Oportunidades e desafios no ensino das ciências militares face aos novos contextos tecnológicos

Capitão Diogo Silva

Introdução

Os novos contextos tecnológicos criam também novas oportunidades e desafios para a defesa. Este documento apresenta algumas considerações sobre estas oportunidades e desafios no largo espectro de operações militares, desde os vários domínios de operação e a sua interação, a detalhes acerca de duas tendências tecnológicas em particular (de entre muitas que poderiam ser escolhidas): autonomia e digitalização das operações para o ciberespaço. Estas considerações servirão como base para discutir os desafios que estes contextos levantam ao nível do ensino e formação das ciências militares.

Domínios de operação

Figure 1: Domínios de operação no séc. XX.

No século XIX, os domínios de operação militar estavam limitados apenas a 2: terrestre e marítimo. O século passado, com incríveis novas invenções, viu o nascer e rápido desenvolvimento de novos domínios: ar, espaço (e, de forma embrionário, o ciberespaço). Em cada um dos domínios, surgiram inúmeras tecnologias que permitiram não só um maior leque de acções possíveis, como também um acelerar na velocidade das operações militares.

Contudo, a crescente produção e consumo de dados, habilitados por melhores tecnologias digitais e de comunicação que permitem um conhecimento situacional claro e detalhado, também requerem uma maior integração entre domínios.

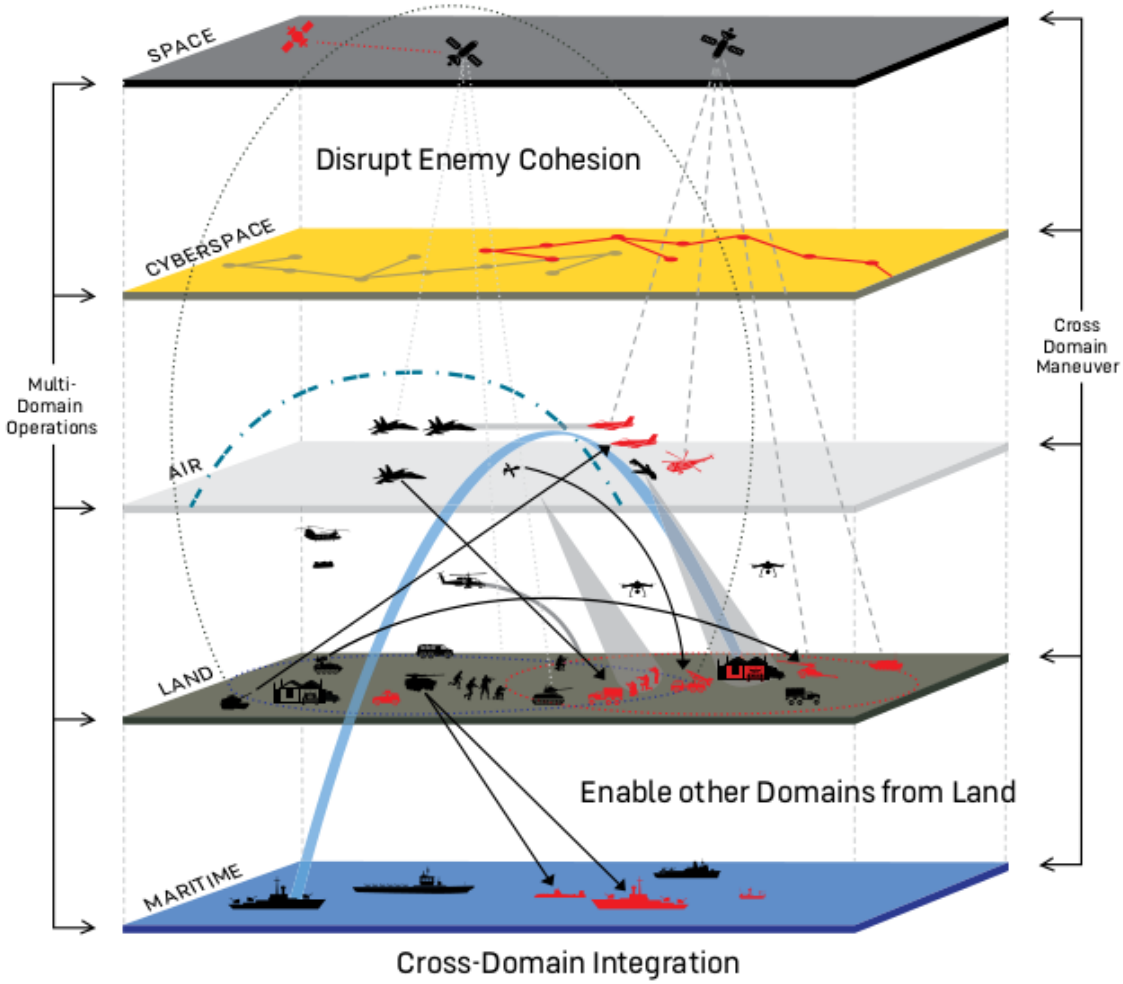
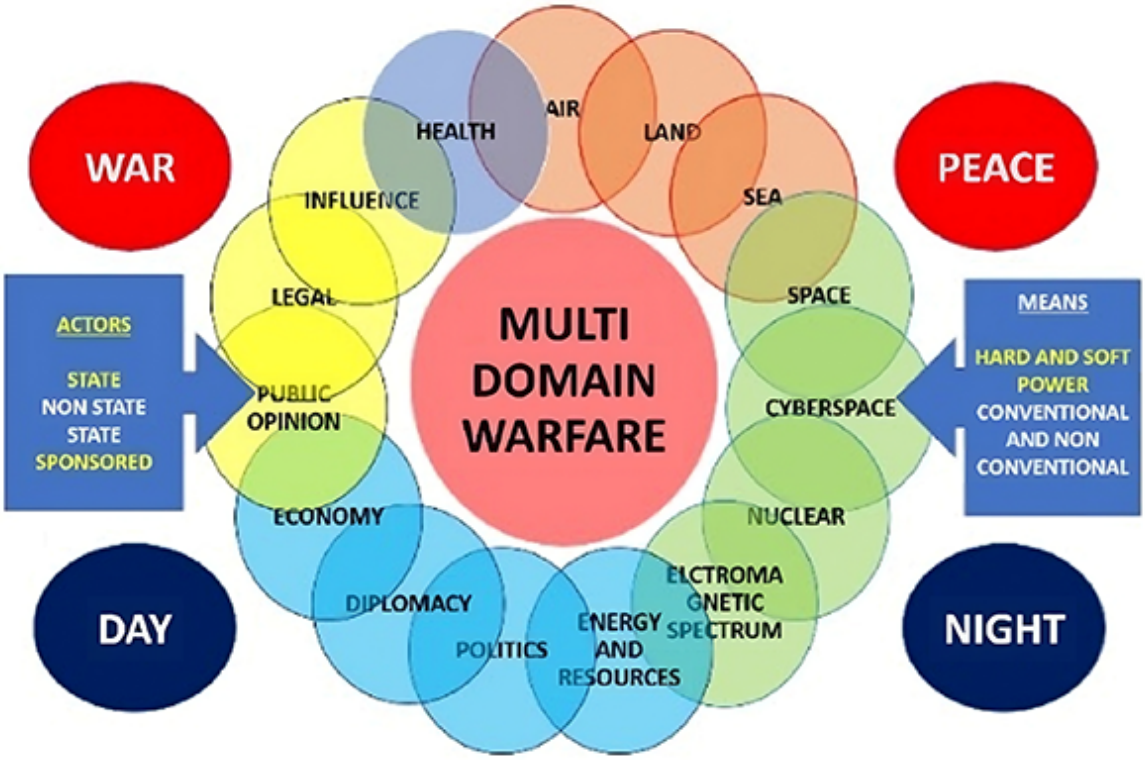


Figure 2: Modernizing how we fight [1]

[1]Modernization — Modernizing how we fight: Future combat will require a different approach than what the Joint Force has previously taken. Multi-Domain Operations (MDO) will enable the Army to give the


WAR
PEACE
ACTORS
STATE
NON STATE
STATE
SPONSORED
MEANS
HARD AND SOFT
POWER
CONVENTIONAL
AND NON
CONVENTIONAL
MULTI
DOMAIN
WARFARE
AIR
HEALTH
LAND
INFLUENCE
SEA
LEGAL
SPACE
PUBLIC
OPINION
CYBERSPACE
ECONOMY
NUCLEAR
ELCTROMA
GNETIC
SPECTRUM
DIPLOMACY
ENERGY
AND
RESOURCES
POLITICS
DAY
NIGHT

Hoje, falamos em operações multi-domínio, com acções paralelas, sincronizadas e em simultâneo em distintos domínios de operação, com objetivos táticos diferentes mas convergentes ao mesmo objetivo operacional.

Os domínios aqui apresentados são, contudo, apenas a ponta do icebergue. Todos os domínios estão em contacto com as dimensões humana, legal, cultural, política, opinião pública, etc. A nossa noção de defesa, para que esta cumpra o seu propósito, tem de crescer além do que eram os grandes chavões e faróis do passado.

Autonomia

A adoção de autonomia nos processos é uma tendência que tem vindo a ser acelerada. Podem ser identificadas duas categorias distintas: informação e robótica.

Por **autonomia na informação**, refiro-me a autonomia aplicada a dados, sem estar necessariamente encorpada, nem interagindo com sistemas físicos. Alguns exemplos passam pelo processamento de dados, com o intuito de extração de informação para os sistemas de decisão. Apesar de os novos contextos operacionais colocarem à nossa disposição uma quantidade de fontes de dados sem precedentes, estes dados não se traduzem imediatamente em contribuições úteis para os sistemas de decisão.

Se no passado o grande esforço para transformar os dados em informação útil estava sob a responsabilidade de humanos (analistas, decisores, comandantes, etc.), hoje nenhum humano consegue acompanhar, em tempo útil, o ritmo e volume de dados produzidos. É necessário, portanto, garantir que colocamos a tecnologia ao serviço de um problema que ela mesma criou (e isto é outra tendência só por si), e criar mecanismos para a **análise automática de dados**. A análise estatística sempre teve um lugar nas caixas de ferramentas dos analistas, mas hoje, com a emergência de novas capacidades dos sistemas de aprendizagem automática e inteligência artificial (IA), um novo leque de possibilidades foi aberto, e temos de tirar partido dele.

Paralelamente, a autonomia tem vindo a ter cada vez mais expressão em domínios encorpados, onde **sistemas robóticos** fazem cada vez mais e melhor. Este sistemas autónomos podem dar uma grande contribuição numa tipologia de missões especifica - as chamadas **missões DDD** (*dull*, *dirty*, *dangerous*):

- missões aborrecidas (*dull*) são as que envolvem tarefas monótonas e repetitivas, e.g.patrulhamento marítimo, onde é necessário foco prolongado no tempo;

Joint Force a decisive advantage by forcing an enemy to confront multiple threats simultaneously from multiple domains. The MDO concept guides our entire modernization effort, describing the capabilities we need to compete and win on the future battlefield. –US Army (2020) AMERICA'S ARMY: READY NOW,INVESTING IN THE FUTURE FY19-21 accomplishments and investment plan

- missões "sujas" (*dirty*) referem-se a operações em ambientes não adequados para humanos, e.g. áreas radioativas;
- missões perigosas (*dangerous*) são as que apresentam um risco à nossa integridade, e.g. operar em ambiente hostil.

Desta forma, estes sistemas permitem, por um lado, otimizar eficiência, e por outro minorar o risco colocado aos recursos humanos. Uma maior integração e complementaridade homem-máquina, visando uma operação mista e resiliente, tira partido dos pontos fortes de cada um, enquanto se colmata as suas vulnerabilidades.

E as capacidades avançadas que estes sistemas robóticos apresentem, cada vez mais frequentemente, já não estão apenas ao alcance de organizações e empresas com grande capacidade de investimento. Muito pelo contrário, a disseminação livre do conhecimento e aos baixos custos permitidos pela globalização garantiram a **democratização de tecnologias de autonomia**, e é atualmente possível comprar sistemas aéreos com funcionalidades de autonomia nos locais mais banais, comercializados como bens de consumo eletrónicos, ou até brinquedos. Estes sistemas podem ser adquiridos por qualquer pessoa, sem identificação, formação específica ou compromisso nos limites à sua utilização. E estes sistemas comerciais de baixo custo podem ser facilmente armados e utilizados em contextos operacionais, precisamente o que está a acontecer na guerra da Ucrânia.

Adicionalmente, está ao alcance do cidadão comum, sem conhecimentos técnicos avançados, construir um destes sistemas seguindo tutoriais simples e de livre acesso, usando componentes de baixo custo e facilmente adquiridos. Estes mesmos sistemas de baixo custo podem ser programados e dotados de maior capacidade de autonomia por indivíduos com maior capacidade técnica, não sendo contudo necessário o investimento de milhões e o envolvimento de largas equipas de engenheiros como tradicionalmente acontece no complexo militar-industrial.

Integração no ciberespaço

A vida no ciberespaço é, cada vez mais, uma realidade. Uma boa parte da população conduz, pelo menos parcialmente, a sua vida (profissional e pessoal) neste novo espaço sem fronteiras. As transformações digitais, que são cada vez mais pedidas e bem-vindas, trazem consigo uma nova vaga de eficiência e novas possibilidades, mas também novos riscos, ameaças e desafios.

No cerne desta transformação está a informação. O ciberespaço é, resumidamente e de forma simplificada, informação em fluxo. Por esta razão, é crucial ver **informação como um *asset* militar**. É a produção e trânsito de informação que permitiu aumentar a eficiência em cada um dos domínios de operação. Também é a informação que permite uma integração transversal dos domínios, florindo em operações multi-domínio. Por estas razões (entre muitas outras), a informação tem de ser vista como um bem essencial a usar e defender de forma estratégica, no planeamento das operações e na sua execução.

O seu papel determinante na sociedade significa que temos de garantir a **supremacia no ciberespaço**, tal como percebemos a importância de garantir a supremacia aérea quando o domínio do ar tomou expressão nas operações militares. Isto traduz-se pela nossa habilidade em ter acesso e poder usar o ciberespaço para os interesses nacionais. Mas também significa que, idealmente, conseguimos projetar o nosso poder cibernético para acções ofensivas, em caso de necessidade.

Existem, contudo, riscos e ameaças emergentes. A autonomia já foi discutida, mas merece especial menção nesta aplicação particular. Estamos, ainda, numa fase de assimilar o impacto que tecnologias avançadas, mas de fácil acesso, como o ChatGPT têm na nossa sociedade, nas mais variadas áreas. Não obstante, o progresso não pára, e hoje já temos os ChatGPTs dos criminosos[2], que facilitam e ajudam a automatizar o processo de criação de software malicioso, campanhas de cibercrime, entre outros. Esta é uma tendência que não se irá reverter, dada a ubiquidade e baixa barreira de entrada para utilização deste tipo de ferramentas. Pelas mesmas razões, as nossas cadeias de ciberdefesa devem, também, integrar cada vez mais mecanismos de automação para monitorização e análise de ataques e ameaças, identificação de falhas de segurança e geração de propostas de reparação, entre outras tarefas que fazem parte do quotidiano dos profissionais e investigadores da área.

A outra ameaça é a computação quântica. O tipo de computadores que irá permitir a aplicação útil deste tipo de computação está cada vez mais perto de ser conseguido. Vários grupos no mundo competem para o desenvolvimento do primeiro computador quântico com uma dimensão suficiente para aplicações práticas. Estes computadores apresentam-se como uma ameaça séria para uma grande variedade de tipos de criptografia[3], que são amplamente usados, tanto em contextos civis como militares.

Tangentes: geopolítica e ética

Ligado a tudo o que foi anteriormente descrito estão duas dimensões importantes: considerações geopolíticas na defesa e ética. À medida que estamos, todos nós, cada vez mais integrados (e dependentes) de novas e mais avançadas tecnologias, frequentemente integradas no ciberespaço, torna-se crucial para as nações garantirem o acesso e produção dos materiais e equipamentos que possibilitam os novos contextos tecnológicos, e tomam uma importância estratégica em inúmeras facetas da sociedade. Não será, portanto, surpresa quando observamos que estas mesmas tecnologias têm, também, cada mais vez influência nas decisões e orientações geopolíticas. A título de exemplo, a importação de semicondutores na China é superior à de petróleo [4]. E o discurso corrente sobre inteligência artificial, por exemplo, é semelhante a

[2]https://www.wired.co.uk/article/chatgpt-scams-fraudgpt-wormgpt-crime
[3]https://www.techtarget.com/searchdatacenter/feature/Explore-the-impact-of-quantum-computing-on-cryptography
[4]Miller, C. (2022). Chip War: The Fight for the World's Most Critical Technology

outro momento no nosso passado não muito distante: a corrida ao espaço [5] E dada a natureza multidisciplinar, pervasiva e disruptiva, este tipo de discurso não é surpreendente.

E se, por um lado, estamos a fazer rápidos e frequentes avanços no nosso desenvolvimento tecnológico, estes têm de ser acompanhados avanços paralelos acerca do seu uso justo, legal e ético. As forças armadas e organizações securitárias, como operadoras destas novas ferramentas e utilizadores de novos domínios como o ciberespaço, têm de se perguntar o que podem ou não fazer, o que é legal, o que é correto e alinhado com os nossos valores culturais e principios constitucionais. Num espaço sem fronteiras como o ciberespaço, onde o anonimato é fácil e a atribuição de ações é difícil, considerações desta natureza são difícieis. E ao contrário de outras áreas de operação militar, onde as linhas do que é correto e legal estão bem desenhadas, nos novos contextos tecnológicos estas linhas são pálidas e pouco claras. E isto reflete-se na Lei Humanitária Internacional, são necessárias novas adições para regular e limitar o espectro de acção nos novos domínios, e com as novas ferramentas.

Recentemente, as considerações legais sobre o uso de IA têm borbulhado na percepção pública, em resposta a variadas situações, onde o plágio nas escolas e o uso legal de informação pública nos treinos destes sistemas são apenas dois exemplos. Também aqui a resposta é variada, mostrando a clara falta de consenso no plano internacional, desde a proibição por um lado (como no caso da Itália[6]) até à legalização do uso de quaisquer dados, independentemente de direitos de autor, para o treino destes sistemas (como o Japão[7] fez). Mas o uso destas tecnologias em situações críticas, onde a vida e morte estão em jogo, toma, naturalmente, uma importância acrescida. Sistemas de armas autónomos letais podem apresentar enormes vantagens táticas na condução da guerra, mas muitas questões não têm respostas claras. De quem é a responsabilidade quando o sistema erra nas suas decisões? Como é que estes sistemas influenciam a nossa forma de pensar sobre a guerra? Tornar-se-á mais frequente? Mais ou menos humana? O Secretário-Geral da ONU e o Presidente do Comité Internacional da Cruz Vermelha já fizeram um apelo conjunto[8] à proibição deste tipo de armas.

Ensino

Dado o contexto (admitidamente reduzido e limitado à brevidade esperada do documento), estamos agora numa melhor posição para discutir o ensino das ciências militares. Num mundo

[5] John R. Allen and Amir Husain, "The Next Space Race Is Artificial Intelligence", Foreign Policy Magazine, https://foreignpolicy.com/2017/11/03/the-next-space-race-is-artificial-intelligence-and-america-is-losing-to-china/

[6] https://www.bbc.com/news/technology-65139406

[7] https://petapixel.com/2023/06/05/japan-declares-ai-training-data-fair-game-and-will-not-enforce-copyright/

[8] https://www.icrc.org/en/document/joint-call-un-and-icrc-establish-prohibitions-and-restrictions-autonomous-weapons-systems

em permanente, e acelerada, mudança, quais serão as bases para a formação dos nossos militares, quer os que estão a ser preparados para iniciar a carreira, como os que estão a ter formação ao longo da vida?

> "Education should **prepare** young people **for jobs that do not yet exist**, using **technologies that have not yet been invented**, to solve **problems of which we are not yet aware**" - Richard Riley

Nesta nova realidade incerta e dinâmica, temos de preparar os nossos militares e civis ligados à defesa (e não só) para trabalhos e funções que ainda não existem, usando tecnologias que ainda não foram inventadas para resolver problemas dos quais não estamos cientes. Este é o desafio avassalador que os docentes e decisores ligados ao ensino enfrentam. Perante tamanho desafio, contudo, a melhor estratégia será partir o problema e tentar conquistar cada uma das partes - ou pelo menos dar passos (eventualmente tímidos) nessa direção. Essas partes vão ser:

- o que sabemos
- o que sabemos que não sabemos
- o que não sabemos que não sabemos

O que sabemos é a nossa zona de conforto. É nesta zona que reside o nosso maior contributo como elementos dos processos de ensino e formação. O que podemos fazer aqui é refazer os currículos (cientes que o ritmo de progresso é superior aos dos ciclos de estudos), retirando o que deixou de ter expressão nas nossas operações e acrescentando novos elementos da realidade que enfrentamos, Haverão, naturalmente, conteúdos que são intemporais, dada a sua faceta elementar e transversal. É, contudo, uma ilusão pensar que esses conteúdos não devem ser recontextualizados face ao constante progresso que vivemos. Conhecimentos e competências intemporais só o são se forem aplicáveis em qualquer tempo.

O que sabemos que não sabemos é o que está no horizonte. São as inovações e descobertas que já esperamos, e até contemplamos os novos usos e desafios que trazem. O mais importante que aqui podemos fazer é o investimento na investigação. Só assim podemos dar passos em direção a este horizonte que já imaginamos. Simultaneamente, esta noção do que ainda não existe mas está para vir deve ser passada ao pessoal em formação, o que só é possível se for garantido o investimento nos próprios docentes, permitindo uma frequente atualização do seu conhecimento.

O que não sabemos que não sabemos é o que está além do horizonte. É o que não imaginamos ou adivinhamos. É o que aparecerá de surpresa. A aposta, aqui, passa pelo desenvolvimento de competências transversais. Competências que dotam as pessoas com a capacidade de analisar e decompor problemas complexos em ambientes dinâmicos, entre outras. Adicionalmente, e discutivelmente mais importante, é o incutir de um espírito autodidata. Devemos estar cientes, e aceitar, que qualquer oferta formativa que desenhamos, por mais bem pensada que tenha sido, será invariavelmente insuficiente para preparar os militares para realidades que estão, hoje, além da nossa imaginação, e que apresentarão certamente novos e

complexos desafios à defesa. Esta mensagem deve ser passada aos formandos e discentes, de forma forte e clara, sublinhando a necessidade de estar alerta para o constante desenrolar de novos acontecimentos e descobertas que ocorrem no quotidiano. Em todo o momento, o militar contrastará os novos contextos científicos, tecnológicos, sociais, políticos, económicos, com os atuais esforços no âmbito securitário e da defesa, levando-o a uma análise das oportunidades e riscos que nos enfrentam, e alimentando a nossa capacidade de planeamento, acção e reacção aos vários níveis estratégico, operacional e tático.