Defesa sem Estratégia: Lições da História sobre Vulnerabilidade e Dissuasão

António Guedes de Amorim
Partner e Sales Director na Quidgest, onde lidera o relacionamento com clientes estratégicos, nomeadamente no setor da defesa. Com mais de 25 anos de experiência em transformação digital na Administração Pública, coordenou projetos em Portugal e em Timor-Leste, incluindo iniciativas estruturantes no reconhecimento dos Combatentes da Libertação Nacional.

Bruna Ferreira
Licenciada em Jornalismo e Ciências da Comunicação (Universidade do Porto) e pós-graduada em História (Universidade de Lisboa). Como Storyteller & Content Manager na Quidgest, interessa-se por tecnologia, inovação e assuntos europeus, recorrendo à história como chave para interpretar a atualidade e antecipar o futuro.

João Paulo Carvalho
Licenciado em Economia (ISEG) e mestre em Sistemas de Informação (ISCTE), é Co-fundador e Senior Partner da Quidgest. Com mais de 37 anos de experiência no setor tecnológico, é defensor da transformação digital ao serviço do bem comum e vê na IA Generativa uma aliada para a inovação, a sustentabilidade e o cumprimento dos Objetivos de Desenvolvimento Sustentável da ONU.

Resumo

O regresso da guerra ao continente europeu acelerou uma reflexão há muito adiada: o que significa defender a Europa?
Mais do que armamento, a soberania do século XXI constrói-se com logística, formação, tecnologia e, acima de tudo, capacidade de dissuasão. Este artigo propõe uma leitura crítica dos orçamentos de defesa da UE e sugere que os grandes desafios da defesa contemporânea exigem não apenas soldados, mas sistemas de gestão, inteligência organizacional, interoperabilidade e soberania digital. A partir dos relatórios Draghi, Letta e Heitor, de paralelismos históricos e da experiência prática dos autores, argumentamos que a próxima fronteira da autonomia estratégica europeia será digital, humana e estratégica – e que alguns dos maiores fracassos do passado podem ter sido, afinal, falhas de gestão.

Palavras-chave: Defesa; Estratégia; Europa; Gestão; Tecnologia; História; *Software*; Transformação Digital.

Artigo recebido: 22.07.2025
Aprovado: 20.08.2025
https://doi.org/10.47906/ND2025.171.06

Abstract
Defense without strategy: lessons from History on vulnerability and deterrence

The return of war to the European continent has accelerated a long-overdue reflection: what does it mean to defend Europe?
More than weaponry, 21st-century sovereignty is built on logistics, training, technology, and, above all, deterrence capacity. This article offers a critical reading of the EU's defense budgets and argues that the major challenges of contemporary defense require not just soldiers, but management systems, organizational intelligence, digital interoperability, and sovereignty. Drawing on the Draghi, Letta, and Heitor reports, historical parallels, and based on the author's practical experience, we argue that the next frontier of European strategic autonomy will be digital, human, and strategic – and that some of the most significant failures of the past were, ultimately, failures of management.

Keywords: *Defense; Strategy; Europe; Management; Technology; History; Software; Digital Transformation.*

1. Introdução

A Europa encontra-se numa nova encruzilhada histórica. A guerra voltou ao continente, sob formas assimétricas e tecnologicamente mediadas, radicalmente diferentes das que marcaram o século XX. Infraestruturas críticas, cadeias logísticas e fluxos de informação tornaram-se alvos preferenciais. Tecnologia, energia e geopolítica entrelaçam-se numa nova gramática do poder (Vershinin, 2022). Em paralelo, a multiplicação de ataques terroristas, crimes de ódio e conflitos de matriz política ou religiosa sinaliza que as fragilidades internas do projeto europeu permanecem latentes e exigem mais do que respostas operacionais: exigem pensamento estratégico, capacidade institucional e preparação para o inesperado.

A invasão da Ucrânia pela Rússia teve início em 2014, com a anexação da Crimeia, mas foi a ofensiva militar em larga escala lançada em fevereiro de 2022 que marcou uma rutura profunda na ordem de segurança europeia. Essa escalada devolveu o continente à lógica da ameaça existencial e demonstrou que a dissuasão exige mais do que intenções ou compromissos formais (*Council on Foreign Relations*, 2025). A questão não é apenas se a Europa está disposta a defender-se. É se sabe como o fazer, porque defender-se implica mais do que dispor de forças armadas ou equipamento militar: implica sistemas, processos, informação fiável e capacidade de decisão. A Crise dos Mísseis de Cuba, em 1962, ilustra a importância da gestão da dissuasão. Durante 13 dias, EUA e União Soviética enfrentaram o risco iminente de guerra nuclear. Não foi o arsenal bélico que evitou o pior, mas sim uma combinação frágil de comunicação, prudência e decisão individual[1] (Betts, 1995). O episódio demonstrou que a ausência de coordenação e de sistemas operacionais de gestão de informação pode ser tão perigosa quanto a presença de ogivas nucleares.

Na maioria das situações, não é a coragem individual que determina o desfecho de um conflito, mas a robustez dos sistemas que o sustentam. A história da guerra é também a história da retaguarda: de quem garante o abastecimento, a mobilidade, a alimentação e a atualização da informação operacional (Keegan, 1993; Van Creveld, 2004). Como defendeu Henry E. Eccles, um dos principais teóricos da logística militar, sem bases logísticas eficazes, não há estratégia que sobreviva à realidade operacional (Eccles, 1959). Por conseguinte, não será suficiente para a Europa uma visão excessivamente centrada no armamento e na força visível, em

1 Vasili Arkhipov, vice-comandante de um submarino soviético, recusou autorizar o lançamento de um torpedo nuclear, contrariando os seus superiores num contexto de isolamento e tensão extrema. Sem comunicações com Moscovo, a sua decisão evitou uma guerra nuclear e mostrou como, sem sistemas robustos de comando e controlo, a paz pode depender apenas do bom senso de um único homem.

detrimento da capacidade técnica, logística e organizacional que verdadeiramente sustenta a soberania.

Este ensaio parte de um princípio metodológico claro: compreender o presente exige conhecer o passado e antecipar o futuro implica reconhecer os sinais estruturais do presente. A abordagem escolhida é reflexiva e ensaística, cruzando episódios históricos com desafios contemporâneos de gestão estratégica e tecnológica. Assume-se, aqui, uma perspetiva construtivista da segurança europeia, onde a cultura estratégica não é um dado adquirido, mas uma construção institucional, política e discursiva em constante evolução (Meyer, 2005; Rynning, 2003). Este debate cruza-se ainda com a evolução institucional, como nota Brøgger (2024, p. 3) ao afirmar que *"os compromissos vinculativos e a governação supranacional estão a remodelar o papel da União Europeia na segurança e na defesa"*. Tal ideia confirma que a integração europeia em defesa já não é apenas cooperativa, mas também regulatória.

Mostramos que a defesa, longe de ser um domínio reservado a militares ou decisores políticos, depende também da contribuição articulada de engenheiros, gestores, psicólogos, economistas, programadores e analistas de sistemas. Nas palavras de Georges Clemenceau, "a guerra é uma coisa demasiado grave para ser deixada aos militares" – e, no século XXI, esta gravidade exige competências civis e técnicas amplamente distribuídas. (Clemenceau, cit. in Citador, 2023).

A retaguarda (espaço de planeamento, gestão e decisão) transformou-se na nova linha da frente. As guerras do passado perdiam-se por botas rotas; as do presente, por dados desatualizados; as do futuro, por fluxos de decisão mal configurados (Naisbitt, 1982; Sullivan e Dubik, 1994).

A soberania depende não apenas do aço e da pólvora, mas da capacidade de integração entre atores, tecnologias e domínios operacionais (Agência Europeia de Defesa, 2024a; Luttwak, 2001). Investir em defesa vai mais além das metas orçamentais e da aquisição de equipamentos. Significa aplicar os recursos com rigor, modernizar sistemas, rever processos, integrar dados, garantir interoperabilidade e cuidar das pessoas que executam essas funções estratégicas (Comissão Europeia, 2024a; Draghi, 2025).

Defender a Europa é geri-la com inteligência. E esta inteligência não é apenas natural ou artificial; é estratégica. Fundamenta-se na capacidade de antecipar tendências, alinhar recursos, monitorizar variáveis críticas e adaptar-se em tempo útil. Segundo a definição da Organização para a Cooperação e Desenvolvimento Económico (OCDE), uma lógica de governo antecipatório incorpora, entre outros elementos, a gestão da incerteza, bem como a integração da antevisão, experimentação e inovação como componentes centrais da tomada de decisão estratégica (OCDE, 2023).

A guerra do futuro, e o futuro da paz, serão decididos em *dashboards*[2] e na qualidade da governação da defesa. E, no entender dos autores deste artigo, em colocar a gestão no centro da estratégia.

2. Falhar nos Bastidores É Chegar às Trincheiras Derrotado

Em 1812, durante a célebre campanha russa, Napoleão Bonaparte comandava o maior exército alguma vez reunido na Europa até então: mais de 600 mil homens, provenientes de diversas nações sob domínio do Império. A marcha parecia imparável, mas a História mostrou que a derrota começou muito antes dos confrontos diretos – começou na retaguarda e nos pés dos soldados. Sem equipamento adequado para enfrentar o rigor do inverno russo, milhares morreram durante a travessia; as botas desfizeram-se ao longo da marcha e a logística falhou no essencial: alimentação, aquecimento, transporte, vestuário. (Keegan, 1993; Van Creveld, 2004).

O erro não foi político ou operacional: foi um erro de estratégia logística, uma das componentes da estratégia total, como sublinha Beaufre (1998). A má gestão dos recursos básicos revelou-se mais letal do que qualquer baioneta inimiga.

A lição continua útil, dois séculos depois. As derrotas logísticas já não se medem apenas em quilómetros de lama ou graus negativos, mas em infraestruturas digitais obsoletas e processos fragmentados. A falta de interoperabilidade e coordenação entre departamentos pode criar um fosso entre a decisão política e a execução operacional (contratos com atrasos, aquisições sem alinhamento com *stocks* e decisões críticas suportadas por sistemas obsoletos e dados desatualizados), tornando inútil um orçamento mais alargado (Comissão Europeia, 2024d; Jennings, 2023a e 2023b).

Em 2023, a Alemanha anunciou um fundo extraordinário de 100 mil milhões de euros para rearmamento, como resposta à escalada da guerra na Ucrânia. O gesto foi político, simbólico e estratégico. Contudo, meses depois, o Ministério da Defesa alemão admitia que não conseguia executar o orçamento de forma eficaz, não por falta de recursos, mas por ausência de sistemas de aprovisionamento modernos, inventários atualizados e plataformas com partilha de informação em tempo real (Comissão Europeia, 2024a).

Este não é um caso isolado: segundo a Agência Europeia de Defesa (2024b), apenas 18% das aquisições de defesa dos Estados-Membros foram realizadas de forma colaborativa, longe do objetivo de 35% definido pela União Europeia (UE). Esta

2 Utiliza-se o termo *dashboard* no seu sentido técnico consolidado nas áreas da gestão estratégica e da inteligência operacional apicadas ao comando militar: plataformas digitais de visualização integrada de dados críticos em tempo real, com impacto direto na tomada de decisão. A tradução literal em português seria "painel de controlo".

fragmentação tem um impacto direto na capacidade militar (Ministério da Defesa Nacional, 2014), entendida como *"o conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para a realização de um conjunto de tarefas operacionais ou efeito que é necessário atingir, englobando componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade"*. Na Europa Central e de Leste, esta fragmentação é ainda mais visível. Chovančík e Krpec (2023, p. 371) falam mesmo em "desintegração encoberta" para descrever os efeitos da invasão russa à Ucrânia sobre a cooperação industrial de defesa, revelando que, em vez de convergência, emergem lógicas de competição e dependência.

A dissociação entre estratégia logística e execução operacional é um risco permanente. Como sublinha Beaufre (1998), a estratégia logística (tal como a estratégia genética, a estratégia operacional ou a estratégia política) é apenas uma das componentes da estratégia total. Negligenciá-la compromete todo o sistema, por mais sólida que seja a conceção das restantes.

O problema agrava-se quando as infraestruturas digitais não acompanham a velocidade das ameaças, persistem sistemas rígidos e segmentados, e existe baixa capacidade de adaptação a contextos de crise ou inovação doutrinária. Tomem-se como exemplo os seguintes casos:

- O *Louvois*, em França, gerou milhares de erros salariais e afetou a moral das tropas (Cour des Comptes, 2014);
- O *Defence Information Infrastructure*, no Reino Unido, sofreu atrasos e derrapagens orçamentais (*National Audit Office*, 2008);
- E o *Defence Enterprise Accounting and Management System* da Força Aérea dos EUA acumulou problemas de interoperabilidade e custos excessivos (*Government Accountability Office*, 2019).

Ferramentas como o *Balanced Scorecard*[3] (Kaplan e Norton, 2001), devidamente adaptadas ao contexto das organizações públicas (Borges et al., 2024) e não lucrativas (Mishra e Dash, 2007), permitiriam mapear, em tempo real, o estado das operações logísticas, cruzar metas políticas com execução concreta, alinhar prioridades institucionais e garantir transparência ao longo de toda a cadeia de comando.

3 Ferramenta de gestão estratégica desenvolvida por Kaplan e Norton (1992) para o setor empresarial, que avalia o desempenho a partir de quatro dimensões: financeira, clientes/utilizadores, processos internos e capacidade de aprendizagem/inovação. Posteriormente, o modelo foi adaptado a organizações públicas e não lucrativas, colocando a missão e os objetivos estratégicos no centro e ajustando as métricas às realidades não comerciais. No contexto da defesa, o seu valor reside no imenso potencial de interligar áreas tão diversas como gestão de frotas, formação, saúde, habitação, logística de refeições, planeamento orçamental, alocação de recursos ou manutenção operacional – de forma a permitir uma visão holística e integrada em entidades altamente complexas.

A maioria dos sistemas integrados de gestão (ERP ou *Enterprise Resource Planning*) utilizados nas forças armadas europeias, incluindo o Sistema Integrado de Gestão da Defesa Nacional (SIG-DN) em Portugal, carateriza-se pela arquitetura monolítica, rigidez, falta de prontidão e obsolescência tecnológica. Já em 2018, Rocha alertava que "o SIG-DN poderá ser impactado pela obsolescência técnica e funcional dos sistemas de informação que suportam a gestão logística" (Rocha, 2018, p. 88). Em 2019, verificou-se que "a migração de dados para o módulo *Asset Accounting* não foi totalmente concluída, não tendo ocorrido evoluções significativas desde então" (Oliveira, 2019, p. 67), o que comprometeu a fiabilidade da informação. Já em 2020, Rodrigues acrescentava: "persistem limitações na flexibilidade do SIG-DN para responder a novas exigências operacionais" (Rodrigues, 2020, p. 59).

O SIG-DN parece ser uma oportunidade perdida de dar agilidade tecnológica ao sistema de informação fundamental da defesa nacional. Em 2023, o próprio Ministério registava a necessidade de "promover atualizações de *software* e serviços de assistência técnica, assim como adquirir novas licenças, fundamentais para a prestação eficiente do serviço" (Diário da República, 2023), evidenciando que o sistema ainda depende de intervenções formais para evoluir.

A prontidão digital, complementar à prontidão militar, exige arquiteturas tecnológicas modulares, flexíveis, interoperáveis e que privilegiem abordagens *data-centric* em vez de *application-centric*, refere a Organização do Tratado do Atlântico Norte (NATO, 2023a). Algumas administrações e agências multilaterais pioneiras já adotaram plataformas desenhadas para evoluir continuamente, integrando modelação dinâmica de processos e inteligência artificial (IA) para análise preditiva. Estudos do NATO *Innovation Hub* (2023) mostram, inclusivamente, que estas soluções podem adaptar-se a cenários inesperados em poucas horas (e não em ciclos longos de desenvolvimento manual).

Ao integrar objetivos estratégicos, indicadores operacionais e fluxos de decisão automatizados, estas plataformas elevam o nível de governação da defesa: tornam-na mais transparente, auditável e adaptável. Não se trata de digitalizar o que existe, mas de transformar o modo como se decide.

3. Logística: Quem não Conta os Parafusos, Perde os Carros de Combate

Os carros de combate vencem batalhas, mas são os parafusos que os mantêm a funcionar. E sem combustível, munições, comida ou peças sobresselentes, um exército é apenas uma soma de corpos e máquinas à espera do colapso. A história militar é pródiga em vitórias forjadas longe do campo de batalha, mas perto da contabilidade minuciosa de aprovisionamentos nos depósitos de mantimentos e nas oficinas de reparação.

Durante o cerco de Leningrado, entre 1941 e 1944, a cidade resistiu quase 900 dias cercada pelas forças nazis, sem acesso a rotas de abastecimento terrestre. Milhares morreram de fome, frio e doenças, enquanto as autoridades soviéticas tentavam manter alguma estrutura de distribuição alimentar. O chamado "Caminho da Vida", uma rota improvisada sobre o lago Ládoga (primeiro com barcos, depois com camiões sobre o gelo), tornou-se símbolo de resistência e de logística extrema (Glantz, 2002). A gestão racionada de pão, com base em critérios profissionais e militares, determinava quem vivia e quem morria. Leningrado resistiu, provando que: sem comida, não há força e sem logística alimentar, não há defesa.

Durante a Segunda Guerra Mundial, operações como o Dia D exigiram também uma capacidade de planeamento logístico e contabilístico sem precedentes. Os Aliados desenvolveram sistemas de inventário que rastreavam desde veículos até peças minúsculas (como os parafusos que mencionámos no início deste capítulo), de forma a antecipar falhas, minimizar desperdícios e garantir a continuidade operacional.

A guerra do futuro promete ser vencida não só por quem tiver mais *drones* ou satélites, mas por quem conseguir sincronizar dados, algoritmos, sensores e decisões em tempo real; uma visão já explorada por Betts (1995) e refletida em relatórios sobre transformação digital na defesa europeia (NATO Innovation Hub, 2023). Esta sincronização exige o domínio de uma arte menos visível, mas absolutamente essencial: a gestão da cadeia de abastecimento.

Modelos como o *just-in-time*[4], criados para reduzir desperdício e maximizar eficiência, inspiraram tanto a indústria automóvel como a logística militar (Phogat, 2022). Mas são sistemas que exigem precisão absoluta; pois qualquer falha pode comprometer o todo. No campo da moda, por exemplo, a Zara revolucionou o retalho ao criar cadeias logísticas altamente digitalizadas e centralizadas – em menos de 15 dias, a empresa consegue transformar uma ideia numa coleção pronta a vestir (Ghemawat e Nueno, 2006).

O mesmo se aplica às forças armadas: é preciso garantir que mantimentos, equipamentos e dados chegam onde e quando são necessários. Giacomello e Preka (2023, p. 533) reforçam esta ideia ao mostrar que "a profundidade logística e o mapeamento setorial são, em si mesmos, fontes de força" na definição de capacidade militar. Entre o improviso e a escassez, a gestão estratégica do século XXI afirma-se na capacidade de antecipar, modelar e decidir com base em dados fiáveis e fluxos integrados.

4 *Just-in-time* (JIT) é um modelo de gestão logística criado no Japão (Toyota), após a Segunda Guerra Mundial. O objetivo é entregar bens e materiais no momento exato em que são necessários, sem acumular *stocks*.

4. *Edge AI* e Agentes Inteligentes: Decidir no Terreno, Agir em Rede

A guerra moderna evoluiu em escala e ritmo. Já não basta ter superioridade numérica ou tecnológica: é necessário decidir mais rápido, com mais precisão e autonomia, mesmo em contextos adversos. A *Edge AI*[5], inteligência artificial que opera com computação periférica, é um dos estandartes desta nova geração de defesa apoiada pela UE (NATO, 2025; Pool, 2025).

Através do Fundo Europeu de Defesa, são financiados projetos de conectividade segura e de baixa latência, como redes táticas 5G e integração de sensores interoperáveis (Comissão Europeia, 2025a). Entre estes encontram-se iniciativas como o 5G COMPAD (*5G Communications for Peacekeeping and Defence*), que desenvolve comunicações militares de baixa latência para ambientes operacionais exigentes; o ECYSAP (*European Cyber Situational Awareness Platform*), centrado na criação de uma plataforma europeia de consciência situacional em ciberdefesa; e o EICACS (*European Initiative for Collaborative Air Combat Standardisation*), que trabalha na padronização da cooperação em combate aéreo, garantindo interoperabilidade entre aeronaves de diferentes países. Quando instalada em *drones*, veículos blindados ou sensores, esta tecnologia permite respostas imediatas (mesmo com comunicações centrais interrompidas ou saturadas) e possibilita recalcular rotas logísticas durante combates, prever emboscadas com base em dados locais ou desviar suprimentos de forma autónoma. Mas há especialistas a sublinhar que estas infraestruturas podem, em contrapartida, abrir novos pontos de vulnerabilidade: um sistema comprometido pode ser manipulado para fornecer dados falsos ou bloquear cadeias de decisão inteiras (Brundage et al., 2023).

Outra transformação está no aparecimento dos agentes de IA. Ao contrário da IA generativa tradicional (que responde a comandos explícitos), estes agentes atuam de forma autónoma, guiados por objetivos e parâmetros previamente definidos por humanos. São sistemas que compreendem o contexto, priorizam tarefas, aprendem com o ambiente e tomam decisões complexas, mesmo sem supervisão constante (Heckmann, 2025). Tome-se como exemplo um agente de IA a bordo de um *drone* logístico capaz de decidir quando abortar uma missão, alterar o trajeto ou comunicar com outra unidade em caso de falha de rede. Contudo, como alerta Holland-Michel "todos os sistemas dotados de um certo grau de autonomia correm o risco de se deparar com *edge cases* (casos extremos) que ficam fora do âmbito total de dados em que foram treinados ou testados, e têm probabilidade de falhar", o que lembra não só as oportunidades, mas também as fragilidades e limitações, dos agentes de IA em contextos imprevistos (Holland-Michel, 2023).

5 Também referida como "IA de computação periférica" ou "computação no extremo da rede". Trata-se de uma arquitetura em que o processamento de dados ocorre junto à fonte onde são gerados, o que reduz a latência e a dependência de centros de comando.

Durante a Guerra das Malvinas, em 1982, a ausência de informação atualizada e a dependência de comandos centralizados dificultaram a reação britânica a movimentos argentinos (Freedman, 2005). É em situações similares que a descentralização da decisão tática, suportada por tecnologia superinteligente, sobressai como uma necessidade operacional. Na prática, aplica-se o mesmo princípio de cadeias logísticas de alto desempenho no setor civil; empresas como a Amazon ou a DHL operam com redes de decisão distribuídas, onde cada ponto é capaz de agir com base em dados locais. No setor da defesa, esta lógica transforma armazéns em *hubs* inteligentes, veículos em centros de decisão móveis e sensores em atores estratégicos.

A Europa tem vindo a investir em plataformas capazes de simular impactos, integrar dados dispersos e responder em segundos a mudanças no terreno (Agência Europeia de Defesa, 2024a e 2024d). São ferramentas que cruzam logística, inteligência e comando para preparar forças armadas para conflitos híbridos e cenários de múltiplos domínios (da terra ao espaço, passando pelo ciberespaço).

A *Edge AI*, tal como os agentes de IA, não elimina o fator humano: reforça-o. Liberta decisores de tarefas perigosas ou sem valor acrescentado, acelera a execução e reduz o erro. Mais do que introduzir novas tecnologias, trata-se de redesenhar o próprio conceito de comando e controlo. Ainda assim, confiar em sistemas automatizados como se fossem uma "bala de prata" para todos os dilemas da defesa pode revelar-se ilusório. Uma confiança excessiva corre o risco de reduzir a improvisação humana em cenários imprevistos e, pior, desencadear falhas sistémicas graves. Como destaca um estudo da RAND Europe (2024, p. 43), "a militarização da IA pode gerar riscos estratégicos amplificados que vão muito além do nível tático, incluindo decisões neutras tomadas em escalas combinadas de cooperação, competição e conflito, com consequências imprevisíveis".

5. Da Terra ao Espaço: Sincronização Multidomínio

Em 1914, os exércitos do czar marcharam confiantes para a frente de batalha na Prússia Oriental. Tinham vantagem numérica, entusiasmo patriótico e um plano ofensivo ambicioso. Mas o que lhes faltava era invisível: comunicação. Soljenítsin[6], na obra "Agosto 1914", descreve o caos estratégico ao detalhe (Soljenítsin, 1971): o comando russo, sediado a centenas de quilómetros da frente, enviava ordens por telégrafo que demoravam dias a chegar (quando chegavam). Muitas vezes, as ordens contradiziam-se, eram recebidas fora de tempo ou intercetadas. As tropas do general Samsonov avançavam sem coordenação com o flanco do também czarista gene-

6 Aleksandr Soljenítsin (1918-2008) foi Prémio Nobel da Literatura em 1970 e uma das vozes mais influentes da resistência intelectual ao totalitarismo soviético no século XX.

ral Rennenkampf, acreditando numa ofensiva conjunta que nunca se concretizou. O resultado foi desastroso. Os alemães, sob o comando de Hindenburg e Ludendorff, exploraram a falha russa com precisão cirúrgica: isolaram, cercaram e aniquilaram o Segundo Exército russo em Tannenberg. Mais de 90 mil soldados foram feitos prisioneiros e o próprio general Samsonov acabou por se suicidar. A Batalha de Tannenberg foi a prova de que, em guerra, a falta de informação pode ser mortal.

Durante décadas, o campo de batalha foi pensado em compartimentos estanques, designados "domínios operacionais" – uma forma de dividir e organizar o trabalho militar em função do meio físico: terra, mar e ar. Cada força armada treinava, planeava e operava de forma relativamente autónoma. Esta compartimentação funcionou numa era em que o tempo de decisão era mais longo, as ameaças mais previsíveis e o espaço de confronto mais definido. A crise da Ucrânia acentuou esta urgência. Como refere Fiott (2023, p. 450), "em cada crise, surgem oportunidades de integração para a UE na área da defesa", o que confirma que os domínios multidimensionais da guerra aceleram a necessidade de coordenação supranacional".

No entanto, já antes do século XXI, esta abordagem mostrava limitações. Em 1983, a Operação *Urgent Fury*, na invasão de Granada (Cole, 1985), revelou deficiências graves na divisão de trabalho em domínios físicos, com falhas de coordenação e interoperabilidade entre forças. A consequência foi a aprovação, em 1986, do Goldwater-Nichols Act, que reformou o Departamento de Defesa dos EUA e instituiu a organização conjunta dos meios militares (*United States Congress*, 1986).

Desde 2016, a NATO reconhece formalmente cinco domínios operacionais da defesa: terrestre, marítimo, aéreo, espacial e ciberespacial (NATO, 2024a). Cada um exige competências técnicas, operacionais e humanas distintas, mas a verdadeira força está em integrá-los de forma conjunta e combinada, através de uma força multidomínio coerente, conjunta, interoperável e inteligente.

A defesa dos nossos dias exige que radares terrestres comuniquem com *drones* aéreos; que satélites espaciais detetem ameaças navais; que dados captados no mar sejam processados por IA em tempo real. Neste novo normal da soberania, o *software* e a gestão estratégica substituem a rigidez hierárquica por redes adaptativas de comando e controlo, capazes de responder a ameaças simultâneas e assimétricas.

6. Simulação e Gémeos Digitais: Antecipar para não Improvisar

Nenhum plano sobrevive intacto ao primeiro contacto com o inimigo. Esta máxima, atribuída a Moltke, o Velho (Moltke, 1892, p. 291), continua válida; no entanto, o modo como se prepara e testa esse plano pode fazer toda a diferença (Barnett, 1963). No passado, as forças armadas treinavam com base em cenários estáticos, simulações parciais ou exercícios em ambiente controlado. Mas a complexidade dos conflitos obriga a um novo paradigma: a modelação digital.

Os gémeos digitais (*digital twins*) são representações virtuais de sistemas físicos reais (logísticos, operacionais ou infraestruturais) capazes de simular, em tempo real, o comportamento, os impactos e os pontos de falha de uma operação. Conceito amplamente estudado em contextos industriais e cada vez mais aplicado na defesa (Agência Europeia de Defesa, 2024a e 2024c; NATO, 2023b e 2023c), estes modelos nasceram na indústria aeroespacial e foram adotados pelo setor automóvel e energético antes de chegarem ao setor militar (Giberna et al., 2025).

Um dos primeiros exemplos de gémeos digitais surgiu no programa *Apollo* da NASA. Para monitorizar e simular o desempenho de naves espaciais a centenas de milhares de quilómetros, os engenheiros criaram réplicas físicas e digitais dos componentes mais críticos. Estas simulações permitiram identificar e resolver a falha do módulo de serviço da Apollo 13, uma decisão que salvou a sua tripulação[7] (NASA, 1970).

Esta abordagem já se tornou central nos sistemas mais avançados de planeamento militar, porque, mais do que permitir a visualização de cenários hipotéticos, cria ambientes dinâmicos, constantemente atualizados por dados reais (provenientes de sensores no terreno, plataformas operacionais ou fontes meteorológicas) (Giberna et al., 2025).

A NATO e várias forças armadas europeias já começaram a integrar gémeos digitais nos seus centros de comando e treino, como demonstrado pelo consórcio EDDI (*Explore Defence Digital Twins*), lançado pela Agência Europeia de Defesa (2024a e 2024d). Este consórcio, que reúne empresas como Leonardo, Thales e FlySight, mostra que a adoção de gémeos digitais já é uma prioridade da indústria europeia. De igual modo, a Airbus e a Dassault recorrem a este tipo de modelação no FCAS (*Future Combat Air System*), utilizando simulações para prever falhas logísticas, testar componentes e reduzir riscos antes da produção real. Outro exemplo mediático é o GCP (*Global Combat Air Programme)*, uma evolução do antigo programa britânico *Tempest*, depois desenvolvido pelo Reino Unido, a Itália e o Japão. O projeto recorre a gémeos digitais para testar componentes virtualmente, prever o impacto de decisões estratégicas sem colocar recursos em risco, verificar disfunções logísticas com base em dados do histórico ou avaliar a resiliência de infraestruturas críticas perante ciberataques ou falhas de abastecimento (Ministério da Defesa do Reino Unido, 2023; União Europeia, 2023).

O valor destes modelos torna-se ainda mais evidente em contextos de crise (bloqueios marítimos ou ataques a cabos submarinos), dada a sua capacidade de antecipar a rutura de *stocks*, recalcular rotas alternativas ou reconfigurar fluxos de abastecimento em segundos. (OCDE, 2022). Mas os gémeos digitais não se limitam à antecipação de falhas. Servem também como ferramentas de aprendizagem organizacional. Podem ser usados para rever operações passadas, treinar equipas em cená-

7 Os engenheiros da NASA conseguiram replicar no solo, quase em tempo real, as condições exatas a bordo da nave avariada. Usando réplicas físicas e modelos de simulação, calcularam como adaptar os filtros de CO_2 com peças improvisadas, salvando assim a vida dos astronautas.

rios realistas ou testar novas competências de forma iterativa, antes de as aplicar em campo. Representam, por isso, um espaço seguro para errar e aprender com o erro. No plano europeu, a integração destes modelos exige não apenas investimento tecnológico, mas também alinhamento normativo e doutrinário entre nações. Sem regras comuns, interoperabilidade semântica e critérios partilhados de avaliação, os gémeos digitais podem tornar-se ilhas de excelência isoladas. A Comissão Europeia (2025c), através do Fundo Europeu de Defesa tem apoiado iniciativas que promovem a integração destes modelos em redes colaborativas e partilhadas.

7. Ciberespaço: O Novo Campo de Batalha Invisível

A guerra já não se limita a campos de batalha físicos – pode começar num cabo de fibra danificado, num ficheiro corrompido ou numa atualização mal testada. Esta realidade é capaz de paralisar desde hospitais a redes ferroviárias, afetar administrações públicas ou comprometer operações militares (sem um único tiro).

A Estónia foi alvo de um dos primeiros ciberataques geopolíticos coordenados, após uma disputa diplomática com a Rússia. O ataque, uma vaga de negações de serviço (DDoS), comprometeu bancos, jornais, ministérios e até os semáforos de Tallinn (Ottis, 2008). O episódio marcou o início de uma nova era, na qual o poder militar moderno depende tanto de servidores e *firewalls* como de carros de combate e aviões. Mais tarde, em 2015, a invasão digital do Bundestag alemão, atribuída ao grupo APT28 (ligado ao Kremlin), revelou até que ponto as instituições democráticas podem ser vulneráveis. Dois anos depois, o *ransomware* WannaCry comprometeu mais de 200 mil sistemas em 150 países, incluindo o Serviço Nacional de Saúde britânico, que viu hospitais suspenderem serviços e cirurgias por causa de uma falha de segurança negligenciada (*National Audit Office*, 2017).

Portugal também não escapou incólume. Em 2021, o Hospital de Ponta Delgada sofreu um ataque informático que bloqueou sistemas clínicos e administrativos. No ano seguinte, o grupo Impresa foi atacado com *ransomware*, resultando na indisponibilidade dos seus *websites*, no bloqueio das comunicações internas e na publicação de mensagens de chantagem por cibercriminosos. No mesmo ano, a Faculdade de Ciências da Universidade de Lisboa perdeu o histórico de *e-mails* de docentes, investigadores e alunos, além de outros serviços digitais essenciais.

Em resposta a esta crescente vulnerabilidade, a NATO reconheceu o ciberespaço como domínio operacional de guerra (NATO, 2024a). Nos anos seguintes, a UE iniciou um esforço legislativo significativo:

- O **Regulamento Geral sobre a Proteção de Dados, o RGPD (2018),** impôs regras claras sobre o tratamento e a proteção de dados pessoais, essenciais também em contexto

militar, onde bases de dados com perfis, localizações e comunicações são altamente sensíveis. (União Europeia, 2016).
- A **Diretiva NIS2 (2023)** alargou as exigências de cibersegurança a operadores de serviços essenciais, incluindo defesa, energia e transportes, com obrigações de monitorização contínua, resposta a incidentes e planeamento de continuidade (União Europeia, 2022).
- O **AI Act (2024)** passou a regular os sistemas de IA de alto risco (como os usados na defesa), impondo requisitos de transparência, ética, rastreabilidade, robustez e supervisão humana (União Europeia, 2024c).

Mas os acontecimentos mostram que a ameaça não reside apenas em ciberataques intencionais. Às vezes, basta um erro técnico para desencadear catástrofes transnacionais. Em julho de 2024, uma atualização defeituosa do *software* de segurança CrowdStrike Falcon, amplamente utilizado em sistemas Windows, provocou uma falha generalizada em serviços digitais críticos por toda a Europa. As companhias aéreas registaram atrasos e cancelamentos em cadeia, o que afetou radares de solo, *check-ins* automáticos e sistemas de rastreamento de bagagens.

Outro caso ocorreu em abril de 2025, quando um apagão elétrico sem precedentes deixou Portugal e Espanha às escuras. A falha teve origem num problema de sincronização entre geradores ibéricos e a rede europeia, agravado por um erro de coordenação na interligação com França. Cerca de 60 milhões de pessoas ficaram sem energia, e vários serviços essenciais (dos transportes à comunicações) foram interrompidos. Embora não tenha havido indícios de ciberataque, o caso ilustrou a vulnerabilidade dos sistemas interdependentes e a urgência de se aplicar as medidas previstas na NIS2 e no AI Act.

O relatório Heitor (2024) mostra-se inequívoco nesta matéria: a Europa precisa de desenvolver capacidades digitais soberanas: plataformas interoperáveis, auditáveis e seguras. Não basta adotar soluções estrangeiras; é preciso garantir que as infraestruturas críticas europeias são compreendidas, controladas e protegidas dentro das suas próprias fronteiras políticas e legais. Na prática, isto implica medidas concretas, que no entender dos autores deste artigo podem passar por:

- Criar normas e arquiteturas comuns de dados, como o *Interoperable Europe Act* e a *Data-Centric Reference Architecture* da NATO, para que informação logística e operacional circule de forma segura entre ministérios e forças armadas (Comissão Europeia, 2024a; NATO, 2023a).
- Introduzir requisitos de cibersegurança e auditabilidade em todos os contratos, previstos no *Cyber Resilience Act* e no *Data Act*, de modo a evitar dependências tecnológicas ou códigos "caixa-preta" (União Europeia, 2023; 2024a e 2024b).
- Certificar *clouds* e serviços digitais de defesa de acordo com o futuro esquema europeu de certificação EUCS (*European Cybersecurity Certification Scheme for Cloud Services*), de forma a garantir padrões comuns de resiliência (Comissão Europeia, 2024c e 2024e).

- Implementar a 5G *Toolbox* para limitar fornecedores de alto risco e proteger redes críticas de comunicações (Comissão Europeia, 2020).
- Por fim, acelerar projetos do Fundo Europeu de Defesa já em curso, como o 5G COMPAD (comunicações táticas), o ECYSAP (consciência situacional cibernética) e o EICACS (interoperabilidade no combate aéreo) (Comissão Europeia, 2025a).

Nesta dinâmica, a guerra na Ucrânia impulsionou a Comissão Europeia a assumir um papel mais central, o que, segundo Håkansson (2024, p. 26), "elevou a Comissão a um ator geopolítico em áreas tradicionalmente dominadas pelos Estados-membros", nomeadamente energia, sanções e política externa.
O ciberespaço não é apenas um domínio adicional – é a dimensão onde se entrelaçam todas as outras. Sem ele, não há comando, não há logística, não há informação. Mas para que esta dimensão funcione de forma segura e eficaz, é necessário que os sistemas estejam preparados para operar em conjunto, entre Estados, tecnologias e instituições (Comissão Europeia, 2025b).

8. Interoperabilidade: Soberania em Rede

Interoperabilidade deixou de ser um jargão técnico e passou a ser o nome do que sustenta qualquer soberania em rede. O conceito vai muito além da compatibilidade técnica entre equipamentos. Implica linguagens comuns, protocolos partilhados, dados normalizados e confiança institucional. Significa que uma força portuguesa consegue comunicar com um comando norueguês, integrar-se com uma logística polaca ou receber apoio médico de uma unidade francesa. Tudo sem fricções, atrasos ou mal-entendidos.
Historicamente, a ausência de interoperabilidade já custou caro. Durante a Guerra do Kosovo (1999), as unidades da NATO enfrentaram dificuldades de coordenação devido a sistemas de comunicação não compatíveis e doutrinas operacionais desalinhadas (Clark, 2001). Também os primeiros meses de 2022 da guerra na Ucrânia expuseram limitações na integração e partilha de dados/ISR (*Intelligence, Surveillance and Reconnaissance*) entre aliados e parceiros, com constrangimentos técnicos e organizacionais que afetaram a velocidade de decisão (Zabrodskyi et al., 2022).
Do lado dos bons exemplos, encontra-se o projeto OCEAN 2020, financiado pela UE, que integrou 42 parceiros de 15 países, incluindo marinhas, indústrias de defesa e centros de investigação. Este projeto testou a interoperabilidade em operações navais, utilizando *drones* aéreos e submarinos, centros de comando móveis e partilha de inteligência em tempo real entre forças multinacionais. Os exercícios demonstraram que, com plataformas abertas e normas comuns, é possível colaborar, mesmo entre forças com doutrinas e tecnologias diferentes (Agência Europeia

de Defesa 2021b e 2021a; OCEAN2020, s.d.). A resposta europeia tem evoluído, e programas como o *Permanent Structured Cooperation* (PESCO) e o Fundo Europeu de Defesa têm financiado iniciativas para a criação de sistemas interoperáveis, desde redes de comando e controlo a plataformas logísticas e sensores partilhados (PESCO, s.d.). O objetivo é claro: reduzir dependências externas, garantir a resiliência interna e projetar capacidade conjunta.

Mas interoperar exige mais do que vontade política e financiamento. Exige *software* compatível, dados auditáveis, sistemas abertos e normas comuns. A multiplicação de plataformas digitais proprietárias, com lógicas fechadas e algoritmos obscuros, representa um risco crescente. A Europa precisa de garantir que as suas infraestruturas críticas, civis e militares funcionam como um ecossistema seguro e transparente. Além disso, interoperar é também partilhar soberania. Ao abrir sistemas a parceiros, abre-se também a porta à vigilância, à sabotagem ou ao erro. Por isso, a interoperabilidade tem de vir acompanhada de governação partilhada, regras claras de responsabilidade e mecanismos de verificação mútuos.

A NATO já avançou com a padronização de procedimentos e sistemas, e a UE tem vindo a definir quadros legais para assegurar a proteção de dados e a segurança de infraestruturas partilhadas. Mas falta, ainda, um passo decisivo: a integração operacional em tempo real. Plataformas como o CJADC2 (*Combined Joint All-Domain Command and Control*), desenvolvidas nos EUA, apontam nesse sentido: um sistema integrado e adaptativo que coordena forças em todos os domínios, com base em dados e inteligência em tempo real (*U.S. Department of Defense*, 2023). Esta ideia cruza-se com as cadeias de abastecimento e a autonomia estratégica. Como demonstram Kleczka et al. (2024, p. 429), "a autonomia estratégica nas cadeias de abastecimento de defesa da UE não é binária, mas existe ao longo de um espectro", o que obriga a calibrar expetativas sobre interoperabilidade e dependências externas.

Para a Europa, este é o desafio: evoluir para um programa *Joint All-Domain Operations*, um "JADO europeu", que respeite a diversidade dos seus membros, mas que funcione como um só corpo em tempos de crise.

9. Os 2% (ou 5%) do PIB só Defendem se Forem Bem Aplicados

Na cimeira de Gales de 2014, a NATO estabeleceu que os seus membros deviam investir pelo menos 2% do PIB em defesa. Mas em 2024, apenas 23 dos 31[8] países tinham atingido essa meta (NATO, 2024c); Portugal manteve-se abaixo, com cerca

8 A NATO tem 32 membros desde 7 de março de 2024, com a adesão oficial da Suécia. Muitos gráficos e infográficos (como o utilizado neste artigo) foram produzidos anteriormente, daí que o número 31 ainda figure.

de 1,6%. Este valor tornou-se um símbolo de esforço, mas não de eficácia, pois o problema central está na finalidade, execução e coerência estratégica do investimento (Universidade Católica Portuguesa, 2024).

Já na cimeira de 2025, em Haia, a NATO avançou com um novo patamar de ambição: um compromisso político de atingir os 5% do PIB até 2035, repartidos entre despesa militar direta (3,5%) e investimentos em resiliência e segurança (1,5%). Contudo, o desafio permanece: garantir que este aumento de recursos seja acompanhado de visão estratégica, planeamento rigoroso e resultados concretos.

A história mostra que, sem estes elementos, até os maiores investimentos podem falhar no terreno. Em julho de 1916, durante a Batalha do Somme, o exército britânico sofreu, só no primeiro dia, mais de 57 mil baixas; muitas ocorreram porque o bombardeamento falhou em cortar o arame e neutralizar a artilharia, e porque limitações severas de comunicações/comando atrasaram ordens no terreno (*Imperial War Museums*, s.d.; Stewart, 2013). Mais de um século depois, o princípio mantém-se: não basta gastar mais; é preciso gastar com sentido de desenvolvimento de capacidades militares que apoiem a estratégia global ao nível estratégico, operacional e tático (NATO, 2022).

Países com níveis semelhantes de despesa diferem na eficácia operacional, ao nível de prontidão, disponibilidade, tempos de geração e sustentação, e desempenho tático. Em alguns casos, os 2% de investimento são absorvidos por custos correntes e ineficiências; noutros, orientar o investimento para capacidades prioritárias (interoperabilidade, logística, modelação e simulação, ciberdefesa) traduz-se em ganhos de prontidão e emprego de forças. Novamente: sem planeamento concertado e aquisições colaborativas assentes em prioridades comuns, o investimento dispersa-se e o impacto reduz-se (Agência Europeia de Defesa, 2024a, 2024b e 2024c).

A Grécia surge como exemplo de ineficiência: apesar de investir historicamente acima dos 2% e até 3% do PIB, enfrenta dificuldades na renovação tecnológica e na interoperabilidade com aliados, mantendo uma estrutura militar pesada, mas pouco adaptada aos desafios da defesa moderna (SIPRI, 2023 e 2024). Já a Finlândia e a Suécia, mesmo antes da adesão formal à NATO, canalizavam recursos para formação, ciberdefesa e integração com parceiros, conseguindo uma transição mais eficaz para os padrões da Aliança Atlântica (NATO, 2022).

Outro exemplo é a Polónia, que desde 2022 tem reforçado de forma massiva a aquisição de armamento pesado (como os HIMARS – *High Mobility Artillery Rocket System*, os tanques K2 *Black Panther* e os caças F-35 *Lightning II*, que melhoraram a prontidão, mas geraram críticas pela dependência de fornecedores externos e pela falta de integração com a indústria europeia). Este contraste demonstra que o volume de despesa não equivale, por si só, à coerência estratégica.

No plano nacional, Portugal tem vindo a aumentar a despesa rumo aos 2% do PIB até ao final de 2025 (através de um reforço de mil milhões de euros) e traçou como

meta alcançar os 3,5% ao longo da próxima década. Contudo, como alerta Marsh et al. (2024, p. 22), "a falta de alinhamento nos gastos de defesa europeus gera dilemas que reduzem a eficácia global", pelo que a meta dos 2% ou 5% só é útil se acompanhada de convergência estratégica. Este esforço enquadra-se na implementação do programa do XXV Governo Constitucional, que coloca a valorização da Defesa Nacional e dos seus profissionais no centro das prioridades estratégicas (Governo de Portugal, 2025).

Na prática, isso significa que parte destes recursos deve ser canalizada para investimentos estruturais: a produção europeia de semicondutores (*European Chips Act*), a exploração e reciclagem de matérias-primas críticas (*Critical Raw Materials Act*) ou a formação de quadros em áreas digitais e cibernéticas que sustentam diretamente a autonomia estratégica europeia (Comissão Europeia, 2023; União Europeia, 2023; Comissão Europeia, 2024c). A confiança dos cidadãos exige igualmente que o esforço de defesa seja transparente, auditável e politicamente escrutinável. Porquê? Porque há uma dimensão ética incontornável: cada euro alocado à defesa é um euro que deixa de ser investido em saúde, habitação ou educação.

É neste ponto que os objetivos de despesa devem ser acompanhados por indicadores de KPI e metas de impacto.

- Quantos sistemas interoperáveis foram ativados?
- Que percentagem das forças está equipada com capacidades de resposta multidomínio?
- Que ganhos logísticos e de sustentabilidade foram alcançados?
- As capacidades desenvolvidas produzem um efeito dissuasor face às ameaças e reforçam a confiança e a cooperações entre aliados, como preconizam os Objetivos de Desenvolvimento Sustentável?

Só respondendo a estas (e outras) perguntas se pode avaliar a eficácia do investimento de 2% ou 5% na defesa portuguesa.

Neste contexto, é relevante destacar o esforço crescente de transformação digital levado a cabo por várias entidades portuguesas do ecossistema da defesa e soberania nacional – Estado-Maior-General das Forças Armadas, Marinha, Exército, Força Aérea, Instituto Hidrográfico, Instituto de Ação Social das Forças Armadas, Secretaria-Geral do Ministério da Defesa Nacional, Direção-Geral de Recursos da Defesa Nacional[9], entre outras.

9 A Direção-Geral de Recursos da Defesa Nacional (DGRDN) foi formalmente extinta, com efeitos a partir de 1 de julho de 2025, no âmbito da reestruturação orgânica do Ministério da Defesa Nacional. As suas competências foram distribuídas por duas novas entidades: a Direção-Geral de Armamento e Património da Defesa Nacional (DGAPDN) e a Direção-Geral de Recursos Humanos da Defesa Nacional (DGRHDN).

Esta rede institucional, interdependente e interdisciplinar, já aplica tecnologia para funções estratégicas como gestão de efetivos, finanças e património, logística militar, manutenção de equipamentos, controlo da informação e apoio à decisão operacional. No plano internacional, estas capacidades alinham-se com práticas já testadas na NATO[10], que permitem medir eficácia, incorporar lições aprendidas e reforçar a prontidão operacional, garantindo que quem serve tem meios à altura (Ministério da Defesa do Reino Unido, 2021; NATO, 2019; NATO Modelling & Simulation Centre of Excellence, 2023).

10. Cuidar de Quem Defende também É Estratégico

Nenhum exército sustenta a soberania se falhar naquilo que a justifica: a dignidade humana. Um soldado com fome não combate, resiste. Um profissional da defesa sem apoio psicológico não protege, sobrevive. E uma família de militar deixada ao abandono não representa coesão, traduz ausência do Estado. Cuidar de quem defende é, igualmente, uma forma de antecipar, preservar e reforçar a força e a paz coletiva das nações.

Na Primeira Guerra Mundial, as causas não-combate tiveram um peso determinante: nas forças dos EUA, as mortes por doença superaram as dos confrontos bélicos, em grande parte devido à gripe de 1918. A guerra não se perdia apenas nas trincheiras; perdia-se, sobretudo, nas enfermarias improvisadas, nas latrinas contaminadas e na retaguarda descurada (Barry, 2004; *U.S. Army*, 2018).

Mas cuidar não é apenas proteger, é também preparar. A prontidão militar exige conhecimentos técnicos e liderança capazes de responder a desafios multidimensionais. Em vários países europeus já se verifica uma transformação estrutural pautada pela integração de competências digitais (engenharia de *software*, cibersegurança, modelação ou gestão da informação e comunicação) na formação de oficiais, o que contribui para reduzir o *gap* entre quem comanda e quem gere ou lida com os diferentes sistemas que sustentam a missão.

Na Alemanha, por exemplo, a Universidade da Bundeswehr forma oficiais em Informática e oferece mestrados em cibersegurança (Universidade Bundeswehr Munich, s.d). Há igualmente oferta institucionalizada de formação em cibersegurança

10 Exemplos de implementação ao nível da NATO: validação de normas de M&S (*Modelling & Simulation*) como C2SIM (*Command and Control–Simulation Interoperation*) em contexto multinacional nos exercícios CWIX (*Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise*). Em Portugal, o Instituto Hidrográfico (Marinha) opera o sistema integrado SINGAP para gestão de recursos humanos, finanças e património; e noutro país europeu, a Marinha Italiana liderou as demonstrações ao vivo do OCEAN2020, integrando meios tripulados e não tripulados com partilha de dados em tempo real.

e operações híbridas ao nível europeu, bem como exercícios de planeamento e simulação à escala europeia (MILEX 23 e *Cyber Phalanx*), o que tem elevado as competências estratégicas e operacionais, e melhorado a interoperabilidade (Agência Europeia de Defesa, 2019a e 2024a; NATO, 2024b).
Capacitar os quadros militares reduz também dependências externas, acelera a tomada de decisão e reforça a coerência em todos os níveis. É uma medida estratégica que prepara para situações de conflito e contribui para a segurança em tempos de paz, através de:

- Apoio à natalidade e parentalidade, com licença adaptada, creches militares e ajudas de custo;
- Habitação digna para militares e famílias, em tempo de paz e em cenários de mobilização;
- Acesso a educação e integração escolar para filhos em realocação interna ou internacional;
- Apoio psicológico contínuo, não apenas em situações de pós-trauma, mas como prevenção de *burnout* e reforço de resiliência;
- Subsídios de deslocação e ajudas de custo para missões e treinos prolongados;
- Sistemas de pensões e compensações por ferimentos, deficiência ou morte em serviço;
- Protocolos de trasladação de corpos com dignidade e apoio emocional às famílias enlutadas;
- Planos de reintegração profissional ou reconversão de carreira para militares em fim de contrato.

Na Guerra das Malvinas (1982), a falta de abrigos e o desrespeito pelos efetivos contribuíram mais para a derrota argentina do que qualquer míssil britânico. Este episódio lembra que são as pessoas, muito antes da tecnologia, que vencem as guerras (Freedman, 2005).
Alguns países incorporaram esta aprendizagem nas suas políticas de defesa: a Noruega, por exemplo, consagrou em documentos estruturantes prioridades explícitas em pessoal, integrando o bem-estar no núcleo da capacidade de dissuasão (Ministério da Defesa Norueguês, 2019; Governo da Noruega, 2024–2025). Já em Timor-Leste, a consolidação da paz incluiu a implementação, com apoio do Programa das Nações Unidas para o Desenvolvimento (PNUD), de sistemas de informação destinados ao registo de combatentes e ao pagamento de pensões, uma iniciativa que aportou transparência, planeamento de carreiras e apoio aos veteranos de guerra e respetivas famílias. Este foi um investimento que fortaleceu a capacidade

do jovem Estado (no início da década 2000) e contribuiu para manter a estabilidade, prevenindo a escalada de tensões internas. (PNUD, 2012).
O cuidado com quem defende a nação começa antes, prolonga-se durante e mantém-se após o combate, constituindo, quando bem executado, um pilar de coesão, segurança e justiça para toda a sociedade.

11. Considerações Finais

Como escreveu Sauli Niinistö (figura central na integração da Finlândia na NATO e reconhecido pela sua visão estratégica em matéria de segurança europeia), *"a segurança é a base sobre a qual tudo o resto assenta"* (Niinistö, 2024). E sem segurança, economia, coesão social e legitimidade política perdem a sustentação.
Esta é também a premissa que sustenta a tese deste artigo: a defesa só é eficaz quando apoiada numa execução estratégica sólida. Sem gestão eficiente, interoperabilidade real e valorização das pessoas, o investimento traduz-se em despesa e não em capacidade. Os autores deste artigo entendem que segurança exige coordenação de recursos, integração de dados e processos, bem como uma dissuasão credível.
No capítulo 1, enquadrámos o desafio: a guerra regressou à Europa em formatos híbridos e acelerados, onde retaguarda e frente de combate se confundem. Garantir uma defesa eficaz exige instituições sólidas, capacidade de antecipação e informação fiável, combinadas com tecnologia (e não dependentes apenas dela).
No capítulo 2, mostrámos como as derrotas começam nos bastidores: por aquisições fragmentadas, inventários desatualizados, ERP monolíticos sem agilidade nem prontidão para a mudança ou sistemas que não "falam" entre si e causam fricção operacional.
No capítulo 3, falámos de logística e de como a cadeia de abastecimento (dados, previsões, reposição, manutenção) é o centro de gravidade que pode separar prontidão de colapso.
No capítulo 4, abordámos *Edge AI* e agentes inteligentes: decidir mais perto do terreno com computação periférica, sensores integrados e automação governada por regras reduz o ciclo OODA (Observar, Orientar, Decidir e Agir) e possíveis falhas humanas.
No capítulo 5, passámos ao multidomínio: terra, mar, ar, espaço e ciberespaço só produzem efeito quando operam de forma conjunta e coordenada, com comando e controlo, inteligência, vigilância, reconhecimento e logística integrados.
No capítulo 6, defendemos modelação, simulação e gémeos digitais. Estes planeiam, testam e ensinam sem expor recursos, aceleram a manutenção e aumentam resiliência; tudo para antecipar, em vez de improvisar.
No capítulo 7, olhámos para o ciberespaço com mais profundidade, recordando que tanto situações intencionais como acidentais se propagam por redes interdependen-

tes. Regulamentações como RGPD, NIS2 e AI Act dão as diretrizes, mas só as rotinas de teste, a auditoria (e as respetivas coimas, se for o caso) comprovam a sua eficácia.
No capítulo 8, sustentámos que interoperabilidade é soberania em rede, via normas abertas, dados normalizados, confiança e governação partilhada. A ambição europeia tem de evoluir para um "JADO europeu" que funcione em tempo real e ligue sensores, decisores e forças de ponta a ponta.
No capítulo 9, mostrámos que 2% (ou mesmo 5%) do PIB só defendem se forem orientados por capacidades (interoperabilidade, logística, modelação e simulação e cibersegurança) e avaliados por medidas de eficácia e desempenho, com processos de aquisição partilhados e escrutínio público.
No capítulo 10, demos prioridade ao fator humano: capacitar, cuidar e reintegrar é o que transforma orçamento em força disponível; e, a longo prazo, sustenta a paz e a estabilidade.
Deste percurso, fica claro que a Europa não parte do zero. A Estratégia Industrial de Defesa Europeia define prioridades até 2035 (Comissão Europeia, 2025b); o Programa Europeu de Investimento em Defesa transforma intenção em produção conjunta e aquisições coordenadas. Em paralelo, a UE tem gradualmente deixado de ser um mero facilitador de mercado para assumir o papel de ator de política industrial na área da defesa, com implicações diretas na coordenação de capacidades e cadeias de valor (Andersson e Britz, 2025).
A estas vozes juntam-se os relatórios Letta, Draghi e Heitor, que fornecem diagnósticos e exigências concretas sobre escala, circulação de conhecimento e competitividade tecnológica. Soma-se ainda Sauli Niinistö, que defende uma "União da Preparação" baseada numa abordagem em que a segurança e a defesa não são responsabilidade exclusiva dos militares, mas sim um esforço integrado que envolve o Estado (ministérios, agências, forças de segurança, sistemas de saúde, educação, proteção civil, etc.) e a sociedade (empresas, ONG, universidades, cidadãos, meios de comunicação, etc.) (Comissão Europeia, 2024a e 2024b; Draghi, 2025; Heitor, 2024; Letta, 2024; Niinistö, 2024)
Os dados da Agência Europeia de Defesa (tanto na compilação anual de despesas como na Revisão Anual Coordenada da Defesa) confirmam a direção, mas fixam a exigência no mesmo ponto: executar melhor, com menos fragmentação, mais normalização e verdadeira escala (Agência Europeia de Defesa, 2024a e 2024b).
Perante uma Europa novamente em guerra e rodeada por focos de instabilidade (religiosos, sociais e económicos), a prioridade é pensar e agir como um sistema: ligar o planeamento ao orçamento, as normas à execução e a política às pessoas, com métricas públicas para prontidão, interoperabilidade e sustentação. Isto significa:

- Financiar o que integra (dados partilháveis, interfaces abertas, formaçã o comum) e desincentivar o que fragmenta;

- Operacionalizar o digital de ponta a ponta (modelação e simulação, manutenção, gémeos digitais, cibersegurança, comando e controlo, e integração em tempo real da informação, vigilância, reconhecimento e logística;
- Tratar o capital humano (os quadros e as famílias) como ativo estratégico, ao nível de retenção, moral e coesão – elementos importantes da dissuasão;
- E medir resultados com critérios de eficácia operacional, não apenas de execução orçamental (Agência Europeia de Defesa, 2024a; Comissão Europeia, 2024a).

A conclusão é clara: despesa não é sinónimo de defesa. Defesa é estratégia em exe cução: sistemas interoperáveis e auditáveis, processos que ligam sensores a decisores, lideranças com autonomia e responsabilidades claras, e pessoas protegidas e capacitadas. É nesta interseção que se define a soberania europeia.

Esta não é, contudo, uma tese estática para a Europa. A leste, persiste uma guerra de alta intensidade; a sul, o Magrebe e o Sahel alternam entre instabilidade e pressão migratória; no Médio Oriente, os conflitos reacendem em ciclos curtos. Do outro lado do Atlântico, a reindustrialização norte-americana avança com tarifas comerciais inesperadas; a oriente, a dependência europeia de cadeias dominadas pela China mantém-se para semicondutores, baterias e metais estratégicos. E dentro das fronteiras europeias, crescem divisões religiosas e identitárias, enquanto a desinformação corrói consensos e as infraestruturas críticas (energia, portos, cabos submarinos, redes digitais) se tornam novos alvos.

Acresce a esta realidade uma guerra cognitiva, sustentada por campanhas de desinformação, manipulação algorítmica e pela exploração de clivagens sociais, cujo objetivo é corroer a confiança pública e enfraquecer a coesão europeia. É um novo campo de batalha (invisível, mas decisivo) que, como nota Zabrodskyi, "precede e acompanha a fase cinética, concebida para paralisar a tomada de decisão e minar a resiliência social" (Zabrodskyi et al., 2022, p. 4).

Defender a Europa é salvaguardar a sua autonomia de decisão e a continuidade de um projeto civilizacional que não nasceu por acaso, mas da experiência dura de duas guerras mundiais. É compreender que o poder de decidir sobre o próprio destino é inseparável da capacidade de o defender. Para isso, os autores deste artigo consideram que a Europa precisa de inteligência, tecnologia e, sobretudo, das suas pessoas; alinhadas por uma estratégia comum que existe desde o Tratado de Paris de 1951 (do qual nasceu a Comunidade Europeia do Carvão e do Aço) e que se consolidou com sucessivas integrações, fazendo da reconciliação e da cooperação o alicerce da paz entre nações outrora inimigas.

Quarenta anos após a adesão de Portugal à União Europeia, este espírito deve traduzir-se numa estratégia que produza capacidade operacional e dissuasão credível. Só assim se assegura, de forma consistente, a preservação dos interesses e valores que a Europa se propõe defender.

Bibliografia

Agência Europeia de Defesa (2024a) *Coordinated Annual Review on Defence (CARD) 2024 – Executive Summary*. Brussels: EDA. Disponível em: https://eda.europa.eu/docs/default-source/documents/card-report-2024.pdf [Consultado a 12 de agosto de 2025].

Agência Europeia de Defesa (2024b) *Defence Data 2023–2024*. Brussels: EDA. doi:10.2836/0704767. Disponível em: https://eda.europa.eu/docs/default-source/brochures/1eda---defence-data-23-24---web---v3.pdf [Consultado a 12 de agosto de 2025].

Agência Europeia de Defesa (2024c) *EDA Annual Report 2024*. Brussels: EDA. Disponível em: https://eda.europa.eu/docs/default-source/brochures/eda-annual-report-2024.pdf [Consultado a 8 de agosto de 2025].

Agência Europeia de Defesa (2024d) *Explore Defence Digital Twins (EDDI): Study on the use of digital twin technologies across combat domains*. Brussels: EDA. Disponível em: https://www.flysight.it/explore-defence-digital-twins-eddi-eda-study-for-the-next-four-years/ [Consultado a 7 de agosto de 2025].

Agência Europeia de Defesa (2021b) *Factsheet: Cyber Phalanx*. Brussels: EDA. Disponível em: https://eda.europa.eu/publications-and-data/factsheets/factsheet-cyber-phalanx [Consultado a 12 de agosto de 2025].

Agência Europeia de Defesa (2019a) *Largest EU-funded defence research project tested in the Mediterranean Sea*. Disponível em: https://eda.europa.eu/news-and-events/news/2019/11/21/largest-eu-funded-defence-research-project-tested-in-the-mediterranean-sea [Consultado a 12 de agosto de 2025].

Agência Europeia de Defesa (2019b) *OCEAN2020 Factsheet*. Brussels: EDA. Disponível em: https://eda.europa.eu/publications-and-data/factsheets/factsheet-ocean2020 [Consultado a 12 de agosto de 2025].

Agência Europeia de Defesa (2021a) *Successful second sea demonstration for OCEAN2020 in the Baltic Sea*. Disponível em: https://eda.europa.eu/news-and-events/news/2021/08/26/successful-second-sea-demonstration-for-ocean2020-in-the-baltic-sea [Consultado a 11 de agosto de 2025].

Andersson, J.J. e Britz, M. (2025) *The European Union's role in European defence industry policy*. Defence Studies, 25(2), pp. 322–341. Disponível em: https://doi.org/10.1080/14702436.2025.2472694 [Consultado a 22 de agosto de 2025].

Barnett, C. (1963) *The Swordbearers: Studies in Supreme Command in the First World War*. London: Eyre & Spottiswoode, p. 35.

Barry, J.M. (2004) *The Great Influenza: The Story of the Deadliest Pandemic in History*. New York: Viking.

Beaufre, A. (1998) *Introdução à Estratégia*. Lisboa: Edições Atena, pp. 45–46.

Betts, R.K. (1995) *Military Readiness: Concepts, Choices, Consequences*. Washington, DC: Brookings Institution Press.

Borges, A.P., Plácido, C., Oliveira, C., Rodrigues, M., Franco, M., Pereira, R. e Silva, R. (2024) *Sucesso na Implementação do BSC em Organizações Públicas e Privadas*. Viseu: PsicoSoma.

Brøgger, T. E. (2024) *A Europe of defence? The establishment of binding commitments and supranational governance in European security and defence.* Journal of European Integration, pp. 1–20. Disponível em: https://doi.org/10.1080/07036337.2024.2379421 [Consultado a 21 de agosto de 2025].

Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., Khlaaf, H., Yang, J. e Anderljung, M. (2023) *Frontier AI Regulation: Managing Emerging Risks to Public Safety*. San Francisco: Centre for the Governance of AI. Disponível em: https://arxiv.org/abs/2307.03718 [Consultado a 22 de agosto de 2025].

Chovančík, M. e Krpec, O. (2023) *Cloaked disintegration – Ukraine war and European defence-industrial co-operation in Central and Eastern Europe, Defense & Security Analysis*, 39 (3), pp. 369–386. Disponível em: https://doi.org/10.1080/14751798.2023.2204596 [Consultado a 21 de agosto de 2025].

Clark, W. K. (2001) *Waging Modern War: Bosnia, Kosovo, and the Future of Combat*. New York: PublicAffairs. Disponível em: https://archive.org/details/wagingmodernwarb00clar [Consultado a 6 de agosto de 2025].

Clemenceau, G. (2023) *"A guerra! É uma coisa demasiado grave para ser deixada aos militares"*. In:*Citador*.Disponívelem:https://www.citador.pt/frases/a-guerra-e-uma-coisa-demasiado-grave-para-ser-c-georges-clemenceau-1781 [Consultado a 6 de agosto de 2025].

Cole, R.H. (1985) *Operation URGENT FURY: The Planning and Execution of Joint Operations in Grenada*. Fort Leavenworth, KS: U.S. Army Center of Military History. Disponível em: https://www.jcs.mil/portals/36/documents/history/monographs/urgent_fury.pdf [Consultado a 3 de agosto de 2025].

Comissão Europeia (2024a) *A new European Defence Industrial Strategy: Achieving EU readiness through a responsive and resilient European Defence Industry*. Joint Communication JOIN (2024) 10 final, Brussels, 5 March 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024JC0010 [Consultado a 11 de agosto de 2025].

Comissão Europeia (2024c) *Cloud computing – Shaping Europe's digital future.* Brussels: European Commission. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/cloud-computing [Consultado a 27 de agosto de 2025]

Comissão Europeia (2024d) *EDIS – Our common European defence industrial strategy.* Brussels: European Commission/EEAS. Disponível em: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en [Consultado a 12 de agosto de 2025].

Comissão Europeia (2024e) *EUCS – European Cybersecurity Certification Scheme for Cloud Services.* Brussels: European Commission. Disponível em: https://ec.europa.eu/newsroom/cipr/items/713799/en [Consultado a 27 de agosto de 2025]

Comissão Europeia (2025c) *European Defence Fund – developing tomorrow's defence capabilities*. Brussels: Directorate-General for Defence Industry and Space. Disponível em: *https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en* [Consultado a 11 de agosto de 2025].

Comissão Europeia (2025a) *European Defence Fund: Funded Projects Overview*. Brussels: European Commission. Disponível em: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en [Consultado a 9 de agosto de 2025].

Comissão Europeia (2024b) *European Defence Fund – official webpage*. Disponível em: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en [Consultado a 11 de agosto de 2025].

Comissão Europeia (2025b) *Future of European Defence. Brussels: Directorate-General for Communication.* Disponível em: *https://commission.europa.eu/topics/defence/future-european-defence_en* [Consultado a 10 de agosto de 2025].

Comissão Europeia (2023) *Proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem*. Brussels: European Commission. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0046 [Consultado a 27 de agosto de 2025].

Comissão Europeia (2020) *Secure 5G deployment in the EU – Implementing the EU toolbox. Brussels: European Commission.* Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020DC0050 [Consultado a 27 de agosto de 2025].

Council on Foreign Relations (2025) *From the Ukraine Conflict to a Secure Europe*, Council on Foreign Relations, June. Disponível em: https://www.cfr.org/report/ukraine-conflict-secure-europe [Consultado a 6 de agosto de 2025].

Cour des Comptes (2014) *Le Système Louvois: rapport public thématique*. Paris: Cour des Comptes.

Diário da República (2023) *Despacho n.º 11801/2024*. Lisboa: Imprensa Nacional-Casa da Moeda. Disponível em: https://diariodarepublica.pt/dr/detalhe/despacho/11801-2024-889940197 [Consultado a 15 de agosto de 2025].

Draghi, M. (coord.) (2025) *The future of European competitiveness: A competitiveness strategy for Europe.* Brussels: European Commission. Disponível em: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en [Consultado a 12 de agosto de 2025].

Eccles, H.E. (1959) *Logistics in the National Defense*. Harrisburg, PA: Stackpole Books. Disponível em: https://archive.org/details/logisticsinnatio00eccl [Consultado a 11 de agosto de 2025].

European External Action Service (2023) *MILEX 23 – EU Crisis Management Military Exercise 2023.* Brussels: EEAS. Disponível em: https://www.eeas.europa.eu/eeas/milex-23-%E2%80%93-eu-crisis-management-military-exercise-2023_en [Consultado a 8 de agosto de 2025].

Fiott, D. (2023) *In Every Crisis an Opportunity? European Union integration in defence and the War on Ukraine.* Journal of European Integration, 45 (3), pp. 447–462. Disponível em: https://doi.org/10.1080/07036337.2023.2183395 [Consultado a 20 de agosto de 2025].

Freedman, L. (2005) *The Official History of the Falklands Campaign. Volume II: War and Diplomacy.* London/New York: Routledge. Disponível em: https://www.taylorfrancis.com/books/mono/10.4324/9780203507858/official-history-falklands-campaign-volume-2-lawrence-freedman [Consultado a 12 de agosto de 2025].

Ghemawat, P. and Nueno, J.L. (2006) *Zara: Fast Fashion*. Harvard Business School Publishing.

Giacomello, G. e Preka, O. (2023) *Sources of strength: mapping the defence sector in Europe,* Defence Studies, 23 (4), pp. 531–560. Disponível em: https://doi.org/10.1080/14702436.2023.2277436 [Consultado a 20 de agosto de 2025].

Giberna, M., Voos, H., Tavares, P., Nunes, J., Sorg, T., Masini, A. e Sanchez-Lopez, J.L. (2025) *On Digital Twins in Defence: Overview and Applications*. Disponível em: https://arxiv.org/html/2508.05717v1 [Consultado a 7 de agosto de 2025].

Gladwell, M. (2005) *Blink: The Power of Thinking Without Thinking*. New York: Little, Brown and Company.

Glantz, D.M. (2002) *The Battle for Leningrad, 1941–1944. Lawrence, KS: University Press of Kansas.*

Government Accountability Office (2019) *DOD Financial Management: Continued Efforts Needed to Correct Serious Weaknesses in the Department of the Air Force's Accounting System*. Washington, DC: U.S. Government Accountability Office.

Governo da Noruega (2024–2025) *Meld. St. 9: Total Preparedness.* Oslo: Forsvarsdepartementet. Disponível em: https://www.regjeringen.no/contentassets/c24e6978185f4a49a7d2689a4741a9b1/en-gb/pdfs/stm202420250009000engpdfs.pdf [Consultado a 12 de agosto de 2025].

Governo de Portugal (2025) *Programa do XXV Governo Constitucional* (secção "Plano de reforço estratégico de investimento em defesa: atingindo 2% do PIB já em 2025"). Lisboa: Governo da República Portuguesa. Disponível em: https://www.portugal.gov.pt/download-ficheiros/ficheiro. aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDEz1MAEA4Ox4%2bQUAAAA%3d [Consultado a 12 de agosto de 2025].

Gray, C.S. (1999) *Modern Strategy*. Oxford: Oxford University Press.

Håkansson, C. (2024) *The Ukraine war and the emergence of the European Commission as a geopolitical actor,* Journal of European Integration, 46(1), pp. 25–45. Disponível em: https://www.tandfonline.com/doi/full/10.1080/07036337.2023.2239998 [Consultado a 22 de agosto de 2025].

Heckmann, L. (2025) *Pentagon ready to let AI make some decisions,* National Defense Magazine. Disponível em: https://www.nationaldefensemagazine.org/articles/2025/4/5/pentagon-ready-to-let-ai-make-some-decision [Consultado a 5 de agosto de 2025].

Heitor, M. (coord.) (2024) *Align, Act, Accelerate – Research, Technology and Innovation to Boost European Competitiveness*. Luxembourg: Publications Office of the European Union. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/2f9fc221-86bb-11ef-a67d-01aa75ed71a1/language-en [Consultado a 7 de agosto de 2025].

Heuser, B. (2010) *The Evolution of Strategy: Thinking War from Antiquity to the Present*. Cambridge: Cambridge University Press.

Holland-Michel, A. (2023) *Recalibrating assumptions on AI: Towards an evidence-based and inclusive AI policy discourse*. London: Royal Institute of International Affairs (Chatham House). Disponível em: https://www.chathamhouse.org/sites/default/files/2023-04/2023-04-05-recalibrating-ai-holland-michel.pdf [Consultado a 21 de agosto de 2025].

Imperial War Museums (s.d.) *First Day Of The Battle Of The Somme | What happened on the first day of the Somme?* Disponível em: https://www.iwm.org.uk/history/what-happened-on-the-first-day-of-the-battle-of-the-somme [Consultado a 11 de agosto de 2025].

Instituto Hidrográfico (s.d.) *Instituto Hidrográfico distinguido com o Prémio Cooperação e Desenvolvimento.* Disponível em: https://www.hidrografico.pt/noticia/57 [Consultado a 12 de agosto de 2025].

Jennings, G. (2023a) *Logistics in Modern European Defence*. London: Jane's Defence Weekly.

Jennings, G. (2023b) European Defence Procurement: Challenges and Perspectives. London: Jane's Defence Weekly.

Kaplan, R.S. and Norton, D.P. (2001) *The Strategy-Focused Organization: How Balanced Scorecard Companies Thrive in the New Business Environment*. Boston, MA: Harvard Business Press.

Keegan, J. (1993) *A History of Warfare*. New York: Vintage. Disponível em: https://archive.org/details/historyofwarfare00keeg [Consultado a 11 de agosto de 2025].

Kleczka, M., Vandercruysse, L., Buts, C. e Du Bois, C. (2024) *The Spectrum of Strategic Autonomy in EU Defence Supply Chains,* Defence and Peace Economics, 35 (4), pp. 427–447. Disponível em: https://doi.org/10.1080/10242694.2023.2180588 [Consultado a 20 de agosto de 2025].

Leonard, M. (2023) *The Age of Unpeace: How Connectivity Causes Conflict*. London: Penguin.

Letta, E. (2024) *Much More Than a Market*. Brussels: European Commission. Disponível em: https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf [Consultado a 11 de agosto de 2025].

Luttwak, E.N. (2001) *Strategy: The Logic of War and Peace*. Cambridge, MA: Belknap Press of Harvard University Press.

Marsh, N., Oliveira Martins, B. e Mawdsley, J. (2024) *European Defense Spending: Trade-Offs and Consequences of Non-Alignment,* EconPol Forum, 25 (4), pp. 20–23. Disponível em: https://www.cesifo.org/DocDL/econpol-forum-2024-4-marsh-martins-mawdsley-european-defense.pdf [Consultado a 20 de agosto de 2025].

Meyer, C.O. (2005) *Convergence Towards a European Strategic Culture? A Constructivist Framework for Explaining Changing Norms*, European Journal of International Relations, 11(4), pp. 523–549. Disponível em: https://eprints.bbk.ac.uk/id/eprint/417/1/Binder1.pdf [Consultado a 10 de agosto de 2025].

Ministério da Defesa do Reino Unido (2023) *Convention on the establishment of the "Global Combat Air Programme – GCAP International Government Organisation"*. London: Ministry of Defence. Disponível em: https://www.gov.uk/government/publications/convention-on-the-establishment-of-the-global-combat-air-programme-gcap-international-government-organisation [Consultado a 6 de agosto de 2025].

Ministério da Defesa do Reino Unido (2021) *Digital Strategy for Defence – delivering the Digital Backbone and unleashing the power of Defence's data*. Disponível em: https://assets.publishing.service.gov.uk/media/60afae56d3bf7f435f43c7af/20210421_-_MOD_Digital_Strategy_-_Update_-_Final.pdf [Consultado a 6 de agosto de 2025].

Ministério da Defesa Nacional (2014) Despacho n.º 11400/2014. Diário da República, 2.ª série, n.º 170, 4 setembro. Disponível em: https://diariodarepublica.pt/dr/detalhe/despacho/11400-2014-56725394 [Consultado a 11 de agosto de 2025].

Ministério da Defesa Norueguês (2019) *Norwegian Defence – Annual Report*. Oslo: Norwegian Ministry of Defence.

Mishra, P.K. e Dash, R. (2007) *Balanced Scorecard for Nonprofit Organizations*. New Delhi: Excel Books.

Moltke, H. von (1892). *Moltke, H. von (1892). Militärische Werke. Band II, Teilband 2: Militärische Korrespondenz. Berlin: Ernst Siegfried Mittler und Sohn, pp. 291.*

Moravcsik, A. (2018) *Preferences, Power and Institutions in 21st Century Europe*. Journal of Common Market Studies, 56(S1), pp.164–179.

Naisbitt, J. (1982) *Megatrends: Ten New Directions Transforming Our Lives*. New York: Warner Books, pp. 1–33.

NASA (1970) *Apollo 13 Mission Operations Report*. Houston, TX: NASA Manned Spacecraft Center. Disponível em: https://www.hq.nasa.gov/alsj/a13/A13_MissionReport.pdf [Consultado a 7 de agosto de 2025].

National Audit Office (2017) *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office. Disponível em: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/ [Consultado a 7 de agosto de 2025].

National Audit Office (2008) *The Defence Information Infrastructure*. London: The Stationery Office.

NATO (2022) *AJP-01 Allied Joint Doctrine* (Edition F, Version 1). Brussels: NATO Standardization Office. Disponível em: https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_%281%29_2437.pdf [Consultado a 12 de agosto de 2025].

NATO (2024a) *Cyber defence*. Brussels: NATO. Disponível em: https://www.nato.int/cps/en/natohq/topics_78170.htm [Consultado a 7 de agosto de 2025].

NATO (2025) *Data Strategy for the Alliance*. Brussels, VA: NATO Allied Command Transformation. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_234937.htm [Consultado a 8 de agosto de 2025].

NATO (2023b) *Digital Twins in Defence Applications*. Norfolk, VA: NATO Allied Command Transformation. Disponível em: https://www.act.nato.int/publications [Consultado a 6 de agosto de 2025].

NATO (2023a) *NATO Data Centric Reference Architecture (DCRA)*. Norfolk, VA: NATO Allied Command Transformation. Disponível em: https://nhqc3s.hq.nato.int/apps/DCRA_Report [Consultado a 11 de agosto de 2025].

NATO (2023c) *NexGen Modelling and Simulation*. 20 September. Norfolk, VA: NATO Allied Command Transformation. Disponível em: https://www.act.nato.int/article/nexgen-modelling-and-simulation/ [Consultado a 13 de agosto de 2025].

NATO (2019) *Preparing for Operational Use of C2-Simulation – Validation at CWIX* (STO-MP-MSG-171-P3). Disponível em: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-171/MP-MSG-171-P3.pdf [Consultado a 12 de agosto de 2025].

NATO (2024c) *Press conference by the NATO Secretary General (statement on 23 Allies at 2%)*. Disponível em: https://www.nato.int/cps/en/natohq/227417.htm [Consultado a 11 de agosto de 2025].

NATO (2024b) *Training Catalogue 2025*. Tallinn: CCDCOE.VA: Cooperative Cyber Defence Centre of Excellence. Disponível em: https://ccdcoe.org/uploads/2024/10/2025_NATO_CCD_COE_Training_Catalogue_final.pdf [Consultado a 12 de agosto de 2025].

NATO (2023d) *Homepage / Courses / Publications*. Disponível em: https://www.mscoe.org/ [Consultado a 11 de agosto de 2025].

NATO Innovation Hub (2023) *Digital Transformation in Defence*. Norfolk, VA: NATO Allied Command Transformation.

NATO Modelling & Simulation Centre of Excellence (2023) *Validating M&S Standards Interoperation in CWIX 2022*. Disponível em: https://www.mscoe.org/document/validating-ms-standards-interoperation-in-cwix-2022/ [Consultado a 8 de agosto de 2025].

Niinistö, S. (2024) Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness. Brussels: European Commission, 30 October. Disponível em: *https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union_en* [Consultado a 7 de agosto de 2025].

OCDE (2023) *Anticipatory Governance*. Disponível em: https://www.oecd.org/en/topics/anticipatory-governance.html [Consultado a 6 de agosto de 2025].

OCDE (2022) *OECD Science, Technology and Innovation Outlook 2023: Sustaining Recovery, Navigating Change*. Paris: OECD Publishing. Disponível em: https://www.oecd.org/en/publications/oecd-science-technology-and-innovation-outlook-2023_0b55736e-en/full-report.html [Consultado a 8 de agosto de 2025].

OCEAN2020 (s.d.) *Project website.* Disponível em: https://ocean2020.eu/ [Consultado a 11 de agosto de 2025].

Oliveira, M. (2019) *Otimização do SIG/DN na gestão de imobilizado no Exército*. Trabalho de Investigação Aplicada. Lisboa: Instituto Universitário Militar. Disponível em: https://comum.rcaap.pt/entities/publication/411565f7-d0c4-4541-af26-f86f9ba11350 [Consultado a 15 de agosto de 2025].

Ottis, R. (2008) *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Tallinn: CCDCOE. Disponível em: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf [Consultado a 7 de agosto de 2025].

Permanent Structured Cooperation – PESCO (s.d.) *Official website.* Disponível em: https://pesco.europa.eu/ [Consultado a 9 de agosto de 2025].

Phogat, S. (2022) *The trouble with JIT in military operations: a review.* Disponível em: https://www.canada.ca/en/army/services/line-sight/articles/2022/01/the-trouble-with-jit-in-military-operations-a-review.html [Consultado a 6 de agosto de 2025].

PNUD (2012) *Support to Civil Service Reform in Timor-Leste – Project Document*. Disponível em: https://info.undp.org/docs/pdc/Documents/TLS/Prodoc_for_Support_to_the_Civil_Service.pdf. [Consultado a 12 de agosto de 2025].

Pool, R. (2025) *Drones with Edge AI: The Future of Warfare?* EE Times Europe, 5 de março. Disponível em: *https://www.eetimes.eu/drones-with-edge-ai-the-future-of-warfare/* [Consultado a 11 de agosto de 2025].

RAND Europe (2024) *Strategic Competition in the Age of AI: Emerging Risks and Opportunities from Military Use of Artificial Intelligence*. Santa Monica, CA: RAND Corporation. Disponível em: https://www.rand.org/pubs/research_reports/RRA3295-1.html [Consultado a 22 de agosto de 2025].

Rocha, A. (2018) *O Sistema Integrado de Gestão da Defesa Nacional (SIG/DN) como suporte à função de abastecimento da logística aérea*. Trabalho de Investigação Aplicada. Lisboa: Instituto Universitário Militar. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/24930/1/07_CapAndreiaRocha_TII_VF.pdf [Consultado a 12 de agosto de 2025].

Rodrigues, P. (2020) *O uso do Sistema Integrado de Gestão da Defesa Nacional (SIG/DN) na Marinha*. Trabalho de Investigação Aplicada. Lisboa: Instituto Universitário Militar. Disponível em: https://comum.rcaap.pt/entities/publication/7d1042e2-2250-48e6-a1dc-4c3a1010000c [Consultado a 12 de agosto de 2025].

Rynning, S. (2003). *The European Union: Towards a Strategic Culture?*, Security Studies, 14(3), pp. 61–93.

SIPRI (2023) *Trends in World Military Expenditure, 2022*. Disponível em: https://www.sipri.org/sites/default/files/2023-04/2304_fs_milex_2022.pdf [Consultado a 12 de agosto de 2025].

SIPRI (2024) *Trends in World Military Expenditure, 2023 (Fact Sheet)*. Disponível em: https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf [Consultado a 5 de agosto de 2025].

Soljenítsin, A. (1971) *August 1914*. New York: Farrar, Straus and Giroux.

Stewart, W. F. (2013). *The Most Aggravating Thing: Communications and Limitations on the Somme,* Canadian Military History. Disponível em: https://canadianmilitaryhistory.ca/the-most-aggravating-thing-communications-and-limitations-on-the-somme-by-william-stewart/ [Consultado a 12 de agosto de 2025].

Sullivan, G.R. e Dubik, J.M. (1994) *War in the Information Age*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College. Disponível em: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1265&context=monographs [Consultado a 9 de agosto de 2025].

União Europeia (2022) *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a assegurar um elevado nível comum de cibersegurança em toda a União (Diretiva NIS2)*. Jornal Oficial da União Europeia, L 333, 27 de dezembro de 2022, pp. 80–152. Disponível em: https://eur-lex.europa.eu/eli/dir/2022/2555/oj [Consultado a 7 de agosto de 2025].

União Europeia (2023) Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements. Brussels: European Union. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454 [Consultado a 27 de agosto de 2025].

União Europeia (2016) *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD)*. Jornal Oficial da União Europeia, L 119, 4.5.2016, pp. 1–88. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Consultado a 7 de agosto de 2025].

União Europeia (2024c) *Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (AI Act)*. Jornal Oficial da União Europeia, L 2024/1685, 12.7.2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=pt [Consultado a 9 de agosto de 2025].

União Europeia (2024b) *Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data*. Brussels: European Union. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854 [Consultado a 28 de agosto de 2025].

União Europeia (2024a) *Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence.* Brussels: European Union. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj [Consultado a 27 de agosto de 2025].

United States Congress (1986) *Goldwater–Nichols Department of Defense Reorganization Act of 1986*. Public Law 99-433, 1 de Outubro de 1986. Disponível em: https://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsCR.pdf [Consultado a 7 de agosto de 2025].

Universidade Bundeswehr Munich (s.d.) *Courses of Study (incl. Computer Science and Cyber Security).* Neubiberg: UniBw M. Disponível em: https://www.unibw.de/home-en/studies/courses-of-study [Consultado a 12 de agosto de 2025].

Universidade Católica Portuguesa (2024) *Vale a pena gastar 5% do PIB em defesa nacional?* Lisboa: Católica Lisbon School of Business and Economics. Disponível em: https://clsbe.lisboa.ucp.pt/pt-pt/noticias/vale-pena-gastar-5-do-pib-em-defesa-nacional [Consultado a 12 de agosto de 2025].

U.S. Army (2018) *Worldwide flu outbreak killed 45,000 American Soldiers during World War I.* Army.mil (News). Disponível em: https://www.army.mil/article/210420/worldwide_flu_outbreak_killed_45000_american_soldiers_during_world_war_i [Consultado a 12 de agosto de 2025].

U.S. Department of Defense (2023) *DoD Chief Digital and Artificial Intelligence Office hosts last Global Information Dominance Experiment (GIDE 8).* Disponível em: https://www.defense.gov/News/Releases/Release/Article/3618250/dod-chief-digital-and-artificial-intelligence-office-hosts-last-global-informat/ [Consultado a 7 de agosto de 2025].

Van Creveld, M. (2004) *Supplying War: Logistics from Wallenstein to Patton*. Cambridge University Press. Disponível em: https://www.cambridge.org/core/books/abs/supplying-war/introduction/31DFE7186A4BFEBB1DC0982FDA71D34C [Consultado a 12 de agosto de 2025].

Van Way III, C.W. (2022) *War, Medicine & Death*, Missouri Medicine, 119(6), pp. 529–532. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC9762220/ [Consultado a 12 de agosto de 2025].

Vershinin, A. (2022) *The Return of Industrial Warfare*. London: RUSI. Disponível em: https://www.rusi.org/explore-our-research/publications/commentary/return-industrial-warfare [Consultado a 11 de agosto de 2025].

Zabrodskyi, M., Watling, J., Danylyuk, O. V. e Reynolds, N. (2022) *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022*. London: Royal United Services Institute (Special Report, 30 de novembro). Disponível em: https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf [Consultado a 11 de agosto de 2025].