GLOBSEC US Foundation

The future of digital deterrence in Central and Eastern Europe

Alena Kudzko, Pavel Macko

www.globsecusfoundation.org

The future of digital deterrence in Central and Eastern Europe

GLOBSEC US Foundation
888 17th Street, NW,
Suite 800, Washington, DC, USA
20006

www.globsecusfoundation.org

GLOBSEC is a global think-tank based in Bratislava committed to enhancing security, prosperity and sustainability in Europe and throughout the world. Its mission is to influence the future by generating new ideas and solutions for a better and safer world. We believe we can change the world by putting together the right stakeholders at the right time for a free exchange of ideas. In an interconnected world, GLOBSEC stimulates public-private dialogue to shape agendas for the future. With global ambitions in mind and building on its Central European legacy, GLOBSEC seeks to contribute to agendas that are critical for Europe. GLOBSEC acts in the spirit of European values and international cooperation.

Lead Authors:

Alena Kudzko, Vice President of GLOBSEC for Policy and Programming

General **Pavel Macko**, Lieutenant-General (ret.), Slovak Army, a defence and security expert

Advising group: The report benefited from the work conducted within the framework of the GLOBSEC Future Security and Defence Council (FSDC). The content of the report was additionally informed by consultations with members of the FSDC.

July 2023

Disclaimer

GLOBSEC's work on the role of technology in defence and digital deterrence has received support from Palantir. The partnership with Palantir adheres to GLOBSEC's policy on intellectual independence.

The future of digital deterrence in Central and Eastern Europe

Russia's belligerent actions over the past decade and a half have culminated in its full-scale invasion and illegal war against Ukraine. Given Russia's track record of aggression, Central and Eastern European (CEE) countries are now raising a legitimate question: are we doing deterrence right?

Ukraine's staunch and legitimate defence of its sovereignty has provided unprecedented lessons regarding what it takes to effectively resist a formidable adversary in the 21st century. It has also spotlighted the clear and powerful insight that modern warfare is increasingly centred around the digital element.

While digital deterrence necessarily includes cyberwarfare, information warfare, and the use of digital technologies more broadly, this report will focus on software and data-driven capabilities. In ways that had not been tested before in a high intensity war between large conventional forces, these capabilities have become a critical enabler of cross-domain operations and an accelerator of more informed decision-making, with speed and at scale. If European allies are to get deterrence right, they cannot do so without more effective integration of software and data into their military capabilities.

This brief highlights the changing role of software in defence and deterrence and the accompanying lessons that can be learned from the war in Ukraine. It also puts forward initial recommendations on the steps CEE countries should take to achieve digital deterrence in the region.

> **Russia's invasion of Ukraine represents a clear failure of deterrence**

The changing thinking on deterrence

Effective deterrence requires that a potential adversary understands that their opponent both wields sufficient capabilities to inflict pain and the will to do so. If potential adversaries calculate that the cost of an attack will significantly outweigh the gains, they will likely forgo it.[1]

For Central and Eastern European countries, Russia's invasion of Ukraine represents a clear failure of deterrence. Though Russia has not directly attacked any NATO members, its actions have proven destabilizing to the European neighbourhood for years. Russia's invasion of Ukraine is particularly alarming considering that the country had previously received security assurances from the U.S., the U.K. and even Russia itself under the 1994 Budapest memorandum.

The invasion highlights the centrality of deterrence to peace and stability for Central and Eastern European nations: Russia will not abandon its hostile behaviour if it senses weakness in its opponents.

As underwhelming as the Russian military has been in Ukraine (against expectations to the contrary[2]), this performance should by no means lead to countries downplaying the Kremlin's ongoing threat. First, there are no signs that Russia has abandoned its ultimate intent to fight for as long as it can to claim what it believes to be its historical sphere of influence. This includes the demand for NATO to revert to its 1997 borders. Rather than retrenching, it is only a matter of time before Russia attempts to regroup, mobilise additional human, financial, and military resources, and attack again. Russia still possesses significant military power, including missiles, submarines, and air force capabilities, and can reconstitute its military to make it more capable and more formidable.[3]

Moscow will only abstain from belligerent actions if they know with certainty that their opponent possesses more dominant capabilities and the political will to use these to stifle potential Russian war aims.

Small CEE countries would be easy pickings for Russia if they had to face the country alone. Hence, NATO and its collective defence commitment have been key for the region's deterrence strategy.

Given Russian tactics in Georgia and Ukraine, the deterrence logic over the past decade has been dominated by an emphasis on conventional combat operations and platform-centric, heavy equipment that was once at the centre of deterrence-by-denial planning – reducing or denying the adversary the ability to achieve their goals through war. As NATO allies increase their military budgets, the

1 For an overview on the theory of deterrence debate, see, for example, Stephen L. Quackenbush, "Deterrence Theory: Where Do We Stand?" *Review of International Studies*, vol. 37, no. 2 (2011), 741-762

2 See, for example, Michael A. Kofman and Jeffrey Edmonds, "Russia's Shock and Awe: Moscow's Use of Overwhelming Force Against Ukraine," *Foreign Affairs* (2022). https://www.foreignaffairs.com/articles/ukraine/2022-02-21/russias-shock-and-awe

3 Robbie Gramer and Jack Detsch, "Russia is already looking beyond Ukraine", *Foreign Policy* (2023), https://foreignpolicy.com/2023/05/22/russia-nato-beyond-ukraine-estonia-baltic-eastern-flank-military-threat/

paradigm has also shifted towards including technology and platform-driven capabilities.

Central and Eastern European countries have the most at stake in ensuring that deterrence does not fail (again). Doing more of the same or merely expanding the size of militaries will not be sufficient against a large aggressive country that has prioritised investing in its military above all else. Additionally, countries in the region still need to resolve the same issues that they have been facing for years – lack of interoperability with other allies and a far from perfect ability to move troops and supplies across the continent.

> **Software-driven capabilities will be part of leaders' calculations from here on - in assessing both their own force and the strength of their adversaries**

To offset these challenges, defence planners increasingly underscore the need to invest in developing smarter, faster, and more connected capabilities to gain an advantage against adversaries through swifter and more precise decision-making and implementation processes. As resources are never infinite, governments need to enact these measures in the most cost-effective way. While larger countries can outspend smaller countries on heavy equipment, the latter group can adopt software-based digital deterrence just as readily as the former. As software maximises the value of hardware – by enhancing its effectiveness, efficiency, precision, speed, and accuracy – and augments military performance, smaller conventional forces can gain an even greater marginal return on investment on these capabilities. The commitment to spend at least 2% of GDP on defence agreed at the 2014 Wales Summit was accompanied by an additional pledge to spend at least 20% of this funding on new equipment, including R&D. As the July 2023 Vilnius NATO Summit is expected to deliver an even stronger defence investment pledge this year[4], it is critically important that software and data-defined capabilities be put front and centre of the capability development process and defence planning.

While the outcome of the war is far from certain, developments in Ukraine demonstrate the potential for digital solutions to tip the balance on the battlefield. The lesson for other countries, including those not currently at war, is to recognise that software-driven capabilities will be part of leaders' calculations from here on - in assessing both their own force and the strength of their adversaries.

Lessons learned from Ukraine: software and digital solutions that deliver an edge on the battlefield

The war in Ukraine is a high intensity and cross-domain conflict. Ukraine's embrace of the digitised battlefield and its information superiority over Russia have been integral to its resilience and continued ability to launch counteroffensive operations.

4 Robbie Gramer, Amy Mackinnon and Jack Detsch, "Eastern Europe Wants NATO to Beef Up Defense Spending", *Foreign Affairs* (2023), https://foreignpolicy.com/2023/02/02/eastern-europe-nato-defense-spending-ukraine-russia-poland-estonia/ ; Sergio Goncalves and David Latona, "NATO's Stoltenberg expects new 2% defence investment pledge at Vilnius summit", *Reuters* (2023), https://www.usnews.com/news/world/articles/2023-05-18/natos-stoltenberg-expects-new-2-defence-investment-pledge-at-vilnius-summit

War is a time competitive process. Speed and precision matter. The side that can better "see and sense" the battlefield, make swifter and more knowledgeable decisions, and more effectively and precisely communicate and execute these decisions.

Software has been employed by Ukraine across numerous areas to maximise the speed, precision, and overall quality of decision-making, and therefore the yield of its military capabilities – capabilities which, in terms of their scale and technological advancement, are in many cases inferior to Russia's.

Ukraine has successfully compensated for its smaller size and smaller pool of conventional capabilities and human resources compared to Russia, in part, by designing, integrating, and deploying software and digital solutions that, in combination with military hardware and traditional capabilities, deliver **speed and precision and enhance decision making capacity.**[5]

Ukraine has demonstrated a model of what software-driven capabilities, including AI, can deliver. The key elements leveraged for that include:

- *Data collection, data processing, and data fusion.* Ukrainians have developed a remarkable ability to collect and process data. This data comes from intelligence sources, physical reconnaissance operations, commercial satellite imagery, weather forecasts, drone flights, sensors, and open-source intelligence.
- *Connectivity and communication systems.* To transmit massive volumes of data, there is a need for bandwidth, speed, and permanent connectivity. A combination of mobile networks, Starlink satellites, and military SATCOMs have been a necessary enabler of Ukraine's data-driven capabilities on the battlefield.
- *Decision-making and decision implementation software with a user-friendly interface.* An elaborate and technologically advanced system of data collection and fusion – with AI networks to process it all – has translated into a tangible battlefield advantage. To a large extent, this is because the front end experienced by soldiers is remarkably user friendly and easy to use.

The emphasis on data-driven warfare is particularly remarkable given the scale of transformation that the Ukrainian defence forces have undergone in transitioning from a post-Soviet system to a more modern and technologically advanced one that attends to horizontal relations and empowers lower levels of command. As part of this transformation, the Ukrainian military changed how it approaches the private sector, commercial technology, and the development of digital skillsets among both military personnel and civilians. Several factors have particularly aided Ukraine in navigating data-driven warfare:

- *Engagement of the private sector.* Even before Russia's full-scale invasion began, the Ukrainian government looked to the private sector for solutions, knowing that companies often have an advantage over the military in terms of speed and agility of tech development and deployment.
- *Integrating dual-use tech and adjusting existing solutions to their needs.* Ukrainians also learned that the use of civilian commercial technologies is now an integral component of defensive war. Similarly, algorithms and approaches that are used to develop civilian applications can be utilized for military solutions. They also understood that the expense and implementation risk of custom solutions might be a disadvantage in comparison with commercial "off-the-shelf" tech that can be deployed and customized quickly to address specific problems.
- *Building an IT-savvy defence force and digitally literate society.* Ukraine has been able to draw on a deep and longstanding pool of IT expertise. Ukrainians with IT skills became embedded in the armed forces and were provided freedom to code, tinker, and innovate. Exigent circumstances demanded that cumbersome top-down processes and unwieldy bureaucratic structures are not an impediment to life-saving innovation on the ground. Ukrainians also managed to organize a total defence involving its entire society. An educated and digitally literate population was ready to embrace the digitisation of the battlefield and contribute through the savvy use of mobile apps and other tech to send in photos and other information about its enemy and receive necessary services from the government enabling societal resilience.

Modern software as an enhancer and integrator of hardware

The lesson learned from Ukraine is not that hardware is becoming irrelevant as the role of software grows. Military hardware will remain fundamental to operations in the physical domain, such as controlling territory and protecting lives. Software, however, *changes the value of hardware by enhancing its effectiveness, efficiency,*

5 For more, see, for example, Nico Lange, "How to Beat Russia: What armed forces in NATO should learn from Ukraine's homeland defense", *GLOBSEC* (2023), https://www.globsec.org/what-we-do/publications/how-beat-russia-what-armed-forces-nato-should-learn-ukraines-homeland; "Lessons for the Next War", *Foreign Policy* (2023), https://foreignpolicy.com/2023/01/05/russia-ukraine-next-war-lessons-china-taiwan-strategy-technology-deterrence/#mauro-gilli; Pete Furlong, Melanie Garson, Jeegar kakkad, "Software and Hard War: Building Intelligent Power for Artificially Intelligent Warfare", *Tony Blair Institute for Global Change,* (2022), https://www.institute.global/insights/geopolitics-and-security/software-and-hard-war-building-intelligent-power-artificially-intelligent-warfare; Seth G. Jones, Riley McCabe, and Alexander Palmer, "Ukrainian Innovation in a War of Attrition", *Center for Strategic and International Studies CSIS* (2023), https://www.csis.org/analysis/ukrainian-innovation-war-attrition

precision, speed, and accuracy.[6] It can also improve the cost-effectiveness and lifespan of hardware. Software can be developed much more swiftly than hardware too. If the symbiosis is designed correctly through continuous upgrades to the "operational system", hardware can continue delivering more and more efficiency and effectiveness without costly and lengthy modifications to physical components. Even an older howitzer model can become many times more efficient if an AI-based platform can quickly and precisely identify the target to fire at.

Importantly, *software can also enable hardware to be connected and embedded into the battlefield*, improving the coordination and efficiency of various complementary elements.

Tying it all together, software plays an important role in promoting better-informed decision-making. It enables militaries to more clearly "see" the battlefield through the fog of war and gain a more coherent and clearer picture of the situation in real time. Beyond improving the efficacy of military outcomes, improved battlefield clarity plays a critical role in enforcing/adhering to international humanitarian law obligations, such as distinction and proportionality, which helps minimise civilian harms and other collateral damage.

Furthermore, software allows decision-making to be based on more accurate and complete information and in a more expedited manner. Software can further ensure that decisions are subsequently disseminated and implemented, with progress on the completion of tasks reported in a timely fashion. This information-decision-action loop is called the OODA loop (observe, orient, decide, and act), and it confers a substantial advantage to the side that can both master the loop and consistently cycle through it at pace.

These multiple software advantages – the enhancement of operational capacity, precision and speed, and connectivity and command and control on the battlefield – should be anticipated in the design of hardware capabilities. Legacy military platforms that lock in strictly custom software in specific hardware cannot reap the benefits from the constant evolution of software.

Peace time innovation: state of emergency vs state of urgency

The war in Ukraine has, by necessity, become a testing ground for next generation digital solutions and software integration. The Ukrainian military, facing no other choice, has indeed taken considerable strides to adopt military tech.

To survive against a conventionally superior force, Ukrainians have been steered towards innovating and innovating fast. Against the backdrop of war, the risk calculation in making decisions about fielding certain technologies is always adjusted against the real probability of casualties and defeat. In many cases, the immediate battlefield advantages delivered by new software (or any tech) for Ukraine significantly outweigh the risks. Following strict and unnecessarily complex procurement procedures or stepping through various levels of bureaucracy meanwhile take a backseat. Decisions about these matters have rather been about mere survival since February 2022.

> **A key challenge, nevertheless, concerns optimising the process to ensure that products can be deployed before they become obsolete**

The state of urgency that has emerged in countries near Ukraine is different though from the state of emergency involving active lethal combat that many Ukrainians find themselves facing. The lack of an imminent military threat to Europe provides space and time to put in place more robust development and testing procedures.

Entirely replicating the innovation process adopted during a war setting to one free from ongoing active military conflict, hence, is neither possible nor desirable. Peacetime provides a different set of guardrails and risk-benefit calculations as well as additional opportunities. When a good idea emerges in peacetime, a well-rounded team, including data scientists, engineers, and ethical experts, can be brought in to work on the project design. It is also feasible to conduct standard test and evaluation processes to ensure that the proposed technology is safe, reliable, effective, and ethically suitable before deployment.

For example, the design and extended timeline for peacetime innovation can alleviate concerns about operational security that have been pronounced in Ukraine. The Ukrainian deployment of data driven capabilities often did not meet military standards. Software has been typically installed on regular civilian phones or tablets that can be hacked more easily or apprehended by the enemy. Data has also been transmitted through commercial mobile networks or satellites, risking interception or corruption before it is fed into algorithms. With their survival at stake, Ukrainians have estimated that if they gain the sufficient advantage of speed to advance on the battlefield most of the time, they can accept occasional setbacks and losses stemming from imperfect operational security.

These factors, meanwhile, need not provide a dilemma in peacetime. Better data transmission protocols and cybersecurity of applications can be worked out given a more well-rounded team and more permitting timeline involved in the software development process.

A key challenge, nevertheless, concerns optimising the process to ensure that products can be deployed before they become obsolete. And at the speed at which digital technology is developing and evolving, change is often measured in a matter of months (or less).

6 For an in-depth overview of software as an enabler of modern defence, including interaction of software and hardware, see Simona R. Soare, Pavneet Singh and Meia Nouwens, "Software-defined Defence: Algorithms at War", IISS (2023), https://www.iiss.org/research-paper//2023/02/software-defined-defence

A cultural shift in understanding the meaning of a "final product" – or rather accepting that products are never final and can be constantly improved upon even after their adoption – will also be needed. Modern software, increasingly powered by AI, improves rapidly through its use in the field. Dragging out concept development over many years, in this regard, produces suboptimal outcomes. The peacetime process, as still mostly practiced today, is tedious and slow, often resulting in products that are nearly obsolete or irrelevant by the time they are deployed. This poses a strategic vulnerability in a software based and digitised environment. Militaries should seek to deploy software capabilities safely and responsibly (and in all cases without compromising legal obligations) at the earliest possible opportunity and in real-world conditions or conditions that approximate the real-world to the best extent possible.

> **"The key to success in many cases has been in finding off-the-shelf solutions that can be customized or adapted to existing bottom-up needs**

The recognition early in the conflict in Ukraine that the best solutions for defence can come from totally unrelated sectors and from any provider, big or small, has seen Ukraine swiftly pivot towards developing structures that facilitate interaction between the military and private providers. Brave1, the Ukrainian coordination platform for defence tech, is a good example here. The key to success in many cases has been in finding off-the-shelf solutions that can be customized or adapted to existing bottom-up needs.

This approach remains valid for peacetime. European militaries generally fail to embrace optimal solutions simply because they are not open to the providers able to offer them. Traditionally, defence officials have primarily focused their efforts on prominent defence contractors in developing capabilities. In many cases, solutions that are needed for modern militaries are already being developed in other sectors. An engagement with the companies behind the relevant tech solutions, meanwhile, is often not sought after both because defence officials are simply not aware of the capabilities they can provide to help achieve defence needs and because necessary security screenings of businesses might take months.

Ukraine has managed to bridge these gaps in war time. Peacetime further enables governments and militaries to set up public-private schemes that encompass a wide variety of potential tech providers and establish guardrails and guidelines for such cooperation that also includes provisions for social and ethical implications.

All told, peacetime enables countries to

> (a) better address operational security through more robust data transmission infrastructure and protocols and cybersecurity provisions; (b) work with more well-rounded development teams that include engineers, data analysts, military users, and ethics experts; (c) go through all stages of test and evaluation procedures before deploying new software; (d) set up structured forums and mechanisms for exchange between a diverse set up private providers and defence officials; (e) and establish and implement guiderails for such cooperation including those concerning ethical use of technology for defence purposes.

The war in Ukraine though has demonstrated that several significant adjustments to the way software and data driven capabilities are developed and deployed can and should be made also in countries not engaged in a hot war.

This includes:

> (a) significant acceleration of the procurement process; (b) earlier deployment of data-driven capabilities and an iterative development process with close interaction between users and developers; (c) reliance on off-the-shelf solution that can be tailored to accommodate operational needs and scaled across the force; (d) and acceleration of security screening procedures for private sector providers and the opening up of defence procurement to a more diverse set of tech companies.

Multilateral and NATO context

Smaller European nations will be among the biggest beneficiaries of the adoption of software-based capabilities due to the ability of tech to enhance and augment otherwise comparatively small national hardware capabilities and contribute fundamentally to even modest efforts at modernization. Yet collective defence is the strongest deterrence component that countries in the region can rely on. CEE countries can be confident that in the event of an attack, the entire Alliance will come to their aid. Their success is dependent on the ability to work with other allies. As with conventional capabilities, though, fragmentation on the use of digital applications will create an interoperability challenge.

Interoperability is not a new challenge for the Alliance. NATO countries have worked to ensure their militaries can smoothly operate together and swap (and share) equipment where needed. A set of principles has been devised to facilitate this.[7] These principles, notably, also apply to software and digital capabilities.

As with hardware, NATO should encourage innovation and interoperability of software solutions across the fleet.

7 NATO, Interoperability: connecting forces, (2023) https://www.nato.int/cps/en/natohq/topics_84112.htm

The use of 20 variations of the same equipment, especially costly platforms, often results in suboptimal outcomes when each requires different components and maintenance or simply are not compatible with other equipment on the battlefield. Residual Soviet-era equipment presents typical problems.

While tech innovation opens up space for multiple solutions and providers, the key is to ensure that all digital solutions follow the same protocols and standards. Software solutions need to be able to talk to one another, allow for information exchange, and provide options for integration into larger platforms. Data collected in one country should be transferable to another country and work for software developed by other providers.

> **Industry involvement will be important, both for expertise sharing and the provision of critical services such as data management and cloud computing**

NATO has laid important groundwork with its Data Exploitation Framework Policy (DEFP)[8], which was adopted in October 2021. The policy aims to ensure that Allies can leverage data as a strategic resource to achieve information superiority and make data-driven decisions at all levels. To accomplish this ambition, NATO aims to facilitate a single logical environment for the Alliance and establish a set of standards to ensure interoperability by design.

The Data Exploitation Framework (DEF) Strategic Plan[9], endorsed in October 2022, further specifies the lines of effort. These include data management and connectivity standardization, data architecture enabled by cloud and other open-architecture capabilities, and the integration of data analytics and AI into NATO's digital capabilities. The NATO Artificial Intelligence Strategy similarly emphasizes the acceleration and mainstream AI adoption in capability development while enhancing interoperability within the Alliance, including through proposals for AI Use Cases, new structures, and new programmes. To get there, NATO should seek standards, common frameworks and APIs.

National authorities have started the implementation of the mentioned strategies and plans, but their success will be contingent on committed funding as well as the ability to adopt a whole-of-enterprise approach and leverage available NATO expertise, particularly that of the NATO Communications and Information Agency. Most fundamentally, industry involvement will be important, both for expertise sharing and the provision of critical services such as data management and cloud computing

As with hardware, pooling resources, including the joint procurement and sharing of software capabilities, should be encouraged both to address the interoperability problem and to promote cost efficiency. AI-driven systems, for example, can be costly and require large data sets to deliver high performance. But sharing digital infrastructure can provide smaller countries with capabilities they otherwise might not be able to afford. Joint procurement also helps ensure that digital infrastructure is fully interoperable.

NATO-wide interoperability standards should be relied upon when developing and acquiring software.[10] As CEE

8 NATO, Summary of NATO's Data Exploitation Framework Policy, (October 2021) https://www.nato.int/cps/en/natohq/official_texts_210002.htm

9 NATO, Summary of NATO's Data Exploitation Framework Strategic Plan, (13 October 2022), https://www.nato.int/cps/en/natohq/official_texts_209999.htm

10 NATO AI Strategy rightly identifies the direction of ambitions to maximize the interoperability of AI-driven capabilities and elaborate international standards and principles for AI use. The implementation of this ambition should be one of the key priorities for the Alliance and its partners. https://www.nato.int/cps/en/natohq/official_texts_187617.htm

countries dramatically expand their budgets and accelerate procurement and acquisition against the backdrop of the war in Ukraine, the focus should be on the new generation of genuinely software driven capabilities rather than incremental upgrades of software embedded in legacy platforms and systems.

The ethics of software driven capabilities

There are additional distinct challenges associated with the deployment of data-driven capabilities. Against the backdrop of global technological competition, the EU's effort to ensure data sovereignty and embed privacy into its data sharing principles is the right intention. Addressing questions surrounding data sharing and data transfers will be key to facilitating shared digital solutions. The formulation of an approach that protects individual rights and privacy – but at the same time removes roadblocks for data-sharing (such as those within the EU and between the EU and the US) – will facilitate the faster and smoother adoption of cutting-edge innovations.

> **Collective defence may eventually depend on the interoperability of AI-driven capabilities**

Policy misalignment within NATO countries – of the kind that exists between the EU, the US, and the UK (but also within the European Union)[11] – can pose major challenges for organisations such as NATO. The EU is yet to work out a shared approach with the US on privacy matters to enable US major tech companies to contribute to European defence based on their full potential.[12] Disparities in software capabilities, data governance, norms of engagement of AI-driven capabilities, and legal regulations between member states can impede the ability of NATO forces to act cohesively. Collective defence may eventually depend on the interoperability of AI-driven capabilities. An ally deviating from a joint position may jeopardise political decision-making, cohesion, consensus, and overall coercive effectiveness.

Another concern that should be addressed early on and in a coordinated manner pertains to the capacity of algorithms to fully comply with international humanitarian law. The place and responsibility for humans in the decision-making process, importantly, must be protected. Proportionality and distinction cannot be easily programmed or algorithmically trained. Provisions for human oversight and human participation in the decision-making loop must be part of the design and deployment process.

Through the proposed Artificial Intelligence Act (AIA)[13], the EU is taking a significant step towards shaping the global regulatory landscape for artificial intelligence. The framework will have profound implications on how EU countries can develop and adopt AI-based applications, especially for the needs of the military. The AIA also underscores the need for clear rules and ethical considerations in the development and deployment of AI systems in military contexts too. Transparency, accountability, and human oversight are prioritised as principles that the EU is seeking to integrate into the regulations. This proactive approach aims to address concerns regarding the potential risks and negative consequences associated with AI in warfare. As the AIA undergoes further legislative review, it promises to establish a framework that fosters ethical standards and ensures the responsible use of AI technologies and the safeguarding of human values and control. The EU's efforts in this regard signal its commitment to upholding, and indeed shaping, global norms which are highly relevant to the use of AI in warfare too.

The need to train algorithms on specific data available only in certain locations or contexts creates further challenges, including with regards to IP rights, data sovereignty, and privacy concerns. Yet a shared digital infrastructure developed based on generic data can be successfully transferred from one national context to another and then further enhanced and trained locally. European nations would need to further streamline their export control regulations to ensure that allies can make use of the infrastructure with the confidence that they can continue to rely on software with IP rights registered elsewhere.

A path forward: policy recommendations

To deter future wars, the transatlantic alliance needs to upgrade its capabilities, and the will to use them if required, to ensure that any potential aggressor can have no doubt that they will fail to achieve their objectives through military means.The digital domain is not only a sphere of its own - digital solutions now underpin other capabilities and pervade all other domains. For 21st century deterrence to succeed, it needs to become more digitally driven.

As European nations rebuild their defence forces, they must factor digital deterrence more robustly into their defence planning and their budgetary allotments. The countries on the Eastern Flank are particularly aware of the need to strengthen deterrence. They have committed unprecedented shares of their budgets to procuring new capabilities and replacing equipment provided to Ukraine. Their efforts will only be successful, though, if they plan for and commit to procuring and integrating advanced software solutions. What follows are a series of recommendations to guide this process.

11 Troels Krarup and Maja Horst, "European artificial intelligence policy as digital single market making", *Big Data & Society*, 10(1), (2023). https://doi.org/10.1177/20539517231153811

12 Alex Engler, "The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment", *Brookings* (2023), https://www.brookings.edu/research/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/

13 AI Act: a step closer to the first rules on Artificial Intelligence, *European Parliament* (2023), https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

- **View software as central.** Modern software cannot be an afterthought or an add-on to hardware capabilities. System design should incorporate software development and updates from the initial stages, and software, including its AI-driven capabilities, should be recognized as a core capability and resourced appropriately, including through separate budget lines.
- **Put more emphasis on commercial off-the-shelf capabilities.** Bespoke hardware dependent software is significantly more costly to develop and maintain and takes longer to update while at the same time does not always deliver top of the line functionality. As commercial technology advances faster, the ability to use commercially available algorithms tailored to specific defence needs must be incentivised and incorporated into procurement and budgeting processes. This also implies that hardware producers should be incentivised to rely more on open architecture modules that make it possible to plug in softwa**re and data from partner providers.**
- **Pool collective resources.** As with other types of capabilities, the pooling of resources and joint procurement would make better capabilities available for countries who otherwise cannot afford them and help improve interoperability. Expansion of European schemes to provide financial support to countries for joint procurement of defence products with a heavier emphasis on software would be a good additional incentive.
- **Ensure interoperability standards.** Software driven capabilities should be designed and procured based on NATO standards to ensure interoperability with other capabilities and between allies. NATO should provide support to the Allies to help embed standards in their capability development process and develop and implement assessment and reviews of interoperability. All NATO Allies should commit financial and human resources to speedily implement NATO AI and data exploitation strategies and plans.
- **Drive for ethical employment and operational effectiveness all in one.** The focus on performance of software driven capabilities should go hand in hand with an emphasis on enabling responsible use. In particular, technical controls and organisational policies need to ensure that a human stays in the loop for critical decision-making wherever appropriate.
- **Prioritise faster adoption and regular update of EU regulations on AI and data transfers.** EU wide regulations would add clarity on shared ethical standards and guidelines. They should also, though, ensure adequate frameworks for safe data transfers necessary for the development of cutting-edge technologies.
- **Field algorithms-based capabilities earlier.** AI-based programs will, by definition, never be one hundred percent ready. Such programs constantly improve as more data becomes available. To enable the earlier deployment of such capabilities, there is a need to adjust procurement and acquisition processes. Iterative development models should become the norm across Europe, substituting the still entrenched waterfall capability development models. The software users should be in close and iterative interaction with developers to continuously assess functionality and adjust.
- **Speed up procurement cycles.** The accelerated advancement of software necessitates a procurement cycle that operates on a significantly different timeframe than what defence forces are accustomed to. The journey from initial product development to implementation and scaling up must be significantly slashed.
- **Invest in meaningful data collection and data processing.** Investments in cutting-edge AI-driven data analysis systems is key for faster and more informed decision-making. For that, defence forces also need to invest in enabling capabilities for high-value data collection – while avoiding over-collection – and secure and reliable data transmission.
- **Involve the private sector earlier.** As the private sector has become key to defence efforts, finding additional ways to collaborate is necessary.
- **Focus on functionality.** Tech and software that delivers solutions to the concrete problems in the field defined by “end-users” – the military – are quicker to absorb and integrate and can deliver more immediate impact. Successful use cases should subsequently be expediently scaled up and deployed across the forces.

Notes

GLOBSEC
IDEAS SHAPING THE WORLD

888 17th Street
NW, Suite 800
Washington, DC
USA 20006

+421 2 321 378 00
info@globsec.org

www.globsecusfoundation.org