. 51). Ao nível da investigação criminal, colocam-se desafios complexos devido à sofisticação tecnológica e à dimensão transnacional, sendo importante que "se procure adequar a ordem jurídica interna aos novos desafios, que se verifique um maior investimento do Estado na capacitação dos recursos humanos policiais sobretudo na área do cibercrime e das ciberameaças" (Elias, 2022, p. 220).

O estudo procurou enunciar quais as principais estratégias, instrumentos e órgãos que lidam com ameaças híbridas. Existem estratégias e capacidades para lidar com alguns dos vetores de ameaça híbrida e outras estão em desenvolvimento, sobretudo ao nível da cibersegurança (Diretiva NIS2) e das infraestruturas críticas – Decreto-Lei n.º 22/2025 relativa à identificação, designação e reforço da resiliência das entidades críticas –, sendo evidente a preocupação do Estado em ser mais resiliente nesta temática, acompanhando a tendência europeia. Verificamos uma fragmentação institucional significativa, relativamente aos órgãos elencados, tutelados por diferentes ministérios, o que nem sempre favorece a resposta ágil que se impõe na prevenção e combate às ameaças híbridas.

Com efeito, a análise desenvolvida ao longo deste trabalho permitiu atingir os objetivos inicialmente propostos e responder à pergunta de partida: o que são ameaças híbridas e de que modo afetam a segurança interna de Portugal?

De facto, as ameaças híbridas têm um impacto no normal funcionamento da sociedade, com a qual a segurança interna lida quotidianamente, ao nível da prevenção e segurança, da ordem pública e também da investigação criminal. Além do trabalho fundamental de cooperação entre os diversos intervenientes, consideramos importante estabelecer protocolos de atuação, realizar exercícios conjuntos, bem como dispor de planos de contingência adequados às ameaças híbridas, elaborados com base em *intelligence* e cenários.

Enquanto limitação do estudo, destacamos que, relativamente à participação de Portugal no Hybrid CoE não conseguimos compreender de que forma a representação portuguesa se materializa, quais os resultados alcançados e quais os objetivos estratégicos e políticos. Apesar da relevância das ameaças híbridas na segurança interna, cremos que o tema tem sido bem mais aprofundado e trabalhado ao nível da defesa, impondo-se o desafio de melhorar e densificar o conhecimento destas matérias através da lente das ciências policiais.

No caso da PSP, impõe-se o desafio de melhorar o policiamento na dimensão do ciberespaço, considerando a relevância que este tem na sociedade atual. Apesar dos passos que foram dados, nomeadamente através da criação da DACCCI, anteriormente referida, importa estender a abordagem além da investigação criminal, envolvendo outras áreas de missão da PSP.

Como linhas de investigação futuras, releva o estudo sobre como se processa a cooperação e coordenação entre os diversos intervenientes na prevenção e combate às ameaças híbridas em Portugal. Destacamos a importância de explorar o impacto da transposição da Diretiva NIS2 na cibersegurança nacional. Estudar as consequências da desinformação e das notícias falsas na segurança objetiva e na perceção de segurança dos cidadãos é igualmente uma área muito relevante e com um forte reflexo na missão quotidiana das polícias. Aprofundar o conhecimento sobre a resiliência das infraestruturas críticas, em especial as vulnerabilidades de setores como energia, transportes e telecomunicações e o impacto do recente Decreto-Lei n.º 22/2025 é igualmente uma área de elevada relevância. Por fim, salientamos a pertinência em estudar as potencialidades da Inteligência Artificial, seja na perspetiva da sua utilização para monitorizar e prevenir

ameaças híbridas, seja na perspetiva da sua utilização por parte de atores hostis e assim mitigar vulnerabilidades.

Concluindo, esperamos, deste modo, dar um modesto contributo para o estudo das ameaças híbridas no contexto da segurança interna, sublinhando-se a necessidade de estas serem consideradas nos planeamentos aos diversos níveis – político, estratégico, operacional e tático.

Referências

Assembleia da República, D. D. (2025). *Votações Efetuadas em 19-09-2025.* Obtido de https://app.parlamento.pt/WebUtils/docs/doc.pdf?Path=hVlmuGJD3rgHuzGeDCz9oRLwwoBwHd96bKqDybu1sXIUhB%2beSgy8H6tSLGkH5t3LxacIZcRrlxBJfn18P8M66XY%2f6vTjI85qwoFhQjkuy%2bQLwPoySFJfVZW21Vy%2f84UwdflNjyZlJwoHHA6%2b37nzBOOYZLvrpUx%2f32G%2bt0gm9194WGfKlDfJs5jhtfWv

Brandão, A. P. (2015). *O Nexo Interno-Externo na narrativa Securitária da União Europeia.* JANUS.NET e-journal of International Relations, Vol. 6, N.º 1, Maio-Outubro 2015. Obtido de https://repositorio.grupoautonoma.pt/entities/publication/203f8e3f-27fb-4a9a-b9ae-749b5a9d2d70

Cibersegurança, C. N. (2025). *6.ª edição do Relatório de Cibsersegurança, tema Riscos e Conflitos.* Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS). Obtido de https://www.cncs.gov.pt/docs/rel-riscosconflitos2025-obcibercncs.pdf

CoE, H. (2025). *Hybrid CoE is an autonomous, network-based international organization countering hybrid threats.* Obtido em 02 de setembro de 2025, de https://www.hybridcoe.fi/

Constituinte, A. (1976). *Constituição da República Portuguesa (VII Revisão Constituicional - 2005).* Obtido de https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx

DNPSP, A. I.-P.-D. (2024). *Despacho n.º 1168/2024, de 31 de janeiro, Define as unidades orgânicas flexíveis da unidade Direção Nacional da PSP*. Diário da República n.º 22/2024, Série II de 2024-01-31, páginas 45 - 83. Obtido de https://diariodarepublica.pt/dr/detalhe/despacho/1168-2024-839796305

DNPSP, D. N. (2025). *Estratégia 2025-2027 Polícia de Segurança Pública.* PSP. Obtido de https://www.psp.pt/Documents/Instrumentos%20de%20Gest%C3%A3o/Documentos%20Estrat%C3%A9gicos/Estrat%C3%A9gia%20da%20PSP%202025-2027.pdf?lang=pt

Elias, L. (2013). *A Externalização da Segurança Interna as dimensões global, europeia e lusófona.* (IPRI-UNL, Ed.) Relações Internacionais. Obtido de https://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri40/n40a02.pdf

Elias, L. (2022). *Ciências Policiais e Segurança Interna: Desafios e Prospetiva (revista e atualizada, 2.ª ed.).* Lisboa: Centro de Investigação (ICPOL) do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

ERSE, E. R. (2025). *Investigação do Grupo de Peritos da ENTSO-E ao Apação Ibérico de 28 de abril de 2025.* ERSE. Obtido de https://www.erse.pt/media/5lupni5p/erseexplica_apag%C3%A3o-reuni%C3%A3o-2set2025-vf.pdf

Europeia, C. (2016). *Comunicação Conjunta ao Parlamento Europeu e ao Conselho, Quadro comum em matéria de luta contra as ameaças híbridas, uma resposta da União Europeia.* Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018

Europeia, C. (2016). *Relatório Conjunto ao Parlamento Europeu e ao Conselho relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia.* Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017JC0030

Europeia, C. (2018). *Comunicação Conjunta ao Parlamento Europeu, ao Conselho Europeu e ao Conselho, Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas.* Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018JC0016&from=PT

Europeia, C. (2020). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europei, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a Estratégia da UE para a União da Segurança.* Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0605&from=EN

Europeia, C. (2024). *Comunicação da Comissão ao Parlamento Europeu e ao Conselho, sobre a luta contra as ameaças híbridas resultantes da instrumentalização da migração e o reforço da segurança nas fronteiras externas da UE.* Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52024DC0570

Europeia, C. (2025). *sobre a ProtectEU: uma Estratégia Europeia de Segurança Interna.* Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económio e Social Europeu e ao Comité das Regiões. Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52025DC0148

Europeia, C. d. (2022). *Bússola Estratégica para a Segurança e a Defesa – Por uma União Europeia que protege os seus cidadãos, os seus valores e os seus interesses e contribui para a paz e a segurança internacionais.* Obtido de https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pt/pdf

Europeu, P. d., Europeia, P. d., & Secretário-Geral , d. (2016). *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.* Obtido de https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

Europeu, P., & da Europa, C. (2022). *Relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.o 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2).* Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022. Jornal Oficial da União Europeia. Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555

Europol. (2025). *O ADN em da criminalidade grave e organizada - Avaliação da Ameaça da Criminalidade Grave e Organizada da União Europeia de 2025 - Síntese.* Serviço das Publicações da União Europeia. Obtido de https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

Fernandes, R. N. (2024). *2024: A soma de todos os riscos geopolíticos.* ICPOL – Centro de Investigação do Instituto Superior de Ciências Policiais e Segurança Interna. doi:https://doi.org/10.57776/vgh4-sz77

Fernandes, R. N. (2025). *Outlets de Desinformação na Nova Geopolítica Digital* . Centro de Investigação (ICPOL) do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

Forum, W. E. (2025). *The Global Risks Report 2025.* https://www.weforum.org/publications/global-risks-report-2025/.

Interna, S. S. (2025). *Relatório Anual de Segurança Interna 2024 (RASI)*. SSI. Obtido de https://www.portugal.gov.pt/pt/gc24/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-rasi-2024

Júnior, H. d., & Brandão, A. P. (2021). *Rupturas conceituais de segurança e meio ambiente no Antropoceno: os nexos securitários em formação desde o pós-guerra fria.* Tempo & Argumento, vol. 13, núm. 32. doi:http://dx.doi.org/10.5965/2175180313322021e0109

Lourenço, N., Lopes, A. F., Rodrigues, J. C., Costa, A., & Silvério, P. (2015). *Segurança Horizonte 2025. Um Conceito de Segurança Interna.* (G. –G. Interna, Ed.) Edições Colibri.

Lusa. (14 de 11 de 2012). S*ete detidos e 48 feridos nos confrontos junto ao Parlamento, segundo a PSP*. *PÚBLICO*. Obtido de https://www.publico.pt/2012/11/14/economia/noticia/greve-ao-minuto-1572391

Ministros, P. d. (2019). *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Resolução do Conselho de Ministros n.º 92/2019. Diário da República n.º 108/2019, Série I de 2019-06-05. Obtido de https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962

Ministros, P. d. (2019). *Aprova a nova estrutura organizacional da Polícia Judiciária.* Decreto-Lei n.º 137/2019, de 13 de setembro, na redação atual. Diário da República n.º 176/2019, Série I de 2019-09-13. Obtido de https://diariodarepublica.pt/dr/detalhe/decreto-lei/137-2019-124680594

Ministros, P. d. (2022). *Estabelece a Lei Orgânica do Estado-Maior-General das Forças Armadas e altera as Leis Orgânicas dos três ramos das Forças Armadas.* Decreto-Lei n.º 19/2022, de 24 de janeiro. Diário da República, 1.ª série. Obtido de https://files.dre.pt/1s/2022/01/01600/0000300097.pdf

Ministros, P. d. (2025). *Transpõe a Diretiva (UE) 2022/2557, relativa à identificação, designação e reforço da resiliência das entidades críticas.* Decreto-Lei n.º 22/2025, de 19 de março. Diário da República n.º 55/2025, Série I de 2025-03-19. Obtido de https://diariodarepublica.pt/dr/detalhe/decreto-lei/22-2025-911488699

Nacional, C. d. (2023). *Relatório do Conselho de Revisão do Conceito Estratégico de Defesa Nacional.* IDN. Obtido de https://www.idn.gov.pt/pt/noticias/Documents/2023/CEDN_teste.pdf

NATO. (2022). *Strategic Concept.* NATO. Obtido de https://www.nato.int/strategic-concept/

Peace, I. f. (2025). *Global Terrorism Index 2025: Measuring The Impact of Terrorism.* Obtido de http://visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf

Peace, I. f. (2025b). *Global Peace Index 2025: Identifying and Measuring the Factors that.* Obtido de https://www.visionofhumanity.org/wp-content/uploads/2025/06/Global-Peace-Index-2025-web.pdf

Pereira, J. (2018). *As Ameaças Híbridas – Uma Abordagem Conceptual no Quadro da OTAN e da UE.* CEDIS Working Papers, outubro 2018.

República, A. d. (2007). *Lei Orgânica da PSP.* Lei n.º 53/2007, de 31 de Agosto (na redação atual). Diário da República n.º 168/2007, Série I de 2007-08-31. Obtido de https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2007-174279072-174332731

República, A. d. (2007). *Orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança.* Lei n.º 9/2007, de 19 de Fevereiro (na redação atual). Obtido de https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2007-162667591

República, A. d. (2008). *Lei de Segurança Interna.* Lei n.º 53/2008 (na redação atual). Diário da República n.º 167/2008, Série I de 2008-08-29. Obtido de https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2008-34501675-108311212

República, A. d. (2009). *Lei de Defesa Nacional.* Lei Orgânica n.º 1-B/2009, de 7 de Julho (na redação atual). Diário da República n.º 138/2009, Série I de 2009-07-20. Obtido de https://diariodarepublica.pt/dr/legislacao-consolidada/declaracao-rectificacao/2009-67356360

República, A. d. (2018). *Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informa.* Lei n.º 46/2018, de 13 de agosto. Diário da República n.º 155/2018. Obtido de https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384

Sari, A. (2020). *Hybrid CoE Trend Report 3, Hybrid threats and the law: Concepts, trends and implications.* Hybrid CoE.

Silva, V. P. (2022). *«Defesa interna, segurança externa»: sobreposição, tensão e complementaridade na coordenação e articulação entre as Forças Armadas e as Forças e Serviços de Segurança em Portugal.* Tese de Doutoramento, ISCTE. Obtido de http://hdl.handle.net/10071/28728

Talbot, H., & Olson, J. (2025). *NewsGuard AI False Claims Monitor, Monthly audit of the 11 leading generative AI tools and their propensity to repeat false claims or decline to provide an answer on topics in the news.* NewsGuard.

Towles, A. (2018). *Um Gentleman em Moscovo* (6.ª edição ed.). (T. Ganho, Trad.) Publicações D. Quixote.

UNDP, U. N. (2025). *Human Development Report 2025: A matter of choice: People and possibilities in the age of AI.* Obtido de https://hdr.undp.org/content/human-development-report-2025