O Conflito da Rússia-Ucrânia. Impactos para a Defesa Nacional em Portugal

Major-general
Paulo Fernando Viegas Nunes

Tendo como base o tema do 1.º workshop 2024, organizado pela Revista Militar, sobre o relevante tema "O Conflito da Rússia-Ucrânia. Impactos para a Defesa Nacional em Portugal", e mais concretamente na participação do 1.º painel dedicado à "Economia de Defesa e Inovação Tecnológica", apresenta-se um breve resumo da comunicação proferida pelo Brigadeiro-general Paulo Viegas Nunes, na qualidade de Presidente do Sistema Integrado de Redes de Emergência e Segurança de Portugal (SIRESP)1.

O orador, salientando as características atuais do ambiente de informação e focando-se com especial relevância na superioridade de informação, na inteligência artificial e na guerra de informação e do conhecimento, defende a necessidade de apostarmos na resiliência das infraestruturas críticas, nomeadamente, no que se refere às comunicações "missão-crítica, interagência e multinível. Neste âmbito, deverá ser tida em consideração não só a aprendizagem recolhida na guerra entre a Federação Russa e a Ucrânia, como também o percurso que vem sendo feito, em Portugal, para tornar o SIRESP mais resiliente e preparado para funcionar como plataforma de comunicações e rede de soberania nacional, assegurando a coordenação entre as Forças Armadas e as Forças e Serviços de Emergência e Segurança, em situações de emergência nacional e em condições de elevada exigência operacional.

O orador recorda que a gestão da informação é um elemento crítico no apoio à decisão nos níveis estratégico, operacional e tático, e que a resiliência informacional é cada vez mais desafiada pelo uso de tecnologias disruptivas e pelo número crescente de ciberataques, nomeadamente, por via da mobilização da inteligência artificial quando utilizada na guerra cognitiva, gerando e manipulando perceções individuais e coletivas, promovendo o acesso aos dados e ao conhecimento como instrumento de exercício do poder. Características que têm contribuído para alterar também o padrão das operações militares, e que vieram contribuir para um maior compromisso do Estado no apoio à capacitação das Forças Armadas. Este apoio materializa-se numa aposta na inovação e na atualização tecnológica dos sistemas de armas, das redes de comunicações e, muito em concreto, na capacidade de proteção dos seus sistemas de apoio à decisão, envolvendo tanto o reforço da sua cibersegurança e ciberdefesa como a condução de operações militares no ciberespaço.

Neste contexto, como exemplo ilustrativo, o orador salienta as recentes alterações produzidas na rede de comunicações de emergência nacional – SIRESP –, que permitiram edificar um sistema resiliente e acessível para todas as Forças e Serviços de Segurança, integrando no mesmos todas as componentes da Defesa Nacional, e muito em particular as Forças Armadas. O SIRESP é definido pelo orador como uma plataforma de comunicações "missão-crítica" interoperável e que pode funcionar, no limiar da transformação tecnológica, num mundo disruptivo em mudança, onde o acesso ao 5G e futuramente ao 6G irá colocar maiores desafios aos Estados e em concreto às Indústrias de Defesa e Centros de Investigação e Desenvolvimento nacionais.

Este "novo" domínio de operações que é o ciberespaço, foi reconhecido pela NATO em 2016, na Cimeira de Varsóvia. No entanto, importa referir que só mais tarde surgiram em Portugal, devidamente integrados, alguns documentos estratégicos estruturantes, tanto no domínio da cibersegurança como da ciberdefesa. Neste âmbito, salienta-se a publicação da Estratégia Nacional de Ciberdefesa, em 2022, e da Estratégia Nacional de Segurança do Ciberespaço 2019-20232, que se encontra em processo de revisão. Este procedimento, atendendo à estruturação da designada "pirâmide das estratégias", conforme formulada por André Beaufre, enquadra-se na necessidade de revisão periódica dos princípios que condicionam o desenvolvimento da estratégia da informação (inclui a estratégia nacional de cibersegurança e ciberdefesa), atendendo aos diferentes domínios de exercício da coação (estratégias gerais) e à natureza dos meios empregues (estratégias particulares). Neste contexto, constata-se que apostar nas tecnologias de informação e no desenvolvimento de capacidades no ciberespaço, elementos condicionadores do exercício do poder neste novo domínio operacional, permitirá condicionar este e todos os outros domínios.

O ambiente da informação é entendido como o único domínio estratégico em que os efeitos são produzidos de forma transversal e simultânea, muito por via da natureza das ameaças híbridas e dos desafios impostos pelos conflitos modernos (muti domínio), o que requer, ainda segundo o orador, uma maior articulação nacional e maior cooperação internacional.

A resiliência cibernética dos ecossistemas digitais é atualmente um dos maiores desafios para os Estados e para as Organizações, pois esta proteção de sistemas tem impacto na resiliência organizacional e operacional, nomeadamente porque no ciberespaço a área de interesse para as operações militares é a infraestrutura de rede global, materializada pela internet. Não se revela assim suficiente garantir a segurança dos sistemas CSI, ou até mesmo a proteção da informação (information assurance), importa, acima de tudo, assegurar a resiliência no cumprimento da missão (mission assurance). Só desta forma será possível garantir a continuidade das operações militares e num ambiente de guerra multidomínio, onde as operações no ciberespaço são permanentes e carecem de uma cooperação interagência e do desenvolvimento de parcerias estratégicas reforçadas para alcançarem os seus efeitos.

Neste contexto, a capacidade do ser humano para lidar com a inteligência artificial e a interação homem-máquina irão desempenhar um papel decisivo na guerra do futuro. A evolução tecnológica e a transformação da natureza dos combates da era moderna, onde o ciberespaço e a inteligência artificial ocupam um papel central, vão inevitavelmente levar o homem a agir e interagir, cada vez mais, com as máquinas, conforme já hoje se assiste na guerra Rússia-Ucrânia. Este novo paradigma, conforme salienta o orador, constitui um dos maiores desafios a enfrentar pelos comandantes operacionais do campo de batalha do século XXI, traduzindo-se muitas vezes o seu sucesso ou insucesso operacional na maior ou menor capacidade demonstrada para manipular e afetar a decisão do adversário, utilizando para esse efeito a designada guerra de informação e a guerra cognitiva para exercer influência e afetar o processo de decisão de um adversário.

Seguindo esta lógica operacional, surge a necessidade de se apostar na transformação tecnológica e de se construir uma infraestrutura de comunicações "missão-crítica", de elevada resiliência e capacidade de recuperação, condição imprescindível para assegurar a soberania do Estado. Neste contexto, face a requisitos cada vez mais exigentes, salienta-se que o SIRESP iniciou em 2022 um processo evolutivo para alcançar o 5G, estabelecendo como objetivo atingir esta meta ao longo dos próximos 10 anos.

Esta evolução tecnológica passa pela capacitação humana, através da criação de uma academia de formação, pela ligação ao meio académico, reforçando a interação com a indústria e pela criação de um "Hub 5G de comunicações missão-crítica" que funcionará como um laboratório que permitirá testar e validar novas soluções tecnológicas, interligando todas estas dimensões. Referindo-se ao exemplo das Jornadas Mundiais da Juventude 2023 (JMJ23), o orador demonstrou como o SIRESP foi capaz de assegurar, com eficiência e eficácia, o apoio ao maior evento alguma vez realizado em Portugal, suportando mais de 7 milhões de chamadas geradas por cerca de 28 mil terminais de comunicações a operar em simultâneo. A disponibilidade da rede foi de 99,9%, o que foi referido pelo Brigadeiro-general Viegas Nunes, como "…um enorme teste de stress ao SIRESP…" e que resultou na integração de várias redes nacionais, federando diversas infraestruturas e criando um ambiente de comunicações cooperativo, mobilizador e interagência, funcionando como um verdadeiro instrumento de resiliência nacional ao nível das comunicações de emergência.

A guerra da Rússia-Ucrânia veio demonstrar a necessidade de assegurar a resiliência e a capacidade de recuperação dos Estados, das Organizações e das Empresas, levando-as a apostarem na inovação tecnológica, a desenvolver sistemas de gestão de informação resilientes, pois o comando e controlo, o acesso à informação estratégica, em tempo real, e a capacidade de atuar em profundidade no campo de batalha, tornou-se essencial em contextos de guerra ou de crise. O SIRESP poderá ser, por tudo o que já foi antes referido, um instrumento mobilizador e essencial para criar sinergias e potenciar o desenvolvimento tecnológico nacional no domínio do 5G, do ciberespaço e da inteligência artificial, oferecendo uma infraestrutura segura, resiliente, e de elevada disponibilidade, capaz de promover uma utilização progressiva destas tecnologias. Em conclusão, o orador refere que a experiência operacional, já adquirida, veio permitir ajustar princípios orientadores, apontando para a necessidade de garantir uma gestão centralizada e assegurar um planeamento integrado, assente numa coordenação operacional permanente e multinível. A execução das operações deverá decorrer com unidade de esforço e de missão, constituindo a resiliência e recuperação dos sistemas de comunicações um fator crítico do sucesso das operações militares e de gestão de crises.

A empresa pública, responsável pela gestão e operação do sistema de emergência nacional, a SIRESP, S.A., transformou-se ao longo dos últimos dois anos, internalizando competências ao nível da gestão e supervisão da rede, reforçando a soberania do Estado sobre esta infraestrutura, e deixando de ser uma empresa gestora de contratos para passar a assumir o papel de operadora de comunicações críticas nacional. Esta aposta, que veio alterar o paradigma existente, consubstancia uma aposta estruturante do Estado, no sentido de assegurar uma maior capacidade nacional de resposta a crises e eventos disruptivos, quer estes sejam impostos pelas alterações climáticas, pelas crises, pelos conflitos ou mesmo pelas situações de guerra.

Em suma, parece ser unânime considerar, até pelo debate gerado no período pós-apresentações, que a guerra em curso, entre a Federação Russa e a Ucrânia, veio elevar a relevância estratégica da segurança, da capacidade de recuperação e da resiliência dos Estados, como fatores de desenvolvimento, onde o ambiente informacional, o ciberespaço, a inteligência artificial e a guerra cognitiva, apresentam um impacto substantivo na segurança cooperativa e na defesa coletiva. Neste âmbito, torna-se claro que todos dependemos de todos, mas onde também todos temos de contribuir com mais e melhores capacidades ao nível da proteção, da segurança e da defesa nacional. Não existindo fronteiras estanques entre estas componentes, o Estado deve dedicar uma atenção prioritária à Defesa Nacional e à capacitação das Forças Armadas, promovendo a sua utilização como fator de resiliência nacional e, neste contexto em particular, o SIRESP é um bom exemplo, ocupando um papel central no reforço e na salvaguarda da soberania nacional.

---

1 O Sistema Integrado de Redes de Emergência e Segurança de Portugal é a rede de comunicações exclusiva do Estado Português para o comando, controlo e coordenação de comunicações em todas as situações de emergência e segurança, tendo sido criado em 2006 como uma parceria entre o governo e o setor privado. Mais informação em: https://www.siresp.pt/.

2 https://diariodarepublica.pt/dr/detalhe/decreto-lei/34-2023-213345452