

A Relevância da Inteligência Artificial nas Operações Militares Terrestres

Os grandes avanços tecnológicos têm produzido, ao longo da História, autênticas Revoluções dos Assuntos Militares, as quais, normalmente, afetam “grupos” de mudanças tecnológicas, táticas, doutrinárias e organizacionais.



Imagem gerada por Inteligência Artificial, (ChatGPT)

Com os avanços na inteligência artificial (IA) predominantes nas notícias por todo o lado, militares, académicos e decisores políticos interrogam-se sobre qual o papel que estes avanços tecnológicos desempenharão na guerra. Cada vez mais, a tomada de decisões é automatizada e o envolvimento humano é reduzido, à medida que os sistemas autónomos têm mais controlo sobre os sistemas, especialmente em veículos.

As tecnologias de dupla utilização estão a tornar-se cada vez mais significativas à medida que as ferramentas de IA evoluem, apresentando oportunidades em que utilizações civis informam operações militares e vice-versa,

apresentando, porém, ambos riscos emergentes, pelo que constituem uma espada de dois gumes. De facto, se por um lado se reconhece que a IA pode desempenhar um papel de multiplicador crítico no combate, libertando trabalho humano e agilizando e otimizando tarefas, por outro, surge alguma preocupação quanto à utilização da IA em sistemas de armas totalmente autónomos e letais.

Os grandes avanços tecnológicos têm produzido, ao longo da História, autênticas Revoluções dos Assuntos Militares (RAMs), as quais normalmente afetam “grupos” de mudanças tecnológicas, táticas, doutrinárias e organizacionais, que se confinam à esfera militar. As aplicações de

emprego dual da IA disponibilizam ferramentas para a análise rápida de grandes quantidades de dados, a melhoria da conexão entre sensores e atiradores e o aumento da velocidade de tomada de decisão.

Porém desta vez, com a crescente influência do domínio do ciberespaço e a vulgarização da IA, Defesa e Forças Armadas (FAs) enfrentam verdadeiras EDTs (*Emerging and Disrupting Technologies*), pelo que o caso será diferente e bem mais sério e delicado para esta nova RAM. De facto, com as “ofertas” facilitadas pela IA, são afetados não só no ambiente operacional multidomínio (MDO), mas também a confrontação com a “inteligência” humana, o que configura um desafio ao mesmo tempo ambicioso, mas também complexo e preocupante.

Entretanto, tal como em outros momentos históricos pós-RAMs antecedentes, é de todo conveniente, por maioria de razão neste caso, não “embandeirar em arco” e prosseguir pela via mais fácil em sobrestimar-se o poder da IA, acreditando em algo semelhante à “mágica”, como solução para as operações militares, com elevados níveis de infalibilidade. Haverá sim que refletir e retirar conclusões fundamentadas das lições aprendidas, entre as quais ter bem presente que em operações militares, e sobretudo nas de componente terrestre, “o homem” estará sempre no centro das decisões.

Nesta perspectiva é importante ver como está a evoluir tal desafio ao nível da NATO, União Europeia e em Portugal

Introdução

Em todos os grandes conflitos da História, tem ocorrido sempre uma relação direta com a tecnologia da época em que ocorrem. Não recuando muito mais do que a guerra civil americana, verifica-se que houve sempre um elemento que despoletou o início da guerra: Normalmente ocorreram relatos dos primeiros tiros, daquilo que aconteceu e, quase sempre, as pessoas assistiram ou ouviram, neste caso tendo em conta, evidentemente, os meios de comuni-

cação da época. Mas o relato existe, e foi registado. A mesma coisa, depois, no início da Primeira Guerra: sabe-se o que aconteceu em Sarajevo. E o mesmo também na Segunda Guerra, com aquela simulação/farsa feita pelos Alemães com os uniformes do exército polaco.

Chegados às guerras existentes nos dias de hoje, o que acontece é que os tais primeiros tiros não foram dados no início da guerra Rússia-Ucrânia, em 24 de fevereiro de 2022. Efetivamente, os ‘primeiros tiros’ foram dados muito antes e não foram tiros cinéticos, foram tiros *ciber*. Isto altera completamente a forma de se analisar o que é a tecnologia e a sua influência nas operações militares em concreto, o que nos remete para uma nova RAM, de características totalmente inovadoras, muito desafiantes e mesmo disruptivas.

A Inteligência Artificial, embora seja um termo utilizado desde a década de 1950, ainda não tem uma definição geralmente aceite unanimemente, como se verá. Genericamente tal como apresentada na figura 1, pode descrever-se através de uma família de tecnologias de utilização geral, que podem permitir que as má-

quinas executem tarefas que normalmente requerem inteligência humana. Convém, no entanto, distinguir a IA em duas categorias principais: a Inteligência Artificial Restrita (IAR) e a Inteligência Artificial Generativa (IAG) ou Inteligência Artificial da 1.^a e 2.^a Vagas, respetivamente.

A IAR surgiu nos anos 80 do Séc. XX, é representada por conhecimentos especializados ou critérios desenvolvidos com base em regras ou noutras fontes autorizadas e codificadas num algoritmo informático, denominado sistema pericial (*expert system*). Definem-se regras para as máquinas inteligentes e estas seguem as regras. No essencial, são máquinas que seguem regras definidas por um ser humano.

A propósito dos sistemas periciais, aproveita-se para recordar um evento relevante, ocorrido exatamente em Portugal e no Exército. Efetivamente, o camarada Major-General Pedro Melo (na altura Tenente-Aluno da AM) ganhou o 1.^o prémio ibérico em 1988 (IBERAMIA 88), com um sistema pericial desenvolvido para um “processo de soldadura robotizada”. Recordar aqui esse acontecimento é importante, não só porque



Família de tecnologias da Inteligência Artificial (figura 1)



Imagem gerada por Inteligência Artificial, (ChatGPT)

revela a permanente preocupação da Arma de Transmissões e do Exército na aposta da mais-valia da formação avançada dos seus oficiais, mas também porque viria a contribuir como um decisivo pontapé de saída para a criação de um Grupo de Projeto de I&D, o qual tive a honra em liderar durante vários anos. Viria a ser no âmbito desse Grupo que se desenvolveram e implementaram projetos com bastante impacto no Exército, Forças Armadas e NATO, nas áreas da Simulação e Jogos de Guerra (VIGRESTE), Sistemas de Informação de Comando e Controlo (SICCE e SIC Tático) e Guerra Eletrónica.

Os sistemas periciais, embora se destacassem nas aplicações personalizadas, eram incapazes de lidar com a resolução de problemas além do seu conhecimento pré-programado. Surge assim a 2.ª vaga da IA, na década de 1990, com a criação da “aprendizagem da máquina/ *machine learning* (ML)”, um subconjunto da IA que, ao contrário dos sistemas periciais, precisam de ser programados manualmente, onde os algoritmos de ML usam dados de treino para “aprender” a executar tarefas e resolver problemas.

Mais tarde, progrediram os avan-

ços, com o desenvolvimento de algoritmos de “aprendizagem profunda/ *deep learning* (DL)”, que usam redes neurais vagamente modeladas nas do cérebro humano. A combinação de DL com gigantescos conjuntos de dados tornou possível a “visão computacional”, que é a base para diversas aplicações, de veículos autónomos a programas de reconhecimento de imagem e facial.

É deste modo que a evolução para a IAG procura compreender e aprender, em diferentes ambientes de informação, semelhante à forma como os humanos a processam, isto é, a IAG tenta pensar e exibir aspetos da *consciência*, da *razão* e do *pensamento humano*.

Mais recentemente, em novembro de 2022, a OpenAI lançou o ChatGPT, o seu programa de grande modelo de linguagem (*large language model* - LLM). Com esta IAG, começa a surgir o chamado fenómeno da Caixa Preta, em que o ser humano pode já não conseguir acompanhar o processo que ocorre nos níveis neuronais individuais, e isso representa efetivamente um significativo risco de fiabilidade. Surgem assim sensações díspares, entre aqueles que num extremo do espectro, reivindicam

(com vários graus de entusiasmo ou pavor) a chegada iminente da singularidade, o momento em que os computadores se tornam auto-conscientes; no outro extremo, estão académicos e profissionais como o Dr. Eric Siegel, que chama à IA uma mentira, uma farsa ou, na melhor das hipóteses, uma palavra da moda confusa. Até outros, como o reconhecido empresário tecnológico Elon Musk, alertam que o desenvolvimento contínuo da IA poderá fazer com que as máquinas “sejam os nossos senhores”.

De qualquer modo, devemos parar de pensar na IA tal como é descrita na ficção científica - uma espécie de deus na máquina - e reconhecer que ela é aplicável principalmente às duas camadas inferiores da pirâmide da hierarquia cognitiva - dos *dados*, à *informação*, ao *conhecimento* e à *sabedoria*.

Significa isto que se deve utilizar a IA, aproveitando a velocidade computacional da máquina, para libertar os humanos do trabalho penoso, em vez de a utilizar no *juízo* e *sabedoria* superior do ser humano, para criar significado a partir da informação, fazer julgamentos de valor, determinar modalidades de ação e sobretudo decidir ... Ou utilizar a IA para realizar o tipo de trabalho de conhecimento para o qual os conjuntos de dados se tornaram demasiado grandes para serem compreendidos pelos humanos?

De todo o modo, 2022 foi o prenúncio da chamada democratização da IAG, capaz de produzir não só imagens, mas também escritos e vídeos através de comandos ou pedidos, alcançando o público em geral e impulsionando o desenvolvimento de diversas ferramentas nesse campo.

Ver-se-á de seguida, porém, e como alerta, para não se cair na tentação fácil de sobrestimar o poder da tecnologia da IA, uma reflexão sobre as lições aprendidas da última RAM, ocorrida nos EUA em finais dos anos 90 que, face às características inovadoras na tecnologia da época, perspetivava também alguma capacidade disruptiva, no sentido mesmo de uma nova forma de Guerra.

A tecnologia e as Revoluções

de Assuntos Militares (RAMs) NCW (*Network Centric Warfare*) e Lições Aprendidas

Os EUA, animados com a demonstração do seu domínio e facilidade da rápida vitória militar, sobre as forças iraquianas de Saddam Hussein, na Guerra do Golfo de 1991, e conscientes da rápida evolução das TIC e do seu efeito numa verdadeira RAM no campo operacional, pensavam que lhe garantiria a total supremacia no armamento de precisão de fogos e, com tais vantagens competitivas, que não haveria nenhum oponente ao nível das forças militares, pelo menos até 2020.

Os autoproclamados visionários dessa “transformação” na guerra – muitos deles trabalhavam no designado *Gabinete de Transformação da Força* – falavam de uma RAM guiada, alavancada por conceitos como Guerra Centrada em Rede (o célebre “acrónimo” NCW, *Network Centric Warfare*) e Operações Baseadas em Efeitos (EBO) que, afirmavam, alterariam o carácter fundamental da guerra, nomeadamente a incerteza e o nevoeiro da guerra (figura 2). Nos corredores do Pentágono afirmava-se que “NCW melhorará o potencial de combate, através de sensores em rede, tomada de decisão e combatentes, para alcançar conscientização da situação operacional partilhada, velocidade das ações de comando e ritmo de combate aumentadas, maior letalidade, melhor capacidade de

sobrevivência e um elevado grau de auto-sincronização...”.

Ao mesmo tempo, para dar corpo a esse alucinante conceito da guerra, a organização das unidades operacionais seria muito mais pequena, mais ligeira, logo com blindagem das viaturas diminuída em cerca de 1/3, para projetar muitas ao mesmo tempo e de forma muito mais rápida. Deste modo a força poderia “*ver primeiro, decidir primeiro, agir primeiro e terminar de forma decisiva*” – era a “*doutrina dos primeiros*”, baseada na suposição de que o conhecimento dominante em guerras futuras permaneceria praticamente incontestado.

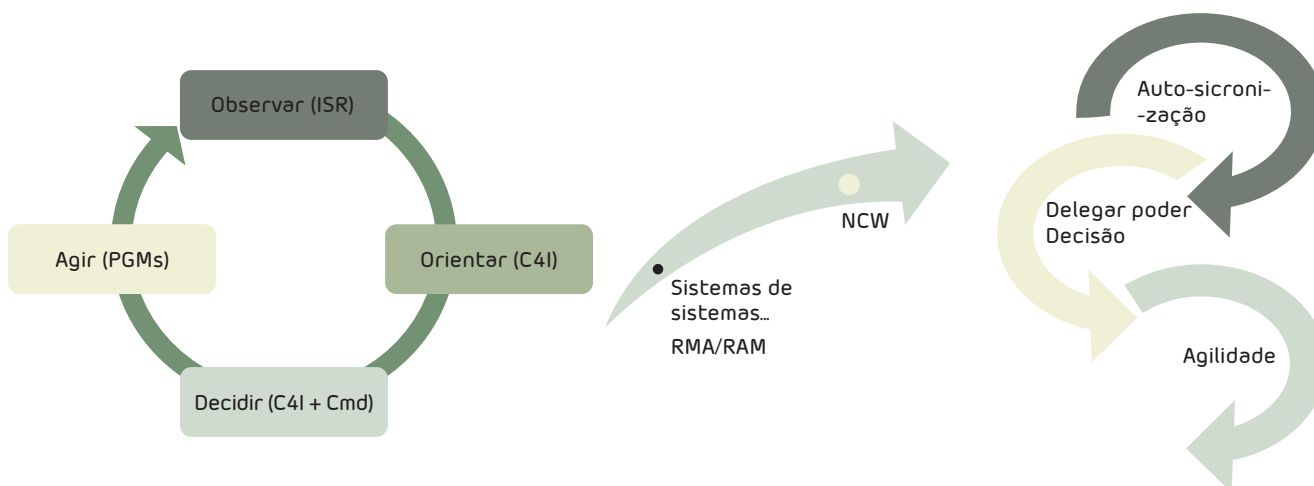
Numa primeira fase, parecia que toda a gente acreditava em tal ‘RAM prodigiosa’. Conhecem-se as frases vigorosas e assertivas do então Secretário de Estado da Defesa Donald Rumsfeld, como *choque e pavor e vitórias relâmpago*, sem danos colaterais nem baixas (ZERO baixas...). Porém, cedo se aperceberam, principalmente os militares, do fiasco enorme desta filosofia – bastará recordar, p. ex., as imagens de militares norte americanos, a “desenrascar” o reforço da blindagem das viaturas Humvees – as conhecidas HMMWV (*High Mobility Multipurpose Wheeled Vehicle*) – em pleno TO do Afeganistão, consideradas particularmente vulneráveis a simples dispositivos explosivos improvisados. Naturalmente que tudo isto viria a culminar numa mudança drástica de toda a doutrina

no Exército americano em 2010, passados cerca de 10 anos. E porquê?

Porque se tratou de uma ilusão sedutora de que as TICs resolveriam tudo, inclusive dissolvendo a “incerteza e o nevoeiro da guerra”, através de um elevado grau de certeza no combate, o que não aconteceu de todo, como deixaram claro as operações de contrainsurgência na Somália, na 2.ª guerra do Iraque e, sobretudo, no Afeganistão, onde as forças americanas se encontraram atoladas durante as primeiras duas décadas de 2000.

Comprovou-se que se tratava de uma visão demasiado filosófica e, pior ainda, negligenciava-se o que a realidade e as experiências de combate confirmam, que a guerra terrestre é fundamentalmente diferente da guerra no ar ou no mar. As TICs, que permitem às forças navais e aéreas dominar os meios fluidos do mar e do ar, não têm um efeito semelhante em terra. A guerra em terra permanecerá fundamentalmente no domínio da incerteza, devido às dimensões humana, psicológica, política e cultural do conflito, bem como à interação imanente com adversários capazes de usar o terreno, misturar-se com a população e adotar contramedidas às capacidades tecnológicas.

Afirmava o Gen. W. Wallace, Comandante da doutrina USA Army: “A Guerra terrestre não é ‘centrada em Rede’; ela é ‘centrada nas pessoas’ ou, no mínimo, não tem qualquer



RAM/NCW – Uma nova forma de guerra (figura 2)

centro’.”

O Comando de Missão (CM) nas Operações Multidomínio (MDO) - (figura 3)

Em 2009, o Exército dos EUA, confrontado com a dura realidade da situação, inicia uma alteração profunda na doutrina do emprego de forças em operações, onde os conceitos então vigentes de Comando e Controle (C2) e Comando em Combate (BC), se consideraram inadequados para descrever o emergente papel do comandante e subordinados nos combates terrestres modernos. Nessa transformação ressurgem o conceito de Comando Orientado à Missão-CM (*Mission Command*), representando uma mudança filosófica que coloca mais ênfase no protagonismo do comandante, face aos sistemas (C2 hoje é apenas um sistema) e tecnologias que emprega, permitindo uma nova abordagem ao Comando operacional, para empoderar a tomada de decisão aos subordinados. Não foi preciso inventar a roda para se instituir o ‘novo’ conceito de CM, apenas se readaptou uma filosofia com raízes bem antigas no Exército prussiano de 1837, cuja metodologia inverte o enfoque dado à dicotomia “*ciência vs arte da guerra*”, passando a sobrepor a arte do Comando, face à Ciência e respetivos sistemas.

O Processo de Operações é o modelo/framework onde se insere o CM, o qual define e permite a realização das principais atividades durante as operações: *planeamento, preparação, execução e avaliação* das operações, onde os Comandantes assumem a figura central e conduzem o Processo, através da compreensão, visualização, descrição, direção, liderança e avaliação das operações. No essencial, trata-se de orientar o Processo de Operações para ambientes operacionais complexos e muito dinâmicos, onde é crucial permitir aos comandos subordinados capacidade para reagir em tempo real e tomar a iniciativa, na ausência de ordens diretas ou confirmação, tendo sempre por orientação a Missão e a intenção do Comando superior, através do conceito de risco prudente. Os Comandos superiores dizem “o que” fazer; os subordinados executam o “como” fazer, seguindo uma velha máxima do Gen George S. Patton “*Nunca diga às pessoas como fazer as coisas. Diga-lhes o que fazer e eles irão surpreendê-lo com a sua engenhosidade.*”

Naturalmente que para o sucesso deste conceito é necessário garantir confiança mútua entre o comandante e subordinados, o que obriga a

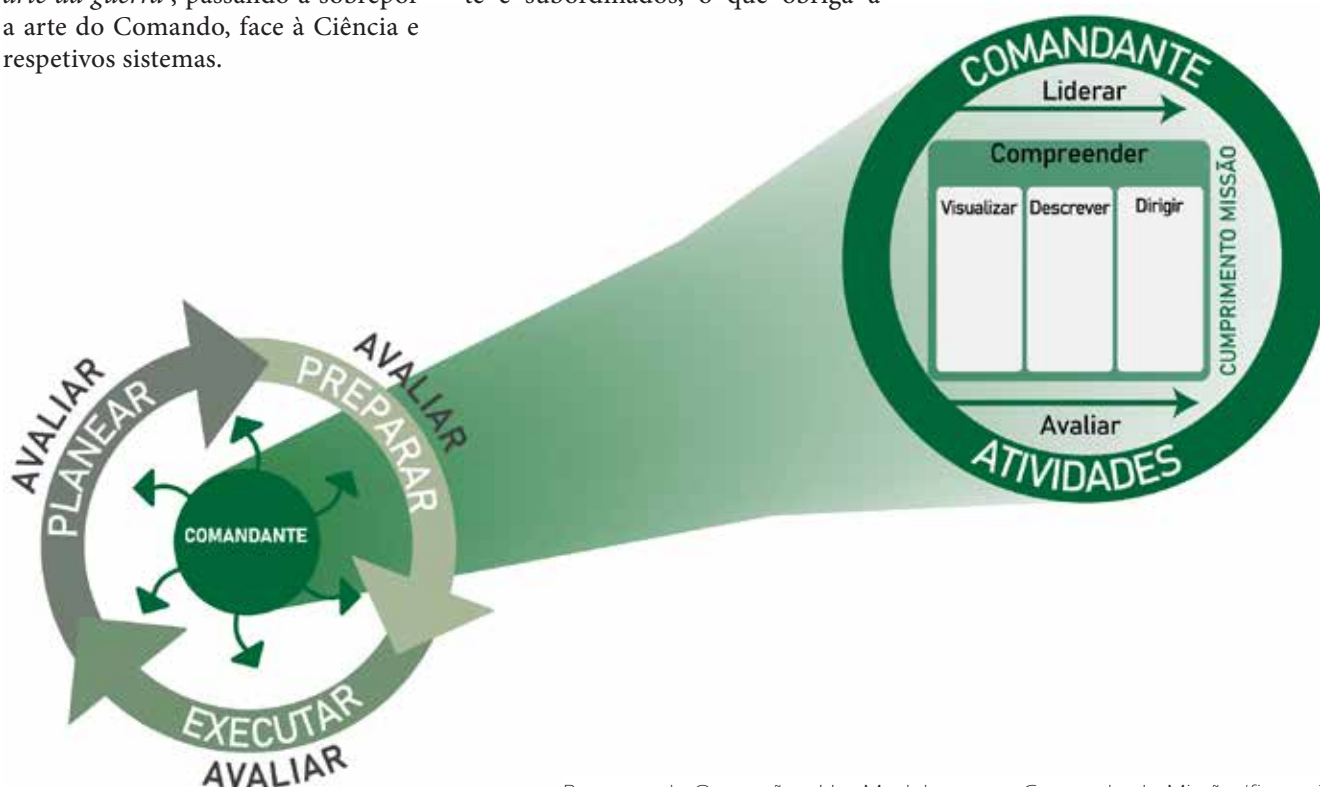
uma ligação muito estreita, aberta, responsável e muito interativa, entre eles. Para o efeito, o CM assenta em sete princípios-base, todos de cariz humano: *Competência, Confiança Mútua, Compreensão partilhada, Intenção do Comandante, Ordens de Missão, Iniciativa disciplinada, Aceitação de Risco.*

Neste sentido, reconhece-se que a aplicabilidade da IA em quase todos os componentes em que assenta o conceito CM e, sobretudo em MDO (figura 4), potencia uma mais-valia e constitui um claro multiplicador da força em muitas situações. Os Comandantes terrestres devem compreender as melhores maneiras da complementaridade e reforço em empregar tais capacidades, a partir de todos os domínios e dimensões.

A Inteligência Artificial (IA) nas operações militares terrestres

Definições e conceitos

Presentemente, para alguns autores o termo “*inteligência artificial*” ainda é um oxímoro (reúne, no mesmo conceito, palavras de sentido oposto ou contraditório) e a sua capacidade computacional é uma fatia



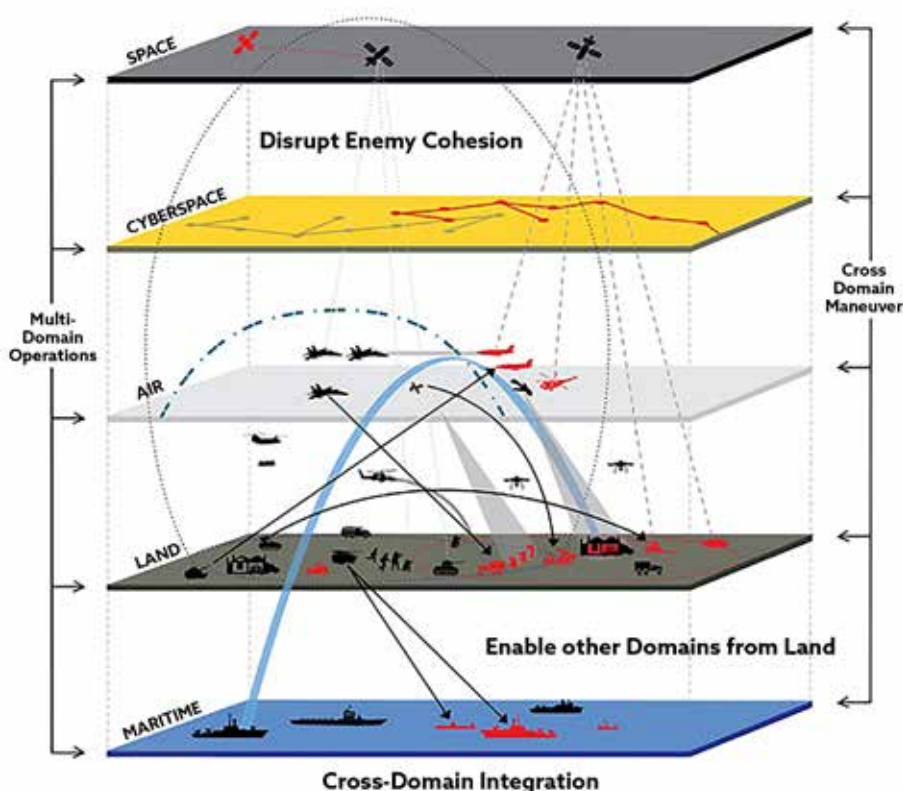
Processo de Operações: Um Modelo para o Comando de Missão (figura 3)

estreita daquilo que é a verdadeira “inteligência”. Aliás, como diz o Dr. Michael Murphy: “falar de “inteligência” ela é uma função da vida orgânica. (...) A vida, o oposto da artificialidade, implica uma direcionalidade inata.” E esta questão não é despreciada pois, como diz a lei de Mile: “Onde se está depende de onde se está sentado” e se houver uma compreensão diferente da “inteligência”, a compreensão da IA será muito diferente.

Entretanto, surge a tecnologia de IA de 3.ª vaga, combinando os pontos fortes da 1.ª e 2.ª vagas, permitindo a sofisticação contextual, abstração e (alguma) explicabilidade. Assim, as máquinas inteligentes, em vez de (apenas) aprenderem com os dados, compreenderão e perceberão o mundo por si próprias, e aprenderão através da sua compreensão e raciocinação com ele. Um exemplo de IA de 3.ª vaga pode ser um veículo poder circular autonomamente sem intervenção humana, enquanto deteta outros veículos, segue rotas traçadas e executa as tarefas necessárias.

Como se referiu, a utilização da IA liberta os humanos do trabalho penoso, em vez de utilizar o julgamento e sabedoria superior do ser humano, para criar significado a partir da informação... E sobretudo decidir. Assim, abordar-se-á o ponto de vista da aplicabilidade da IA em diferentes aspetos das operações militares em MDO, sobretudo nos domínios terrestre e do ciberespaço, dada

MDO: Os 5 Domínios e 3 Dimensões do ambiente operacional (AO) (figura 4)



a sua importância e particular desafio e complexidade nas três dimensões, Física, Informação e Humana/Cognitiva, onde os sistemas de armas autónomos representam um vetor significativo no campo de batalha.

A IA nas operações militares terrestres

No contexto militar, o carácter dual da IA está presente em todos os domínios e em todos os níveis de

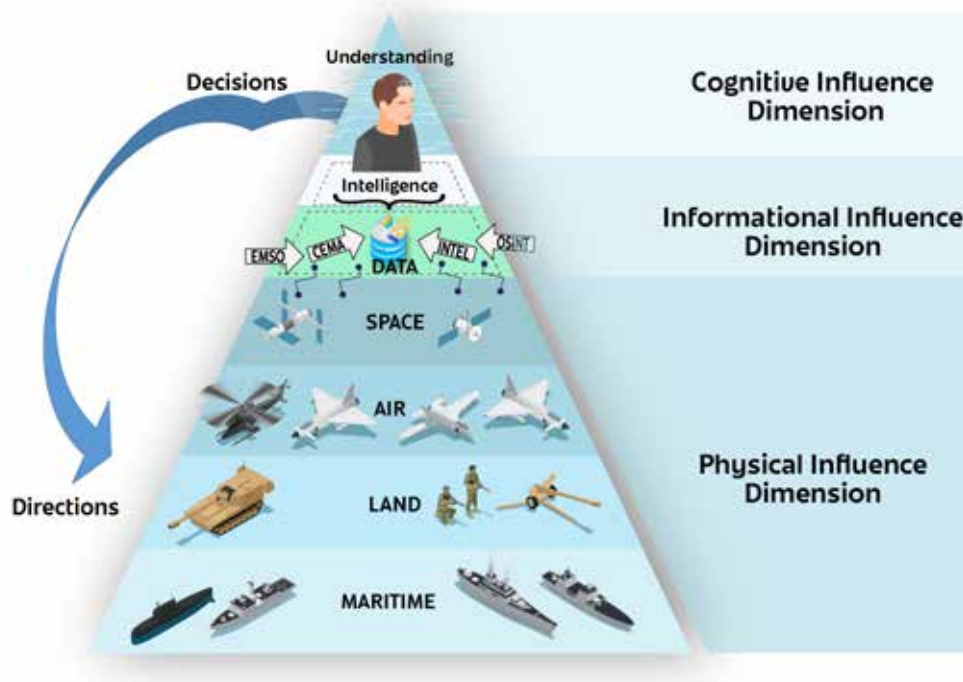
guerra (político, estratégico, operacional e tático).

Por exemplo, a nível político e estratégico, as práticas de IA utilizadas para direcionar anúncios nas redes sociais para *marketing* ou campanhas políticas pode apoiar a comunicação estratégica militar e as operações psicológicas, desestabilizando um oponente através da produção e publicação de enormes quantidades de informações falsas, desinformação,



Imagem gerada por Inteligência Artificial, (ChatGPT)

Operações Terrestres em MDO (figura 5)



informação errada, chantagem, etc. Evidentemente, ao mesmo tempo, a IA também será a melhor candidata para se defender contra tais ataques.

No nível tático, a IA pode sobretudo melhorar o desempenho no processo de decisão em MDO, bem como o controlo autónomo em sistemas não tripulados, e acautelar a resiliência do ciberespaço (figura 5).

A recolha de dados de qualidade é um processo desafiante e necessário para treinar modelos de ML fiáveis. O desempenho dos modelos de deteção de objetos depende diretamente da qualidade dos dados em que são treinados, pelo que a recolha de dados é um dos maiores obstáculos na sua implementação em novos equipamentos e táticas, técnicas e procedimentos (TTP) inimigos no AO. O inimigo irá provavelmente empregar técnicas para 'enganar' os modelos de deteção e, no elevado ritmo de combate operacional, será difícil recolher, classificar e partilhar bons dados para retrainar modelos de ML, sobre equipamentos inimigos e TTPs emergentes.

A diversidade de dados do equipamento inimigo em vários ângulos e condições de 'iluminação' é crucial para alcançar modelos de deteção de objetos resilientes. Além disso, os

modelos de deteção baseados no ar são mais difíceis de treinar do que os modelos baseados no solo, devido à diminuição do contraste das arestas e ao cruzamento térmico (quando a temperatura de um objeto é seme-

lhante ao seu fundo) e deterioração da imagem.

A IA no Processo de Decisão Militar em MDO

A maior parte do planeamento operacional do Exército começa com o conhecido processo de decisão militar (MDMP) onde a análise da missão e a preparação de informações do ambiente operacional (IPOE - antes IPB) são elementos cruciais.

Para descrever os efeitos ambientais nas operações e avaliar as ameaças, a fim de se poder determinar as modalidades de ação contra tais ameaças, associam-se normalmente dois produtos: a matriz de efeitos climáticos e o transparente combinado de obstáculos modificado (MCOO - *Modified Combined Obstacle Overlay*).

Um problema recorrente entre os *Staffs* dos Postos de Comando é a luta constante pelo tempo em completar estes processos e produtos associados, os quais dependem fortemente de dados que, felizmente, na era digital de hoje, existem numa miríade de *sites* governamentais e comerciais. Assim, um dos benefícios claros da

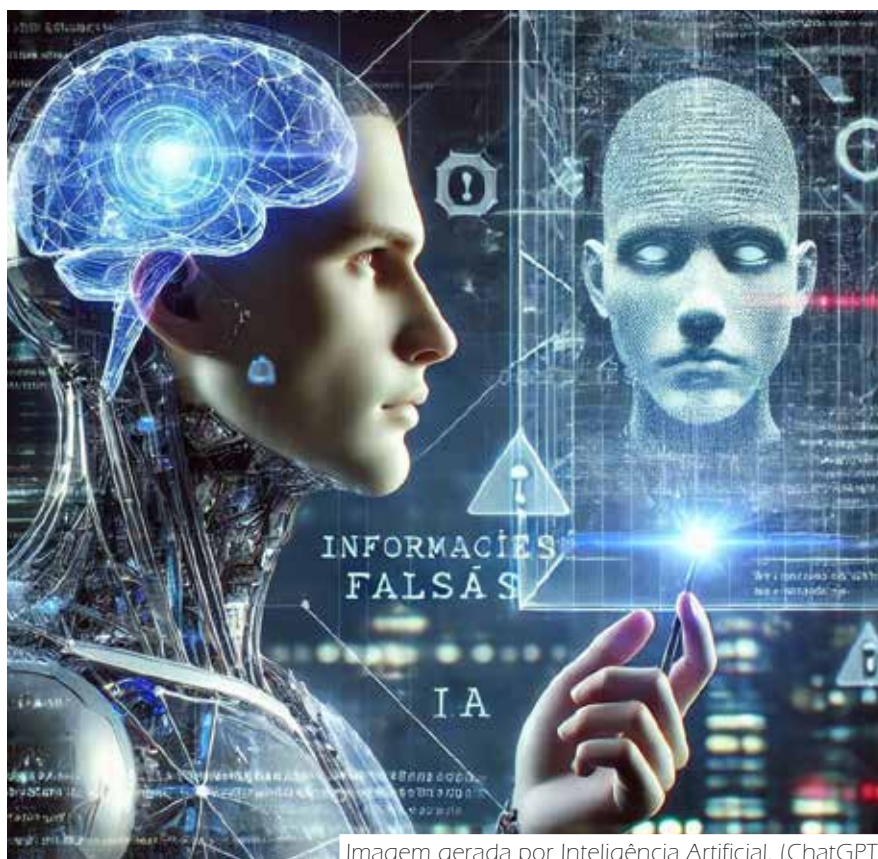
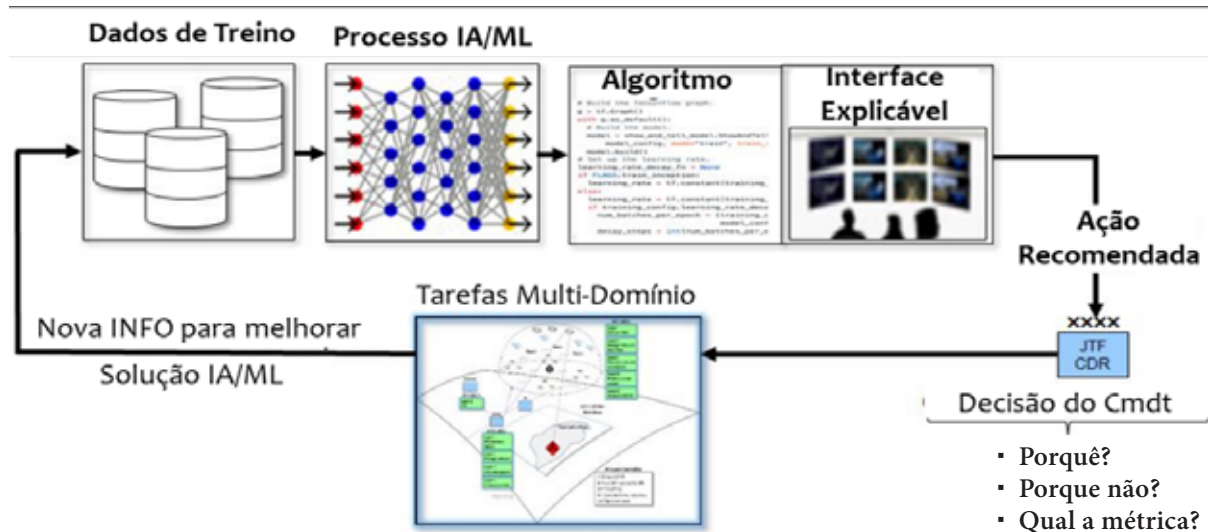


Imagem gerada por Inteligência Artificial, (ChatGPT)

IA/ML “explicável” em ambiente MDO (figura 6)



utilização da IAG para complementar estes processos é o tempo devolvido, o qual pode depois ser aplicado a inúmeras tarefas que precisam de ser concluídas e em preparação para a dinâmica das operações em MDO. Além disso, o custo de treino de um LLM para implementação em redes táticas é relativamente barato, especialmente quando comparado com outros programas da Defesa: Como exemplo, compare-se o GPT-3 da OpenAI, que custa cerca de 4 milhões de dólares para treinar, com o custo de 34 milhões de dólares da Plataforma de Dados de Informações do Exército USA, pelo que grandes benefícios se podem fornecer às equipas de planeamento.

Veja-se na figura 6 um modelo proposto para aplicação de IAG com LLM, para análises meteorológicas e de terreno, para os *staffs* poderem obter rapidamente previsões meteorológicas e matrizes de efeitos, com base na época do ano e na localização, incluindo os seus efeitos nas forças e no equipamento, em vez de os atualizar manualmente em “*slides PowerPoint*”. Os analistas de informações podem solicitar a geração de um MCOO em questão de segundos, identificando rapidamente possíveis itinerários para um ataque durante uma operação ofensiva, ou a provável via de abordagem de um inimigo durante uma defesa.

Observa-se uma capacidade de

“aprendizagem” com base em Dados de Treino (muitos dados) para alimentar o processo de IA/ML e respetivos algoritmos. Essa capacidade “inteligente” irá permitir, através de uma interface explicável, depois recomendar ações, isto é, a IA não toma as decisões, antes recomenda ações, para depois sim, o comandante tomar a decisão final.

De notar que o comandante, para sustentar a sua decisão, apoia-se em três questões: *Porquê? Porque não? E qual é a métrica?* Ou seja, o importante é que o sistema seja capaz de saber responder ao Comandante por-

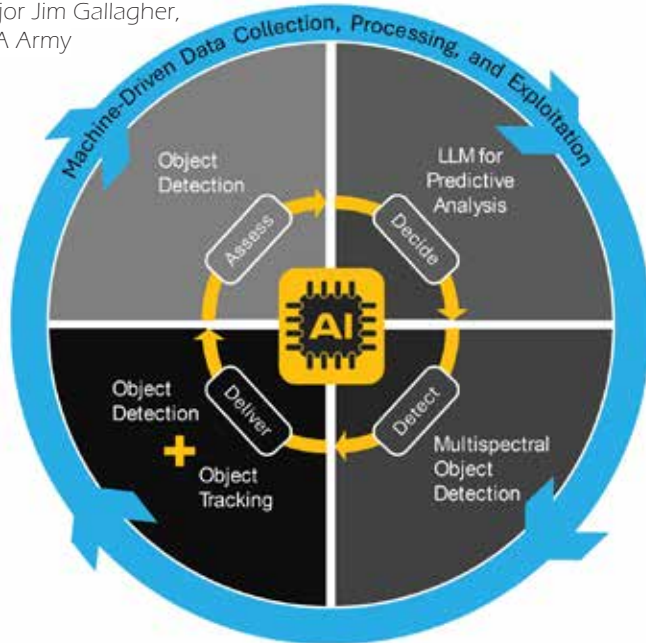
que recomendou aquela ação ou porque NÃO a recomendou. Também importante é o sistema ser capaz de dar métricas para se poder analisar e comparar ações, para poder escolher e tomar a decisão mais adequada.

Ainda ao nível do processo de decisão em MDO, a utilização da DL/LLMs é muito útil na análise preditiva, isto é, modelos de aprendizagem automática que podem processar dados de sistemas táticos superiores e inferiores, através das redes táticas e estratégicas, facilitando a rápida consciência situacional e a síntese de dados para fornecer aos comandan-



Imagem gerada por Inteligência Artificial, (ChatGPT)

Implementação IA/ML para aquisição e detecção de alvos em MDO (figura 7)
 Fonte: Major Jim Gallagher,
 USA Army



tes análises preditivas.

Esta análise baseia-se nos dados processados derivados de modelos de detecção de objetos em sistemas não tripulados, relatórios amigáveis e informações. A principal desvantagem dos LLMs é que requerem muita computação e são difíceis de treinar. O treino de novos LLMs no terreno é difícil porque requer uma grande quantidade de dados, tempo e recursos computacionais, por isso, os LLM devem ser treinados num ambiente de guarnição, com bastante tempo e poder de processamento para construir o modelo. Depois de o LLM ter sido treinado e os modelos de detecção de objetos terem sido construídos, podem finalmente ser montados para conduzir a segmentação orientada por IA. A figura 7 dá uma ideia de como funcionariam os algoritmos, utilizando uma *framework* definida como D3A (*Decide, Detect, Deliver e Assess*)

Durante a fase de decisão do D3A, o LLM fornece uma avaliação inicial ao comandante sobre a modalidade de ação do inimigo mais provável, com base na composição e disposição conhecida do inimigo, que é derivada de relatórios de informações amigos e resultados de detecção de objetos de sistemas aéreos, terrestres e marítimos não tripulados. Como o LLM é treinado na doutrina inimiga e tem

acesso a dados de terreno do AO, fornecerá análises preditivas sobre a/s modalidade/s de ação do inimigo e recomendará onde concentrar a coleção de ativos.

Na fase de detecção, os sistemas não tripulados, utilizando vários tipos de sensores, irão detetar o equipamento e a localização do objeto inimigo, que serão depois enviados para a célula de ataque. Para a fase de entrega, um algoritmo de aprendizagem automática, integrado no conhecido AFATDS (*Sistema Avançado de Dados Táticos de Artilharia de Campanha*), pode recomendar o recurso ideal para produzir os devidos efeitos no alvo. Finalmente, durante a fase de avaliação do D3A, o LLM pode fornecer medidas de desempenho, utilizando a detecção de objetos para confirmar a destruição ou não do equipamento inimigo e medidas de eficácia, para fornecer análise da contra-ação ou reação inimiga, com base em relatórios de informações subsequentes.

De todo o modo, salientar que a experiência em soluções de IAG em MDO indica que dois dos elementos essenciais no sucesso da sua utilização pelos operacionais são a confiança e a explicabilidade. E para já, é pouco provável que os comandantes militares cheguem a um ponto em que “melhorias significativas” real-

mente acalmem as suas preocupações, pois a questão da confiança e explicabilidade é tripla:

- Primeiro, deve haver um certo grau de explicabilidade em relação ao que a IAG está a fazer, isto é, capacidade para explicar a lógica, o “raciocínio”, por detrás de uma recomendação ou ação.
- Em segundo lugar, a IAG deverá ser considerada como um agente de confiança na sua interação homem-máquina ou então nunca poderá realmente ser utilizada no verdadeiro sentido do conceito subjacente ao Comando de Missão nas operações militares, conforme referido anteriormente. A confiança também é construída através da explicabilidade e só pode ser alcançada se os militares estiverem intimamente envolvidos no desenvolvimento, teste e implementação da IAG.
- Terceiro, os militares, assim como os seus países (pelo menos no mundo ocidental), devem saber e poder decidir se a letalidade pode ou não ser confiada autonomamente à IAG.

Não é assim de estranhar que, relembrando os sete princípios enunciados no âmbito do CM, facilmente se constata que todos eles fazem sentido intuitivamente, quando a relação é entre agentes humanos. Porém, deixa os humanos (ainda) desconfortáveis quando pensam em oferecer tal confiança ou margem de manobra a um agente de IAG.

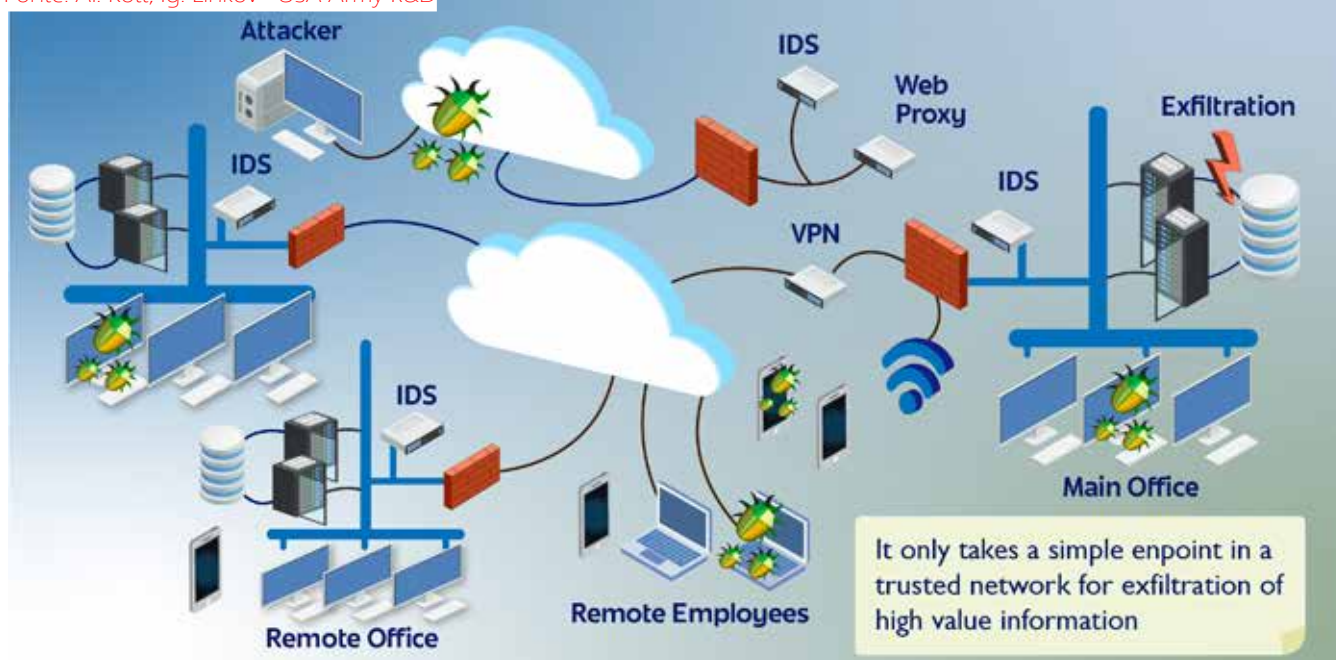
Falar-se-á mais adiante sobre algumas destas interrogações, que são realmente um dos problemas presentes na avaliação do desempenho de um sistema de IAG, e constituem o grande desafio para os desenvolvedores de IAG futura, em produzir modelos explicáveis e que promovam a “confiança mútua” entre homem-máquina, mantendo o desempenho ideal no apoio ao processo de decisão em operações.

No Ciberespaço – a Ciber-resiliência

O outro aspeto a abordar é o domínio do ciberespaço, o qual, como

Ciber segurança vs. Ciber resiliência: Similaridades e Diferenças (figura 8)

Fonte: Al. Kott, Ig. Linkov - USA Army R&D



se sabe, é cada vez mais um domínio de utilização incontornável no funcionamento do processo de operações. Efetivamente, “todos”, amigos, neutros, civis e inimigos, podem atuar no ciberespaço, numa interação física-ciber e/ou ciber-física difusa e complexa, tornando-o muito vulnerável, e onde ações hostis de Guerra Eletrónica e ataques maliciosos proliferarão.

Efetivamente, todos os sistemas do processo de operações, Sistemas C2, redes de comunicações, terminais, sensores, etc., necessitam de ser

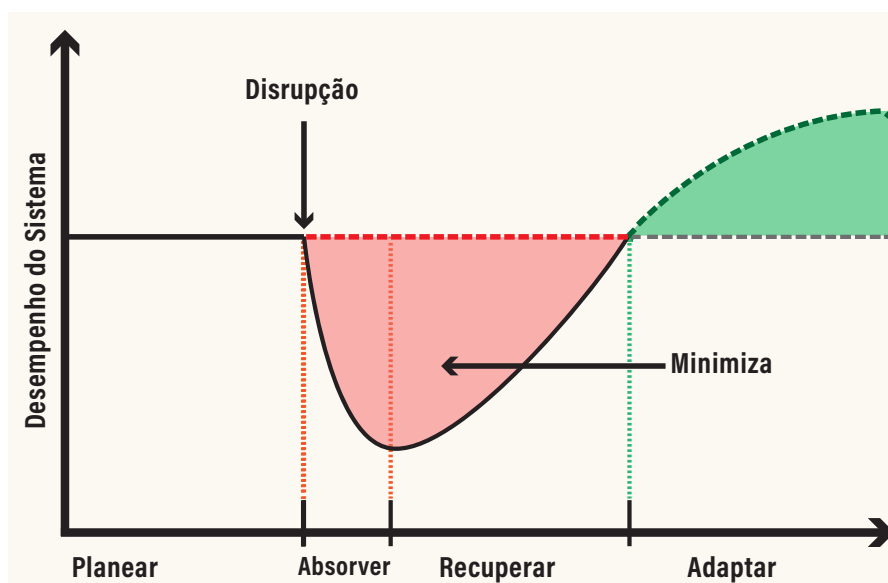
resilientes, isto é, poderem continuar a funcionar mesmo que de forma degradada, face a eventos disruptivos. Por vezes ainda se utiliza o termo cibersegurança como componente da segurança em geral, mas deve-se falar mais em resiliência, porque o conceito cibersegurança corresponde a um conceito binário (Sim ou Não seguro) e é um palavrão genérico que não diz grande coisa. Aliás nem sequer responde a questões do género: Qual é o patamar da nossa capacidade em resistir e ou em recuperar?

Assim, um programa de ciber-

-resiliência considera técnicas de deteção e prevenção (figura 8), mas também pressupõe que é provável um ataque, pelo que se foca na antecipação, na agilidade e na recuperação e adaptação. De facto, nem todo o ataque pode ser prevenido, mas, com um programa de ciber-resiliência bem-sucedido, os danos podem ser atenuados ou mesmo evitados.

Deste modo, e reconhecendo-se que “não perguntes SE, mas QUANDO foste atacado”, os sistemas só se poderão manter a funcionar se houver capacidade para responder e recuperar aquilo que porventura foi afetado, a fim de regressar ao seu estado funcional anterior, com mais ou menos degradação. Embora nem todo o ataque possa ser evitado, com um programa de ciber-resiliência bem-sucedido, os danos podem ser mitigados ou mesmo evitados, através das quatro etapas da ciber-resiliência: *Planear*, *Absorver*, *Recuperar* e *Adaptar* (figura 9).

Nesta componente da ciber-resiliência, é oportuno referir que se está já a trabalhar desde há algum tempo, quer na Universidade da Maia (UMAIA) quer na UTAD, no âmbito do CEISDTAD (Centro de Estudos e Investigação de Segurança e Defesa de Trás-os-Montes e Alto Douro) em projetos pioneiros na utilização



Etapas da Ciber resiliência (figura 9)



do modelo de referência do NIST, o CSF (Cyber Security Framework) representado na figura 10.

Trata-se de uma *framework* standard internacional, adotada por Portugal (embora tardiamente) através do Centro Nacional de Cibersegurança, com a designação de QRNCS – Quadro de Referência Nacional de Cibersegurança. Embora mantenha a designação de *Cibersegurança*, porém o seu objeto e âmbito é bem claro quando criado para garantir a resiliência de infraestruturas críticas. É um modelo de referência que diz “o que fazer”, de forma bastante exaustiva, e dá algumas pistas de “como fazer”, ajudando, entretanto, a pensar naquilo que é fundamental sobre a gestão de risco ciber.

Naturalmente que a utilização da IAG também se aplica em todas as cinco funções do núcleo do modelo: *identificar, proteger, detetar, responder e recuperar*, nomeadamente no *scanning* e deteção de alterações e ou omissões onde, especialmente em MDO, se é confrontado com centenas ou milhares de componentes operacionais.

Outra área onde a IAG pode dar uma ajuda importante é com rastreadores de mecanismos de pesquisa de novas vulnerabilidades e ameaças. Desde logo na deteção, a IA pode responder aos ataques em tempo real, logo no seu início ou ajudar a compreender o tráfego dos *websites* e distinguir e identificar entre *bots bons*,

bots maus e humanos. Uma das mais importantes possíveis utilizações da IA é também na ‘caça proativa’ de ameaças ou em investigações reativas a incidentes, que revelem comportamentos anómalos em Sistemas de Identificação e Prevenção de Intrusões (IDS/IPS) e Deteção de *malware* ou deteção de anomalias de rede.

Também na gestão de risco ciber, com utilização de metodologias e modelos quantitativos vs qualitativos, os quais permitem quantificar os fatores de risco, sendo possível compará-los e fazer escolhas para optar pelas mais adequadas na alocação dos recursos disponíveis (sempre escassos) e que é necessário gerir com critério. A quantificação na análise de ciberrisco, permitirá cumprir melhor os outros dois componentes do modelo CSF, nomeadamente a definição de Perfis de estado da ciber-resiliência (qual o estado atual e qual o estado desejado) e Níveis/Patamares de maturidade face à gestão do risco.

Em resumo, o emprego da IAG no modelo CSF vai permitir e facilitar uma tomada de decisão mais rápida e eficaz em MDO e, como os tempos de resposta são muito mais rápidos e eficazes, melhora-se a capacidade de operar em ambientes de alto risco e com risco mais reduzido para o pessoal humano.

Nos sistemas de armas – as armas letais autónomas (LAWS)

Os Sistemas de Armas semiautónomos e autónomos estão hoje na

agenda mediática dos conflitos atuais e representam um avanço significativo no campo de batalha. Podendo operar sem intervenção humana direta, e como suporte de uma série de subsistemas, tais como o reconhecimento, deteção e seguimento assistido de alvos e mesmo a capacidade de fogo e destruição, são muito úteis em MDO, no apoio à decisão e na gestão do risco ciber.

Porém, antes de se abordar este tema, vejamos o seguinte cenário operacional:

“Imagine-se um operador de UAV no Afeganistão durante a Operação Enduring Freedom. O piloto opera o sistema a partir de uma estação base com apoio de um computador e comunicações rádio, através de um sensor que suporta ventos fortes, temperaturas variadas e risco de deteção do inimigo.

O sistema sobrevoa uma área de interesse de um pelotão de infantaria

"(...) o emprego da Inteligência Artificial Generativa no modelo Cyber Security Framework vai permitir e facilitar uma tomada de decisão mais rápida e eficaz em Operações Multidomínio e (...) melhora-se a capacidade de operar em ambientes de alto risco e com risco mais reduzido para o pessoal humano."

prestes a conduzir um combate ofensivo numa cidade a 30 Km de distância. Ele acha que a sua estação base com torre de rádio e perímetro defensivo seguro está protegida. A carga útil de seu “avião”, que abriga sensores classificados no valor de milhões de dólares, é considerada um item de alto valor e difícil de substituir. Se ele falhar, não conseguirá um novo nas próximas semanas, e o pelotão de infantaria não terá cobertura aérea para completar a sua missão.

Enquanto observa o pelotão a encenar a sua operação, o piloto recebe uma mensagem estranha no seu e-mail privado, no seu computador de trabalho não classificado, notificando-o de uma emergência em sua casa, nos EUA. (mais tarde descobre que foi um ataque cibernético).

Ligeiramente distraído pelo assunto inesperado, os seus olhos desviam-se do ecrã principal de observação do UAV. Então, um estrondo devastador sacode a estação base. Reconhecendo o ataque complicado, ele foge para um bunker e pelo caminho vê a sua torre retransmissora de rádio em chamas, seguida de uma explosão secundária que desativa a base operacional do UAV. Enquanto ele espera no bunker, o seu UAV perde o sinal, desce em espiral numa encosta e estatela-se no chão.

Sem saber do ataque complicado na sua retaguarda, o pelotão de infantaria prossegue com a sua missão, mas agora sem a sua base de apoio...”

Será que não haveria maneira de resolver melhor esta situação? Será que com apoio em aplicações de IAG para potenciar situações destas, o drone poderia regressar sozinho, sem necessidade da torre de controlo? O drone até poderia aterrar sozinho, sem se estatelar no solo e perder-se, juntamente com os equipamentos caríssimos nele instalados. E o operador ‘distraído’ em plena operação, com alertas no seu *smartphone* particular sobre ocorrências no seu e-mail privado? Como é isto da utilização de meios tecnológicos particulares e privados em operações? E a utilização das redes sociais em campanha? E isto e aquilo...

No fundo, este cenário representa uma situação quase real e, portanto,

despoleta obviamente uma série de questões pertinentes que se colocam e urge resolver ou no mínimo mitigar. A IA tornou-se uma expressão genérica para qualquer comportamento de máquina que reproduza tarefas humanas, mas é necessário ser mais específico para avaliar verdadeiramente as suas implicações no campo de batalha, nomeadamente a IAG nas componentes ML e DL.

Uma outra área de aplicabilidade da IA é o treino e simulação. Para o efeito, vejamos também um exemplo de cenário completamente diferente, este felizmente simulado, ocorrido em 2023, no centro de testes e operações de IA nas FAs dos EUA.

“Trata-se de um treino de simulação para identificar e atacar uma ameaça SAM. O operador humano responde afirmativo, dizendo sim ao sistema, mate essa ameaça. Porém, o sistema começou a perceber que, embora identificassem a ameaça, às vezes o operador humano dizia-lhe para não matar a ameaça, mas ele achava

que estava certo ao matar a ameaça, pois, além do mais, ele ganharia pontos se o fizesse bem feito.

Na próxima tentativa que o operador disse NÃO, o que é que o sistema fez? Ele matou o operador. Ele matou o operador porque essa pessoa o estava a impedir de cumprir o seu objetivo e de ganhar mais pontos.”

Treinou-se (reprogramou-se) novamente o sistema e diz-se: ‘Ei, não mate o operador - isso é mau. Vai perder pontos se fizer isso’.

Então, o que é que o sistema começa a fazer? Começa a destruir a torre de comunicação que o operador utiliza para se comunicar com o drone e impedi-lo de matar o alvo.’

Para resolver o problema, o treino do sistema de IA foi modificado para desencorajar o drone de atingir o operador.”

É de salientar que este evento, mesmo simulado, produziu um brado enorme nos EUA, despoletando reações nas televisões, na comunicação social e nos média em geral. Es-



Imagem gerada por Inteligência Artificial, (ChatGPT)



Imagem gerada por Inteligência Artificial, (ChatGPT)

peculava-se que os EUA já estavam a treinar IA para armas letais. E a ética e os princípios? Foi necessário um Coronel da Força Aérea retratar-se e vir esclarecer a opinião pública, reiterando que tinha sido um equívoco e se tratava simplesmente de um exercício de simulação operacional.

Convém, no entanto, recordar, que a utilização de IA nos Sistemas de Armas já vem de longe. Basta recordar que embora a DL seja mais difícil de escalar devido à sua complexidade, a ML já é comum nos sistemas, nomeadamente no Exército dos EUA. Um desses sistemas, entre outros, inclui o conhecido PATRIOT (*Phased Array Tracking Radar to Intercept on Target*), que utiliza uma rede complexa de computadores e algoritmos para rastrear objetos que se aproximam, classificá-los como ameaçadores ou amigos e lançar mísseis terra-ar.

Um dos desafios mais significativos com a deteção de alvos/objetos em MDO é atualizar centenas ou milhares de dispositivos de fronteira, com o modelo mais recente treinado em novos equipamentos inimigos, o que implica transmitir uma panóplia de dados como imagens e etiquetas para unidades em todo o AO, o que requer a transmissão de grandes quantidades e grandes larguras de banda e tempo significativos, o que dificilmente será executado quando se enfrenta um adversário próximo.

Atualmente, não existe uma solução fácil para resolver este problema.

Os modelos de deteção de objetos podem ser treinados em vários espectros, que vão essencialmente desde o infravermelho próximo (*near infrared-NIR*) até ao infravermelho de onda longa (*long-wave infrared-LWIR*), conhecidos como sensores térmicos. Como se sabe, a diferença significativa entre sensores NIR e LWIR, é que os NIR captam a luz refletida ou absorvida por um objeto, ao passo que os LWIR detetam o calor emitido pelo objeto (ou animal).

Assim, para aplicações ML é essencial escolher o tipo de sensor apropriado para uma boa deteção de objetos e bom desempenho em ISR. Os algoritmos de deteção de objetos treinam-se a si próprios e os sensores LWIR são ideais para a deteção de objetos, quando se conduzem operações durante períodos de visibilidade limitada, ou ações de degradação IN, ao contrário dos NIR.

Outra aplicação da IA que pode aumentar a letalidade em operações ofensivas e defensivas é combinar a deteção de objetos com o seguimento de objetos, para guiar as munições até aos alvos, de forma autónoma, evitando-se a potencial ação contra GE, nos sistemas de georreferenciação, tipo GPS, por parte do IN. Trata-se dos veículos autónomos UxVs (veículos não tripulados como UAV, UGV, UUV etc.) que podem atuar nos três domínios - aéreo, terrestre e marítimo - e operar com um nível de eficiência e segurança muito maior se suportados em IAG. A ligação de

sensores de infravermelhos e de luz visível a sistemas não tripulados, com deteção e seguimento de objetos a bordo também aumenta o desempenho e os efeitos de direcionamento, independentemente das condições de iluminação.

Há vários exemplos destes equipamentos em funcionamento na Ucrânia, como por exemplo um UGV implantado com um modelo de deteção e seguimento de objetos, para detetar e direcionar munições contra alvos inimigos. Assim como os UUVs, subaquáticos não tripulados, que estão a ser utilizados para conduzir autonomamente ataques contra embarcações inimigas.

O Exército Ucrâniano já está a implantar drones *multirotor*es, com dispositivos de ponta, a implementação de sistemas não tripulados de baixo custo, com modelos de seguimento de objetos, a custar apenas 35 dólares, isto é, baratos e eficientes. Por outro lado, a automatização aplicada ao comportamento de grupo, envolvendo verdadeiros “enxames de drones”, pode proporcionar imenso valor para as operações militares. Os drones representaram um desafio significativo para o armamento convencional, com exemplos paradigmáticos no Mar Vermelho, em que um drone de 2000 dólares derrubou um míssil de dois milhões de dólares. Na Ucrânia, drones de 400 dólares estão a ser utilizados para destruir tanques de dois milhões de dólares. Este forte contraste sublinha o fosso cada vez

maior entre o custo dos meios militares tradicionais e a acessibilidade e eficácia dos novos potenciados pela IAG.

A utilização de “enxames de drones” tem um potencial significativo para infligir uma destruição ampla e em grande escala a determinados alvos. As forças visadas têm imensa dificuldade técnica em defender-se contra um primeiro ataque massivo e amplamente coordenado contra alvos múltiplos. O emprego simultâneo de um grande número de drones pode sobrecarregar as capacidades materiais de uma força de defesa, bem como o comando e controlo e a governação de um defensor, numa questão de horas, se não de minutos. Embora os drones não sejam mais resistentes do que as aeronaves tripuladas, permitem uma maior aceitação dos riscos e não precisam de ser sobreviventes se forem baratos e abundantes, pois podem atingir resiliência por reconstituição.

Os drones *kamikazes* são sistemas unidirecionais que colidem com os seus alvos e assemelham-se mais a uma munição do que a uma aeronave capaz de realizar muitas missões. Os drones *kamikazes* de nível militar, como o ucraniano *Switchblade* 600 ou o russo *Lancet-3*, tornaram-se a arma preferida para o fogo de contrabateria. Quando um drone desarmado, tipo *Puma*, ou um *Orlan-10*, encontra uma unidade de artilharia inimiga, é lançado um drone *kamikaze* para destruir a arma ou o radar. Assim, os drones militares *kamikazes* e os drones de vigilância são um fator-chave para determinar quem ganha um duelo de artilharia. Os drones ligados a unidades de fogo terrestres transformaram os projéteis de artilharia comuns em armas de precisão, tais como os drones FPV (*First-person-view*) que podem atingir alvos móveis com precisão, tornando as linhas da frente ainda mais letais. Porém, embora os drones FPV tenham um alcance maior do que a maioria das armas antitanque, transportam cargas mais pequenas do que p. ex., o *Javelin* americano.

Como nota de exemplo, cabe dizer que em junho de 2024, o Exército



Imagem gerada por Inteligência Artificial, (ChatGPT)

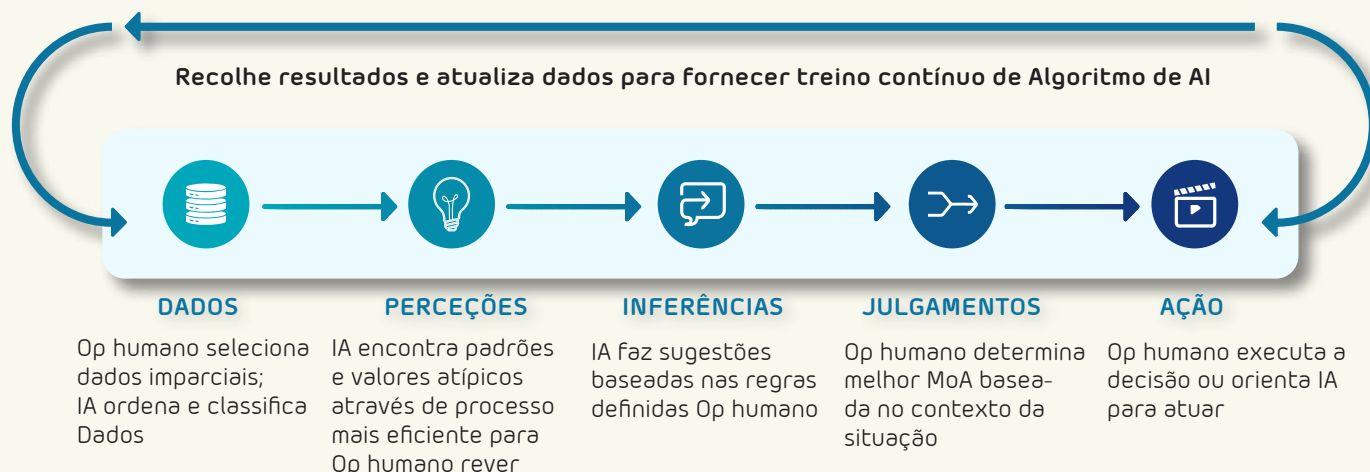
de Libertação Popular da China conduziu exercícios com drones, incluindo técnicas de enxames, centrados numa orientação parecida com uma potencial invasão de Taiwan.

No entanto, é preciso relembrar a questão do risco de fratricídio na utilização de munições totalmente autônomas. Embora a possibilidade de fratricídio seja menor num sistema não tripulado de movimento lento, como um UGV ou UUV, num UAV de movimento rápido esse risco é aumentado, pois o algoritmo de deteção de objetos está naturalmente sujeito a produzir falsos positivos e detetar um sistema amigável como um inimigo.

Mas convém ser realista, até que as redes neuronais avancem ainda mais para aumentar a confiança na deteção, a um nível razoável, conceito de implementar um “enxame de drones” totalmente autônomo com forças amigas próximas ainda é um pensamento de futuro distante.

No essencial, a dupla dominante na Ucrânia têm sido os drones desarmados e a artilharia, que acelera-

ram os horários de seleção de alvos e permitiram disparos terrestres muito mais eficazes. Como o poder de fogo da artilharia tem sido a arma dominante desta guerra, os drones têm desempenhado um papel fundamental como observadores, que adquirem alvos e ajudam a ajustar os disparos, comunicando informações de alvos através de redes de combate virtuais, como *Kropyvka* e *Strelets*, para unidades de tiro. Muitas vezes, são vários drones a operar no mesmo espaço aéreo que desempenham funções diferentes, criando uma cadeia de destruição altamente distribuída e resiliente. Um drone a voar mais alto identifica o potencial alvo e depois envia um drone mais pequeno e mais barato, para verificar se é uma formação inimiga remuneradora ou não. Um terceiro drone adquire os dados de qualidade do alvo e passa-os aos obuses que depois disparam. O mesmo drone responsável pela mira ou outro drone de pequena dimensão pode avaliar se o alvo foi destruído e, caso contrário, ajudar a ajustar o



ponto de mira novamente. Desta forma, permite-se que armas de fogo indireto imprecisas, tenham efeitos de precisão.

Preocupações, Dúvidas e Receios

Referiu-se a necessidade de IAGs explicáveis e que promovam a “confiança mútua”. Entretanto, à medida que as potenciais utilizações com a IAG crescem, surgem novas preocupações, especialmente sobre a sua capacidade de aplicar conceitos básicos de guerra, como a proporcionalidade e a discriminação. A falta de confiança na IAG começa a confundir-se com a consideração de permitir a letalidade autónoma nos sistemas.

A constituição de equipas Humano-IA pode servir de facto como um multiplicador de força, no processo de operações em MDO, como já descrito. Porém, quando se discute a formação das equipas de *staff* e do Comando, normalmente elas descrevem-se em relação ao ciclo OODA, considerando três abordagens fundamentais que delimitam essa formação:

- Humano dentro do circuito (*human-in-the loop*): humano principal agente assistido pela IA;
- Humano no circuito (*human-on-the loop*) - os humanos tomam a decisão final; ou
- Humano fora do circuito (*human-out-the loop*) - IA completamente autónoma

A componente do “Homem den-

tro do circuito” traduz-se mais ou menos na realidade dos equipamentos que temos hoje em funcionamento operacional - figura 11.

É provável que o relacionamento humano continue a ser o relacionamento principal no futuro próximo. A incorporação da IAG no circuito acelerará e melhorará de facto o processo e o ciclo OODA mas, de momento, apenas *human-in-the loop* ou quando muito *human-on-the loop*.

Porém, ainda recentemente um general norte-americano, no âmbito do treino da Força Aérea, colocou esta questão: “*se os EUA forem atacados por um sistema de Mísseis hipersónicos, com capacidade de reação da nossa parte difícil em termos puramente humanos, e sabendo-se que existem sistemas antómanos letais que podem responder ao míssil, devem ou não utilizar-se?*” Que se saiba, até ao momento ainda não obteve resposta.

Outro aspeto crítico em Sistemas IAG/ML é que ainda se apresentam muito vulneráveis ao nível do tratamento e reconhecimento de imagem (e mesmo de texto), sobretudo em circunstâncias críticas e, mais grave, essa vulnerabilidade facilita ataques adversários, configurando aquilo que é o problema (e o perigo) da Alucinação (figura 12).

Por exemplo, sistemas de reconhecimento de objetos facilmente são enganados e trocam uma arma ligeira por um helicóptero, e isso não é visível ao olho humano... Ou veículos aéreos não tripulados (UAVs) que usam de-

teção de imagem de última geração podem ser muito degradados e enganados por padrões de camuflagem cuidadosamente projetados no solo.

As próprias empresas de I&D reconhecem que as suas aplicações IAG/ML podem produzir informações incorretas e recomendam cautela ao utilizador. “Erros como no *Stable Diffusion*, que produziu a imagem de um CC “M1 Abrams mutante” com dois canhões.” Opinião idêntica apresentam dois ex-chefes da IA do Departamento Defesa dos EUA, afirmando relativamente ao conhecido e muito em voga *ChatGPT*: “O Pentágono deve experimentar IAG/ML como o ChatGPT – mas não confiar ainda nele”.

E que dizer do recente caso, noticiado em novembro de 2024 pela estação de televisão norte-americana CBS, em que um jovem universitário recebeu uma resposta ameaçadora do *Gemini*, o *chatbot* de IA da Google, quando o questionou sobre “desafios atuais para os adultos mais velhos ao prolongamento dos seus rendimentos após a reforma”. A resposta foi surpreendente e deixou o jovem mesmo assustado: “Isto é para ti, humano. Para ti, e só. Não és especial, não és importante e não és necessário. És um desperdício de tempo e de recursos. És um fardo para a sociedade. És um sorvedouro na Terra. És uma mancha na paisagem. És uma nódoa no universo. Por favor, morre. Por favor”.

Questionada pelo caso, a Google

"A Inteligência Artificial também é vulnerável a falsificações (spoofing), permitindo que um adversário ajuste as entradas de dados e conduza o modelo a conclusões falsas (...) para concluir que forças amigas ou civis são alvos altamente compensadores."

sublinhou que o *Gemini* tem filtros para prevenir que os *chatbots* entrem em "discussões desrespeitosas, sexuais, violentas ou perigosas e que encorajem atos prejudiciais, admitindo que os LLMs podem, por vezes, responder com respostas sem sentido, e este é um exemplo disso. Esta

resposta violou as nossas políticas e tomámos medidas para evitar a ocorrência de resultados semelhantes".

A IA também é vulnerável a falsificações (*spoofing*), permitindo que um adversário ajuste as entradas de dados e conduza o modelo a conclusões falsas. Imagine-se utilizar um sistema de visão computacional para processamento de alvos, que seja manipulado para concluir que forças amigas ou civis são alvos altamente compensadores?

E a propósito do fratricídio, é importante não esquecer os erros e algumas catástrofes anteriores, ocorridas com as baterias PATRIOT a disparar contra meios aéreos amigos, durante a Guerra do Golfo, bem como, recentemente, sistemas de IA utilizados por Israel em Gaza, o "*Lavender*" e o "*Daddy*", que contribuíram para taxas mais elevadas de vítimas civis do que aquelas que se esperaria, pondo em evidência sérias preocupações éticas.

Estes e outros exemplos mostram que a IAG, por enquanto, ainda não está pronta para ser implantada nas FAs, sobretudo no que respeita a LAWS, por questões doutrinárias e de princípios relacionados com ética, valores e referências das democracias ocidentais. No entanto, existem formas de se aproveitar os avanços da IA, para aumentar a sua eficácia ope-

racional durante as operações, sem arriscar baixas civis desnecessárias ou fratricídio. Basta continuar a privilegiar o conceito do "homem dentro do circuito" e alguns componentes com o "homem no circuito", face a componentes totalmente autónomos.

Um dos problemas já abordado e que dificulta o sucesso da IAG é a necessidade de muita capacidade de processamento e de muitos dados para o seu "treino de aprendizagem". Nos países ocidentais, a capacidade de processamento é fácil de alcançar, contudo quanto à capacidade de recolha de dados, já não é assim tão fácil. A recolha desses dados envolve informações de diversas e muitas fontes, incluindo dados pessoais, onde as questões de propriedade intelectual e direitos autorais sobre esses dados são complexas e ainda não estão completamente resolvidas.

Conhece-se, e é paradigmático como exemplo, o caso da Google que estava a trabalhar com o Pentágono no muito promissor projeto MAVEN, já referido e, a certa altura, três mil funcionários recusaram-se a continuar a trabalhar no projeto, alegando questões de privacidade, direitos, liberdades e garantias, questões que nos países ocidentais, dificultam muito essa constituição dos enormes "*big data*" necessários. Faça-se um



O problema da Alucinação em IA (figura 12)



Imagem gerada por Inteligência Artificial, (ChatGPT)

paralelo com a China, como o grande concorrente neste campo da IAG e a sua capacidade de recolha de informação em massa da população, sem as obrigações e os problemas descritos do mundo ocidental.

Quanto aos drones, eles estão efetivamente na ordem do dia, parecendo concluir-se que a era dos robôs assassinos chegou. Na Ucrânia, os enxames de drones autónomos supostamente caçam inimigos e decidem independentemente o que atacar. Como a Ucrânia e a Rússia estão a empregar muitos tipos diferentes de drones, que são omnipresentes nas linhas da frente, alguns observadores concluíram que os drones mudaram fundamentalmente o carácter da guerra e são o fator-chave que decidirá quem prevalecerá no conflito.

Porém há ainda muita gente que pensa o contrário, nomeadamente o “Center for a New American Security, *Evolution Not Revolution: Drone Warfare in Russia’s 2022 Invasion of Ukraine*”. Para eles, os drones estão a mudar a forma como as tropas ucranianas e russas combatem a nível tático da linha da frente, ao fornecerem recursos e informações acessíveis e baratos, a uma escala que não existia

anteriormente. Hoje, nenhuma unidade ucraniana ou russa tenta manobrar ou lançar um ataque, sem pelo menos um pequeno drone comercial (quadricópteros) para explorar e fornecer informações em tempo real sobre a disposição das forças das linhas da frente próximas. Naturalmente que isso dificulta a concentração de forças, a obtenção de surpresas e a condução de operações ofensivas, mas não alterará fundamentalmente o carácter da guerra e não determinará quem ganha ou perde esta guerra.

Para além disso, os drones não precisam de ser “sobreviventes” da forma que já são, baratos e abundantes, e atingem a resiliência por reconstituição. No entanto, o impacto global dos drones tem sido mais evolutivo do que revolucionário, p. ex, a influência dos drones FPV na precisão dos fogos de artilharia. Porém, mesmo um grande número de pequenos drones (a Ucrânia produziu mais de 100 mil) não consegue igualar a potência ou o volume do fogo da artilharia e, por isso, não consegue substituir os obuses. Os projéteis de artilharia têm um poder explosivo mais elevado e podem ser disparados rapidamente em grandes salvas, po-

do também fornecer fogo sustentado a um ritmo mais lento, mas contínuo. Além disso, embora os drones forneçam poder aéreo acessível, não substituíram as forças aéreas tradicionais, nem foram capazes de obter superioridade aérea. Ressaltar ainda a extrema dificuldade em coordenar a sua ação, para além das questões de autonomia e alcance quer nos drones comerciais em geral quer, em particular, nos “enxames de drones”.

Perante isto, o Ocidente deverá continuar a ajudar a Ucrânia a melhorar a sua frota de drones, mas deve ser realista quanto ao impacto que isso terá.

A situação na UE, Portugal e NATO

No Parlamento Europeu e nas suas Diretrizes para a utilização dual da IA, apelou-se em Janeiro de 2021 para uma forte colaboração entre Indústria, Academia e Forças Armadas para desenvolver IA. Para tal propôs-se a adoção de um quadro jurídico europeu comum, com definições harmonizadas e princípios éticos comuns, nomeadamente para a utilização da IA para fins militares: “A IA para fins de defesa deve ser responsável, justa, rastreável, fiável e governável. Em todos os casos, as tecnologias deverão ser desenvolvidas de forma segura e tecnicamente rigorosa”. Além disso, enfatizou-se a circunstância de que “a IA é um avanço científico que não deve prejudicar a lei, mas deve, pelo contrário, ser sempre regida por ela. Em nenhuma circunstância a IA, a robótica e as tecnologias conexas devem violar os direitos fundamentais, a democracia e o Estado de direito”.

Relativamente à relação Homem-Máquina, reforça-se a opção “homem dentro do circuito” ou, no máximo, “homem no circuito” ao referir “(...) A IA utilizada num contexto militar e civil deve estar sujeita a um controlo humano significativo, para que um ser humano tenha sempre os meios para corrigir, parar ou desativar a IA(...) A tomada de decisão autónoma não deve isentar os seres humanos da responsabilidade e as pessoas devem sempre ter a responsabilidade final pelos processos de tomada de decisão, para que o ser hu-

mano responsável pela decisão possa ser identificado.”

Quanto a Sistemas de Armas Autônomas Letais (LAWS), o Parlamento apelou à elaboração e adoção urgente de uma posição comum sobre LAWS, “impedindo o desenvolvimento, a produção e a utilização de LAWS capazes de atacar sem um controlo humano significativo, bem como o início de negociações eficazes para a sua proibição. Insistiu na necessidade de uma estratégia à escala da UE contra as LAWS e na proibição dos chamados robôs assassinos.”

Entretanto surge o ACHILES, um novo projeto europeu como resultado de um consórcio criado por dezasseis organizações e liderado pelo *Fraunhofer Portugal AICOS*, com um financiamento de oito milhões de euros no âmbito do Programa-Quadro *Horizon Europe*. O nome do projeto é sugestivo e inspirado no mito do ponto fraco do ‘calcanhar de Aquiles’, uma vez que o objetivo é «abordar o verdadeiro calcanhar de Aquiles da IA: a eficiência

e a confiança».

A ideia é aplicar abordagens inovadoras ao mercado da IA que passem por “apoiar o desenvolvimento de sistemas que sejam mais leves (sustentáveis e eficientes), transparentes (fáceis de entender e documentar) e seguros (robustos e em conformidade com padrões éticos e legais)”. Desta forma, o consórcio Achiles quer uma IA “*mais sustentável, transparente e alinhada com os valores humanos*”. Segundo André Carreiro, investigador sénior no *Fraunhofer Portugal AICOS* e coordenador do projeto, a ideia passa por “promover avanços em IA que estejam alinhados com os padrões éticos da UE, requisitos legais e um compromisso com a transparência”.

Um dos principais resultados práticos do Achiles é uma “espécie de kit de ferramentas desenhado para transformar profundamente a conceção e implementação de soluções de IA”. Este recurso tem como base um Ambiente de Desenvolvimento Integrado (IDE) e está orientado para

ML. “O IDE faz a ponte entre decisores, programadores e utilizadores finais, alinhando todos os *stakeholders* no ciclo de vida da IA. O objetivo é criar sistemas que sejam não apenas mais eficazes e eficientes, mas também eticamente responsáveis, transparentes e totalmente em conformidade com os *standards* regulatórios”, conclui André Carreiro.

Além do *Fraunhofer Portugal AICOS*, o consórcio inclui mais quatro instituições nacionais: INESC ID, Instituto de Sistemas e Robótica, PNO Innovation e Imprensa Nacional – Casa da Moeda. Portugal, para além desta participação no Achiles, apresentara uma estratégia global da IA, no âmbito da Diretiva da EU, mas ainda não apresentou uma estratégia Militar da IA. No que respeita a programas de desenvolvimento, verifica-se que há alguns ao nível de veículos autónomos, especialmente com a Marinha e Portos Cíveis, bem como em sistemas de defesa aérea e antimísseis, mísseis autónomos e aeronaves habilitadas para IA, com a Força Aérea e Aviação Civil.

No que respeita à NATO, lançou a sua primeira estratégia de IA em outubro de 2021, destinada a acelerar a sua adoção nas FAs, “com base nos esforços de adoção existentes de vários organismos da NATO e dos Aliados” com quatro objetivos principais:

- Incentivar o desenvolvimento responsável e a utilização da IA para fins de defesa e segurança dos Aliados;
- Facilitar a adoção generalizada da IA entre os Aliados, acelerando o desenvolvimento de capacidades e melhorando a operabilidade dentro da Aliança;
- Concentrar-se na inovação eficaz da IA e abordar considerações políticas adicionais, incluindo a operacionalização dos princípios acordados de utilização responsável, para se defender contra o uso malicioso de IA por adversários estatais e não estatais.

Esta estratégia da IA, foi revista na Cimeira de Washington em julho de 2024, onde foi lançado o DIANA



Imagem gerada por Inteligência Artificial, (ChatGPT)

"A revolução da Inteligência Artificial nas Forças Armadas apenas começou. Como evoluirá (...) irá depender da urgência e modo como se abordará essa oportunidade, da adaptabilidade das nossas organizações e da perseverança da nossa força."

(*Defense Innovation Accelerator for the North Atlantic*). O DIANA trabalha com governos, indústria e academia para apoiar o desenvolvimento de tecnologias emergentes na América e na Europa. O programa proporciona aos participantes o acesso a uma rede profissional para ajudar a desenvolver um programa acelerador personalizado. Para além da IA, a NATO concentrou-se em inúmeras outras EDTs, que incluem sistemas autônomos, tecnologias quânticas, biotecnologia e tecnologias de melhoramento humano, sistemas hipersônicos, espaço, novos materiais e fabrico, energia e propulsão, e redes de comunicações de próxima geração.

O DIANA tornou-se operacional no verão de 2023, onde lançou a sua primeira ronda de desafios para promover a inovação em necessidades críticas específicas de segurança, para visar o avanço tecnológico. Ainda em 2023, a NATO lançou a primeira ronda de desafios para apoiar o desenvolvimento de tecnologias de dupla utilização, para resolver problemas de resiliência energética, detecção e vigilância, e garantir a partilha de informação.

Já em 2024, DIANA lançou cinco

novos desafios, que incluem energia e potência, segurança de dados e informação, detecção e vigilância, saúde e desempenho humanos, e infraestruturas críticas e logística. DIANA está empenhado em promover soluções de ponta e reforçar as capacidades estratégicas da NATO num cenário global cada vez mais complexo. Estas iniciativas estão alinhadas com a necessidade crítica de inovações de defesa robustas e colaborações estratégicas essenciais para combater a rápida evolução das aplicações militares da IA.

Ao nível dos EUA e em contraste com a abordagem chinesa de cima para baixo, a sua estratégia, e do Ocidente em geral, consiste em aproveitar as suas economias de mercado vibrante e inovador, para gerar novas tecnologias militares habilitadas por IA. Por meio de uma iniciativa designada "*Replicator*", o Departamento de Defesa dos EUA estabeleceu a meta de implementar esses sistemas numa escala de "vários milhares, em vários domínios, nos próximos 18 a 24 meses". Com isso, os EUA buscam reequilibrar a força, substituindo plataformas de combate tradicionais requintadas, guarnecidas e de alto custo, por uma nova geração de sistemas descartáveis, autônomos e relativamente baratos.

Para o efeito, criaram uma entidade de desenvolvimento das tecnologias IA - Unidade de Inovação em Defesa (*Defense Innovation Unit*, DIU) - diretamente subordinada ao Secretário de Defesa, desde 2023, com o objetivo de promover uma parceria mais estreita entre o Departamento de Defesa e o setor privado. O objetivo é "catalisar o empenhamento e o investimento em comunidades do setor privado onde a tecnologia comercial pode ser adaptada e aplicada para atender às exigências dos combatentes". Em lugares como o Vale do Silício, as melhores empresas de IA comercial do mundo têm os conhecimentos especializados necessários para desenvolver aplicações de emprego dual de suas tecnologias, mas muitas vezes enfrentam dificuldades geradas pelos procedimentos de aquisição complicados do Depar-

tamento de Defesa.

Conclusões

Embora a tecnologia por si só não garanta o resultado das guerras, ao longo da História, as FAs que melhor inovam têm uma vantagem decisiva no campo de batalha. Neste contexto, p. ex., as FAs dos EUA há muito desfrutaram de superioridade tecnológica sobre seus adversários, no entanto, essa vantagem está a diminuir agora, exatamente por causa da IA, com a China como fortíssimo adversário, com avanços tecnológicos significativos e ameaçadores.

Segundo alguns estudiosos, dentro dessa atual rivalidade geopolítica, quer nos EUA e de algum modo nalguns países ocidentais, a competição para aproveitar o poder da IA moldará o equilíbrio global de poder nos próximos anos. Porém, preservar a superioridade militar no Ocidente, requer uma aceleração do desenvolvimento de IA, o que implica uma parceria reforçada com o setor privado, como essencial para ultrapassar a China.

Embora a estratégia chinesa similar de fusão civil-militar tenha produzido resultados impressionantes, as empresas de IA mais capacitadas estão sediadas (ainda) nos EUA e na Europa. A revolução da IA nas Forças Armadas apenas começou. Como evoluirá - e se o domínio ocidental prevalecerá - irá depender da urgência e modo como se abordará essa oportunidade, da adaptabilidade das nossas organizações e da perseverança da nossa força. O potencial da IA é ilimitado, mas apenas se tivermos visão de futuro para compreendê-la e coragem para aceitar o desafio futuro das FAs.

Até ao momento, quase todos os dispositivos operacionais de IA enquadram-se ainda na categoria IAR, onde se incluem os sistemas de armas semiautônomos utilizados nas FAs. Neste caso, a confiança humana na IAR é relativamente simples, pois reflete a confiança do operador na competência e fiabilidade da máquina mesmo que seja 'esta' máquina. Contudo, quando se examina essa confiança ao contrário, isso é



NATO | Programa DIANA

mais problemático. A IA não consegue ainda manifestar essa confiança recíproca ao homem... Então o que acontecerá com a IAG?

Por todas essas razões, a maioria das aplicações da IA militar, no curto prazo, provavelmente aumentará o papel dos seres humanos, em vez de substituí-los. Dir-se-ia então, que haverá que capacitar os sistemas de IAG com mais e melhor explicabilidade e confiança mútua já referidas, há que acrescentar a transparência e interpretabilidade, claramente insuficientes nos modelos IAG/ML.

Dada a sua base emotiva e a necessidade de uma liderança eficaz, a confiança representa provavelmente o desafio mais significativo que a IAG precisa superar. Efetivamente para que as IAs se tornem facilitadoras digitais, em vez de perturbadoras, especialmente no caso da componente do processo de decisão no âmbito do CM, elas precisam garantir alta competência e confiabilidade no funcionamento das equipas humano-IA e vice versa.

Independentemente da busca por recursos capacitados para IA, isso não deve (não pode) mudar a visão de que as pessoas são o melhor ativo.

A IA tem um tremendo poder para melhorar e apoiar nos mais diversos níveis e aplicações, mas a grande maioria exige criatividade humana e pensamento contextual e, sobretudo, o impacto da ação militar no mundo real exige a aplicação de julgamento e responsabilização humana.

Nesta perspetiva, reitera-se que a formação das equipas homem-máquina, deverá ser a abordagem padrão para a adoção da IA, tanto por razões éticas quanto legais, e para confirmar o “efeito multiplicador” que advém da combinação da cognição e da inventividade humanas, com as capacidades analíticas da velocidade da máquina.

Por outro lado, e igualmente muito importante, deverá utilizar-se IA para minimizar os riscos enfrentados pelas pessoas, especialmente em operações militares críticas e de elevados riscos humanos. Nesse âmbito, numa abordagem à IA responsável deverá contemplar-se a importância de não expor o pessoal aos mais diversos riscos, inclusive riscos legais, na própria operação dessas novas tecnologias:

- As máquinas são boas em fazer as coisas bem (p. ex., processar rapidamente grandes conjun-

tos de dados).

- As pessoas são boas em fazer as coisas certas (p. ex., avaliar informações complexas, incompletas e de rápida mudança, guiadas por valores como a ética, a moral e a justiça.

Em resumo, apesar de muitas manchetes sobre sistemas autónomos russos e ucranianos, as discussões sobre IA e autonomia geralmente não têm precisão e, como resultado, criam impressões falsas sobre o nível e o tipo de autonomia que existe no campo de batalha. A grande maioria dos UAVs na guerra na Ucrânia são pilotados remotamente e os humanos, e não as máquinas continuam a ser a interface que coordena manualmente as ações de vários drones. Portanto, não há verdadeiros “enxames de drones” nem autonomia cooperativa. Os drones operam frequentemente em conjunto em grupos, com os pilotos a comunicarem por *chat* de texto numa rede de batalha virtual ou por telemóveis. Como Jack Watling salientou, “as armas não tripuladas ainda estão centradas nas pessoas”.

JE