THE ROLE OF DUAL-USE TECHNOLOGIES IN HYBRID WARFARE: A DOUBLE-EDGED SWORD?

Borislav Bankov (1), Stefan Bojilov (2)*

(1) GATE Institute, Sofia University "St. Kliment Ohridski", Sofia, Bulgaria;
(2) Leiden University, Leiden, the Netherlands

* Corresponding Author, e-mail: borislav.bankov@gate-ai.eu

Abstract: The concepts of "hybrid warfare" and "dual-use technologies" have two striking similarities. Both link the military with the civilian domains; both are also heavily used in Western security architecture. It is thus surprising that very little academic literature explores their interrelationship. To fill this gap, the present article asks how dual-use technologies influence hybrid warfare. It is argued that dual-use technologies are a double-edged sword as they enable hybrid aggressors but also help counter hybrid warfare. On the one hand, the versatility, lower acquisition costs, and adaptability of dual-use technologies increase the risk of hybrid campaigns. On the other, they can improve allied interoperability and resilience against hybrid threats. It is thus recommended that researchers, analysts and decision-makers consider dual-use technologies when investigating or mounting a defense against hybrid adversaries.

Key words: hybrid warfare, dual-use technologies, dual-use items.

1. INTRODUCTION

When, in 2014, the North Atlantic Treaty Organization (NATO) and the European Union (EU) adopted the term "hybrid warfare" (HW) to condemn the illegal annexation of Crimea, the term started gathering significant academic and policy attention. The consensus was that HW describes the “grey zone” between war and peace, whereby various actors combine regular with irregular warfighting. HW thus captures the blurring of military and civilian targets, technologies, and infrastructure. To address these critical developments, both NATO and the EU have adopted various measures to counter HW.

Dual-use technologies (DUTs) are also a term that links the military with the civilian domains. DUTs, a subset of dual-use items, have both military and civilian applications and exist across a wide range of technological fields such as aerospace and computing. Consequently, both NATO and the EU have created new entrepreneurial formats that aim to accelerate dual-use innovations on the basis of a stronger collaboration with the private sector. Initiatives such as NATO’s Defence Innovation Accelerator for the North Atlantic (DIANA) and the EU’s Hub for European Defence Innovation (HEDI) reflect the growing importance of DUTs in the relationship between technology and security.

While there are many academic works on both HW and DUTs individually, there is a literature gap regarding their interrelationship. This academic oversight is surprising, as both terms pertain to the blurring of civilian and military domains and are heavily used in Western security. Thus, the purpose of this article is to propose a new research agenda on HW and DUTs, which could ultimately support the development of new robust policies that tackle the implications of new technologies on the modern battlefield. This article thus asks the following question: How do DUTs influence HW? This article argues that DUTs are a double-edged sword because they enable hybrid aggressors but also help counter HW. On the one hand, the inherent versatility, lower acquisition costs, and adaptability of DUTs can increase the risk of hybrid campaigns. On the other hand, DUTs can improve allied interoperability and resilience against hybrid threats. Thus, while DUTs aggravate HW, they simultaneously offer opportunities for enhancing the security and cooperation of allies facing such threats. Studying the dual nature of DUTs is crucial to understanding the role of emerging technologies in modern conflict. This article thus recommends that researchers, analysts, and decision-makers in the security and defense sector consider DUTs when examining or responding to cases of HW.

This article begins with a brief literature review, which further expounds the current gaps in academic knowledge. Then, the text defines HW and explores if the authors of the concept considered DUTs in their original work. This is followed by an overview of DUTs. After, the text examines the nexus between HW and DUTs, formulating proposals for further research and policy change. Finally, the conclusion sums up the findings.

2. LITERATURE REVIEW

The academic discourse on DUTs has historically focused mainly on their chemical, biological, radiological and nuclear (CBRN) applications [1]. Specifically, the primary concern, connected to DUTs, has traditionally been related to the proliferation of CBRN technologies, their malign use by hostile actors, and regulation through export controls. Being highly versatile and applicable in both civilian and military sectors, emerging and disruptive technologies have expanded the initial scope of DUTs research due to similar concerns over unintended proliferation and their potential to be used in modern conflict.

Recent studies more often than not acknowledge the role of DUTs (such as artificial intelligence (AI), cyber technologies, and autonomous systems) in hybrid conflicts [2]. For example, some scholars highlight how DUTs are central to NATO and EU security strategies, pointing to DUTs integration into defense innovation to counter hybrid threats [3]. Others illustrate how hybrid adversaries exploit supply chains, information systems, and infrastructure, leveraging DUTs to destabilize states while maintaining plausible deniability [4]. Finally, there are authors who focus on the ethical challenges of DUTs, advocating for governance mechanisms that balance innovation with security risks [5].

Despite these developments, a significant gap remains in understanding the specific mechanisms through which DUTs influence HW strategies. While existing studies look at some aspects of the HW-DUTs nexus, the majority of works do so in a case-specific or sectoral way rather than providing a holistic understanding of the mechanisms through which DUTs enable hybrid actors and enhance countermeasures. Furthermore, there is a lack of a comprehensive analytical framework that systematically examines how DUTs

shape both the offensive and defensive dimensions of hybrid conflicts. Failing to address these critical questions limits understanding of how emerging technologies are reshaping modern conflict and what the appropriate policy response is. In summary, there exists a critical need for new academic studies that examine the implications of DUTs on HW.

3. HYBRID WARFARE

Frank Hoffman of the United States Marine Corps (USMC) was the first to write in-depth on HW. In his seminal work – Conflict in the 21st Century: The Rise of Hybrid Wars – he claimed that HW features "a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. These multi-modal activities can be conducted by separate units or even by the same unit but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects. The effects can be gained at all levels of war" [6].

While Hoffman's 2007 definition of HW did become prominent within the security and defense community, HW became a widespread buzzword only after 2014, following the EU's and NATO's decision to adopt the term in regard to the illegal annexation of Crimea. However, the surge in the term's popularity also created significant conceptual confusion around HW as the Kremlin's operations at the time did not match Hoffman's earlier definition of the phenomena. That is, while Hoffman focused on the kinetic and violent aspects of HW, in 2014 Russia mainly employed non-violent operations such as cyber-attacks and election manipulation. Hence, while the EU's and NATO's decision to use HW as a keyword in their messaging against Russia was politically justified, it did not have significant conceptual underpinning. To be sure, this led to much academic debate and criticism that HW had become a fashionable but not a rigorous theoretical framework [7]. In order to avoid adding to the confusion and support the conceptual clarity of HW, this article would apply Hoffman's original definition of the concept.

Hoffman does not use the term "DUTs" in his work but repeatedly acknowledges the importance of technologies in modern war. He recognizes that the West has failed to properly assess the benefits but also all risks related to information, sensor and other new technologies. The USMC officer goes on to suggest that the West sees technologies only as a security provider but has failed to grasp that some adversaries have learned to apply those new technologies in unanticipated ways. Thus, Hoffman hints at the fact that some commercial technologies can be used creatively to the detriment of the West, yet he does not specify if they are dual-use. This is a critical oversight since defining if a product is dual-use has legal and policy implications, such as import and export regimes. Therefore, more conceptual clarity is needed to support the required legal and policy discussions on DUTs and HW. Besides, there have been significant technological breakthroughs since Hoffman's 2007 work, which require revisiting his thinking on technology and conflict.

Before discussing DUTs, let us outline the core causal mechanisms that constitute HW; these could become the building blocks of the discussion on the role of technology in modern war. To make a detailed account of HW, Hoffman borrows ideas from three concepts. Firstly, he studies "fourth generation warfare", which highlights the rising role of non-state actors in modern conflict. Specifically, those actors are filling in the political

vacuum created by the central government of fragile states. Secondly, the officer draws parallels with "compound warfare", suggesting that due to the advent of communication devices, the units across the extended battlefield can now reach an entirely new level of operational coherence or multi-domain coordination. Finally, he studies the ideas of "unrestricted warfare" that today, there are many more operational domains beyond the traditional land, sea, and air, and, importantly, the cost of entering into a new domain is decreasing. For instance, cyber operations do not require decades-long investment into heavy military equipment and specialized training, such as in the naval domain. The analysis would examine if DUTs have a role in each of those causal mechanisms.

4. DUAL-USE TECHNOLOGIES

Dual-use items and, specifically, DUTs refer to technologies such as thermal imaging and telecommunication jamming, which can be utilized for both civilian and military purposes. The term gained prominence during the Cold War, particularly through the development of export control regimes aimed at preventing the Soviet Union from accessing military-relevant items. Dual-use was used to describe any items that could support the West's adversaries in rebuilding their industrial infrastructure and war potential. The nomenclature was also used as a security protocol for the classification of defense-related research and development (R&D). Those policies were developed and regulated by the NATO allies, Australia and Japan, through the Coordinating Committee for Multilateral Export Controls (CoCom), which was phased out after the Cold War.

The end of the Cold War brought about significant changes in DUTs policy that remain relevant to the present day. Firstly, economic pressures and concerns over market competitiveness took precedence over export control issues, leading to the relaxation of regulations. This shift was exemplified by the Wassenaar Arrangement, which, in comparison to CoCom, has a larger membership and a reduced scope of regulated items due to the broader trend toward liberalization of trade and industry collaboration. Secondly, the rapid advancement of the digital age has significantly changed how DUTs are developed. During most of the Cold War, the direction of technology transfer was described by the concept of "spin-off", that is the potential of military technologies to be adapted for civilian purposes. This approach led to significant innovations in aerospace and computing. Towards the end of the Cold War, the focus shifted to the military benefiting from civilian technologies, which also changed the language to "spin-on". Spin-on technologies are relevant to this day, as exemplified by digital information technology. Importantly, because of its comparative advantage in innovation and agility, the private sector has played a significant role in driving the shift towards spin-ons, as firms could more rapidly develop and commercialize new technologies compared to government-led R&D efforts. These tendencies have motivated the establishment of accelerator programs such as NATO's DIANA and the EU's HEDI, which aim to harness the potential of startups for the benefit of the security and defense sector.

While institutional initiatives address DUTs, defining them remains complex and contested. Some argue that dual-use is an inherent property of technologies, while others emphasize intent and contextual factors such as regulatory frameworks and geopolitical concerns [8]. Recent scholarship highlights how the classification of a technology as

dual-use depends on its application and perceived risks, leading to varying policy approaches. This ambiguity complicates efforts to balance innovation with security.

For the purposes of this article, DUTs are defined broadly as technologies with both civilian and military applications, which understanding is aligned with Regulation (EU) 2021/821 of the European Parliament and of the Council of the EU setting up a regime for the control of exports, brokering, technical assistance, transit and transfer of dual use items. To be sure, what makes any good, software or technology dual-use is a complex question, and it is outside the scope of this article to account for all of those complexities. This article thus has limitations: it does not focus on a single case study in detail; instead, it provides illustrative examples and their possible implications for HW in order to lay the foundations for a broader discussion on DUTs and emerging security challenges.

5. HYBRID WARFARE AND DUAL-USE TECHNOLOGIES

The opening argument was that DUTs both enable hybrid actors and help counter HW. By drawing on Hoffman's investigation of HW and other literature on the role of emerging technologies in modern conflict, below this article explores both scenarios.

5.1. Dual-use technologies as an enabling factor for hybrid warfare

Firstly, Hoffman is a supporter of the idea, earlier operationalized by the concept of "fourth generation warfare", that non-state actors are becoming increasingly more potent, even though they do not enjoy the warfighting resources and capacities that a state has. In his seminal work, the officer studies how Hezbollah leverages various regular and irregular tactics against Israel. The Shia militant group's approach fits the definition of HW. DUTs empower such non-state aggression in at least two ways. On the one hand, they help non-state actors utilize the information vacuum, left by failing states, which increases the legitimacy of these non-state actors and empowers them to wage hybrid wars against local and neighboring governments. Specifically, information technologies are versatile and allow non-state actors to accomplish several tasks in the information domain simultaneously and efficiently. For example, on social media and other digital platforms, non-state actors could spread propaganda, mount psychological warfare against any entity, and recruit new fighters to support their operational readiness.

On the other hand, the lower operational cost of DUTs allows non-state actors to develop more traditional warfighting capabilities beyond the information domain. For example, DUTs help non-state actors gather open- and closed-source intelligence, as well as conduct cheap reconnaissance and surveillance. Technologies that were once exclusive to the state, such as geospatial intelligence satellites, are now available in the civilian market, with private companies offering high-resolution satellite imagery with attractive payment plans. Further, state militaries, national laboratories, universities, and industry groups were once the only entities with access to advanced technologies. However, commercially available DUTs are now equipping non-state actors with advanced capabilities to wage conflict in the physical domain. The low barriers to entry associated with commercially available technology are empowering non-state actors to level the playing field against well-funded national militaries. For example, technologies such as additive manufacturing (that is, 3D printing) and unmanned aerial vehicles allow

these non-state groups to manufacture and deploy sophisticated weapons without the need for extensive resources or specialized training. Having access to kinetic items with significant firepower, coupled with the freely available know-how from the Internet on how to use those operational capabilities, empowers non-state actors to wage HW.

Secondly, "compound warfare" is another concept that Hoffman uses to inform his thinking on HW. This mode of war is characterized by complete operational integration between regular military forces and irregular troops. This synergy enhances the operational effectiveness since it leverages the distinct strengths of both conventional and unconventional forces. When Hoffman analyzed "compound warfare", he concluded that irregular forces have historically served as a strategic supplement but have not effectively complemented the warfighting at the tactical level. The officer examined cases such as the British Expeditionary Force's involvement in the Arab Revolt against the Ottomans. These cases demonstrated how irregular forces were valuable for strategic objectives yet faced challenges in seamlessly integrating with day-to-day operations due to the slow military communications at the time. Hence, to Hoffman, this characteristic of HW did not exist in the past. Yet, the contemporary landscape has shifted significantly as a result of easy access to sophisticated telecommunications and intelligence tools. Owing to such DUTs, irregular forces can now effectively integrate into the command structure of regular armies, resulting in closer coordination and operational cohesion.

A telling example is the International Legion of Territorial Defense of Ukraine that operates under the command structure of the Armed Forces of Ukraine. DUTs and, more specifically, telecommunication devices have enabled such efforts. These technologies are versatile and facilitate real-time communication, strategic planning, and operational execution, dismantling the barriers that previously impeded tactical and operational cohesion. Modern telecommunication devices enable secure and instant communications between irregular and regular forces in Ukraine, ensuring alignment of strategic targets and effective coordination in the theatre of operations. Further, advanced intelligence-gathering tools enhance situational awareness, allowing irregular forces to operate with a level of precision that was previously unattainable. This technological evolution supports a more integrated approach to modern warfare, where the distinction between regular and irregular forces becomes less pronounced. The capability to seamlessly merge these forces at both operational and tactical levels enhances overall military effectiveness and demonstrates the transformative impact of modern technology on HW.

Thirdly, "unrestricted warfare" is another concept that influenced Hoffman. This concept, originally coined by two Chinese colonels, opened the USMC officer to the idea that warfare is no longer confined to the traditional military arena. Today, there are new operational domains that a technologically inferior actor can employ to offset its relative weakness against a superior adversary; examples of new forms of conflict are lawfare, economic, psychological, and cultural warfare. To develop their concept, the two Chinese colonels recognized that globalization and technological advancements have led to the creation of different operational domains, compelling political and military decision-makers to integrate all available means of warfare. Emerging DUTs can enhance the ability of actors to engage in HW by providing access to new operational domains, such as the cognitive one, for a much lower cost. For instance, while generative AI is proving beneficial for many civilian applications, it also has malicious uses when

utilized in psychological warfare [9]. Cognitive technologies like deepfakes enable actors to manipulate information, orchestrate coordinated disinformation campaigns, and conduct psychological operations with very high effectiveness. The capability to produce realistic fake videos or audio recordings can erode public trust in institutions, create confusion, and sway public opinion, making these DUTs potent tools in HW.

AI tools can also be weaponized to target civilian infrastructure, a hallmark of HW and "unrestricted warfare". AI enables malicious actors to execute cyberattacks in a cheap, effective, and automated manner by employing software that scans large datasets (e.g. Shodan) for vulnerable systems [10]. These cyber capabilities can be employed for financial gain or the disruption of critical services, undermining public trust in state institutions. This targeting inflicts damage and also serves to demoralize societies, making it an effective tool in the HW arsenal. Additionally, the deniability associated with such operations allows malicious state and non-state actors to distance themselves from these activities, providing a layer of protection against direct reprisal. For example, states often deny their affiliation with hacker groups or other non-state actors engaged in these malicious activities, much like how Russia has consistently denied involvement with various cybercriminal organizations that serve its geopolitical interests. The plausible deniability not only complicates the process of attributing cyberattacks and propaganda campaigns to specific actors but also muddies the waters of retribution. By obscuring the true source of these actions, actors operate in a “grey zone” where the distinction between state-sponsored and independent actions is deliberately blurred. This ambiguity makes it difficult for targeted states to mount a coherent and justified response to HW, whether through diplomatic channels, economic sanctions, or military action.

5.2. Dual-use technologies as a countering factor for hybrid warfare

Having introduced scholars, experts, and military officers to the new hybrid mode of war, Hoffman then suggests a way forward to ensure the West does not fall victim to HW. One can distinguish three policy recommendations within Hoffman’s work. The analysis below explores how DUTs support the implementation of those policy ideas.

Firstly, to deny hybrid attacks, Hoffman calls for an increased resilience of national critical infrastructure. Hybrid actors often target such infrastructure that can be military (e.g. naval bases) and non-military (e.g. electric grids). Manufacturing and deploying DUTs enhances national resilience. That is, due to the heavier regulations, DUTs must comply with more standards, frequent inspections, and rigorous quality control. These stricter production protocols lead to increased performance, reliability, and safety, which results in a more resilient technology in comparison to that with a single purpose. For example, a dual-use global positioning system, manufactured in the United States (US), needs to comply not only with the International Organization for Standardization’s (ISO) standards (e.g. ISO 17575 and 14819 Series), but also with the US International Traffic in Arms Regulations, which impose additional and more stringent standardization. Thus, modifying civilian technologies into DUTs creates significant technical challenges, as military systems must last longer and perform better, even in adversarial conditions.

Yet, if those challenges are overcome, the final product is more robust and reliable which makes it a difficult target for any hybrid adversary. Importantly, those challenges are indeed manageable as companies that manufacture DUTs generally have access to

more resources for R&D and, once there is a minimum viable product, for testing. For instance, in 2020, the US Department of Defense awarded private companies 600 million dollars to test 5G technologies. A spokesperson for the Pentagon stated that this deal was a win-win: The government benefited from adopting an advanced technology that enhances the lethality of US troops and the effectiveness of US military communications, while the innovators gained access to well-equipped testing ranges, which are otherwise difficult to obtain [11]. This resulted in more robust 5G technologies, which can greatly increase the resilience of crisis communications in the event of a hybrid campaign.

Secondly, Hoffman suggests that Western forces need to achieve full operational capability to conduct multi-modal warfare to match the hybrid adversaries' tactical advances in case of all-out HW. There exist various new DUTs, which can enhance allied forces' interoperability and cohesion across the different domains of operations. For example, virtual reality (VR) simulators already provide a cost-effective alternative to military exercises. In addition to being more affordable than physical exercises, VR systems have two additional advantages, specifically in relation to achieving more operational cohesion. On the one hand, VR technology is not constrained by time and can easily bring together different armed forces located in different time zones, which is otherwise a significant logistical burden. On the other hand, they are not constrained by space either. That is, VR can simulate mixed terrains, whereby the navy, the army, and other units operate together to test their capacity to wage combined arms warfare in different domains such as land, water, and air. To be sure, VR technologies are not going to replace real-life military exercises soon, but they can already scale up the training regimen and provide options for iterative learning since VR allows officers to commit operational mistakes without the physical consequences incurred during real exercises.

Except for human interoperability, mainly achieved through military training and exercises, DUTs can also increase technical interoperability so that different military assets such as tanks, boats, and fighter jets can "speak" to each other. For example, the new large language models (LLMs) can facilitate the communication between various military platforms. Armored vehicles, military airplanes, and other capabilities often use distinct communication protocols and diverse data formats, mainly due to manufacturing and design differences. LLMs can be trained as a real-time "translator" that converts the different data formats into the same standard. In other words, data interoperability, whose popularity is currently surging within data science circles, can contribute to military interoperability. In addition, AI models can be programmed to recognize warfighting patterns, thus providing recommendations to increase operational cohesion. A key feature of hybrid adversaries is that they quickly adapt to create surprise. Allies could thus utilize DUTs to maintain shared situational awareness and act accordingly.

Thirdly, Hoffman argues that allies need to enhance their capability to degrade any adversary's operational cohesion during HW. If the distinguishing feature of a successful hybrid actor is their capacity to seamlessly integrate different units across various domains, then a critical task is to disrupt their command, control, and communications (C3) systems, which are the "central nervous system" of any forces. A compromised C3 system would thus cost a hybrid actor's ability to wage multi-modal operations. In general, there are three ways to target C3: jamming, deception, and destruction. DUTs could support the execution of all those tasks. For example, jamming antennas have been

available since the 1990s and are useful for electronic warfare as well as the protection of civilian airports and other high-value public spaces. More recently, advanced capabilities such as swarm drones present new options to jam the radar systems of an adversary. Regarding deception, an obvious candidate is social media, which is already the weapon of choice for conducting cost-effective psychological operations (PSYOPS) through posting fake images and videos. A remarkable new development in the PSYOPS field is holographic projection technologies. Such tools can simulate the presence of troops or vehicles and, in effect, distort the enemy's situational awareness, especially in low-visibility weather conditions. Companies such as Hypervision Technologies claim to already offer such innovative solutions [12]. Finally, if the destruction of C3 systems is concerned, advanced cyber software can be used to disable the servers. Allied forces have already used such cyber capabilities to damage the critical infrastructure of hybrid actors. A telling example is the Stuxnet attack. Yet, another option is to utilize the same microwave technology, which is used for heating and drying. Microwave weapons exist and, if directed at enemy command centers, can permanently damage electrical circuits.

5.3. Academic and policy implications

The above findings underscore the necessity for a nuanced approach to leveraging DUTs, balancing their potential to advance multimodal military capabilities against the risks posed by their misuse by hybrid actors. Table A sums up the findings. Yet, further research is required to fully understand the dynamic nature of DUTs vis-à-vis HW.

Table 1. Summary of findings

	Causal mechanism	***Technology example***
DUTs enabling HW	The lower costs of DUTs empower non-state actors	3D printing and unmanned aerial vehicles
	DUTs support regular and irregular troops' integration	Instant and secure communication networks
	DUTs create new easy-to-access operational domains	Cognitive technologies such as deepfakes
DUTs countering HW	DUTs have stricter production protocols, enhancing resilience	Global positioning systems, manufactured in the US
	DUTs help human and technical interoperability	VR technology for cost-efficient military exercise
	DUTs can be used to degrade the adversary's C3 systems	Holographic projection tools to distort situational awareness

One topic of scientific and practical value is related to regulatory measures. More specifically, future research should delve into how regulatory frameworks can strike the right balance between ensuring security and empowering dual-use innovations by means of public-private partnerships. The EU's Defence Industrial Strategy and NATO's newly adopted Industrial Capacity Expansion Pledge share the common goal of accelerating new technologies to sharpen allied technological edge through innovation and strategic

partnerships. A challenge lies in designing trade controls and regulations that effectively limit adversaries' access to sensitive technologies while empowering innovation from the free market. Governments must explore ways to align national security interests with commercial priorities, recognizing that restricting technology transfer can also benefit private companies by reducing technology theft and safeguarding intellectual property. Future research should focus on the ways to foster public-private partnerships to develop shared strategies that balance enforcement costs with mutual gains, ensuring strategic competitors cannot exploit regulatory gaps. Additionally, studies could explore adaptive regulatory mechanisms that evolve alongside new technologies and innovation cycles. Such research would investigate how to streamline export control processes, harmonize international trade laws, and integrate advanced compliance tools. By addressing these questions, research can offer actionable solutions for improving government-industry collaboration and strengthening the resilience of civilian and defense assets against HW.

While more research is required to further exploit the effect of DUTs on HW, the present findings can inform several policy recommendations. Clearly, to derive value from DUTs while minimizing the associated hybrid risks, the West needs to outsmart and outperform its adversaries in regard to defense innovation. The policy challenge lies in the fact that, unlike hybrid actors such as Russia, where technological R&D is driven by the central government and directly deployed in the military, the innovation in the Euro-Atlantic area takes place mainly in the private sector, where startups and innovators compete by virtue of their ideas. Certainly, the free market leads to better technological advancements, yet the military potential of those innovations is not automatically realized to the benefit of the end-users in the security and defense sector. International defense accelerators such as NATO's DIANA are starting to bridge those gaps, but they still suffer from several shortcomings that need to be addressed at the policy level.

Firstly, the traditional capability development process in the defense sector requires extensive technical documentation. The primes in the military-industrial complex have mastered those requirements. However, startups do not have the staff, time, or culture to record the entire process of their product development. As a result, when a business opportunity arises to collaborate with the defense sector, innovative companies face the significant challenge of retroactively creating extensive technical documentation, which often discourages them from engaging with the public sector. This institutional mismatch needs to be addressed by removing some of the bureaucracy while educating young innovators on why basic documentation is still critical to a successful product lifecycle.

Secondly, national and intergovernmental institutions use specific language that is unfamiliar to startups. For example, both the EU and NATO use the so-called technology readiness level (TRL) to measure the development stage of any product. Yet, the TRL scale is unknown to most entrepreneurs who instead use more intuitive language such as "prototype" and "minimum viable product". Institutions should make every effort to be easily understood by the broader innovation community. Thirdly, organizations such as NATO tend to proliferate many institutional formats, which offer startups multiple points of entry into the defense sector, but at the same time, create confusion and corporate anxiety about the best way to pitch one's innovation idea. For example, the distinction between DIANA and NATO's Innovation Fund, another recently established Allied tool for public-private partnerships, remains unclear to targeted startups. Instead,

the defense sector would benefit from offering innovators a very clear workflow that efficiently utilizes their corporate time and resources to tackle hybrid threats.

6. CONCLUSION

The analysis confirmed the initial hypothesis: DUTs have a transformative impact on how HW is waged and defended against. New technologies such as thermal imaging enable hybrid aggressors but can also serve as countermeasures against HW. DUTs empower hybrid actors by lowering the barriers to the acquisition and deployment of advanced technologies. This results in higher operational integration of regular and irregular units and in the creation of new domains of operations such as the cognitive sphere, which can be exploited by hybrid actors. At the same time, DUTs strengthen the national resilience, interoperability, and counter-HW capabilities of allied governments by virtue of technological advancements in critical infrastructure, training simulators, and counter-C3 operations. It is thus highly recommended that researchers, experts, and decision-makers in the defense sector consider DUTs when examining or responding to cases of HW. This article suggest that, in doing so, they need to develop a sophisticated strategy that ensures a judicious balance between DUTs' role in advancing multimodal military capabilities and the risks associated with their potential misuse by hybrid actors.

ACKNOWLEDGMENT

This research was supported by the GATE project, funded by the H2020 WIDESPREAD-2018-2020 TEAMING Phase 2 programme, under grant agreement no. 857155.

REFERENCES

[1] Tucker, J.B. Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies. The MIT Press, US, 2012, (368 p.)

[2] Mazal, J. The Dual Use of Civilian and Military Technologies in the Battlefield of the Future. In book *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment. Studies of the Central European Professors' Network* (eds. Zombory, K., Szilágyi, J.E.), Central European Academic Publishing, Miskolc-Budapest, Hungary, 2024, Chapter 6, pp. 259-307.

[3] Geri, M. EU-NATO Cooperation and Innovation in Emerging Disruptive Technologies to Stop Russian-Chinese Hybrid Warfare in the Energy Transition. *Security and Defense Scientific Journal*, vol. 2, 2024, pp. 19-36.

[4] Jasper, S. Resilience Against Hybrid Threats: Empowered by Emerging Technologies – A Study Based on Russian Invasion of Ukraine. In book *Handbook for Management of Threats. Springer Optimization and Its Applications* (eds. Balomenos, K.P., Fytopoulos, A., Pardalos, P.M.), Springer, Germany, 2023, Chapter 10, pp. 209–226.

[5] Hähnel, M. Conceptualizing Dual Use: A Multidimensional Approach. *Research Ethics.* Advance online publication. https://doi.org/10.1177/17470161241261466

[6] Hoffman, F.G. *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, December 2007. URL (Visited on 19.08.2022): https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[7] Libiseller, C. 'Hybrid warfare' as an academic fashion. *Journal of Strategic Studies*, vol. 46, no. 4, 2023, pp. 858-880.

[8] Hähnel, M. Conceptualizing Dual Use: A Multidimensional Approach. *Research Ethics.* Advance online publication. https://doi.org/10.1177/17470161241261466

[9] Kreps, S. *Democratizing harm: Artificial intelligence in the hands of nonstate actors*, Brookings, Nov 2021. URL: https://www.brookings.edu/articles/democratizing-harm-artificial-intelligence-in-the-hands-of-non-state-actors/ (Visited on 11.08.2024).

[10] *Addressing risks from non-state actors' use of commercially available technologies*, US Department of Homeland Security, 2022. URL: https://www.dhs.gov/sites/default/files/2022-09/Addressing%20Risks%20from%20Non-State%20Actors.pdf (Visited on 31.07.2024).

[11] Lopez, C.T. *DOD Kicks Off World's Largest Dual-Use 5G Testing Effort*, US Department of Defense, Oct 2020. URL: https://www.defense.gov/News/News-Stories/Article/Article/2378047/dod-kicks-off-worlds-largest-dual-use-5g-testing-effort/ (Visited on 09.11.2024).

[12] *Next-Gen Defense: 5 Ways Holographic Display Tech Supercharges Military Operations*, Hypervision Technologies, Sep 2023. URL: https://hypervision.co.in/next-gen-defense-5-ways-holographic-display-tech-supercharges-military-operations.html (Visited on 10.11.2024).

Information about the authors:

Borislav Bankov is a project leader at the GATE Institute, where he is responsible for GATE's role as a NATO test center for dual-use technologies. Prior to GATE, he worked at NATO and Europol. His research focuses on the EU's and NATO's response to hybrid warfare.

Stefan Bojilov is a BSc student of International Relations and Organisations at Leiden University and a former trainee project manager at the GATE Institute. His duties were related to GATE's role as a NATO technology test center, as well as research on hybrid warfare and disinformation. He is currently an intern at NATO Headquarters Allied Joint Force Command Brunssum.

Manuscript received on 28 December 2024