idn brief

Março de 2026

Tecnologias Emergentes e Defesa

DIRETORA
Isabel Ferreira Nunes
COORDENADOR EDITORIAL
Luís Cunha
CENTRO EDITORIAL
Filipa Teles
DESIGN EDITORIAL
Núcleo de Desenho do IDN - Paulo Jorge Pereira
PROPRIEDADE, DESIGN GRÁFICO E EDIÇÃO
Instituto da Defesa Nacional

ISSN 2182-5327
Depósito Legal 340906/12

Tecnologias Emergentes e Defesa

Dual-Use e Tecnologias de Informação e Comunicação: um Contributo para a Sua Compreensão

Coronel João Assis Barbas
Chefe de Equipa Multidisciplinar do Centro de Estudos e Investigação do IDN
Diretor do Curso de Defesa Nacional

O termo *dual-use* surgiu no contexto da Guerra Fria para descrever tecnologias desenvolvidas com finalidade militar, mas que possuíam também relevante aplicação civil.

A consolidação jurídica deste conceito ocorreu inicialmente a partir das convenções internacionais de controlo de armamento e dos regimes de exportação associados, como o Acordo de Wassenaar de 1995, visando impedir que tecnologias civis avançadas fossem desviadas para fins militares, especialmente por regimes ou grupos considerados desestabilizadores ou terroristas.

No ordenamento jurídico português ele surge inicialmente no DL n.º 130/2015, de 9 de julho, relativamente ao regime de controlo das exportações, transferências, corretagem, trânsito e assistência técnica de produtos de dupla utilização, que adotou as medidas necessárias à aplicação do Regulamento (CE) n.º 428/2009, do Conselho Europeu.

O DL n.º 130/2015 define produtos de dupla utilização como "quaisquer produtos, incluindo suportes lógicos e tecnologia, que possam ser utilizados tanto para fins civis como para fins militares e que, se utilizados para fins não pacíficos, designadamente na produção de armamento convencional e de armas de destruição maciça, podem pôr em risco a estabilidade, a segurança e a paz mundiais."

A história oferece inúmeros exemplos de tecnologias *dual-use*, de apropriação pela sociedade civil de invenções ou inovações do domínio militar, mas igualmente em sentido inverso.

• A utilização em armamento militar da dinamite inventada por Alfred Nobel para utilização na mineração e construção civil.

• O aço e alumínio de alta resistência, inicialmente desenvolvidos para a indústria ferroviária e naval, tornaram-se vitais na construção de armamento e veículos militares.

• O motor de combustão interna inventado em meados do Séc. XIX utilizado na indústria e em automóveis foi posteriormente adotado em plataformas militares (ex.: carros de combate, aviões, navios).

• O avião, nascido como uma curiosidade dos irmãos Wright no princípio do Séc. XX, foi posteriormente adotado e transformado durante a Primeira Guerra Mundial como uma plataforma de vigilância e combate, dando uma terceira dimensão à guerra.

Em sentido inverso, existem também muitas apropriações pela sociedade civil de inovações militares.

• Os primitivos transmissores de rádio usados para comunicações de mensagens de texto diplomáticas e militares passaram, em meados do Séc. XX, a ser extensivamente utilizados na sociedade.

• O radar, desenvolvido para detetar a aproximação de aviões inimigos durante a Segunda Guerra Mundial foi posteriormente aplicado na aviação, navegação e meteorologia.

• Os equipamentos criados para apoiar a descodificação de mensagens cifradas durante a Segunda Guerra Mundial ou Sistemas de Direção de Tiro (defesa aérea e costeira) anteciparam o desenvolvimento do "computador".

• Os modelos matemáticos e estatísticos (ex.: filas de espera, simulação, etc.) utilizados durante a Segunda Guerra Mundial para resolver problemas complexos e otimizar recursos foram adotados pela indústria, impulsionados pela computação e o crescimento económico, dando origem à investigação operacional.

Potenciar tecnologias militares em produtos de utilização civil ou vice-versa implica a adoção de políticas alicerçadas em estratégias sustentáveis,

públicas e privadas. Do outro lado do Atlântico, após a Segunda Guerra Mundial, os EUA adotaram uma estratégia industrial *dual-use* que alavancou a inovação do setor privado, para atender às necessidades da Defesa, ligando investigação de ponta, universidades, centros de inovação e o Departamento de Defesa.

O modelo privilegiou investimento público massivo, transferência tecnológica e uma cultura empresarial orientada para a inovação disruptiva. O Estado atua como um cliente-âncora, definindo necessidades estratégicas e requisitos, fornecendo financiamento, e adquirindo produtos para incorporação nas capacidades militares de defesa. Esses produtos, podem ser concebidos especificamente para as Forças Armadas ou adaptados a estas.

Em sentido oposto, a transferência de tecnologias de defesa para produtos comerciais ocorre principalmente através de contratos de licenciamento e de transferência de *know-how*, com mecanismos como o *Defense Advanced Research Projects Agency* (DARPA) a promover a transição de tecnologias do setor público para o privado.

O processo envolve contratos de licenciamento para utilização e cedência para transferência de propriedade do conhecimento. Estas tecnologias podem então ser convertidas em produtos comerciais, impulsionando a inovação e o crescimento económico, reduzindo a necessidade, nomeadamente, de investimento em I&D.

O objetivo é criar um ciclo de *feedback* onde os avanços comerciais possam ser adaptados para aplicações militares ou as tecnologias militares incorporadas em produtos comerciais de consumo civil. Em qualquer dos casos, o setor privado impulsiona o ritmo da evolução tecnológica do país, desenvolvendo produtos inovadores ajustados à procura da Defesa e partilhando o risco, fortalecendo a segurança nacional e, ao mesmo tempo, apoiando o crescimento económico.

A Europa segue um modelo mais regulatório e cooperativo, articulado entre Estados-membros, indústria e programas europeus como o *Horizon Europe* ou o Fundo Europeu de Defesa.

Esta abordagem procura reduzir fragmentação, apoiar Pequenas e Médias Empresas (PME) e promover autonomia estratégica, incentivando tecnologias com impacto simultâneo civil e militar. Na UE, o *dual-use* é essencial para fortalecer a Base Tecnológica e Industrial de Defesa da UE (EDTIB), permitindo: acelerar inovação através de tecnologias civis emergentes; reduzir custos e dependências externas; fomentar interoperabilidade entre Estados-membros; encurtar ciclos de desenvolvimento de capacidades.

A Comissão Europeia tem reforçado políticas de convergência entre prioridades civis e de defesa, particularmente em áreas como cibersegurança, semicondutores, inteligência artificial, espaço, comunicações seguras e computação avançada. Nesta abordagem, não é despiciendo as origens e foco essencialmente político e económico da UE, assim como os condicionamentos que os Estados-membros colocaram na política europeia de Defesa, que agora procuram fazer evoluir.

As TIC são eminentemente duais. Elas envolvem múltiplos elementos e são hoje o núcleo de diversas capacidades militares, nomeadamente, nos seguintes domínios: Comando e controlo (C2); Inteligência, vigilância e reconhecimento (ISR); Ciberdefesa; Mobilidade e Logística; Simulação e treino; Processamento de dados e IA; e Gestão de sistemas complexos.

As TIC contribuem decisivamente para:

• Tomada de decisão rápida e informada, através da recolha e compilação rápida de dados, análise de dados / intelligence, partilha de informação *real time* ou *near-real time* aos diversos níveis de comando, em diversos formatos, com eventual filtragem, se e quando necessário;

• Comando, Controlo e Coordenação de Forças, através de sistemas de comunicação entre unidades terrestres, aéreas, navais e cibernéticas, etc., com recurso a redes seguras, sensores, sistemas de comando e controlo (C2), sistemas geo-intel, sistemas de messaging, etc.;

• Ciberdefesa e proteção de infraestruturas críticas, através da deteção avançada de ameaças, análise forense, mitigação de ataques, recuperação de sistemas, condução de operações ISR, suporte de operações defensivas e ofensivas;

• Superioridade informacional, através de meios de vigilância e reconhecimento, utilização de drones e satélites, fusão de dados provenientes de múltiplas fontes, etc.;

• Eficiência Logística visando garantir a operacionalidade das forças, na gestão de aprovisionamento (ex.: munições, alimentos, sobressalentes, etc.), transportes, etc.;

• Formação, simulação e treino, através da utilização de simuladores, realidade virtual, sistemas de modelação e análise;

• Interoperabilidade entre forças Conjuntas e Combinadas, através da conjugação de sistemas de C2, simuladores, realidade aumentada, etc.;

O *dual-use* constitui hoje um pilar fundamental da inovação tecnológica, do desenvolvimento de capacidades de defesa modernas e da autonomia estratégica europeia. As TIC *dual-use* são um elemento essencial dessa transformação, permitindo que Estados, indústria e sociedade desenvolvam soluções partilhadas, resilientes e sustentáveis financeiramente num contexto global de risco permanente.

Tecnologias emergentes para o treino das Forças Armadas

Luís Carlos Teixeira
Business Development & Marketing Manager na ETI

Ao longo dos últimos anos, temos assistido a uma mudança do paradigma da guerra, com a introdução massiva de veículos não tripulados em cenários de combate. Estas plataformas começaram por ser comandadas remotamente, o que implicava a necessidade de afetação de recursos humanos na sua operação, sendo, portanto, a sua utilização limitada pelo número de militares com treino para as operar. Todavia, com o desenvolvimento tecnológico no campo dos sensores e no campo da inteligência artificial, os veículos não tripulados vão ganhando um grau de autonomia que possibilita a sua utilização sem a necessidade de operadores em permanência.

Se considerarmos a *framework* GALA (*General Automation Level Allocation*), as plataformas não tripuladas passam do nível 1 (os operadores têm pouco suporte da automação) para os níveis 3 (sistema supervisionado pelo operador) a 5 (sistema completamente autónomo), dependendo do tipo de ação em causa, sendo que, por questões éticas, um ataque necessitará sempre de comando humano. Assim, tendencialmente, os militares vão tornar-se operadores da plataforma, decidindo os aspetos relevantes de cada missão (ex.: realizar uma missão de patrulha ou um ataque; quando atacar um alvo; quando divergir para outra missão, etc.), mas não os procedimentos operacionais (velocidade de rotação da descolagem, aproximação para aterrar, manobra evasiva contra uma ameaça). Neste cenário, o número de entidades combatentes será muito maior, tornando o ambiente de combate muito mais complexo do que no passado. Acresce a esta mudança de paradigma o fator velocidade, já que estas novas plataformas se deslocam muito mais rapidamente do que no padrão da guerra clássica. Desta forma, as decisões têm de ser tomadas de forma muito mais rápida, não podendo esperar pela tradicional cadeia de comando, o que conduzirá a uma muito maior delegação na tomada de decisão.

Em paralelo, a evolução tecnológica tem transformado também as plataformas tripuladas, estando estas a ficar com um nível de automação cada vez maior. Tendencialmente, a execução de procedimentos standard vai deixar de necessitar de intervenção humana, pelo que o operador será confrontado com decisões tomadas pelo assistente virtual da plataforma, decisões essas que terá de compreender em tempo útil.

Perante estes dois novos paradigmas, torna-se evidente que o treino operacional das Forças Armadas tem de ser ajustado a este novo cenário. O treino deixa de se concentrar principalmente em operar uma plataforma seguindo procedimentos operacionais e passa a priorizar a compreensão do cenário de guerra e a capacidade de interagir com uma grande variedade de entidades. Esta realidade aplica-se mesmo aos militares de níveis hierárquicos mais baixos. A mudança no treino implica o aparecimento de novas tecnologias, complementares aos sistemas atuais.

Comecemos pelos algoritmos de inteligência artificial (IA), a usar em ambiente de treino, com dois propósitos.

Em primeiro lugar, para suporte aos instrutores nas várias vertentes. Para o desenvolvimento de um treino efetivo, mesmo em ambiente de treino individual, o cenário a criar deverá ser muito mais complexo quando comparado com o atual padrão. E para além de as forças controladas por computador requererem algoritmos de IA para assegurar um comportamento realista, será necessária a criação de um assistente virtual para que o instrutor consiga preparar cenários de treino e para o auxiliar no decurso do exercício.

É importante salientar que, em termos de entidades envolvidas num exercício, poderemos estar na escala dos muitos milhares. Como o treino focar-se-á nas decisões tomadas, a avaliação dos participantes será mais complexa, registando-se já a utilização de algoritmos de IA no âmbito da análise dos exercícios não só no que toca às decisões tomadas, mas também a parâmetros fisiológicos dos participantes (ex.: o nível de stresse atingido).

Um segundo propósito para o uso de IA no treino, prende-se com a necessidade de os operadores confiarem na IA. A capacidade da IA está em fase de crescimento acelerado, pelo que o nível de sofisticação dos assistentes virtuais vai atingir um nível que fará com que o operador não consiga entender imediatamente o que está em causa, atrasando ou mesmo impedindo a tomada de decisão. O treino afigura-se, pois, essencial e urgente para a aquisição desta confiança e competência.

Estes módulos de IA têm de ser, necessariamente, idênticos aos da plataforma real, o que nos leva a uma nova tecnologia emergente para o treino: os gémeos digitais. Com os gémeos digitais atinge-se um nível mais detalhado do que com os simuladores clássicos. É usado o mesmo software instalado na plataforma e os modelos físicos são mais detalhados, já que incluem os dados dos múltiplos sensores que se encontram na plataforma. Desta forma, o treino pode, inclusive, considerar fenómenos como um desgaste realista do equipamento. Ainda neste âmbito, o aumento da capacidade da computação gráfica associada às imagens por satélite e à inteligência artificial trouxe uma nova tecnologia que pode ser vista como os "gémeos digitais do terreno", com a capacidade de treinar num cenário virtual constituído como uma réplica idêntica ao cenário real. Por exemplo, antes de uma força se deslocar para uma missão no exterior, esta pode ambientar-se às ruas e à paisagem, de modo que, quando chegar efetivamente ao local da missão, já esteja devidamente familiarizada com o terreno. Pode inclusive treinar com base nas condições climatéricas que irá encontrar.

Este treino deve ser feito da forma mais imersiva possível e, para se conseguir essa imersividade, estão a despontar os óculos de realidade estendida, a saber: realidade virtual; realidade mista; e realidade aumentada. Estas tecnologias possibilitam o treino em ambientes completamente imersivos e, no caso da realidade aumentada, mesmo em ambiente operacional. Neste momento, assistimos ainda ao emergir acelerado de soluções de realidade mista, um ambiente sintético que junta a visão de elementos reais e de realidade aumentada, e onde, num cenário real, podem ser introduzidas entidades não reais com as quais se pode interagir.

Este conjunto de tecnologias, muitas delas com origem na indústria dos jogos, a médio prazo poderá conduzir à criação de um metaverso militar para treino, operando numa nuvem própria e consistindo numa rede de mundos digitais persistentes nos quais as forças podem realizar o seu treino, planear e experimentar nova doutrina.

Em jeito de conclusão, estas novas tecnologias emergentes irão potenciar o treino na sua vertente mais relevante: a compreensão dos cenários, cada vez mais complexos, da guerra moderna.

Transformação digital e resiliência: Desafios para a Segurança e Defesa

Prof. Doutor Gil M. Gonçalves
e Prof. Doutor Pedro C. Diniz
Departamento de Engenharia Informática (DEI)
Faculdade de Engenharia da Universidade do Porto (FEUP)

A transformação digital assume-se cada vez mais como um fenómeno estrutural e transversal, com impacto profundo na forma como os processos são concebidos, operados e governados em todos os setores, desde a agricultura à indústria, passando pelos serviços. A sua natureza pervasiva e ubíqua influencia hoje, de forma decisiva, a competitividade económica, a eficiência organizacional e a resiliência dos sistemas técnicos e sociais. A sua transversalidade e ubiquidade levou mesmo a uma inversão do fluxo de inovação da indústria para a academia, no que se tem designado por *spin-in*.

No contexto europeu, esta dinâmica assume relevância nos domínios da segurança e da defesa, nos quais a transformação digital é simultaneamente um fator crítico de vantagem estratégica e uma fonte de novos riscos sistémicos. Um aspeto singular desta transformação digital reside no facto de que se trata de uma tecnologia multifuncional (dual/triple use), na qual as mesmas técnicas fundamentam uma crescente competitividade industrial, aspeto crucial no âmbito da segurança pública, tornando-se cada vez mais relevante quer no contexto da indústria, quer no setor

da defesa. Tecnologias de encriptação amplamente utilizadas em e-commerce são hoje essenciais para comunicações seguras em contextos sensíveis. Métodos de processamento de imagem e inteligência artificial desenvolvidos para despistagem das mais variadas patologias médicas ou para aplicações industriais são facilmente adaptáveis à deteção, identificação e monitorização de ativos em teatros de operações.

Esta convergência tecnológica confere à transformação digital um caráter estratégico singular, plenamente alinhado com as prioridades europeias de autonomia estratégica aberta e de soberania tecnológica.

Como outras tecnologias emergentes e potencialmente disruptivas, a transformação digital levanta desafios a três níveis. Primeiro, o problema de inserção da tecnologia, que tipicamente inclui aspetos de escala, interoperabilidades com sistemas existentes (*legacy systems*), bem como novos aspetos de *governance* de dados, além dos requisitos éticos, de confiança e de certificação. Segundo, os aspetos ligados às organizações, como a resiliência das cadeias de fornecimento e os processos de aquisição, validação e adoção tecnológica, que são tradicionalmente longos e rígidos neste domínio. Por fim, mas não menos importante, o aspeto humano, segundo o qual o surgimento de uma nova tecnologia cria tensões na formação adequada de recursos humanos em termos de competências, originando o *skill gap*.

É precisamente neste enquadramento que os instrumentos europeus assumem um papel estruturante. O Horizonte Europa promove o desenvolvimento científico e tecnológico de base, incluindo tecnologias digitais avançadas, inteligência artificial, cibersegurança e sistemas ciber-físicos, com uma forte ênfase em aplicações de uso duplo e na transição dos resultados de investigação para a inovação. O *European Defence Fund* (EDF), por sua vez, constitui o principal instrumento para apoiar a investigação colaborativa e o desenvolvimento de capacidades de defesa, promovendo a consolidação da base tecnológica e industrial de defesa europeia. Complementarmente, a *European Defence Agency* (EDA) desempenha um papel central na coordenação de prioridades de capacidades, harmonização de requisitos e promoção de sinergias entre Estados-membros, indústria e academia.

No panorama europeu e, em particular, no contexto nacional, esta transformação apresenta, além dos desafios, uma enorme janela de oportunidade. O ecossistema universitário, com os seus centros e institutos de investigação associados, é vibrante e de reconhecida qualidade internacional. Paralelamente, estão já estabelecidos polos de inovação digital (*Digital Innovation Hubs* - DIH), como é o *Connect5*, bem como infraestruturas de experimentação e teste (Testing and *Experimentation Facilities* - TEF), orientados para apoiar o setor privado, nomeadamente as pequenas e médias empresas (PME), e entidades públicas na adoção de tecnologias digitais avançadas. Embora estes instrumentos estejam maioritariamente focados em aplicações civis e industriais, existe um claro potencial – ainda subexplorado – para a sua articulação sistemática com os domínios da segurança e da defesa, em linha com os objetivos do Fundo Europeu de Defesa (*European Defence Fund* - EDF) e da Agência Europeia de Defesa (*European Defence Agency* - EDA).

No cenário de segurança e defesa, o panorama da integração matura de tecnologias digitais mantém-se aquém do que seria desejável, como abundantemente evidenciado e mesmo exacerbado pelas necessidades e realidade do contexto geopolítico atual.

Urge assim, a nosso ver, uma aposta concertada que permita alinhar de forma mais eficaz os instrumentos europeus existentes com as necessidades concretas da segurança e da defesa. Tal aposta deverá estruturar-se em torno de três pilares fundamentais: a) integração de programas de investigação e desenvolvimento de tecnologias de uso duplo/triplo; b) partilha de conhecimento e treino avançado de recursos humanos para acelerar a adoção de tecnologias digitais; e c) estabelecimento de mecanismos de coordenação para o desenvolvimento de produtos e sistemas multiuso, interoperáveis e certificados, focados prioritariamente em segurança e defesa.

Em síntese, na Europa, a resiliência em segurança e defesa exige uma abordagem integrada, multiator e centrada no fator humano. Só através, por um lado, da articulação coerente entre investigação, inovação, desenvolvimento de capacidades e formação e, por outro, da cooperação efetiva entre academia, indústria, Estados-membros e instituições europeias será possível converter o potencial da transformação digital num verdadeiro ativo ao serviço da segurança, da defesa e da autonomia estratégica europeia.

Transformação Digital na Defesa: da Tecnologia à Capacidade Operacional

Dário Pedro
CEO Beyond Vision | PhD in AI for UAV

A transformação digital no setor da defesa tem sido amplamente discutida ao longo da última década, mas continua, em muitos casos, por se concretizar de forma efetiva no terreno. O desafio deixou de ser tecnológico. Hoje, a questão central é operacional: como transformar tecnologias emergentes em capacidades reais, fiáveis e integradas nas missões.

A experiência da *Beyond Vision*, desenvolvendo e operando sistemas não tripulados em contextos civis e militares, demonstra que a diferença entre inovação e impacto está na capacidade de integrar tecnologia em cenários reais, muitas vezes adversos e imprevisíveis. A digitalização na defesa não pode ser entendida como a adoção isolada de ferramentas. Tem de ser vista como a integração global de sistemas completos, nos quais plataformas, sensores, comunicações e software trabalham de forma coordenada.

Um dos principais vetores desta transformação é a crescente utilização de sistemas autónomos, em particular UAV (*Unmanned Aerial Vehicle* – veículo aéreo não tripulado), como o BVQ418 e o BVT516. Estes sistemas evoluíram rapidamente de plataformas experimentais para ativos operacionais, utilizados em missões de vigilância, reconhecimento, proteção de infraestruturas críticas e apoio à decisão. No entanto, a maturidade tecnológica de um drone não se mede apenas pela sua performance em condições ideais, mas sim pela sua capacidade de operar de forma consistente em ambientes degradados, nomeadamente em cenários com interferência eletromagnética, negação de GNSS ou condições meteorológicas adversas.

Neste contexto, a resiliência tornou-se um requisito central. A capacidade de operar em ambientes contestados implica o desenvolvimento de sistemas redundantes, fusão de sensores e algoritmos avançados de navegação e perceção. Tecnologias como odometria visual, navegação inercial assistida por inteligência artificial e sistemas antijamming deixam de ser diferenciais e passam a ser requisitos-base para qualquer solução credível no domínio da defesa.

Outro ponto crítico é a transformação de dados em informação acionável. A proliferação de sensores gerou uma quantidade massiva de dados, mas a sua utilidade depende da capacidade de os processar, correlacionar e apresentar de forma clara aos decisores. Plataformas digitais como a plataforma *beXStream* C4ISR assumem aqui um papel determinante, permitindo integrar múltiplas fontes de informação e gerar uma visão operacional comum em tempo real.

A inteligência artificial surge como um elemento estruturante desta transformação. No entanto, importa desmistificar a sua aplicação. O valor da IA na defesa não está em soluções genéricas, mas sim na sua integração em *pipelines* operacionais específicos, onde contribui para tarefas concretas como deteção automática de ameaças, classificação de objetos, otimização de rotas ou apoio à tomada de decisão. A eficácia destes sistemas depende da qualidade dos dados, da robustez dos modelos e, sobretudo, da sua validação em ambiente real.

A interoperabilidade é igualmente um desafio relevante. As Forças Armadas e entidades de segurança operam com sistemas heterogéneos, muitas vezes adquiridos em momentos distintos e sem uma arquitetura comum. A transformação digital exige a adoção de *standards* e a criação de interfaces que permitam a integração progressiva de novas capacidades, evitando a criação de silos tecnológicos.

Do ponto de vista industrial, a Europa enfrenta um momento decisivo. A necessidade de reforçar a autonomia estratégica implica não só investir em tecnologia, mas também garantir capacidade de produção, integração e operação dentro do espaço europeu. Empresas como a *Beyond Vision* demonstram que é possível desenvolver soluções competitivas a nível global, combinando inovação com capacidade de execução.

Importa também reconhecer o papel do duplo uso. Muitas das tecnologias que hoje são críticas na defesa têm origem em aplicações civis, desde a inteligência artificial até aos sistemas de comunicações. Esta convergência cria oportunidades, mas também exige uma abordagem equilibrada, que permita acelerar a inovação, mantendo os níveis de segurança e controlo exigidos.

Por fim, a transformação digital na defesa é, acima de tudo, uma transformação organizacional. A adoção de novas tecnologias implica mudança de processos, formação de recursos humanos e, sobretudo, uma cultura orientada para a experimentação e a adaptação

contínuas. Programas de testes operacionais, como exercícios conjuntos e ambientes de experimentação, são essenciais para validar soluções e reduzir o tempo entre o desenvolvimento e a utilização no terreno.

Em conclusão, a transformação digital na defesa não se fará apenas com investimento em tecnologia, mas com a capacidade de transformar essa tecnologia em soluções operacionais, robustas e integradas. O futuro passará por sistemas cada vez mais autónomos, conectados e inteligentes; mas o verdadeiro fator diferenciador continuará a ser a capacidade de os colocar ao serviço das missões, de forma eficaz e fiável.

Para tal, será igualmente essencial uma maior proximidade entre a defesa e a indústria. Só com mecanismos que permitam uma adoção mais rápida de novas tecnologias será possível acompanhar o ritmo de inovação atual. Em paralelo, a criação de modelos de contratação mais previsíveis e sustentáveis permitirá às empresas investir de forma contínua em capacidades críticas, incentivando um foco estratégico no setor da defesa.

Este alinhamento deve ser acompanhado por ciclos de feedback mais frequentes entre os utilizadores operacionais e a indústria, garantindo que o desenvolvimento tecnológico responde a necessidades reais e evolui de forma iterativa.

A capacidade de adaptação rápida será, cada vez mais, um fator decisivo. A experiência demonstra que não é a tecnologia mais avançada que faz a diferença, mas sim aquela que funciona quando é realmente necessária.

idn Instituto da Defesa Nacional

Calçada das Necessidades, 5, 1399-017
Lisboa
Tel +351 211 544 700
idn.publicacoes@defesa.pt