O Papel da Inteligência Artificial e das Tecnologias Emergentes na Proteção Contra Ameaças Híbridas

Estágio EuroDefense-Portugal: Outono 2025

Trabalho de Investigação

Coordenador: Eng.º Paulo Moniz

Autores:
Constança Martinho
Daniela Simões
Julia Peixoto
Mariana Raimundo
Tomás Barradas

Índice

1. Metodologia

1.1 Abordagem Metodológica

O presente trabalho de investigação adota uma metodologia qualitativa, com o objetivo de compreender o papel da Inteligência Artificial (IA) na mitigação e prevenção de ameaças híbridas. A escolha desta abordagem prende-se com a elevada complexidade do tema, bem como com a sua natureza multidimensional, que articula diversas dimensões, tais como a tecnológica, militar, informacional, social, institucional e política. Atendendo a estas características, torna-se também essencial explorar as dinâmicas entre os atores envolvidos, as suas capacidades e as estratégias que mobilizam.

Para que esta análise seja passível de ser conduzida, proceder-se-á, no Capítulo III, à operacionalização e clarificação conceptual de noções centrais ao estudo, nomeadamente Ameaças Híbridas, Tecnologias Emergentes e o uso da IA no âmbito da Segurança e Defesa.

A análise qualitativa proposta irá assentar na interpretação de documentos académicos, institucionais e de carácter estratégico, permitindo explorar a evolução das respostas institucionais, das opções estratégicas adotadas e das narrativas e opções políticas subjacentes à adoção/incorporação de tecnologias emergentes enquanto instrumentos de segurança. Considerando a natureza difusa das ameaças híbridas e a crescente integração das tecnologias emergentes e disruptivas, como a IA, nas esferas da segurança e da defesa, revela-se fundamental adotar uma abordagem contextualizada, crítica e interdisciplinar, capaz de captar a complexidade e interdependência dos fenómenos em análise.

1.2 Questões de Investigação e Modelo de Análise

Na sequência do enquadramento metodológico apresentado acima, o presente trabalho estrutura-se em torno de duas questões centrais de investigação.

i) Em que medida a IA tem vindo a ser integrada nas políticas e práticas dos Estados, em resposta a ameaças híbridas?

ii) Que limitações técnicas, éticas ou institucionais condicionam a integração da IA nas políticas e práticas dos Estados em resposta a ameaças híbridas?

Com vista a responder a estas questões, conduzir-se-á uma análise qualitativa dos documentos e materiais recolhidos, incluindo documentos estratégicos da União Europeia, como a *Bússola Estratégica*, o *Cyber Solidarity Act*, o *EU Hybrid Fusion Cell* e o *Plano de Ação Contra a*

Desinformação, e da NATO (em português OTAN, i.e., Organização do Tratado do Atlântico Norte), nomeadamente o seu *Conceito Estratégico* e as iniciativas de inovação no âmbito da ciberdefesa e da Inteliência Artificial. Esta análise é ainda complementada por fontes académicas e documentos produzidos por centros especializados, tais como o Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), localizado em Helsínquia, e o CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence), localizado em Tallinn.

Adicionalmente, recorrer-se-á à análise de casos reais, ilustrativos da prática de ameaças híbridas, nomeadamente ações atribuídas à China, no âmbito de interferência económica e digital em países europeus, e à Rússia, particularmente no que respeita à anexação da Crimeia e à disseminação de campanhas de desinformação dirigidas à União Europeia (UE). Estes exemplos, permitem-nos observar a articulação entre a manifestação de ameaças híbridas e as respostas baseada na incorporação de tecnologias emergentes, como a IA, evidenciando, ao mesmo tempo, o seu potencial e as limitações que se colocam à sua utilização no domínio da segurança e defesa.

2. Introdução

2.1. Enquadramento do Tema

As *ameaças híbridas* constituem, na atualidade, um dos desafios mais complexos e transversais à segurança internacional. Caracterizam-se pelo uso articulado de instrumentos militares e não militares, combinando meios convencionais e irregulares, visíveis e encobertos, com o propósito de explorar vulnerabilidades estruturais dos Estados e das sociedades democráticas.

De acordo com a NATO, estas ameaças podem manifestar-se através de "ataques cibernéticos, campanhas de desinformação, pressões económicas e operações de influência", operando frequentemente abaixo do limiar de um conflito armado formal (NATO, 2024). Também a UE entende as ameaças híbridas como ações coordenadas que combinam instrumentos diplomáticos, militares, económicos e tecnológicos, conduzidas por atores estatais e não estatais, com o objetivo de desestabilizar processos políticos e sociais de um estado (European Commission, 2024).

Num contexto internacional profundamente marcado pela digitalização e interconectividade, as fronteiras entre paz e conflito tornaram-se cada vez mais difusas. A segurança e a defesa nacional dos Estados passou a depender, não apenas de capacidades militares tradicionais, mas também da resiliência informacional, cibernética e tecnológica (Instituto da Defesa Nacional, 2023).

Paralelamente, o avanço de tecnologias emergentes, como a Inteligência Artificial, a IoT[1], o 5G, a computação quântica, *o blockchain* e a análise massiva de dados, têm alterado profundamente o panorama estratégico e de segurança internacional. Se por um lado estas tecnologias criam novas vulnerabilidades (por ex., a sua adoção acelerada aumenta a superfície de ataque cibernético e expõe infraestruturas críticas a formas de sabotagem ou interferência invisíveis e altamente sofisticadas), simultaneamente, também criam novas oportunidades (por

[1] A Internet das Coisas (IoT, do inglês Internet of Things), pode definir-se como o conjunto de objetos físicos, incluindo eletrodomésticos, veículos e acessórios como *smartwatches*, que estão ligados à internet e que podem comunicar entre si. Estes objetos possuem sensores, software e tecnologia de comunicação que lhes permite recolher, processar e partilhar dados de forma autónoma, sem necessidade de intervenção humana constante. (Caixa Geral de Depósitos, 2025)

exemplo, oferecem instrumentos inovadores de prevenção, deteção e resposta a ameaças multidimensionais, tais como as ameaças híbridas).

2.2. Objetivos do Trabalho

O presente trabalho tem como objetivo analisar o papel das tecnologias emergentes, com especial destaque para a Inteligência Artificial (IA), na proteção contra ameaças híbridas.

Deste modo propõe-se:

- Explorar o conceito de ameaças híbridas e as diferentes tipologias existentes, examinando o seu papel.
- Analisar os fundamentos e aplicações da IA no contexto do conflito armado e não armado.
- Avaliar a integração destas tecnologias nas estratégias de defesa cibernética e segurança no plano internacional
- Identificar os principais desafios técnicos, éticos e institucionais associados à sua implementação.

Com base nestes objetivos, pretende-se compreender em que medida a inovação tecnológica pode reforçar a resiliência estatal e institucional, num ambiente estratégico cada vez mais volátil.

2.3. Relevância do Tema

A relevância do estudo sobre o papel das tecnologias emergentes na proteção contra as ameaças híbridas reside na crescente interdependência entre a transformação digital, a segurança global e a resiliência democrática das sociedades contemporâneas.

Na atual Era da Informação e da Conectividade Total, os Estados e as organizações enfrentam um ambiente estratégico em que as fronteiras entre guerra e paz, segurança interna e externa, ou esfera civil e militar, se tornam cada vez mais difusas. As ameaças híbridas exploram precisamente estas zonas de indefinição, i.e., zonas cinzentas entre guerra e paz, combinando instrumentos tecnológicos, económicos, informacionais e psicológicos para alcançar objetivos políticos sem desencadear um conflito convencional. O avanço acelerado de tecnologias como a IA, a Internet das Coisas, o 5G, a computação quântica, o *blockchain* e a análise massiva de dados têm ampliado simultaneamente as capacidades defensivas e as superfícies de ataque.

Ao nível das organizações internacionais, tanto a UE como a NATO reconhecem que a revolução digital transformou a natureza do conflito contemporâneo, tornando indispensável o investimento em capacidades tecnológicas avançadas, capazes de detetar, prevenir e responder a ataques multidimensionais (NATO, 2024), e exigindo abordagens coordenadas que integrem a dimensão tecnológica, normativa e societal (European Commission, 2024).

Por conseguinte, compreender a relação entre tecnologias emergentes e ameaças híbridas revela-se essencial para:

- A formulação de políticas eficazes de cibersegurança;
- A preservação da soberania digital;
- A proteção da confiança pública;
- A estabilidade institucional.

A importância do tema decorre ainda do seu impacto direto sobre a governação e a cooperação internacional. Vráb (2025) argumenta que as tecnologias emergentes redefinem o conceito de soberania, uma vez que o controlo de dados, algoritmos e redes passou a ser um elemento central do poder nacional e da autonomia estratégica. Também o *UK Government* (2025) destaca que as tecnologias emergentes podem simultaneamente fortalecer e fragilizar os sistemas de segurança, consoante o modo como são implementadas e reguladas.

Assim, a proteção contra ameaças híbridas requer a coordenação entre instituições civis, militares e privadas (Tsaruk e Korniiets 2023), bem como a harmonização de políticas europeias e transatlânticas no domínio da cibersegurança e da inovação tecnológica. O relatório do *European Union Agency for Cybersecurity* (ENISA, 2024) salienta a necessidade de criar ecossistemas de segurança digital resilientes, nos quais as tecnologias emergentes sejam utilizadas para detetar vulnerabilidades, partilhar informações e mitigar riscos antes que se transformem em crises.

Por fim, a natureza interdisciplinar do tema, cruzando os campos da ciência política, dos estudos de segurança, da engenharia informática, da ética e governação global, reforça a sua pertinência académica e estratégica. Na prática, o estudo das tecnologias emergentes no contexto das ameaças híbridas oferece um espaço de investigação essencial para compreender como a inovação tecnológica molda o poder, a soberania e a segurança no século XXI,

constituindo uma necessidade estratégica para assegurar a estabilidade, a resiliência e a liberdade das sociedades contemporâneas.

3. Enquadramento Teórico

3.1. Conceito de Ameaças Híbridas

De acordo com o European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), o conceito de ameaças híbridas refere-se à combinação coordenada de instrumentos militares e não militares, utilizados de forma ambígua e frequentemente encoberta para explorar vulnerabilidades estruturais. A sua principal característica reside na ambiguidade e dificuldade de atribuição, dificultando a identificação de responsabilidades e a adoção de medidas de resposta proporcional (Hybrid CoE, 2024).

3.1.1 Definições Conceptuais Dentro da NATO e UE e o seu Impacto nas Organizações

Impacto na NATO. O reconhecimento e a definição interna do fenómeno em causa, levou a que a Organização se adaptasse e preparasse face a uma tipologia de conflito que, até então, não se enquadrava nos reconhecidos modelos tradicionais de paz e guerra. Assim, a NATO passa a entender que as atividades híbridas empregam uma vasta gama de medidas militares, paramilitares e civis, abertas ou encobertas, num desígnio altamente integrado (Jan Jakub Uziębło, 2017). Uma outra evolução diz respeito ao facto da doutrina da Organização passar a considerar que as operações híbridas contra a Aliança, poderiam atingir o nível de um ataque armado e, consequentemente, levar à invocação do Artigo 5º do Tratado do Atlântico Norte[2].

Como resultado do reconhecimento do fenómeno das ameaças híbridas, a NATO passa também a focar-se na resiliência e na dissuasão, desenvolvendo: a ideia de "dissuasão por negação", i.e., reduzir o benefício percebido de uma ação através do reforço das defesas; e a "dissuasão pela resiliência "*deterrence-by-resilience*", que envolve a garantia da capacidade de sobrevivência do governo e da resiliência da sociedade e infraestruturas críticas (Jan Jakub Uziębło, 2017).

Por fim, a NATO expandiu o conjunto das suas ferramentas e estratégias, adotando uma abordagem específica contra atores e ameaças e, deste modo, desenvolvendo o conceito de apoio híbrido (*Counter Hybrid Support Team*). Este ponto exigiu também da Organização a

[2] O Artigo 5º do Tratado do Atlântico Norte, que consubstancia a criação da NATO, afirma o Princípio da Defesa Coletiva em que, um ataque armado contra um ou mais membros, constitui um ataque contra todos.

melhoria da partilha de informações e do estabelecimento de "indicadores de alerta precoce" (Jan Jakub Uziębło, 2017).

Impacto na União Europeia. O impacto da problemática das ameaças híbridas na UE está particularmente relacionado ao desafio de ligar as suas capacidades civis e políticas a questões de segurança, entendidas como do foro militar noutras organizações.

Ao nível de mecanismos de resposta concretos, note-se a criação do Centro de Fusão Híbrida da UE (*UE Hybrid Fusion Cell*), incorporado no Centro de Situação e Informações da UE, cujo objetivo é analisar os padrões das campanhas híbridas e fornecer consciência situacional aos decisores.

Não obstante, face à estrutura de governação da UE e ao seu quadro legal complexo, embora os Estados-membros tenham cedido grande parte da sua soberania à Organização aquando da sua adesão, estes retêm o poder de definir as suas próprias políticas de segurança, pelo que o combate às ameaças híbridas em cada Estado-membro se trata de uma responsabilidade nacional. Assim, esta idiossincrasia assume-se como fator inibidor de uma resposta central unificada ao fenómeno das ameaças híbridas. Neste sentido, torna-se bastante relevante a questão da coordenação e resiliência, uma vez que o papel da UE se centra em fornecer uma plataforma para harmonizar respostas e construir resiliência social, económica e política a nível nacional e europeu.

3.2. Tecnologias Emergentes no Contexto de Segurança

As tecnologias emergentes (Inteligência Artificial (IA), *machine learning*, computação quântica, a Internet das Coisas (IoT), as redes 5G, o *blockchain* e a análise de *Big Data*), assumem um papel duplo no contexto das ameaças híbridas: são simultaneamente multiplicadores de ameaça e instrumentos determinantes de mitigação.

Segundo a Agência da União Europeia para a Cibersegurança (ENISA), a disseminação destas tecnologias, embora traga ganhos de eficiência e inovação, amplia a superfície de ataque digital, tornando o ecossistema mais vulnerável e exigindo abordagens de segurança integradas e proativas (ENISA, 2024). De forma semelhante, o *Hague Centre for Strategic Studies* (HCSS) e a TNO (*Netherlands Organisation for Applied Scientific Research*), sublinham que estas tecnologias funcionam como "multiplicadores de ameaça", uma vez que permitem

acelerar, escalar e sofisticar operações híbridas, conferindo aos atores hostis novas formas de coordenação e impacto (HCSS & TNO, 2024).

Paralelamente, a mesma transformação tecnológica abre possibilidades inéditas para a defesa, nomeadamente através da utilização de algoritmos inteligentes para detetar comportamentos anómalos, prever ataques ou automatizar respostas a incidentes cibernéticos. O Centro de Excelência para a Defesa Cibernética Cooperativa (CCDCOE) da NATO destaca que compreender as implicações estratégicas das tecnologias emergentes é essencial para garantir a resiliência dos sistemas críticos e a soberania digital dos Estados (CCDCOE, 2020).

Aplicadas à proteção contra ameaças híbridas, estas tecnologias podem reforçar diversas dimensões da segurança. Entre as principais aplicações defensivas destacam-se:

- Através da IA e *Big Data*: deteção precoce de padrões anómalos e a monitorização em tempo real de fluxos de informação, facilitando a identificação de tentativas de intrusão, manipulação ou interferência em redes sociais.
- Recurso a sensores inteligentes, à IoT e aos chamados "gémeos digitais", (versões virtuais de objetos reais) permite: supervisão contínua e adaptável das infraestruturas críticas, aumentando a sua resiliência operacional.
- O *blockchain* oferece mecanismos de autenticação e rastreabilidade que reforçam a integridade da informação e das transações, mitigando riscos associados à desinformação e à adulteração de dados sensíveis.
- As tecnologias emergentes permitem realizar simulações avançadas para treino e planeamento estratégico face a cenários híbridos e não híbridos. Através de simulações avançadas e ambientes virtuais, é possível testar e aperfeiçoar respostas institucionais, reforçando a coordenação entre entidades civis, militares e privadas. Este tipo de planeamento preditivo é fundamental para reduzir o impacto de ataques coordenados que combinam domínios cibernéticos, económicos e psicológicos.

Note-se que, a utilização das tecnologias emergentes, na proteção eficaz contra ameaças híbridas, exige uma abordagem multidimensional que integre fatores políticos, jurídicos e sociais. O reforço da literacia digital, a promoção da cooperação internacional, a criação de estruturas de governação resilientes e a articulação entre setores público e privado são elementos centrais neste processo (Instituto da Defesa Nacional, 2023).

Contudo, como observámos acima, o uso destas tecnologias na segurança nacional não está isento de riscos. O governo britânico alerta que as tecnologias emergentes podem igualmente ser exploradas por adversários para contornar sistemas de defesa, quebrar criptografias ou manipular dados de forma indetectável (UK Government, 2024). Além disso, a rápida evolução tecnológica tende a gerar um desfasamento entre capacidades ofensivas e defensivas, o que fragiliza os mecanismos de resposta institucional e a atualização das políticas de cibersegurança (CCDCOE, 2020).

Em síntese, as tecnologias emergentes representam simultaneamente uma fonte de vulnerabilidade e uma oportunidade estratégica na mitigação das ameaças híbridas. O seu impacto dependerá da capacidade das instituições em integrá-las de forma ética, coordenada e sustentável, garantindo um equilíbrio entre inovação tecnológica, segurança e proteção dos valores democráticos. Assim, compreender o papel destas tecnologias é essencial para delinear políticas de defesa que sejam simultaneamente preventivas, adaptativas e resilientes, num contexto internacional onde a fronteira entre a guerra e a paz é cada vez mais permeável.

3.3. Dimensão Política

A IA, em particular, transformou profundamente a forma como o poder é exercido no plano internacional. A sua incorporação nas indústrias de defesa contemporâneas, nomeadamente nos setores de vigilância, logística e cibersegurança, tem impacto estratégico significativo.

Entre as inovações mais discutidas encontram-se os sistemas de armas letais autónomos (SALAs), os programas de previsão e seleção de alvos, e os mecanismos de coordenação sustentados por algoritmos de aprendizagem automática. Embora proporcionem benefícios estratégicos, estas tecnologias levantam dilemas éticos e implicações sociais de grande relevância, sobretudo no que concerne à responsabilidade e à autonomia decisória.

Face a isto, observa-se hoje uma competição tecnológica desenfreada entre as grandes potências, intensificada pela IA (a qual é fator central da geopolítica), em que as potências adotam diferentes abordagens para salvaguardar os seus interesses e assegurar a sua soberania na disputa armamentista tecnológica. Nos últimos anos, especialistas, formuladores de políticas e líderes mundiais, dos EUA, da China e da Rússia, têm adotado uma visão instrumentalista e solucionista da tecnologia, especialmente diante de um cenário geopolítico volátil e da crescente competição tecnológica entre si. (Shaw, 2013)

Esta divisão no sistema internacional, proveniente da desigualdade tecnológica e da corrida para a sua evolução, descrita como *cortina de ferro* (Esposito, 2025) cria um ambiente dominado pela desconfiança mútua no cenário internacional, com padrões tecnológicos incompatíveis devido à falta de regularização e gerando mais barreiras a uma cooperação global.

Para além disto, esta nova corrida armamentista, para atores como a China e Rússia, assume-se como oportunidade essencial para desafiar a hegemonia estadunidense no campo militar. A IA tornou-se um mecanismo com capacidade de mudar o predomínio ocidental, substancialmente dos Estados Unidos desde o fim da Guerra Fria, no contexto bélico. Deste modo, entende-se a utilização da IA, do ponto de vista da sua dimensão política, como um agente da instabilidade global devido à falta de coordenação, cooperação e à complexidade associada às limitações e dificuldades no processo de regulamentação e democratização das novas tecnologias.

3.4. Dimensão Social e Institucional

A dimensão social das tecnologias emergentes no contexto das ameaças híbridas constitui um dos aspetos mais sensíveis e determinantes para a estabilidade das sociedades contemporâneas.

A tecnologia, longe de ser um domínio neutro, interage profundamente com os comportamentos humanos, com as estruturas de poder e com a própria perceção da realidade. Assim, o impacto social das ameaças híbridas manifesta-se sobretudo na forma como estas exploram vulnerabilidades cognitivas e emocionais da população, amplificadas pela omnipresença das plataformas digitais e pela velocidade de circulação da informação.

A ascensão das tecnologias emergentes permitiu a personalização extrema da comunicação digital, mas também abriu espaço à manipulação informacional e à segmentação social dirigida. Atores mal-intencionados, sejam estatais ou não estatais, utilizam dados recolhidos de forma massiva para criar campanhas de desinformação sofisticadas, adaptadas aos perfis individuais dos utilizadores, com o objetivo de influenciar opiniões políticas, polarizar comunidades e minar a confiança nas instituições democráticas (Mlinac, 2025).

Neste sentido, o fenómeno das ameaças híbridas transcende a dimensão tecnológica, assumindo contornos sociais e psicológicos. Ao disseminar narrativas falsas ou distorcidas, estas campanhas exploram divisões já existentes, culturais, ideológicas, religiosas ou

socioeconómicas, transformando as plataformas digitais em campos de batalha informacional. De acordo com a organização Friends of Europe (2024), as operações híbridas de influência não procuram apenas comprometer sistemas técnicos, mas sobretudo corroer o tecido social, reduzindo o capital de confiança que sustenta a coesão democrática. Esta desestruturação da confiança cívica tem efeitos diretos sobre a perceção pública da verdade, a credibilidade das fontes jornalísticas e a participação dos cidadãos, conduzindo a um ambiente de crescente desinformação.

Um dos impactos mais relevantes deste fenómeno é a fragilização da literacia digital e da capacidade crítica das populações. A desigualdade no acesso à informação e à educação tecnológica cria clivagens sociais profundas, tornando certos grupos mais suscetíveis à manipulação e à radicalização online. As campanhas de desinformação direcionadas aproveitam precisamente estas desigualdades para explorar medos e preconceitos, promovendo desunião e hostilidade entre comunidades. Este processo, como observa Stănescu (2023), contribui para a transformação da segurança digital num problema de segurança social, uma vez que as ameaças híbridas passam a atuar não apenas sobre infraestruturas, mas sobre a perceção e o comportamento das pessoas.

A nível institucional, a utilização maliciosa das tecnologias emergentes tem repercussões significativas sobre a legitimidade e a eficácia das instituições públicas. Quando a confiança nos meios de comunicação, nos processos eleitorais ou nas políticas governamentais é corroída, os cidadãos tornam-se mais propensos a acreditar em fontes alternativas, não verificadas. A proliferação de notícias falsas, *deepfakes* e campanhas de desinformação baseadas em IA pode criar perceções distorcidas de crise, alimentar descontentamento social e até gerar movimentos de contestação baseados em narrativas fabricadas. Deste modo, as ameaças híbridas produzem efeitos tangíveis sobre o equilíbrio político e social, podendo mesmo influenciar processos eleitorais e a estabilidade democrática.

Por outro lado, importa salientar que as tecnologias emergentes, quando devidamente reguladas e aplicadas, também oferecem oportunidades significativas para fortalecer a resiliência social. Iniciativas de literacia digital, programas de educação mediática e projetos de verificação de factos (*fact-checking*) desempenham um papel essencial no reforço da capacidade da sociedade para reconhecer e resistir à manipulação informacional. Tsaruk e Korniiets (2023) A associação Friends of Europe (2024) enfatiza que a construção de "resiliência digital" deve ser encarada como uma prioridade de segurança nacional e europeia, envolvendo não apenas governos, mas

também o setor privado, a academia e a sociedade civil. Assim, o investimento em competências digitais e a promoção de uma cultura de segurança informacional pode reduzir substancialmente o impacto das operações híbridas, transformando a tecnologia num fator de risco em um instrumento de coesão e defesa social.

Além disso, a resposta social às ameaças híbridas exige um compromisso coletivo com os valores democráticos e com a ética digital. A implementação de políticas públicas que promovam a transparência algorítmica, o combate à desinformação e a proteção dos dados pessoais é fundamental para restabelecer a confiança dos cidadãos na esfera digital. O equilíbrio entre liberdade de expressão e segurança informacional torna-se, assim, um dos principais desafios das democracias modernas.

Nessa perspetiva, a dimensão social das tecnologias emergentes é não apenas um reflexo das suas vulnerabilidades, mas também uma oportunidade para redefinir a cidadania digital e a participação cívica no século XXI. Em última análise, compreender esta dimensão é indispensável para assegurar que a inovação tecnológica contribua para o fortalecimento, e não para a erosão, dos valores e estruturas sociais que sustentam as sociedades democráticas.

3.5. Dimensão Científico-Militar

A guerra é um evidente propulsor da tecnologia, o que não se torna diferente no contexto do aumento das ameaças híbridas. Decorrente da urgência causada pela natureza específica das ameaças híbridas, a crescente procura por implementar novos tipos de armamento, táticas e estratégias cria um ambiente propício à evolução científico-tecnológica.

Deste modo, evidencia-se uma evolução das ferramentas tecnológicas, no contexto militar e de segurança e defesa, por exemplo, ao nível do desenvolvimento de drones, veículos de combate automatizados ou tecnologias que visam aumentar a assistência e o bem-estar dos combatentes. Particularmente, as soluções baseadas em IA, nomeadamente ao nível de capacidades sobre-humanas de deteção precoce de ameaças e comportamentos cibernéticos hostis, surgem também como complemento promissor aos métodos convencionais de segurança.

4. Tipologias de Ameaças Híbridas

Nesta secção apresentam-se as tipologias de ameaças híbridas mais comuns, evidenciando os seus mecanismos de atuação e os impactos que podem produzir na estabilidade e segurança dos Estados. Destacam-se:

Ciberataques. Ataques com alvo a infraestruturas digitais, como redes elétricas, sistemas de comunicação e redes governamentais, com o objetivo de causar perturbações, inviabilizar o funcionamento total de sistemas e roubar informações.

Desinformação e manipulação de informação. Inclui campanhas de desinformação, propaganda e manipulação de informações para influenciar a opinião pública, interferir em processos eleitorais e criar divisão social.

Coerção e/ou pressão económica. Envolve o uso de ferramentas económicas, como coerção, sanções ou manipulação do comércio para exercer pressão política.

Subversão política/interferência eleitoral. Esta categoria inclui manobras políticas secretas, interferência eleitoral e uso da corrupção para ganhar influência.

Ameaças de uso da força militar. Pode variar desde o uso convencional da força militar até táticas mais ambíguas, como guerra por procuração, o uso de forças especiais ou mesmo ameaças de ação militar para intimidar adversários.

Tecnologia. Inclui a exploração de vulnerabilidades tecnológicas, como as da infraestrutura 5G, para criar novos vetores de ataque.

Energia. Envolve o uso de controlo sobre o fornecimento de energia como meio de coerção.

4.1. Casos Ilustrativos da Prática de Ameaças Híbridas

Como exemplos práticos, destaca-se a Rússia, que emprega estratégias híbridas sofisticadas, como a interferência política, as atividades cibernéticas maliciosas, a pressão e coerção económicas, subversão, agressão e anexação. A postura militar coerciva e a retórica também são usadas como parte integrante das suas estratégias híbridas, para perseguir os objetivos políticos e minar a ordem internacional baseada em regras.

Adicionalmente, a China emprega operações híbridas e cibernéticas maliciosas, bem como a sua retórica de confronto e desinformação, visando atacar os aliados da NATO e prejudicar a sua segurança. Concretamente, a China procura controlar os setores tecnológicos e industriais

essenciais, infraestruturas críticas, materiais e cadeias de abastecimento estratégico, frequentemente utilizando a sua influência económica para criar dependências estratégicas.

Face ao exposto, podemos afirmar que na prática, as características principais das ameaças híbridas se encontram na combinação de:

- Táticas, sendo que estas raramente dependem de um único método, pois usam uma combinação coordenada de ferramentas para atingir os seus objetivos;
- O facto de se encontrarem abaixo do limiar da guerra, i.e., permanecem frequentemente abaixo do nível que desencadearia uma resposta militar tradicional, tornando-as difíceis de atribuir e combater;
- Erosão de confiança, uma vez que o objetivo final é muitas vezes, enfraquecer uma sociedade-alvo, a partir de dentro, quebrando a confiança entre o seu povo, as suas instituições e o seu governo;
- Linhas difusas, visto que esbatem as distinções tradicionais entre guerra e paz, combatentes e civis, e atores estatais e não estatais.

5. Políticas e Estratégias Europeias de Combate às Ameaças Híbridas

Enquadramento institucional e estratégico da UE relativamente às ameaças híbridas.

No atual contexto institucional e legal da UE, a responsabilidade principal pela luta contra as ameaças híbridas pertença a cada Estado-membro. No decorrer deste facto, os Estados muitas vezes coordenam-se entre si para combater coletivamente estas ameaças. Dentro das principais estratégias, encontramos: a Estratégia Global da UE (EUGS, 2016); a Comunicação Conjunta sobre Contrariar Ameaças Híbridas (2016); a Estratégia de Segurança Cibernética da UE (2020); e a Bússola estratégica da UE (2022).

Concretamente, a abordagem estratégica da Organização, relativamente a esta tipologia de ameaças, prende-se: na prevenção e deteção precoce (monitorização e partilha de informações); na resiliência das infraestruturas críticas e das sociedades democráticas; na resposta coordenada entre instituições europeias e Estados-membros.

Enquadramento institucional da UE e as Ameaças Híbridas

A resposta da União Europeia às ameaças híbridas assenta numa arquitetura institucional multissetorial, dispondo de um conjunto de organismos e mecanismos que asseguram a coordenação estratégica, a partilha de informações e a resposta operacional às ameaças híbridas, designadamente:

- **Serviço Europeu de Ação Externa** (SEAE). Coordena políticas externas e segurança. Inclui o *Hybrid Fusion Cell* (célula de análise de ameaças híbridas).
- **Comissão Europeia**. Implementa as políticas de cibersegurança, energia, comunicações e desinformação.
- **Conselho da União Europeia**. Implementa as políticas de cibersegurança, energia, comunicações e desinformação.
- **Agência da União Europeia para a Cibersegurança**. Coordena as medidas técnicas e de resposta a incidentes.
- **Centro Europeu de Excelência para Contrariar Ameaças Híbridas** (Hybrid CoE, estabelecido em 2017). Assume-se como um vetor fundamental para a partilha inter-organizacional (UE-NATO) de boas práticas em matéria de ciberdefesa, desinformação e proteção de infraestruturas e investigação.

- **Centro de Informações e Situação da UE** (EU INTCEN). Fornece a análise de informações estratégicas.
- **Mecanismos de resposta a crises da UE**. Coordenam as respostas interinstitucionais em caso de ataque híbrido.

5.1. Relevância da UE na Necessidade de Respostas Coordenadas Face às Ameaças

Como observado anteriormente, as ameaças híbridas apresentam uma natureza transnacional e multidimensional, podendo atingir simultaneamente diversos Estados-membros e setores críticos, como infraestruturas partilhadas e mercados comuns. Também a interdependência económica, energética e digital no seio da União, realça a insuficiência da ação isolada de cada Estado, exigindo mecanismos de respostas coordenados e consistentes a nível europeu.

Deste modo, a UE apresenta um valor único acrescentado neste domínio, precisamente devido à sua capacidade de articular as várias dimensões civis, económicas e de segurança. A disposição de mecanismos de cooperação e coordenação política, como o SEAE e o Hybrid CoE, leva à mobilização de recursos comuns, e assim, este tipo de estruturas permite o desenvolvimento de políticas comuns de resiliência, promoção de troca de informações e coordenação de respostas entre Estados-membros e parceiros estratégicos como, por exemplo, a NATO.

A coordenação europeia é, de facto, indispensável para garantir respostas coerentes e eficazes perante ameaças híbridas, que visam destabilizar sociedades democráticas, evitando a duplicação de esforços e assegurando as respostas rápidas e consistentes de cooperação UE-NATO. A conjugação de esforços entre as instituições europeias, Estados-membros e aliados externos reforça a resiliência coletiva, a eficácia global da segurança euro-atlântica e afirma a credibilidade da UE enquanto ator de segurança global.

5.2. Evolução do Enquadramento Político e Estratégico da União Europeia

A evolução do enquadramento político e estratégico da UE reflete o processo contínuo de aprofundamento da integração e adaptação de novos desafios globais e a redefinição das prioridades comuns. Recentemente, foram criadas estratégias e políticas que visam o combate às ameaças híbridas numa transição de uma postura fragmentada para uma estratégia mais integrada e de longo prazo. O fortalecimento da resiliência, da ciberdefesa e da cooperação

internacional passou a ser central para a segurança e estabilidade da União num contexto global cada vez mais complexo.

- **Bússola Estratégica (*Strategic Compass*).** A Bússola Estratégica de 2022 define o plano de ação para reforçar a segurança e defesa da UE até 2030, promovendo uma cultura estratégica comum e maior capacidade de proteger os cidadãos e contribuir para a paz internacional. Impulsionada pelo regresso da guerra à Europa com a invasão russa da Ucrânia e pelas atuais mudanças geopolíticas, a Bússola Estratégica visa fortalecer a autonomia estratégica da UE, melhorar a sua atuação em crises e salvaguardar os valores e interesses europeus. O documento apresenta ainda medidas concretas com prazos definidos para garantir uma implementação eficaz.

- **EU Hybrid Fusion Cell.** Visa melhorar o conhecimento situacional da UE face às atividades híbridas, reforçando a partilha e análise de informações entre os Estados-membros, instituições europeias e parceiros. Instalada no UE INTCEN do SEAE, funciona como um ponto único para recolher, analisar e difundir dados, classificados ou de fonte aberta, sobre as ameaças híbridas internas e na vizinhança da UE, apoiando as decisões estratégicas e avaliações de risco. Para isso, articulam-se estruturas nacionais e europeias, requerendo pontos de contacto em cada Estado-membro, incluindo a formação para detetar os sinais precoces de ameaças.

5.3. Outras Estratégias da UE

Strategic Communication. Consiste em responder de forma rápida e eficaz à desinformação difundida por diferentes autores de ameaças híbridas, usando campanhas factuais e coordenadas que envolvem as redes sociais e os meios de comunicação tradicionais. Visa também sensibilizar o público, reforçar a resiliência social e controlar a narrativa política. Para isso, recorre a linguistas e especialistas em redes sociais para monitorizar os conteúdos externos à UE e garantir respostas direcionadas. Aqui, revela-se importante que os Estados-membros articulem os mecanismos comuns para apoiar o combate à desinformação internamente.

Centro de Excelência para o combate a ameaças híbridas. Funciona como uma rede multinacional dedicada à I&D de conceitos e tecnologias que reforcem a resiliência dos Estados-membros. Analisa também como as estratégias híbridas são aplicadas, apoiando a harmonização de políticas e doutrinas, e promovendo os programas de investigação e exercícios práticos. A sua força reside na cooperação entre especialistas civis, militares,

académicos e o setor privado, trabalhando em articulação com os centros de excelência da UE e da NATO em áreas como a ciberdefesa, comunicação estratégica e a resposta a crises (Hybrid CoE).

6. Inteligência Artificial: Fundamentos e Áreas de Aplicação

A IA enquanto tecnologia multiuso, pode ser aplicada em diferentes cenários, desde a saúde até à defesa. Embora não exista uma definição única e universalmente aceite para o conceito de *Inteligência Artificial*, o MIT Media Lab descreve a IA como o desenvolvimento de *"sistemas capazes de realizar tarefas que normalmente requerem inteligência humana, tais como raciocínio, aprendizagem e resolução de problemas".* Uma característica que distingue os sistemas de IA, para além da demonstração de capacidade de raciocínio semelhante à dos seres humanos, é a capacidade de analisar grandes quantidades de dados e informação em questão de segundos, algo que os seres humanos não são capazes de fazer. (Rahnama, 2025)

O crescente interesse popular dado à IA dá-se em grande parte graças à inteligência artificial generativa. No entanto, as suas origens remontam a quase sete décadas, com a Conferência de Dartmouth em 1956, onde um grupo de cientistas reunido no "Dartmouth Summer Research Project on Artificial Intelligence, procurava *"descobrir como fazer com que as máquinas usem linguagem, formem abstrações e conceitos, resolvam tipos de problemas agora reservados aos humanos e se melhorem a si mesmas".* (McCarthy et al., 1955)

Deste modo, embora as tecnologias de IA existam já há várias décadas, os avanços mais importantes e que deram ao público a conhecer a IA foram dados na última década. Segundo James McDonald (2024), foram "*os avanços no poder da computação, a disponibilidade de enormes quantidades de dados e novos desenvolvimentos de algoritmos de software*" que permitiram os avanços significativos mais recentes. (McDonald, J. 2024) É importante realçar que contrariamente à programação tradicional, que se baseia na escrita manual de código, os sistemas de IA aprendem a resolver problemas através da análise de dados. (McDonald, J. 2024)

Note-se que a IA pode ser classificada de diferentes maneiras, nomeadamente segundo a forma de aprendizagem, a capacidade e a função desempenhada.

Segundo a forma de aprendizagem existem dois métodos principais: *Machine Learning* e *Deep Learning.*

- *Machine Learning: consiste* num método de análise no qual os algoritmos aprendem ao receber grandes quantidades de dados, assim adquirem conhecimentos e são capazes de fazer previsões e tomar decisões. (James McDonald 2024)

- *Deep Learning:* método mais sofisticado de IA, que utiliza processos complexos inspirados no cérebro humano, redes neurais artificiais (ANN, Artificial Neural Networks). Estes processos permitem aos computadores identificar padrões complexos que, de outro modo, seriam difíceis de identificar usando somente *machine learning.* (James McDonald 2024)

Segundo a capacidade, existem 3 métodos principais: a Inteligência Artificial Restrita *(ANI - Artificial Narrow Intelligence)*; Inteligência Artificial Geral *(AGI - Artificial General Intelligence)* e Superinteligência Artificial *(ASI - Artificial Super Intelligence).*

- Inteligência Artificial Restrita: tipo mais comum de IA, utilizado nos dias de hoje, destinado a realizar uma atividade específica, podendo ser mais simples (como um filtro para detetar e-mails *spam*) ou mais complexa (como um sistema de condução autónoma nos carros).
- Inteligência Artificial Geral: ainda hipotética, espera-se que esta realize tarefas como um ser humano, aplicando conhecimento em diferentes contextos.
- Superinteligência Artificial: também hipotética de momento, refere-se aos sistemas que são mais inteligentes do que o ser humano. (James McDonald 2024)

Segundo a função desempenhada, existem 3 métodos principais: *Expert System; Predictive AI; Generative AI.*

- *AI Expert Systems:* imitam a capacidade de decisão de um ser humano numa determinada área.
- *Predictive AI:* utiliza *machine* ou *deep learning* para analisar grandes quantidades de dados para prevenir futuros eventos, por ex., para analisar dados meteorológicos e prever a meteorologia.
- *Generative AI:* respeita a uma nova forma de IA que surgiu na cena global no final de 2022 graças ao *chatbot* ChatGPT. Este tipo de IA, tem a capacidade de criar texto, imagens e vídeos de alta qualidade, que se assemelham a conteúdo criado pelo ser-humano. Está na base do atual interesse pela IA, trazendo ao de cima a necessidade de debater e tentar regular e garantir o seu uso responsável e ético. (James McDonald 2024)

Nos anos mais recentes, ganhou ainda relevo o conceito de *frontier models*, que designa os sistemas de IA mais avançados em termos de escala, capacidade computacional e sofisticação algorítmica. (Iguazio, n.d.) Treinados com volumes massivos de dados e elevado poder de processamento, estes modelos ampliam significativamente as capacidades da IA generativa e preditiva, chegando a possuir capacidades de raciocínio mesmo quando não foram especificamente programados para tal. (Iguazio, n.d.)

Em particular, no domínio da *Generative AI*, como é o caso do modelo GPT-5 da empresa OpenAI, estes modelos podem gerar vídeos hiper-realistas, sintetizando e simulando voz com elevado grau de fidelidade, simular raciocino lógico, apresentando cenários estratégicos com base em múltiplas variáveis e ainda desenvolver projetos de programação complexa, como websites e aplicações informáticas (Público 2025)

7. O Papel da IA na Prevenção e Mitigação de Ameaças Híbridas

Num contexto global cada vez mais digital, as ameaças híbridas (como ciberataques e campanhas de desinformação) preocupam indivíduos e organizações, por apresentarem não só riscos de segurança (possibilitam o acesso a dados confidenciais), como riscos financeiros.

De modo a combater estas problemáticas, a integração da IA surge como uma possibilidade na área da deteção, prevenção e mitigação. A sua utilização é essencial, visto que estas ameaças podem levar à perda de informação confidencial, resultar em perdas financeiras significativas e comprometer a privacidade dos cidadãos. Deste modo, os diferentes setores devem estar capacitados para identificar e conseguir responder a estas ações maliciosas. (Andrei Mccall 2024)

7.1. Aplicação da IA na prevenção e mitigação de ameaças híbridas

Ciberataques

Tipologia de ameaças híbridas mais comuns no seio da UE. Dentro dos exemplos concretos de ciberataques, o DDoS (*Distributed Denial of Service*) ou *ransomware* são instrumentos capazes de gerar instabilidade social e económica. De facto, a distribuição dos tipos de incidentes é dominada por ataques DDoS, que representam cerca de 76,7% dos casos registados. Esta categoria é predominantemente impulsionada por grupos hacktivistas, responsáveis pela maioria dos incidentes DDoS recolhidos, com os grupos de cibercrime a contribuírem com uma fração marginal, muitas vezes ligada à extorsão (por exemplo, DDoS com resgate). (Jamila Boutemeur et. al 2025)

Com base nos objetivos avaliados, as atividades cibernéticas que afetam a UE dizem respeito principalmente a incidentes motivados por ideologias, realizados exclusivamente por hacktivistas através de DDoS. As operações com motivação financeira são realizadas principalmente por operadores cibercriminosos, enquanto alguns casos estão associados a grupos hacktivistas e ameaças alinhadas com o Estado. (Jamila Boutemeur et. al (2025)

Os DDoS são ataques que utilizam múltiplos recursos para sobrecarregar servidores, privando o cliente de utilizar os serviços, podendo causar grandes prejuízos a empresas e governos. No entanto, são difíceis de detetar e prevenir, porque o tráfego do ataque é semelhante ao tráfego normal na maioria dos casos. Com o desenvolvimento de tecnologias emergentes, como

computação em nuvem, e técnicas de IA, os invasores podem lançar ataques DDoS com baixo custo, tornando muito mais difícil a sua deteção e prevenção. Algumas técnicas de IA, como algoritmos de aprendizagem automática, têm sido utilizadas para classificar o tráfego de ataques DDoS e detectar ataques DDoS, tais como Naive Bayes e Random Forest Tree. (Dragoș Glăvan et al 2019

Para combater os ciberataques, a UE criou instrumentos como o *Cyber Solidarity Act* em 2023 para reforçar a capacidade de deteção e resposta a incidentes cibernéticos graves através da criação de equipas europeias de ciber-resposta rápida. (DSA, 2022)

Manipulação e Interferência Estrangeira de Informação

Quanto às campanhas de desinformação, também conhecida como Manipulação e Interferência Estrangeira de Informação (MIEI) estas são um "padrão de comportamento, na sua maioria não ilegal, que ameaça ou tem o potencial de afetar negativamente valores, procedimentos e processos políticos. Tal atividade é de natureza manipuladora, conduzida de forma intencional e coordenada. Os autores desta atividade podem ser atores estatais ou não estatais, incluindo os seus representantes dentro e fora do seu próprio território." (Magonara & Malatras, 2022)

Entre novembro de 2023 e novembro de 2024, o Serviço Europeu de Ação Externa (SEAE) identificou 505 incidentes de manipulação e interferência de informação estrangeira, que afetaram 90 países e 322 organizações distintas. (European External Action Service, 2025)

A Federação Russa mantém-se como um dos principais ofensores neste domínio, sendo responsável por uma parte significativa das operações MIEI na União Europeia, com o objetivo de moldar a perceção global em seu favor. Para além de operar na Europa, também direciona estes ataques para os EUA, NATO, Médio Oriente, África e América Latina, com maior ocorrência em períodos de eleições para expandir a sua influência. (European External Action Service, 2025) Estas táticas são na sua maioria realizadas nas redes sociais pelo seu baixo custo-benefício, com o X (Twitter) contando com 88% dos acidentes. (European External Action Service, 2025)

As operações MIEI são na sua maioria simples, como a publicação de textos, imagens e vídeos, notícias falsas, complementadas com o uso de *bots* para artificialmente expandir a visibilidade deste conteúdo. Particularmente, cada vez mais se aplica IA à criação de áudios e vídeos *deepfakes* disseminados automaticamente por *bots*. (European External Action Service, 2025)

De modo a tentar mitigar este problema, a IA pode ser utilizada na deteção de conteúdos que digam potencialmente respeito a campanhas de desinformação, identificando os padrões que ocorrem na disseminação de desinformação e utilizando mecanismos de verificação de factos. (Pilati & Venturini, 2025).

Neste âmbito, para proteger as democracias europeias contra a manipulação de informação e interferências estrangeira, a UE apresenta políticas como a *UE vs Disinfo* (2015), Plano de Ação Contra a Desinformação (2018), Plano de ação para a democracia europeia (2020) e Digital Services Act (DSA, 2022)

8. Desafios da Implementação da IA na Deteção e Mitigação de Ameaças Híbridas

Importa considerar que tanto no caso dos ciberataques DDOS, como nas Campanhas de Manipulação e Interferência Estrangeira de Informação, a IA é o instrumento por excelência utilizado pelos atores que os levam a cabo.

Relativamente aos ataques DDoS, a maioria utiliza algum género de automatização, o que torna difícil distinguir entre atividade legítima e maliciosa pela IA, aumentando a possibilidade de gerar falsos positivos e bloquear tráfego legítimo, ou falsos negativos e deixar passar ataques reais. No caso de MIEI, a IA também é utilizada na criação de conteúdos *deepfake,* que cada vez mais se assemelham a conteúdos reais, dificultando a sua distinção por parte dos instrumentos de IA utilizados. Em particular, este facto leva à possibilidade de se censurar a liberdade de expressão de pessoas reais e não desinformação.

Para evitar esta ocorrência é necessária a verificação e atualização das bases de dados que os mecanismos de IA que detetam estas ameaças utilizam, para evitar que os sistemas *machine learning* a tomar decisões erradas. Consequentemente, a própria tecnologia de IA precisa de maior investimento, de forma a poder estar um "passo à frente" dos atacantes, implicando maior investimento financeiro e técnico.

Assim, a resposta da UE às ameaças híbridas, apesar dos avanços na construção de um quadro político e estratégico comum, continua limitada por desafios estruturais e institucionais. A falta de coordenação entre os EM, marcada por prioridades e perceções de risco assimétricas (nomeadamente o facto de os países de leste "viverem" as ameaças híbridas como perigos imediatos, enquanto estados do sul e oeste privilegiam temas como a segurança energética e resiliência climática), dificultam bastante a criação de uma abordagem verdadeiramente integrada.

As próprias limitações jurídicas e institucionais da União, onde a segurança e a defesa permanecem em áreas intergovernamentais que exigem consenso, reduzem a sua agilidade e capacidade de resposta rápida.

Soma-se ainda a fragmentação de recursos e capacidades, devido não só à dependência de contribuições voluntárias dos EM e à ausência de um mecanismo unificado de comando e controlo, como às assimetrias em termos de capacidades de investimento entre os países do norte, do leste e do sul da Europa.

Por fim, a rápida evolução tecnológica coloca novos desafios, dado que a utilização estratégica de IA, Big Data e sistemas automáticos de deteção requer investimentos significativos, quadros éticos sólidos e maior coordenação transnacional. Assim, embora o quadro europeu seja cada vez mais robusto, a sua eficácia continua condicionada enquanto não forem superadas estas limitações de coordenação, soberania, e a integração plena das tecnologias emergentes.

9. Conclusão

O presente trabalho de investigação orientou-se fundamentalmente por duas questões, sendo a primeira "*Em que medida a IA tem vindo a ser integrada nas políticas e práticas dos Estados, em resposta a ameaças híbridas?"* e a segunda, "*Que limitações técnicas, éticas ou institucionais condicionam a integração da IA nas políticas e práticas dos Estados em resposta a ameaças híbridas?"*.

A investigação realizada permite-nos concluir, em relação à questão I, que a Inteligência Artificial assume um papel relevante enquanto instrumento integrado na área da segurança, sobretudo naquilo que são as políticas europeias de ciberdefesa e de combate à desinformação, através de sistemas de deteção de ataques em tempo quase real e identificação de campanhas de manipulação de informação.

Simultaneamente, a investigação confirma o caráter dual da IA, uma vez que, identifica que os mesmos avanços tecnológicos que permitem reforçar a proteção e prevenção face a ameaças híbridas, também potenciam as ameaças levadas a cabo por atores hostis, que empregam a IA, entre outras atividades, na realização de ciberataques e campanhas de desinformação.

Adicionalmente, em relação à questão II, referente aos desafios que se colocam à aplicação das tecnologias emergentes, particularmente da IA, na segurança e defesa, a investigação conduzida identifica um conjunto de limitações que condicionam a integração eficaz da IA e que tornam as respostas às ameaças híbridas fragmentadas e reativas, em vez de estratégicas e antecipatórias. Estas limitações são, sobretudo, ao nível técnico, por exemplo, a necessidade constante de atualização, ao nível ético, por exemplo, problemas de transparência algorítmica, e ao nível institucional, por exemplo, no caso da União Europeia, a falta de respostas preventivas, fortes assimetrias em termos de capacidades de investimento e perceção de ameaças, e falta de coordenação entre Estados-Membros.

Em síntese, conclui-se que a IA é já um pilar essencial das políticas de Organizações Internacionais, como a União Europeia, no combate às ameaças híbridas; no entanto, a sua integração plena está longe de concluída e é condicionada por desafios técnicos, éticos e institucionais significativos, devendo a União dar maior prioridade e investimento à integração da IA na segurança e defesa, procurando superar as limitações na sua operacionalização.

Por último, importa mencionar que o trabalho permitiu ainda identificar que estas lacunas, que são também potencializadas pela complexidade do fenómeno das ameaças híbridas, geram

novas oportunidades de investigação para o desenvolvimento e aplicação da Inteligência Artificial no contexto do combate a esta problemática.

Tendo em conta a complexidade do tema, propõe-se que se realize uma abordagem interdisciplinar mais completa, que deverá combinar as ciências políticas, segurança, tecnologia e sociologia, para compreender plenamente o impacto das ameaças híbridas nas democracias e a utilização da Inteligência Artificial como mecanismo por excelência para o combate às mesmas. Esta abordagem deve apostar numa análise quantitativa que seja capaz de avaliar eficácia de diferentes políticas levadas a cabo pelas Organizações Internacionais.

10. Bibliografia

Boutemeur, J., et. al (2025). *Enisa Threat Landscape* 2025. DOI: 10.2824/1946374

Caixa Geral de Depósitos. (2025). *Iot: o que é a Internet das Coisas e como funciona?* https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/internet-das-coisas.aspx?srsltid=AfmBOooCrbLQ08etUWf-pDCqoX-hN8sJR1I-uheMRaPeUxdtcHgusumm

CCDCOE (n.d.). *CCDCOE*. [online] Available at: https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats/.

CCDCOE. (2020). *The impact of new and emerging technologies on cyber defence and security.* NATO Cooperative Cyber Defence Centre of Excellence. Recuperado de https://ccdcoe.org/uploads/2020/12/5-The-Impact-of-New-and-Emerging-Technologies_ebook.pdf

Consilium. (2019). *Hybrid threats*. [online] Available at: https://www.consilium.europa.eu/en/policies/hybrid-threats/.

Consilium. (2022). *Ameaças híbridas*. [online] Available at: https://www.consilium.europa.eu/pt/policies/hybrid-threats/#wha [Accessed 13 Nov. 2025].

COUNTERING HYBRID THREATS. (n.d.). Available at: https://defence-industry-space.ec.europa.eu/document/download/3b90af44-dbf6-4ea7-a24a-b6c60305c9be_en?filename=Factsheet%20-%20Countering%20Hybrid%20Threats.pdf.

Europa.eu. (2016). *EUR-Lex - 52016JC0018 - EN - EUR-Lex*. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

Eurodefense.pt. (2025). *STRATEGIC COMPASS: Unir a Europa num Ocidente mais coeso*. [online] Available at: https://eurodefense.pt/strategic-compass/ [Accessed 13 Nov. 2025]

European Commission (2020). *Cybersecurity Strategy | Shaping Europe's digital future*. [online] digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

European Commission. (2023). *Strategic communication and countering information manipulation*. [online] Available at: https://commission.europa.eu/topics/countering-information-manipulation_en.

European Commission. (2024). *Defence Industry and Space*. [online] Available at: https://commission.europa.eu/about/departments-and-executive-agencies/defence-industry-and-space_en.

European Commission. (2024). *Hybrid threats.* European Union. Recuperado de https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en

European External Action Service (2022). *A Strategic Compass for Security and Defence | EEAS Website*. [online] www.eeas.europa.eu. Available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

European External Action Service (2025). *In 3rd EEAS Report on Foreign Information Manipulation and Interference Threats.* https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

EU HYBNET & Hybrid CoE. (2021). *Conceptual framework on hybrid threats.* Joint Research Centre of the European Commission. Recuperado de https://euhybnet.eu/wp-content/uploads/2021/06/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf

ENISA. (2024). *Foresight cybersecurity threats for 2030.* European Union Agency for Cybersecurity. Recuperado de https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf

Esposito, M. (2025, July 24). *AI geopolitics and data centres in the age of technological rivalry*. World Economic Forum. https://www.weforum.org/agenda/2025/07/ai-geopolitics-data-centres-technological-rivalry

Friends of Europe. (2024). *Countering hybrid threats: The vital need for digital resilience.* Friends of Europe. Recuperado de https://www.friendsofeurope.org/insights/countering-hybrid-threats-the-vital-need-for-digital-resilience/

Genini, D. (2025). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives*. doi:https://doi.org/10.1177/2336825x251322719.

Glăvan, D. Răcuciu, C. Moinescu, R. and Antonie, N,. *Scientific Bulletin of Naval Academy, DDoS detection and prevention based on artificial intelligence techniques* Vol. XXII 2019, pg. 134-143. doi: 10.21279/1454-864X-19-I1-018

HCSS & TNO. (2024). *New technologies changing strategies: Hybrid threats.* The Hague Centre for Strategic Studies & TNO. Recuperado de https://hcss.nl/wp-content/uploads/2024/05/New-Technologies-Changing-Strategies-Hybrid-Threats-HCSS-TNO-2024.pdf

Hybrid CoE. (2024). *Hybrid threats – Understanding the grey zone.* European Centre of Excellence for Countering Hybrid Threats. Recuperado de https://www.hybridcoe.fi/hybrid-threats/

Iguazio (n.d.) *What is a Frontier Model?* https://www.iguazio.com/glossary/frontier-model/

Instituto da Defesa Nacional (IDN). (2023). *Ameaças híbridas e a defesa europeia.* E-Briefing Papers, n.º 3. Recuperado de https://www.idn.gov.pt/pt/publicacoes/ebriefing/Documents/E-Briefing%20Papers/E-Briefing%20Papers%203.pdf

International Committee of the Red Cross (ICRC). (2021). AI and machine learning in armed conflict: A human-centred approach. International Review of the Red Cross. https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ai-and-machine-learning-in-armed-conflict-a-human-centred-approach-913.pdf

Magonara, E., Malatras, A., (2022). *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity - Threat Landscape. Enisa* https://www.enisa.europa.eu/sites/default/files/publications/Foreign%20Information%20Manipulation%20and%20Interference%20%28FIMI%29%20and%20Cybersecurity%20-%20Threat%20Landscape.pdf

Mattis, J.N. and Hoffman, F. (2005). *Future Warfare: The Rise of Hybrid Wars*. [online] U.S. Naval Institute. Available at: https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars

McCall, A. (2024). A*I and Cybersecurity: Detecting and Mitigating Cyber Threats.* https://www.researchgate.net/publication/385850065_AI_and_Cybersecurity_Detecting_and_Mitigating_Cyber_Threats

McCarthy, J., Minsky, M. L., Rochester, N., Shannon, C. E., (1955). *A Proposal for the Darmouth Summer Research Project on Artificial Intelligence* http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf

McDonald, J. (2024). *Introduction to Artificial Intelligence (AI) Technology: Guide for travel & Tourism Leaders | WTTC Research Hub.* https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/2024-wttc-introduction-to-ai.pdf

Mlinac, N. (2025). *Hybrid intelligence as a carrier of disinformation and hybrid threats in cyberspace. National Security and the Future*, 26(1), 45–58. https://doi.org/10.37458/nstf.26.1.2

NATO (2024). *NATO's response to hybrid threats*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm.

NATO (2024). *Hybrid Threats and Hybrid Warfare Reference Curriculum*. [online] Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf.

NATO (2024). *NATO's response to hybrid threats*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm.

NATO. (2024). *Countering hybrid threats.* North Atlantic Treaty Organization. Recuperado de https://www.nato.int/cps/en/natohq/topics_156338.htm

Pilati, F,. and Venturini, T,. (2025) *The use of artificial intelligence in counter-disinformation: a world wide (web) mapping*. Front. Polit. Sci. 7:1517726. doi: 10.3389/fpos.2025.1517726

Público. (2025). *ChatGPT ficou mais "inteligente", "honesto" e simples de usar. https://www.publico.pt/2025/08/08/enter/noticia/chatgpt-ficou-inteligente-honesto-simples-usar-2143339#*

Rahnama, H. (2025). *AI Glossary/Dictionary, MIT Media Lab. MIT Media Lab.* https://www.media.mit.edu/tools/ai-glossary-dictionary

Robert-schuman.eu. (2025). *Hybrid threats: the new horizons for a 'Europe of internal security'?* [online] Available at: https://www.robert-schuman.eu/en/european-issues/787-hybrid-threats-the-new-horizons-for-a-europe-of-internal-security.

Shaw, I. G. R., 'Robot wars: US empire and geopolitics in the robotic age', Security Dialogue, vol. 48, no. 5 (2017); and Holmqvist, C., 'Undoing war: War ontologies and the materiality of drone warfare', Millennium: Journal of International Studies, vol. 41, no. 3 (2013).
Singh Gill, A. (2019). Artificial Intelligence and International Security: The Long View. Ethics & International Affairs, 33(2), 169–179. https://www-cambridge-org.dcu.idm.oclc.org/core/journals/ethics-and-internationalaffairs/article/artificial-intelligence-and-international-security-the-long-view/4AB181EAF6485014222579349 82A4DD5.

Stănescu, M. (2023). *Understanding hybrid threats and their societal impact: Republic of Moldova case study. Land Forces Academy Review*, 28(4), 255–264. https://doi.org/10.2478/raft-2023-0030

Terekhov, V. (2025, 18 de fevereiro). The role of AI and machine learning in military decision-making software. Attract Group. https://attractgroup.com/blog/the-role-of-ai-and-machine-learning-in-military-decision-making-software/

Tsaruk, O., & Korniiets, M. (2023). *Hybrid nature of modern threats for cybersecurity and information security.* SCRD, 19(2), 32-38. Recuperado de https://scrd.eu/index.php/scrd/article/download/63/56

UK Government. (2024). *Emerging technologies and their effect on cyber security.* Government Communications Headquarters (GCHQ). Recuperado de https://www.gov.uk/government/publications/emerging-technology-pairings-and-their-effects-on-cyber-security/emerging-technologies-and-their-effect-on-cyber-security

Uziębło, J. (2017). *DEPARTMENT OF EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats*. [online] Available at:

https://www.coleurope.eu/sites/default/files/research-paper/edp-5-2017_uzieblo_0.pdf [Accessed 13 Nov. 2025].

Vráb, F. (2025). *Hybrid threats in the digital age: A comprehensive analysis of evolving attack vectors and mitigation strategies.* International Journal of Advanced Natural Sciences and Engineering Researches, 9(1), 174-183. Recuperado de https://as-proceeding.com/index.php/ijanser/article/view/2429

Zhang, L., Chen, Y., Williams, R., & Patel, S. (2023). AI-driven threat detection: Enhancing cybersecurity through intelligent anomaly analysis. IEEE Transactions on Information Forensics and Security, 18, 2245–2261. https://doi.org/10.1109/TIFS.2023.1234567