Soberania Tecnológica: o Exemplo da Ucrânia

António Eugénio
Assessor de Estudos do IDN. Coronel da Força Aérea Portuguesa. Mestre em Gestão de Sistemas de Informação pelo ISEG.

Resumo

Este artigo aborda as alterações tecnológicas evidentes na Guerra da Ucrânia e que permitiram a manutenção da soberania ucraniana perante o assalto russo desencadeado a 24 de fevereiro de 2022. As principais tecnologias necessárias à resiliência do Estado e da sociedade, como um todo, são essencialmente digitais e exploram os novos domínios de confrontação, designadamente o espaço e o ciberespaço. Por outro lado, potenciam as capacidades de alguns sistemas tradicionais, numa ligação em rede entre os diversos setores da governação, da sociedade civil, da diáspora e do voluntariado, sendo observadas implicações nos diferentes níveis de decisão, nomeadamente político, estratégico, operacional e tático. As primeiras lições deste conflito remetem para a necessidade de uma reflexão profunda sobre as dependências externas e interdependências internas relativas às tecnologias emergentes, em especial no que concerne às indústrias de defesa nacionais, último reduto da soberania.

Palavras-chave: Ucrânia, Guerra, Tecnologia, Soberania, Rússia, Digital.

Abstract
Technological Sovereignty: the Example of Ukraine

This article explores the technological changes already evident in the Ukraine War that allowed the maintenance of Ukrainian sovereignty in the face of the full-scale Russian invasion unleashed on February 24, 2022. The bulk of the technologies needed for the resilience of the state and society as a whole is essentially digital and exploits the new domains of confrontation, namely space and cyberspace. Additionally, those technologies leverage the capabilities of certain traditional systems, networking the government, civil society, the diaspora and volunteers, across different levels of decision-making, specifically political, strategic, operational and tactical. The first lessons of this conflict appeal for a thorough consideration on the external dependencies and internal interdependencies related to emerging technologies, especially concerning the national defense industries, the last stronghold of sovereignty.

Keywords: *Ukraine, War, Technology, Sovereignty, Russia, Digital*.

Artigo recebido: 29.05.2023
Aprovado: 22.06.2023
https://doi.org/10.47906/ND2023.165.04

"The power of advanced algorithmic warfare systems is now so great that it equates to having tactical nuclear weapons against an adversary with only conventional ones."
Alex Karp, Presidente do Conselho de Administração da Palantir.

Introdução

A guerra na Ucrânia, desencadeada pela invasão plena da Rússia em 24 de fevereiro de 2022, é o mais grave conflito armado entre Estados a seguir à Segunda Guerra Mundial. Pelo seu impacto à escala global, oferece, desde já, uma oportunidade para o estudo de determinados fatores associados ao fenómeno dos conflitos armados. Neste artigo, concentraremos a nossa atenção num conjunto de tecnologias habitualmente designadas como emergentes. Por tecnologias emergentes, entendemos os avanços tecnológicos que se encontram em desenvolvimento e que apresentam o potencial para destronar uma tecnologia atual ou alterar atividades, organizações e culturas. A OTAN define-as como tecnologias ou descobertas científicas das quais se espera que alcancem a maturidade nos próximos vinte anos, que não sejam de uso alargado ou cujos efeitos para a defesa da Aliança não sejam completamente claros[1]. Pretendemos explorar o contributo que um conjunto de tecnologias teve na resiliência da Ucrânia e suscitar uma reflexão mais aprofundada sobre estas questões no âmbito da defesa nacional. Especulamos sobre a possibilidade de uma sociedade em rede, que mistura sistemas legados com outros mais avançados, estar em melhores condições para enfrentar um assalto de um país cujo aparelho militar resulta de uma era industrial e com sistemas de decisão fortemente centralizados. Como veremos, a explicação da resiliência ucraniana ao ataque russo poderá estar na capacidade de interligação em rede de diferentes componentes da sociedade, permitindo uma consciência situacional superior à desenvolvida pelos russos; isto devido ao acesso que têm a um leque alargado de tecnologias otimizadas para processar informação que potencia a decisão descentralizada e oportuna a todos os envolvidos. A abordagem do tema será feita de forma ilustrativa e para os diferentes níveis de decisão.
Esta introdução incide na possibilidade de a Guerra da Ucrânia poder ser um conflito formativo de uma nova ordem mundial, de cujo desenlace poderá resultar o reforço da liderança mundial do Ocidente ou um pendor para a afirmação das autocracias reunidas em torno da China. Como antecedente próximo da incorporação tecnológica ucraniana, indicaremos a transformação digital iniciada no consulado do presidente ucraniano Volodymyr Zelensky, em 2019, cuja política, resumida no conceito de um "Estado como um serviço" e no lema "Um Estado num *Smartphone*!", permitiu aproveitar todas as vantagens de uma sociedade em rede e iniciar um conjunto de

1 https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

reformas valorizadas por muitos setores. No nível político de decisão, apontaremos o fornecimento contingente do serviço de Internet de banda larga por satélite e a migração das bases de dados do Estado para os serviços de "nuvem", como fulcrais para a manutenção da soberania política da Ucrânia, pelo contributo que deram para a continuidade do funcionamento dos serviços oficiais perante o ataque físico, cibernético e informacional russo, assim como a implementação de uma plataforma de inovação tecnológica para a área da defesa, como último reduto de sustentação da autonomia estratégica. No nível estratégico, destacamos o setor do espaço e as técnicas de inteligência artificial que permitiram a ação flanqueadora da Ucrânia perante o assalto russo com ferramentas tecnológicas avançadas. No plano operacional, salientam-se os sistemas que permitem alcançar uma consciência situacional alargada pelo uso, também, da inteligência artificial e da aprendizagem algorítmica (*machine learning*). No que se refere ao nível tático, sobressaem os sistemas de decisão aplicados pelas unidades de baixo escalão clássicas, como a artilharia, apoiadas por sistemas de obtenção de alvos próximos, informação de tiro e *drones* aéreos e navais, evidenciando a mescla entre sistemas legados e emergentes. Por fim, faremos uma referência ao apoio da diáspora e do voluntariado, tornado possível pelas novas tecnologias.

Desde os primórdios da Humanidade que o domínio de determinadas tecnologias está associado ao desenvolvimento e à segurança. Nos últimos quinhentos anos, sucessivas revoluções tecnológicas têm propiciado alterações significativas no crescimento económico dos Estados, assim como na sua capacidade para projetar poder para fora das suas fronteiras ou reagir a ameaças e riscos contra o seu território. Foi a competência de interligação de tecnologias relacionadas com os negócios e com o armamento que permitiu a alguns Estados alcançarem uma projeção global. Começando com Portugal, seguido pelos Países Baixos, Reino Unido e, mais recentemente, pelos Estados Unidos, observam-se ciclos de liderança dos assuntos mundiais, explicados pela coevolução de conhecimentos científicos aplicados no comércio e nos assuntos militares. Estudiosos destes temas associaram a inovação em setores-chave da economia a ciclos longos de crescimento, que depois permitem a um Estado afirmar-se na liderança política dos assuntos globais[2]. Por outro lado, durante os períodos de guerra parece haver uma aceleração na inovação em determinados conglomerados industriais que poderão gerar alterações substanciais na economia e na sociedade nos períodos subsequentes, significando, por vezes, modificações estruturais no paradigma socio-tecnológico dos Estados envolvidos[3].

2 Cf. Modelski, G. e Thompson, W., 1996. *Leading Sectors and World Powers*. University of South Carolina Press.

3 Cf. Coccia, M., 2017. 'The Relation between War, General Purpose Technologies and Dynamics of K-Waves for Technological, Economic and Social Change', disponível em https://ssrn.com/abstract=2951279

A guerra na Ucrânia parece estar destinada a um particular destaque na reversão do processo de globalização, até aqui liderado pelos Estados Unidos da América e seus aliados. A ação militar russa e a afirmação da China como potência económica global e dominante em setores tecnológicos avançados (37 em 44 possíveis[4]) podem fazer emergir um sistema internacional assente em blocos de países com contornos mais evidentes, incluindo a formação de uma aliança anti-hegemónica tutelada por países autocráticos com forte pendor antiocidental. A situação geopolítica mundial é de novo caracterizada por uma corrida armamentista que tem na Ucrânia um laboratório em tempo real[5]. A "auditoria" da guerra é implacável: ganha quem melhor se adapta às circunstâncias do combate. Tratando-se de uma guerra convencional entre dois Estados, como se julgava já ser impossível de conceber, todos os recursos da Ucrânia[6] foram mobilizados para a sua defesa existencial. O Estado que melhor se está a adaptar, para já, às circunstâncias do combate moderno, é a Ucrânia. E grande parte da vantagem adquirida diz respeito à gestão e aplicação de novas tecnologias, quer na abordagem governamental – necessariamente interministerial, mas com um foco específico na transformação digital com extensão à área da defesa –, quer na ativação do planeamento civil de emergência, quer ainda na organização da resistência por atores privados e voluntários civis. É um caso evidente de integridade das políticas de defesa, dado abrangerem toda a sociedade e todo o governo. O combate centra-se atualmente na disputa pela superioridade tecnológica em apoio à decisão informada, por pessoas e por máquinas. A Ucrânia poderá emergir desta guerra como uma potência digital e as suas forças armadas como as mais fortes de toda a Europa. O seu exemplo está a ser estudado por muitos países e por muitas organizações internacionais. Este texto resulta da consulta a fontes abertas e a análise é efetuada segundo os diferentes níveis: político, estratégico, operacional e tático, além de fazer uma referência à diáspora ucraniana e ao voluntariado.

Antecedentes

Para melhor compreendermos o contexto que conduziu ao uso alargado de novas tecnologias na Guerra da Ucrânia, teremos de regressar ao ano de 2019. Nesse ano, houve eleições presidenciais e quem as ganhou foi Volodymyr Zelensky, que iniciou uma liderança pós-pós-soviética, rompendo com três décadas de liderança oligárquica manietada pelo Kremlin. A campanha eleitoral que o elegeu foi essencialmente

4 Cf. https://techtracker.aspi.org.au/our-report/

5 https://www.militarytimes.com/news/2022/09/21use-us-for-combat-zone-tests-ukraine-minister-tells-us-war-industry/

6 Unidade política com a maior área territorial exclusivamente na Europa, com mais de 600.000 km^2.

virtual, sem comícios, sem debates, sem entrevistas de fundo, ainda que apoiada na série de televisão que o fez famoso, "Servo do Povo", emitida pelo canal de televisão 1+1, dominado pelo oligarca Igor Kolomoyskyi (a quem foi retirada a nacionalidade ucraniana, no ano passado, por pressão dos EUA[7]). Os resultados da segunda volta das presidenciais diluíram praticamente as divisões internas de anteriores eleições e atribuíram uma enorme legitimidade a um presidente improvável, com uma agenda disruptiva.

Quem dirigiu a campanha digital foi Mykhailo Fedorov, um empreendedor, cujo estúdio, SMM[8], de Zaporizhia, tinha Zelensky como cliente. A campanha foi marcada por uma rutura completa em termos de metodologia e de mensagem face a outras. Foi conduzida, essencialmente, em redes sociais utilizadas pelos eleitores mais jovens (Telegram e Instagram), tendo sido lançada uma ambiciosa estratégia de transformação digital do país, inspirada nos países bálticos.

Aos 28 anos, Mykhailo Fedorov foi empossado como vice-primeiro-ministro e ministro da Transformação Digital da Ucrânia, e mandatado para implementar o lema do novo presidente: "Um Estado num *Smartphone*"[9]. Este programa pretende transformar a Ucrânia no Estado mais conveniente e acessível do mundo, tornando, assim, o Estado num serviço, como uma aplicação comercial, diminuindo a burocracia e aumentando a transparência e a acessibilidade.

Mykhailo Fedorov foi considerado pelo periódico "The Politico" como "Nº 1 Rule-breaker" no Tech 28 Ranking – Class of 2022[10] e passou pela Web Summit, em Lisboa, em novembro de 2022[11]. Em março deste ano, viu as suas competências serem alargadas pelo parlamento ucraniano, ao ser empossado como vice-primeiro-ministro da Inovação, Desenvolvimento da Educação, Ciência e Tecnologia[12].

Fundamental para a implementação da visão do "Estado num *Smartphone*" tem sido o portal de governo eletrónico e a aplicação móvel *Diia*[13] (que quer dizer "ação" e é também um acrónimo ucraniano para "O Estado e Eu"). Esta solução alberga um autêntico ecossistema digital, que vai desde a carteira eletrónica e serviços oficiais até ao apoio à formação de seis milhões de ucranianos em literacia digital, tendo em vista a digitalização e acessibilidade completa aos serviços do Estado. Outro objetivo é que o setor das tecnologias de informação alcance os 10% do PIB e que a cobertura de Internet de banda larga atinja 95% do território ucraniano. Os cidadãos

7 https://observador.pt/2022/07/24/zelensky-tera-retirado-cidadania-ucraniana-a-um-dos-o-ligarcas-mais-poderosos-do-pais/
8 https://smmstudio.com/en/target-en/
9 https://www.president.gov.ua/en/news/ya-mriyu-pro-derzhavu-u-smartfoni-volodimir-zelenskij-55585
10 https://www.politico.eu/tech-28-2022/
11 A sua comunicação está disponível no YouTube: https://www.youtube.com/watch?v=Dxa8M8MttLE
12 https://www.pravda.com.ua/news/2023/03/21/7394383/
13 https://diia.gov.ua/

podem, assim, usar o seu passaporte digital (primeiro país do mundo a fazê-lo), a par de outros documentos, receber pensões, aceder a registos e outras funcionalidades de governo eletrónico. A sua popularidade é evidente pelo número de utilizadores (cerca de 50% da população ucraniana residente) e o grau de satisfação, de 95%, com o serviço.

Após a invasão plena pela Rússia, em fevereiro do ano passado, novos serviços foram rapidamente acrescentados, como o relato de danos provocados pelos ataques, recebimento de indemnizações por danos provocados pela guerra, acesso aos serviços do Estado por deslocados, incluindo o registo de bebés, e até fazer o relato da presença de forças russas, enviando fotografias e vídeos usando a aplicação eVorog[14] ("eInimigo").

A implementação da reforma digital ucraniana foi apoiada por diversas entidades externas, nomeadamente americanas, britânicas, suíças e da União Europeia (Programa EGOV4UKRAINE)[15]. Portanto, e apesar da guerra, ou talvez por causa dela, o setor das tecnologias de informação ofereceu uma aceleração ao processo de transformação digital, permitindo à Ucrânia evidenciar uma resiliência perante o ataque russo que muitos julgavam ser impossível.

Nível Político

A manutenção da soberania política da Ucrânia muito deve ao apoio da infraestrutura tecnológica das *Big Tech* americanas. Desde logo, a Starlink[16] da Space X, que ofereceu uma alternativa de comunicações por satélite em substituição da rede da Viasat[17] (também uma empresa de comunicações por satélite americana) que foi vítima de um ataque cibernético bem-sucedido, horas antes da invasão por parte da Rússia[18], e que era fundamental para o comando e controlo das forças ucranianas.

Dois dias depois deste ataque, Mykhailo Fedorov publicava um *tweet* que ficou famoso, em que provocava Elon Musk estabelecendo um paralelismo entre a colonização de Marte e a invasão russa, e entre os foguetes dele e os russos que caíam em alvos civis na Ucrânia. Musk respondeu imediatamente no Twitter e em termos práticos. Foram reorientados 50 satélites da constelação Starlink e enviados

14 https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters

15 https://eufordigital.eu/discover-eu/egov4ukraine/

16 Uma constelação de mais de 3.200 satélites que garante serviços de Internet de banda larga. https://www.starlink.com/

17 https://www.viasat.com/

18 https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/

5.000 terminais para a Ucrânia (75% doados pelo próprio Musk e 25% comprados pela US AID[19]).

Atualmente, a Ucrânia dispõe de cerca de 25.000 terminais no seu território. A rede Starlink tem provado ser mais resiliente aos ataques cibernéticos russos e tem permitido o fornecimento de serviços de Internet em toda a Ucrânia, incluindo nas zonas ocupadas, possibilitando o contacto entre familiares dispersos e o acesso a notícias não censuradas pela Rússia. Tornou possível, ainda, o comando e controlo das forças armadas, pela utilização de comunicações cifradas que possibilitam inclusive o controlo de *drones*. Embora envoltas em polémica devido às restrições impostas por Elon Musk acerca da cobertura da Crimeia, em outubro de 2022[20], e do reforço sobre o seu uso civil, que terá afetado a sua utilização para o controlo de *drones*, em fevereiro deste ano, este tipo de constelações são consideradas de tal modo importantes que a China está a considerar o lançamento da sua própria rede, com receio que a Starlink, ou outra rede semelhante, possa ser implementada sobre Taiwan[21].

Uma das formas mais significativas de resiliência, que a maior parte das empresas já leva em consideração, é a designada continuidade de serviços. Os planos para a sua garantia tornaram-se imprescindíveis após o 11 de setembro de 2001, que demonstrou a vulnerabilidade dos dados essenciais aos negócios numa circunstância de destruição física. O mesmo pode ser dito no que respeita a um Estado. Com a progressiva digitalização dos serviços do Estado, torna-se fundamental incorporar as bases de dados nos planos de proteção de infraestruturas críticas, pois serão elas que permitirão a continuidade de funcionamento dos serviços essenciais ao cidadão. Perante o ataque russo à Ucrânia, nas formas cibernética e cinética, e a ameaça de se perder uma quantidade significativa de dados da Administração Pública, houve necessidade de transferi-los para serviços de "nuvem" – para tal, as autoridades ucranianas obtiveram o apoio da Microsoft e da Amazon, entre outras –, tendo sido transferidos 10 petabytes[22] de informação, assegurando, assim, a continuidade dos serviços do Estado, em geral, e dos órgãos de soberania ucraniana, em particular. Também deve ser destacado o apoio da Google na prestação de serviços de cibersegurança, entre outros aspetos[23]. Numa época caracterizada pela digitalização da sociedade, poderemos, então, afirmar que são condições essenciais para a manutenção da soberania de um país a manutenção do acesso à Internet de banda larga e aos serviços de "nuvem", bem como a sua

19 Agência americana de apoio ao desenvolvimento internacional https://www.usaid.gov/

20 https://www.techarp.com/military/elon-musk-blocked-starlink-crimea/

21 https://www.economist.com/china/2023/05/18/why-china-fears-starlink

22 1 PB = 1000000000000000 B = 10^{15} bytes = 1000 terabytes.

23 https://blog.google/outreach-initiatives/public-policy/new-ways-were-supporting-ukraine/

segurança, pois só assim se poderá garantir a continuidade da prestação dos serviços do Estado.

Estes requisitos são necessários, mas não suficientes para a manutenção da soberania de um Estado, dada a sua dependência de entidades externas. Para assegurar uma certa autonomia estratégica, haverá que balancear as dependências externas com as interdependências internas, em termos tecnológicos. Essa autonomia provirá do modo como cada Estado consegue combinar os meios tecnológicos externos e internos em apoio da sua estratégia e, consequentemente, da manutenção de sistemas críticos. Numa altura de mudança de paradigma tecnológico, toda a atenção deve ser colocada na capacidade inovadora das indústrias de defesa nacionais, dado o facto de serem elas o último reduto de soberania nacional por apoiarem a satisfação das necessidades das forças armadas. No entanto, as forças armadas, confrontadas com um extenso rol de tecnologias emergentes, poderão ser tentadas a manter um certo rigor doutrinário na utilização de sistemas legados. Não é o caso das Forças Armadas ucranianas, pois foram motivadas pelo ímpeto da transformação digital promovida pelo governo e desenvolveram uma abertura à experimentação que ilustraremos mais à frente. Aqui tem lugar preponderante a política de inovação de defesa, promovida de um modo interministerial. Para obter sinergias com o programa de transformação digital, foi lançada no passado mês de abril uma plataforma de coordenação da inovação de defesa, designada por Brave 1[24], tendo sido colocada sob a tutela do já referido vice-primeiro-ministro para o Desenvolvimento da Educação, Ciência e Tecnologia e ministro para a Transformação Digital, Mykhailo Fedorov. Esta é uma implementação conjunta entre o Ministério da Defesa, o Estado-Maior-General das Forças Armadas, o Conselho de Segurança e Defesa Nacional, o Ministério das Indústrias Estratégicas e o Ministério da Economia ucranianos, e está desenhada de forma a indicar claramente quais são as prioridades do governo, visando a colaboração de todos os intervenientes da indústria tecnológica de defesa, fornecendo-lhes todo o apoio que necessitam (organizacional, informacional e de financiamento) para o desenvolvimento de projetos na área da defesa.

Nível Estratégico

No nível estratégico, queremos destacar dois setores tecnológicos emergentes, que subiram recentemente a esse patamar: espaço sideral e inteligência artificial. Com efeito, a Guerra da Ucrânia é a primeira em que se verifica uma verdadeira operacionalização militar do domínio espacial, uma vez que ambas as partes dispõem ou têm acesso aos serviços proporcionados por plataformas espaciais. Os contornos dessa

24 https://brave1.gov.ua/en/

operacionalização só agora começam a ser esboçados e apontam para a necessidade fundamental de qualquer Estado assegurar o acesso ao espaço e, em último caso, garantir a exploração resiliente de plataformas espaciais, como forma de projeção da sua soberania, num contexto de "bens comuns globais".

Com um legado que lhe permitiria ser a quarta potência espacial mundial por alturas da sua independência, a Ucrânia tem um passado rico na exploração espacial, com forte envolvimento dos seus nacionais no programa espacial soviético. Além disso, destacava-se um *cluster* de cerca de 130 empresas desse setor na região de Dnipropetrovsk, que era conhecida como *Rocket City*. Aí eram fabricados mísseis intercontinentais balísticos, satélites e motores-foguete, entre outros produtos. No entanto, anos de desinvestimento e o boicote russo (desde logo ao sistema Zenit, ali fabricado, que era suposto substituir o conhecido Soyuz) levaram à decadência do setor do espaço enquanto prioridade ucraniana. Só nos últimos anos foi possível recuperar o rumo do desenvolvimento espacial, havendo produção de diversos componentes para programas espaciais de outros países.

Em 2015, Elon Musk declarou o foguetão Zenit como o seu favorito, logo a seguir aos seus. Diversos programas com países como o Brasil e o Canadá permitiram à Ucrânia marcar ainda mais a sua independência da Rússia. Em janeiro do ano passado, um mês antes do assalto a Kyiv, uma nave Falcon 9 da Space X lançou o primeiro satélite totalmente ucraniano, o Sich-2-30, montado na gigante Yuzhnoye, em Dnipro. Este satélite integra a rede Copernicus de observação da Terra da Agência Espacial Europeia. Em janeiro deste ano, foram lançados, também pela Falcon 9, mais dois satélites ucranianos, incluindo um construído com fundos do Ministério da Educação e Ciência, comemorativo do 30º aniversário da independência da Ucrânia.

Desde 2020, a Ucrânia é também signatária dos acordos Artemis da NASA para exploração da Lua. Com o pedido de adesão expedita da Ucrânia à União Europeia, aumentam as possibilidades deste país vir a integrar a Agência Espacial Europeia.

Como foi referido atrás, a Starlink, pela capacidade de oferecer os serviços de infraestrutura de rede, é talvez a mais relevante de todas as empresas (estrangeiras) que permitem uma resiliência extraordinária ao Estado ucraniano. No entanto, existem outras empresas comerciais, paradigmáticas do designado *New Space*, cujo envolvimento oferece novos desafios ao pensamento estratégico de defesa nacional, demonstrando que a equação para uma defesa eficaz não pode passar sem a sua exploração. São conhecidos os casos da empresa HawkEye 360º[25], na localização do empastelamento do sinal GPS, e das firmas de observação da Terra, no fornecimento de informações relevantes para a decisão estratégica e obtenção de provas para efeitos de processos relacionados com crimes de guerra, como são exemplos

25 https://www.he360.com/

as americanas Maxar[26], Black Sky[27], Planet Labs[28], a canadiana MDA[29], a finlandesa ICEYE[30] e a portuguesa Geosat[31]. Em contraponto, na Rússia, o setor do espaço está em declínio acentuado[32].

O envolvimento destas firmas no conflito da Ucrânia levou um jornal britânico a afirmar, num artigo recente, que a Ucrânia está a flanquear a Rússia com munições das *Big Tech*, que a inteligência artificial está a mudar o conflito moderno e que esta é a verdadeira frente de batalha[33]. Deste modo, umas forças armadas com um potencial de combate tradicional reduzido e que utilizem as modernas técnicas digitais podem exponenciar as suas capacidades, pelo uso que fazem da informação relevante e tempestiva, face a outras forças armadas que usam técnicas analógicas. Parte da superioridade informacional da Ucrânia relativamente à Rússia é alcançada através de um esforço contínuo de fusão de um conglomerado de fontes espaciais e não só. Em redor da Ucrânia, Bielorrússia e Rússia, diversos países ocidentais realizam voos de reconhecimento que fornecem informações sobre o dispositivo russo[34]. De salientar, entre outros, o uso do *drone* americano RQ-4, com uma autonomia de 30 horas, que realiza voos a sul da Crimeia, em espaço aéreo internacional, e que opera a partir da Base Aeronaval de Sigonella, na Sicília. Alguma da informação recolhida é partilhada com as autoridades ucranianas.

No que diz respeito à inteligência artificial, a firma norte-americana Palantir[35] apresenta-se como o paradigma de serviço crítico ao nível estratégico, uma vez que fornece dados suficientemente precisos sobre alvos de oportunidade (*time sensitive targets*). A fusão e exploração da imensidão de dados provenientes do teatro de operações estará (alegadamente) a cargo dessa polémica empresa (que terá estado por trás da localização de Bin Laden e da deteção do escândalo financeiro piramidal de Bernard Madoff), que usa diversos métodos de análise de dados (*big data and analytics*) e aprendizagem algorítmica, podendo ter consequências a todos os níveis de decisão. Consultar a página da plataforma Gotham[36] e Meta Constelation[37], desta empresa, permite-nos conjeturar sobre as potencialidades de apoio à decisão destas técnicas,

26 https://www.maxar.com/
27 https://www.blacksky.com/
28 https://www.planet.com/
29 https://mda.space/en/
30 https://www.iceye.com/
31 https://geosat.space/
32 https://www.wired.com/story/russias-space-program-is-in-big-trouble/
33 https://www.thetimes.co.uk/article/ukraine-is-outflanking-russia-with-ammunition-from-big-tech-lxp6sv3qz
34 https://www.key.aero/article/what-are-nato-isr-aircraft-really-doing-ukraines-border
35 https://www.palantir.com/
36 https://www.palantir.com/platforms/gotham/
37 https://www.palantir.com/offerings/metaconstellation/

e imaginar o que poderá ter acontecido ao navio-almirante da Frota do Mar Negro, o cruzador Moskva, em abril do ano passado. O *software* utiliza imagens de satélite comerciais, sensores térmicos, radar, eletro-óticos, da rede GSM e até da mencionada aplicação eVorog para oferecer sugestões de envolvimento de alvos com uma ordem de grandeza trinta vezes superior aos métodos analógicos.

O presidente da Palantir, Alex Karp, foi o primeiro líder de uma empresa ocidental a visitar a Ucrânia em junho do ano passado, tendo-se reunido com o presidente Zelensky e com o ministro Fedorov[38]. Desde então, muitos outros dirigentes empresariais visitaram Kyiv, incluindo Eric Schmit, ex-CEO da Google, em setembro de 2022[39].

Ainda no nível estratégico, um dos casos mais interessantes para estudo será, porventura, a utilização das novas tecnologias na área das operações de informação e influência. As atividades da designada Internet Research Agency[40], ligada a Yevgeny Prigozhin, chefe do Grupo Wagner, têm vindo a ser expostas por estudos oficiais americanos e pela comunidade de OSINT. Desde 2013, utiliza inteligência artificial e aprendizagem algorítmica para a criação de vídeos *deep fake*, perfis inautênticos e até uma agência noticiosa (Peacedata.net) para produção de conteúdos para diversos meios de comunicação social. Os perfis inautênticos existem em diversas redes sociais para dar maior coerência às personagens, republicam notícias e fazem comentários em matérias fraturantes. Os vídeos *deep fake* visam o descrédito das lideranças ocidentais em geral e da ucraniana em particular. Sites como o StopFAKE.org[41] e o bellingcat[42] têm ajudado a expor as técnicas russas utilizadas neste capítulo. Também neste aspeto a Google tem prestado assistência à Ucrânia, através da monitorização da ameaça e da remoção de milhares de vídeos e canais da plataforma Youtube. Apesar do enorme investimento em inteligência artificial feito pelo governo russo[43], esta é a única evidência em fontes abertas da sua utilização pela Rússia, para além do seu uso em *drones* de reconhecimento e em baterias antiaéreas.

Por aqui se vê que a gestão da informação de um teatro de operações moderno tem consequências estratégicas e que a abrangência e o volume de dados gerados em ciclos de tempo cada vez mais curtos não são compagináveis com o seu tratamento feito apenas por pessoas. Esta guerra algorítmica coloca desafios à soberania dos Estados, uma vez que a maior parte das empresas que dominam estas tecnologias são civis e, como se vê no caso ucraniano, estrangeiras.

38 https://www.defensenews.com/land/2022/06/02/palantirs-karp-is-first-western-ceo-to-visit-zelenskyy-amid-invasion/

39 https://scsp222.substack.com/p/the-first-networked-war-eric-schmidts

40 https://spyscape.com/article/inside-the-troll-factory-russias-internet-research-agency

41 https://www.stopfake.org/ru/glavnaya-2/

42 https://www.bellingcat.com/

43 https://www.cna.org/archive/CNA_Files/centers/cna/sppp/rsp/russia-ai/russia-artificial-intelligence-autonomy-putin-military.pdf

Nível Operacional

Ao nível operacional, podemos situar outro conjunto de tecnologias, também baseadas em inteligência artificial e aprendizagem algorítmica, que têm vindo a ser utilizadas na Ucrânia, por entidades oficiais, por empresas e até por voluntários. São exemplos disso a empresa Clearview[44], que oferece soluções de reconhecimento facial utilizadas nas fronteiras e também em casos de identificação de prisioneiros de guerra e até de cadáveres de soldados russos. É conhecida, também, a utilização dos serviços de escuta, tradução e transcrição de comunicações russas, em tempo real, pela firma Primer[45].

As Forças Armadas ucranianas têm ativo um sistema de consciência situacional designado Delta[46] que integra todos os *inputs* de diversas fontes, num sistema georreferenciado em tempo real, ou quase real, que é utilizado para ataques a alvos de oportunidade e que utiliza ferramentas de previsão, como por exemplo a evolução possível de colunas militares, e que oferece à Forças Armadas ucranianas uma capacidade de envolvimento mais eficaz e oportuno. O sistema foi apresentado num evento designado *Think-Tank for Information Decision and Execution Superiority* (TIDE) *Sprint* no *NATO Allied Command Transformation*, em outubro do ano passado[47].

Outra funcionalidade da georreferenciação diz respeito à localização de telemóveis utilizados por inimigos no campo de batalha. Forças russas fizeram uso alargado destes dispositivos, o que permitiu identificar concentrações de unidades através do acesso à rede GSM. Cruzando com outra informação pertinente, foi possível a revelação da tática russa e, como tal, planear as ações subsequentes. Foi este tipo de ferramentas que esteve na base do ataque mais mortífero de toda a guerra a forças russas, com centenas de mortos, em Makiivka, no início deste ano[48]. Por outro lado, a penetração ucraniana nos telemóveis "Era Cryptophone"[49], utilizados pelos escalões de topo das Forças Armadas russas, assim como a utilização desregrada de telefones comuns, conduziu ao abate de cerca de 40 oficiais de postos superiores, incluindo 12 generais[50].

44 https://www.clearview.ai/.
45 https://primer.ai/ .
46 https://mil.in.ua/en/news/the-defense-forces-of-ukraine-to-introduce-the-delta-system/
47 https://mezha.media/en/2022/10/28/the-unique-ukrainian-situational-awareness-system-delta-was-presented-at-the-annual-nato-event/
48 https://observador.pt/2023/01/05/himars-provocaram-ataque-devastador-em-quartel-russo-veja-as-imagens-da-destruicao-em-makiivka/
49 https://asiatimes.com/2022/05/the-fatal-failure-of-russias-era-cryptophone-system/
50 https://www.businessinsider.com/ukraine-russian-officer-elite-decimated-9-who-were-killed-in-combat-2022-3

Nível Tático

Ao nível tático, mais uma vez, a fusão de informação proveniente de diversas fontes teve consequências em dois campos tecnológicos distintos, um tradicional, a artilharia, e outro emergente, o dos *drones* aéreos e navais. No que respeita à arma estrela da Guerra da Ucrânia, a artilharia, são conhecidas duas aplicações: o GIS ARTA[51] e o Kropyva[52] (que quer dizer urtiga). Ambos os sistemas foram desenvolvidos por utilizadores militares, a partir de calculadores de tiro usados por unidades que combatem na linha da frente desde 2014. Visam aumentar a consciência situacional das unidades no terreno e diminuir o tempo de resposta entre a deteção de alvos e o tiro das baterias. São normalmente descritos como "ubers da artilharia" pela afetação da peça mais bem colocada para o envolvimento de um alvo particular; sendo que encurtaram o tempo de resposta de quinze minutos para menos de um. Existe ainda outro, designado por Virazh Planshet, que é aplicado à artilharia antiaérea e que foi desenvolvido por cientistas militares ucranianos.

Estes sistemas recebem informação de aquisição de alvos proveniente de diversas fontes de informação. A melhor e mais popular é a proveniente de *drones* aéreos. Neste caso, as coordenadas dos alvos são transmitidas em tempo real dos *drones* para as baterias.

No que se refere ao uso de *drones*, esta guerra é a primeira guerra de *drones* entre Estados, uma vez que ambos os lados utilizam um conjunto alargado destes sistemas. Neste âmbito, assume particular relevo o papel de uma organização designada Aerorozvidka[53] (Reconhecimento Aéreo), designada por alguns como uma "*start-up* de guerra". Começou com um comandante de batalhão, em 2014, e alguns entusiastas de tecnologias que começaram por adaptar câmaras GoPro a *drones* comerciais para exploração de unidades de baixo escalão. Cresceram e passaram a integrar os serviços de informações ucranianos. Depois, foram extintos e reativados. Hoje, alguns dos seus elementos integram um centro de experimentação das Forças Armadas ucranianas e a Aerorozvidka apresenta-se como uma organização não governamental (ONG) que promove o uso e a recolha de donativos para o desenvolvimento de plataformas não tripuladas. Algumas delas, como o octocóptero R-18[54], têm capacidade para transportar cargas letais. São inúmeros os *clips* de vídeo obtidos por *drones* de vários tipos que são usados na missão de recolha de informações, reconhecimento, aquisição de objetivos, ataques suicidas e até luta aérea entre *drones*. O seu emprego foi inspirado, em grande parte, na experiência anteriormente obtida na segunda guerra

51 https://gisarta.org/en/

52 https://medium.com/@x_TomCooper_x/kropyva-ukrainian-artillery-application-e5c6161b6c0a

53 https://aerorozvidka.ngo/

54 https://mezha.media/en/2022/04/26/r18-octocopter-from-aerorozvidka-ukrainian-drone-destroying-the-enemy/

do Nagorno-Karabakh, em 2020. Preencheram diversas lacunas sentidas pelas forças em combate e foram rapidamente incorporados nas operações militares.
Entretanto, com o decorrer da guerra, e com os conceitos tradicionais de controlo do ar em questão[55], uma vez que os sistemas antiaéreos de ambos os lados tornavam o uso do espaço aéreo particularmente arriscado, também a Rússia se viu obrigada ao uso intensivo de *drones* aéreos. É bastante significativo que este país seja o segundo maior exportador de grandes sistemas de armas, com 22% do *share* mundial[56], e que tenha de recorrer ao Irão para importar *drones*. Como acontece com qualquer sistema ofensivo, já são evidentes os esforços para contrariar o uso de *drones*. Os sistemas *anti-drone* vão para além da tradicional artilharia antiaérea, cujo uso se revela economicamente desfavorável, face à desproporção de custos entres os *drones* e as munições ou mísseis utilizados para os abater. Uma das firmas que oferece uma resposta a esta ameaça é também americana; trata-se da Dedrone[57].
No capítulo dos *drones* navais, no final de outubro do ano passado, verificou-se um ataque por uma canoa de fibra de carbono, não tripulada, com carga explosiva e remotamente pilotada através da Starlink (portanto, para lá do horizonte), ao porto de Sebastopol, na Crimeia, atingindo novamente o navio-almirante da Frota do Mar Negro, desta feita a fragata Admiral Makarov[58]. Depois do ataque, a sua existência e fabrico tornou-se conhecida e foi lançada uma campanha de angariação de fundos para a sua construção em massa[59]. Cada veículo destes custa cerca de 250.000 dólares e pode ser financiado através da plataforma United 24[60]. Já em maio deste ano, foi revelado mais um *drone* naval submarino, designado Toloka[61], que coloca sérios desafios às plataformas navais tradicionais, assim como às instalações portuárias.

Diáspora e Voluntariado

A diáspora ucraniana tem sido fundamental para o apoio tecnológico externo que a Ucrânia tem recebido.
A vaga de emigração, que se seguiu à independência do país, deu origem a uma geração de especialistas profundamente ligada ao setor tecnológico americano. Esta

55 https://www.airforce-technology.com/features/air-enial-over-supremacy-lessons-from-ukraine/
56 https://www.sipri.org/publications/2023/sipri-fact-sheets/trends-international-arms-transfers-2022
57 https://www.dedrone.com/
58 https://www.theguardian.com/world/2022/oct/30russias-black-sea-flagship-damaged-in-crimea-drone-attack-video-suggests
59 https://mezha.media/en/2022/11/11/ukrainian-naval-drones-first-details-and-fundraiser-on-united-24/
60 Uma plataforma de recolha de donativos patrocinada pelo presidente ucraniano. https://u24.gov.ua/
61 https://www.navalnews.com/naval-news/2023/05innovative-submarine-drone-is-ukraines-new-weapon-against-russian-navy/

diáspora mobilizou-se para o apoio à Ucrânia. Ao contrário, o êxodo russo pode conduzir a que os emigrantes russos do setor tecnológico não regressem ao seu país, face ao perigo de serem mobilizados para uma guerra de conquista. A este facto deve juntar-se a possibilidade das empresas tecnológicas que saíram da Rússia, fruto das sanções internacionais, poderem refugiar-se temporariamente na Ucrânia. De facto, todo o setor tecnológico russo está em profunda crise, sendo paradigmático o caso de desmantelamento da gigante Yandex, a maior firma da Internet russa[62].

Entre os notáveis ucranianos do setor tecnológico destaca-se Max Levchin[63] que fundou, com o germano-americano Peter Thiel, a conhecida PayPal. Este último foi um dos primeiros investidores particulares no Facebook e é um dos cofundadores da Palantir, mencionada atrás. Outro dos ilustres ucranianos da economia digital é Jan Koum[64], co-fundador do WhatsApp.

No enquadramento da guerra, o presidente da Uber Works (uma aplicação para trabalhos temporários), Andrey Liscovich, deixou as suas funções para colocar os algoritmos ao serviço do esforço de guerra do seu país natal, liderando um fundo de *procurement* logístico para as Forças Armadas ucranianas[65]. Como último destaque, indicamos Oleg Rogynskyy, líder de uma *start-up* de sucesso que aplica a inteligência artificial à área das vendas, ajudando agora a coordenação do apoio a deslocados ucranianos[66].

Por fim, devemos referir um conjunto de iniciativas no capítulo do voluntariado tecnológico que utilizam diversas maneiras de ajudar a Ucrânia a enfrentar a agressão russa. Desde logo, o IT Army of Ukraine[67], cujos participantes (*hackers* voluntários), no mundo inteiro, podem assediar alvos cibernéticos russos utilizando *software* desenvolvido para o efeito. Esta iniciativa reforça a operação do cibercomando ucraniano que é constituído por 10.000 militares.

Outra originalidade da guerra da Ucrânia é que ela é a primeira *crypto-war*, uma vez que é possível canalizar doações em criptomoedas para o esforço de guerra, com várias carteiras a serem disponibilizadas por entidades governamentais e outras organizações, levando, inclusive à regulamentação do seu uso no sistema financeiro ucraniano[68].

62 https://www.technologyreview.com/2023/04/04/1070352ukraine-war-russia-tech-industry--yandex-skolkovo/

63 https://www.forbes.com/sites/jeffkauflin/2022/03/15/as-ukrainian-born-max-levchin-donates-to-refugees-he-keeps-affirm-on-course-despite-an-85-drop-in-its-stock/

64 https://techukraine.org/2022/06/21/whatsapps-founder-jan-koum-is-the-biggest-philantro-posts-during-the-war/

65 https://www.inc.com/melissa-angell/zaporizhzhia-andrey-liscovich.html

66 https://www.ft.com/content/63c0e9cf-2609-413d-a67d-f3b0fa8c3b2f

67 https://itarmy.com.ua/?lang=en

68 https://www.eiu.com/n/war-torn-ukraine-embraces-crypto/

Neste sentido, uma ONG com a designação de Army SOS[69] faz o encontro entre necessidades das Forças Armadas ucranianas e os doadores. A equipa que está por trás desta plataforma foi a criadora do sistema Kropyva referido atrás, em 2014. Outras, como a Come Back Alive[70], focam-se na aquisição de itens específicos por campanhas, como por exemplo equipamento de visão noturna; a Army of Drones[71], na aquisição de *drones*; e ainda outra na recolha de impressoras 3D[72] (utilizadas na fabricação de alhetas estabilizadoras das granadas lançadas por *drones* e outros componentes).

No que concerne ao desenvolvimento de aplicações, é conhecida a popularidade da MilChat[73], utilizada por cerca de 600.000 militares como alternativa à aplicação de mensagens WhatsApp; a ComBat Vision[74] que permite obter as coordenadas geográficas de qualquer câmara de vídeo, estática, a bordo de um *drone* ou telemóvel; e ainda uma aplicação que permite avisar da iminência de um ataque aéreo.

Conclusão

O desempenho tecnológico de todos os níveis, desde o político ao tático, permitiu à Ucrânia resistir à agressão russa, evidenciando uma abordagem em rede defensiva, que mistura capacidades militares clássicas com os meios mais modernos de deteção, decisão e ação contra uma hierarquia ofensiva, cujo processo de decisão e cultura têm tido mais dificuldade em tirar partido das novas tecnologias, apesar da sua superioridade convencional. Para isso foi fundamental o processo de reformas iniciado no consulado do presidente Zelensky com a implementação do governo eletrónico e do lema "Um Estado num *Smartphone*!", que permitiu aos cidadãos ucranianos o acesso a um conjunto de serviços úteis e orientou todo o aparelho do Estado para a resiliência, envolvendo a diáspora e os voluntários individuais e coletivos.

Por outro lado, a integração tecnológica expedita de apoios externos e a interligação de setores-chave internos demonstram uma certa agilidade institucional que, para já, tem permitido à Ucrânia manter a sua soberania, apesar do recurso a empresas maioritariamente americanas.

As primeiras lições da Guerra da Ucrânia demonstram claramente que estamos num ponto de inflexão das tecnologias base de defesa e que os Estados devem

69 https://armysos.com.ua/
70 https://savelife.in.ua/en/
71 https://www.bbc.com/news/technology-65389215
72 https://3dprintingforukraine.com/
73 https://milchat.app/en/
74 https://combat.vision/

prestar atenção ao progresso científico-tecnológico geral, dedicando uma atenção particular às tecnologias emergentes, de modo a identificar debilidades estruturais e potencialidades nacionais, em especial no que respeita às suas indústrias de defesa, último reduto da sua soberania.