ARMIS et LITTERIS

The Defence Horizon Journal

WarTech Nexus | Theresan Military Academic Forum 2025 | Armis et Litteris 48

WarTech Nexus: Industrialising the Future of Autonomous Warfare

Theresan Military Academic Forum 2025

EINSATZBEREIT FÜR ÖSTERREICH

BUNDESHEER.AT

UNSER HEER

IMPRINT

MEDIUM OWNER, PUBLISHER AND PRODUCER:

Republic of Austria,
Federal Ministry of Defence (BMLV),
Roßauer Lände 1, 1090 Vienna

EDITORIAL OFFICE:

BMLV, Institute for Basic Officer Training,
Theresan Military Academy,
together with
The Defence Horizon Journal,
ISSN: 2710-3722

COVER DESIGN,

Lukas Bittner
Cover picture: shutterstock.com/RoProy and Bundesheer/Paul Kulec

TYPESETTING AND LAYOUT:

Lukas Bittner

PRINTING:

BMLV / Army Printing Centre (Heeresdruckzentrum),
Arsenal, 1031 Vienna, Kelsenstraße 4
ISBN: 978-3-9505531-5-4

30. 10. 2025

ARMIS et LITTERIS
und
THE DEFENCE HORIZON JOURNAL

WARTECH NEXUS: INDUSTRIALISING THE FUTURE OF AUTONOMOUS WARFARE

THERESAN MILITARY ACADEMIC FORUM 2025

PUBLICATION SERIES OF THE THERESAN MILITARY ACADEMY

48 EDITION

More Information

https://www.milak.at/tmaf2024

and

https://www. https://www.tdhj.org/

FOREWORD

Honourable generals and officers, esteemed rectors, scientists, dear cadets and students, and dear friends of the Theresan Military Academy! Respected readers!

TMAF 2025 was a huge success! TMAF is a venue where brilliant minds converge and exchange innovative research approaches, scientific methodologies, and contemporary research designs. It is, indeed, a place of mutual learning. Sharing scientific insights and learning from one another are certainly the noblest practices that can occur in science. We gather at this esteemed conference to receive feedback from our peers, refine our ideas, explore new research avenues, and ultimately publish outstanding papers. I am proud that we are embedded in the global scientific community. It is an absolute pleasure to welcome so many wonderful international research partners and friends from various countries, military universities, and research institutions. We stand together in our task to provide meaningful research. International cooperation and joint projects in the Military Sciences are so important. We provide our society certainty and security, even in the most turbulent times. We protect the foundations of democracy. We defend our values and our democratic ways of living. There is that axiomatic proverb: “Si vis pacem, para bellum”. If you desire peace, prepare for the war. An essential part of that is what we are doing right here, too: excellent research in the military sciences. It is novel, interesting, and meaningful. It is driven by issues and problems we face in practice. Crucial military questions arise from a practice-driven craving for answers from rigorous science, and scientific insights provide innovative pathways for practice, enabling new and fascinating questions. This is research, this insatiable curiosity to understand more rather than less. The results of our research efforts have led to innovation and further developments, such as dual-use projects. It is in this sentiment of scientific endeavour that I invite you to read and enjoy the following contributions! Hoping to see you all again at TMAF 2026!

Dr. Michael König, MBA
Chair University of Applied Sciences Board

FOREWORD

Modern Technologies and Warfighting

The beginning of the 21st century marked a significant shift in the traditional pattern of conflict that had been familiar up to that point. Digitalisation, the development of potent information technologies and Artificial Intelligence, created the conditions for a revolution in warfare. A decisive developmental step was achieved, namely the increasing automation and autonomisation of military weapons systems.

Today's international armed forces are equipped with modern weapon systems that make it possible to have a lethal effect at any time, anywhere in the world and without endangering their own personnel. The boundaries of space and time have thus been significantly altered for military operations. The previously known parameters for military operational thinking—i.e., force, space, time, and information—are beginning to change as a result, and new possibilities also arise at the strategic level regarding the use of means.

In contrast to a nuclear missile with its devastating area effect, the military now has a family of unmanned weapon carriers and weapon systems at its disposal, which promise an unprecedented precision in the use of weapons in the air, on land and on water. The next step in warfare was taken with the human-made possibility of using unmanned, semi-autonomous, robot-like weapon systems. The remote-controlled deployment of airborne, unmanned, designated reconnaissance systems and their increasing use for the transfer and deployment of lethal weapons open previously undreamed-of possibilities for modern armed forces.

In the longer term, it can be assumed that ultimately, fully autonomous reconnaissance and weapons systems using low levels of artificial Intelligence will be able to independently resolve situations of moderate complexity at the end of a corresponding development process. The current development of such systems, along with their advantages and disadvantages, must therefore be clearly addressed by military and political decision-makers to the broader public. With the selection of our topics for the Theresan Military Academic Forum, we are helping to identify the current and future requirements for military professionals to develop the necessary skills in basic officer training.

Colonel (GS) Dr. Markus Reisner, PhD
Programme Director & Head of the Institute for Basic Officer Training at the Theresan Military Academy

FOREWORD

We live in an era marked by uncertainty, where shifting power balances, technological disruption, and renewed geopolitical rivalry force us to rethink what war means. The conflict unleashed by Russia's invasion of Ukraine has reminded Europe and the broader world that war is neither a relic of the past nor confined to distant regions. At the same time, it has accelerated trends that will shape the future of conflict for decades to come.

The pages that follow invite readers to explore this transformation. They argue that the wars of tomorrow will be unlike the conventional images of massed armies or decisive battles. Instead, war is increasingly hybrid in nature—blending military force with economic, technological, and informational means, often remaining below the threshold of formal declarations. Disinformation campaigns, cyberattacks, sabotage, and political manipulation already blur the line between war and peace. What was once a clear distinction has become a grey zone of constant competition and instability.

This hybridisation of conflict is not happening in isolation. It is driven by deeper forces: ageing populations, climate change, widening inequality, governance crises, and rapid technological innovation. Together, these global dynamics intensify power rivalries, pull states into new arenas of competition, and stretch existing political and legal frameworks beyond recognition. The result is a world where conflict feels omnipresent, shifting from distant battlefields to the very fabric of society.

As this book shows, the scope of war is expanding in striking ways. The Arctic, once a remote frontier, is becoming a hotspot of competition as melting ice reveals untapped resources and new shipping routes. Outer space, essential for modern communication and militaries, risks becoming the next battlefield as major powers test the limits of outdated treaties. And perhaps most unsettling of all, the human mind itself is emerging as a domain of conflict. In an age of "cognitive warfare," perception and decision-making can be manipulated as easily as territory once was.

Technology sits at the heart of this transformation. Artificial intelligence enables autonomous systems, advanced reconnaissance, and lightning-fast data analysis, promising both operational superiority and profound ethical challenges. Social media platforms amplify influence operations, making disinformation cheaper, faster, and more targeted than ever before. Meanwhile, breakthroughs in neurotechnology and biotechnology blur the boundaries between human and machine, soldier and civilian, promise and peril. Brain-computer interfaces, enhanced performance, and even engineered biology may redefine what it means to fight, to resist, or simply to remain human.

The ethical questions raised are urgent. Should states demand biological or neurological enhancements of their soldiers? Can societies preserve human dignity in the face of weaponised science? And how can laws designed for an earlier age of war be adapted to realities where conflicts are fought across borders, infrastructures, and minds?

This foreword cannot offer definitive answers, nor does the book claim to predict the future with certainty. What it does offer is a framework for thinking about what lies ahead. It reminds us that war is not vanishing; it is mutating. It urges us to see hybrid conflict not as an anomaly but as the new normal. It challenges us to grasp that the Arctic, space, and the human mind are no longer abstract frontiers but contested domains of power. And it calls on us to confront the double-edged nature of technology: a source of resilience and innovation, but also of vulnerability and control.

As you turn the pages, you will find not only an analysis of these trends but also a deeper question running throughout: are we witnessing a radical break from the past, or merely the latest stage in humanity's long struggle over power and survival? The future of war may lie somewhere in between. However, its shape will undoubtedly affect every individual, every society, and every institution.

This book is an invitation to reflect, to question, and to prepare. It asks us to think not just about the future of war, but about the future of humanity in a world where war itself refuses to disappear.

Colonel Daniel Hikes-Wurm
Department of Defence Policy and Strategy at the Austrian Federal Ministry of Defence

PROLOGUE

The University of Applied Military Sciences has to provide practical training at university level. The skills taught must be such that the officers being trained can meet the current and future demands of the military profession, in line with the latest scientific findings. This requires teaching and research staff who are qualified in science, professional practice, and education. Application-oriented research and development work by members of the teaching and research staff underscores this expertise. Scientific symposia, such as our Theresan Military Academic Forum (TMAF), ensure that disciplinary knowledge and ongoing scientific research and development can be integrated into research-led education, thereby contributing to excellence.

Our annual TMAF has been moved from autumn to spring for organisational reasons. This required considerable effort, as it had a significant impact on both the follow-up to last year's event and the preparation for this year's event. The TMAF provides the necessary framework, but it relies exclusively on the quality and commitment of the speakers, as well as the sustainability of the publications. We would therefore like to express our sincere thanks to the numerous international speakers and authors, as well as the reviewers working behind the scenes for our partner, The Defence Horizon Journal. We are all pleased that this step has been completed with the publication of our 'Armis et Litteris'.

Digitalisation, automation and autonomisation have profoundly changed modern warfare. The use of artificial intelligence and machine learning is just one example of developments that are influencing current and future warfare and, among other things, presenting military strategists, the Western community of values and international legal norms with new challenges. We therefore explored the question: 'Is the global West losing its edge in warfare?'

In this Armis et Litteris, we are publishing 17 articles by authors from 14 nations. The authors teach and/or conduct research at military and civilian higher education institutions, or work in industrial companies in this field. Their valuable contributions to current and future autonomous warfare can be read here. We hope you enjoy reading these valuable articles.

Colonel Michael Moser
Head of the Organising Committee

CONTENT

01

INNOVATIVE TECHNOLOGIES IN THE DEVELOPMENT OF EXPLOSIVES AND PYROTECHNICS FOR MODERN WARFARE

DORIS DASOVIĆ

- **Author:** Doris Dasović; military applications, explosives engineering; military engineering, technology studies. The views contained in this article are the author's alone and do not represent the views of the Croatian Ministry of Defence.

- **Abstract:** Explosives and pyrotechnics play a critical role in modern military technology. Recent advancements in nanotechnology, artificial intelligence, and 3D additive manufacturing are transforming the development, applications, and safety of these technologies. This paper examines how these disruptive technologies shape the future of explosives while addressing the challenges of their ethical application. Special attention is given to AI's ability to detect, deactivate, and defend against explosive threats, significantly impacting military doctrines.

- **Problem statement:** How do innovations in explosives and pyrotechnics challenge traditional military applications and doctrines?

- **Bottom-line-up-front:** Disruptive technologies are revolutionising explosives, requiring careful consideration of their risks and applications.

- **So what?:** Militaries, policymakers, and researchers must collaborate to responsibly develop and implement these technologies in order to modernise capabilities while addressing ethical challenges

The Role of Explosives and Pyrotechnics in Military Technology

The rapid evolution of technology has introduced unprecedented innovations in military applications, particularly in pyrotechnics and explosives. Developments in nanotechnology, artificial intelligence (AI), and three-dimensional additive manufacturing ("3D printing") have transformed the design, deployment, and security of explosive devices. These new technologies hold immense strategic benefits in military applications, but also raise serious geopolitical and ethical concerns.[1]

Explosives have been a key component of military operations for centuries, with ongoing advancements making them more precise, powerful, and effective. Pyrotechnics, such as signal flares and illumination rounds, have also evolved to serve in critical tactical roles. The development of smart explosives and sophisticated detonation systems has transformed battlefield strategies. However, these innovations must be carefully managed to prevent misuse and mitigate risks posed by non-state actors.[2]

The evolution of explosive materials has been a cornerstone of military engineering, progressing from black powder to today's compounds. The introduction of TNT, RDX, and PETN in the 20th century revolutionised explosive power and efficiency. The first recorded use of black powder, a mixture of charcoal, sulfur, and potassium nitrate, dates to 9th-century China, where it was employed in early firearms and rudimentary explosive devices. The introduction of nitroglycerin in the 19th century marked a significant leap forward, though its instability limited its practical applications. This challenge was overcome with the invention of dynamite by Alfred Nobel in 1867, which provided a safer and more manageable form of explosive power.[3]

The 20th century witnessed further breakthroughs with the development of high-explosive compounds, including TNT, RDX, and PETN. These materials offered greater stability, increased explosive force, and enhanced versatility, revolutionising both military and industrial applications. As technology continues to advance, modern research focuses on producing explosives with controlled detonation properties, reduced environmental impact, and improved safety in handling and storage. Understanding the historical progression of explosive materials is essential to appreciating the innovations that now define modern military strategy.[4]

More recently, nanotechnology has enabled the development of more powerful yet controlled explosive materials. By manipulating substances at the molecular level, scientists can enhance stability and effectiveness, reducing accidental detonations while maximising impact.[5] One notable application is the use of nano-aluminium in energetic materials, which significantly improves combustion rates and overall explosive efficiency. Nano-aluminum particles enhance the reactivity of traditional explosive compositions, allowing for more controlled and predictable detonation sequences. This technology is already being explored for use in advanced military-grade explosives, offering increased power while reducing sensitivity to unintended detonation.[6]

Nanotechnology in Explosives Development

Looking ahead, nanotechnology is poised to play an increasingly significant role in military innovations, particularly in the field of explosives and ordnance. Scientists are already making strides in developing self-repairing nanostructured materials, which could revolutionise the reliability of explosive devices. These materials would allow explosives to autonomously restore structural integrity if compromised before detonation, ensuring their effectiveness in critical combat scenarios.[7] This breakthrough could drastically reduce the likelihood of malfunctions that may render a device ineffective or, conversely, cause unintended detonations.

Additionally, AI-integrated nanotechnology is paving the way for smart explosives with the ability to modify their detonation power based on real-time environmental factors and target characteristics. Current advancements in nanotechnology have already enabled the development of nano-energetic materials that enhance explosive efficiency and stability,[8] while AI-driven targeting systems are improving precision in modern munitions.[9] Some military-grade explosives now incorporate sensor-based fuze mechanisms that adjust detonation based on impact conditions.[10]

However, fully autonomous, AI-regulated explosives capable of dynamically altering their energy output in response to real-time battlefield data remain largely theoretical. While research is underway to integrate nanoscale sensors with AI-driven decision-making systems, such self-adjusting explosives have yet to be deployed in active military operations. Future developments may allow these smart explosives to analyse environmental data and modify their detonation profile accordingly, but these capabilities are still in the experimental phase.[11]

These intelligent explosives could adjust their energy output to maximise damage against hardened targets while minimising collateral impact in civilian areas. Such developments could significantly enhance the precision and efficiency of military operations, providing armed forces with more adaptable and controlled weaponry.[12]

As nanotechnology becomes more deeply embedded in military strategy, governments, defence agencies, and research institutions must collaborate to establish ethical and legal frameworks for its application. Without proper oversight, these advanced technologies could fall into the hands of rogue actors or hostile entities, leading to dangerous and unforeseen consequences. By implementing strict regulatory guidelines and international agreements, the global community can ensure that the advancement of nanotechnology in military explosives remains both responsible and secure.[13]

However, the development of such regulatory frameworks faces significant obstacles. First, the rapid pace of technological innovation often outstrips the ability of policymakers to draft, debate, and implement comprehensive regulations. Many countries prioritise military superiority over regulatory oversight, leading to a lack of transparency and cooperation on international arms control agreements.[14]

Second, nanotechnology is a dual-use technology, meaning it has both civilian and military applications. Many of its advancements are developed for commercial or medical purposes before being adapted for defence, making it difficult to regulate without impacting beneficial industries. This overlap creates a regulatory grey area where military research can continue under the guise of civilian innovation.[15]

Finally, geopolitical tensions and national security concerns often prevent countries from agreeing on enforceable international standards. Nations with advanced military nanotechnology programs may be unwilling to impose restrictions that could limit their strategic advantages. Additionally, enforcing compliance across multiple nations, especially non-allied or rival states, remains a major challenge. Without a coordinated global effort, the risk of proliferation and misuse will continue to grow.

Artificial Intelligence in Explosive Threat Detection

Artificial intelligence is revolutionising the deployment, detection, and neutralisation of explosives in modern warfare. One example is the integration of AI-driven reconnaissance tools with satellite imaging and ground-based sensors to detect and neutralise explosive threats before detonation.[16]

These systems can rapidly process vast amounts of data, recognising potential dangers with a level of speed and accuracy that surpasses human capabilities. According to the U.S. Department of Defence, AI-driven threat detection technologies significantly reduce false alarms while improving the precision of countermeasure deployments.[17]

AI is also transforming explosive ordnance disposal (EOD) operations. Traditionally, bomb disposal has been a high-risk task for human specialists. However, AI-integrated drones and robotic units can now autonomously locate, assess, and neutralise explosive threats with minimal human intervention. These autonomous systems can operate in hazardous environments, reducing the risk to military personnel and increasing the success rate of EOD missions.[18]

Beyond detection and disposal, AI is being utilised for predictive threat analysis. Machine learning algorithms can evaluate patterns of enemy activity and predict the likelihood of explosive threats in specific areas. This proactive approach enables military forces to take preemptive action, mitigating risks before they materialise on the battlefield. AI-powered reconnaissance tools, when combined with satellite imagery and real-time data analysis, can provide invaluable insights into enemy movements and explosive deployment strategies.[19]

Ethical Considerations and Regulatory Challenges

While AI and nanotechnology offer tremendous benefits for military explosives, their integration also raises pressing ethical and security concerns. Determining responsibility in the use of AI-powered systems in warfare may not be as complex as often suggested. Just as a soldier is held accountable for pulling the trigger, responsibility for an AI-enabled action could similarly rest with the human operator authorising or overseeing its use. While it is true that AI lacks moral reasoning and operates on algorithms and data patterns, this does not eliminate the role of human judgment in its deployment. Suppose an autonomous system were to mistakenly identify a civilian as a threat. In that case, the accountability should remain with those who designed, authorised, or supervised its use, much like any other military tool. However, this reinforces the need for clear accountability structures, rigorous oversight, and internationally agreed-upon rules of engagement to ensure ethical and legal use of AI in warfare.[20]

Similarly, adversaries could exploit nanotechnology-driven smart explosives and self-repairing materials if they are not properly secured. There is a growing concern that non-state actors or terrorist organisations could gain access to these advanced technologies, potentially creating highly unpredictable threats. Governments must implement rigorous cybersecurity measures and regulatory protocols to prevent the unauthorised proliferation of these innovations.[21]

The increasing integration of artificial intelligence (AI) and nanotechnology in military applications has prompted discussions on the need for comprehensive global governance frameworks. According to the Carnegie Endowment for International Peace, without proper regulations, the unchecked advancement of AI and nanotechnology in military systems—particularly explosives—could escalate armed conflicts and increase risks to civilian populations.[22] Similarly, the U.S. Department of Defence emphasises that while AI enhances military efficiency, its rapid implementation without ethical oversight may lead to unintended strategic consequences.[23]

However, the debate on AI governance in military applications is far from universal. Western nations, particularly those in Europe, often emphasise adherence to international law and ethical restrictions in military AI and advanced weaponry. In contrast, authoritarian states such as Russia, China, and North Korea prioritise strategic advantage and military dominance, often imposing fewer limitations on their use of emerging defence technologies. This disparity creates a global security dilemma—how can democratic nations uphold ethical leadership in warfare without falling behind in technological capabilities?

This challenge is threefold. First, democratic nations, especially in Europe, must strike a balance between advancing military technology and adhering to moral values. This balancing act becomes increasingly difficult as adversaries who disregard ethical concerns may gain a tactical edge in AI-driven warfare, cyber operations, and autonomous weapon systems.[24]

Second, the lack of a unified ethical and legal standard presents direct security risks. Countries that impose fewer restrictions on AI in military applications may gain strategic superiority, compelling others to weigh the extent to which they are willing to compromise on ethical concerns to maintain deterrence. The Carnegie Endowment for International Peace warns that this technological arms race could undermine existing global security structures and lead to destabilisation.[25]

Third, even among Western allies, differences in ethical, moral, and legal standards impact military interoperability. The United States adopts a pragmatic, capability-driven approach to AI in warfare, while Germany imposes more restrictive oversight. In contrast to these two perspectives, France pushes for technological advancement with a cautious regulatory approach. These disparities create challenges for NATO and allied military operations, where interoperability depends on shared military doctrines and standardised regulations. Effective collaboration requires ongoing dialogue, unified ethical guidelines, and clear protocols for the integration of AI and autonomous systems in joint military efforts.[26]

Ultimately, addressing these challenges requires a strategy that balances ethical responsibility with security imperatives. While maintaining strict moral standards may leave democratic nations vulnerable, an unchecked arms race in AI and autonomous weaponry could destabilise global security. Finding common ground among Western allies—and engaging with broader international players—will be crucial to shaping the future of military technology while preventing ethical erosion in modern warfare.

The Future of AI in Battlefield Intelligence

The continued evolution of AI will further enhance battlefield intelligence and combat capabilities—including those involving explosives and pyrotechnics. Future developments may include AI-driven swarm intelligence, where groups of autonomous drones coordinate in real time to conduct reconnaissance, threat assessment, and even explosive ordnance delivery or neutralisation.[27] These drone swarms could autonomously map enemy positions, identify targets for explosive payload deployment, and relay critical data to command centres without constant human oversight. This technology would enable militaries to execute highly coordinated operations such as area denial using smart explosives, synchronised strikes, and automated mine-clearing missions while minimising risk to human personnel.[28]

The U.S. military and several defence agencies globally are already experimenting with AI-controlled drone swarms that can carry and deploy explosives to assess their effectiveness in complex combat scenarios.[29] AI-powered robotic soldiers equipped with advanced sensors and adaptive learning algorithms could be deployed in hazardous environments, including explosive ordnance disposal (EOD) operations or logistics missions involving transport of pyrotechnic materials [30]. In the future, humanoid or quadruped robots may assist in high-risk explosive tasks alongside soldiers, offering real-time situational awareness and precision handling of volatile payloads.

Moreover, integrating AI with quantum computing will significantly accelerate data processing for applications such as the detection and disarming of improvised explosive devices (IEDs), threat prediction, and decryption of enemy communication related to explosives logistics.[31] This fusion of AI and quantum capabilities could redefine cryptographic and counter-explosive warfare, allowing for faster identification and neutralisation of threats. AI-driven holographic battlefield simulations may also help visualise explosive impact zones or predict chain-reaction risks, aiding tactical planning and minimising collateral damage.[32]

Future AI-powered command centres could simulate scenarios involving explosive usage in urban and open terrain, adjusting deployment strategies in real time. These dynamic simulations would enhance decision-making, reduce operational risks, and improve the precision of explosive engagement in various military contexts.[33]

Ultimately, as AI continues to transform modern warfare, its integration with explosive technologies presents both powerful capabilities and new risks. Ensuring ethical deployment, robust cybersecurity, and international cooperation will be essential to mitigate the misuse of AI in contexts involving pyrotechnics and explosives.[34] Future AI-powered command centres could simulate multiple battle scenarios simultaneously, adjusting strategies based on real-time intelligence and adversary movements. These simulations could provide dynamic war-gaming environments where commanders test various tactical approaches under changing conditions. This would enhance decision-making, reduce operational risks, and improve training for military personnel.[35]

Ultimately, these advancements in AI, robotics, and quantum computing could redefine modern warfare by enhancing strategic agility, reducing human exposure to combat risks, and providing a decisive technological edge in battlefield intelligence. However, the successful implementation of these technologies will require strict ethical oversight, robust cybersecurity measures, and international cooperation to mitigate potential misuse.

3D Printing and Its Military Applications

The rise of 3D printing technology has revolutionised the rapid prototyping and production of explosives and related components. Marciniak notes that fused deposition modelling (FDM) techniques allow for the creation of intricate explosive devices with precise control over material composition and structure.[36] This advancement improves the effectiveness of military ordnance while reducing production costs.

However, the accessibility of 3D printing technology raises concerns about the proliferation of advanced explosive devices. Hossain et al. warn that non-state actors could exploit this technology to manufacture weapons outside traditional supply chains.[37] To mitigate these risks, international regulations and monitoring mechanisms are essential.[38]

While there have been limited confirmed cases of large-scale weapon production by non-state actors using 3D printing, early signs indicate that the risk is growing. Reports suggest that criminal organisations and extremist groups have experimented with 3D-printed firearm components, indicating a potential shift toward more complex weaponry, including explosives.[39]

The primary barriers preventing widespread misuse include the high costs of industrial-grade 3D printers, the difficulty of acquiring stable explosive precursors, and the technical expertise required to create functional explosive devices. However, as these technologies become more accessible and materials science advances, these barriers may weaken over time.[40]

While regulations are often proposed as a solution, their effectiveness in this case is debatable. Non-state actors that might misuse 3D printing for illicit weapon manufacturing operate outside legal frameworks and are unlikely to comply with international treaties. This raises the question of whether international regulations and monitoring mechanisms can effectively mitigate such risks. However, regulations can still play a role in mitigating risks by controlling access to high-performance 3D printers, restricting the availability of specific printing materials used in explosive devices, and monitoring the online dissemination of digital blueprints for military equipment and explosive components.[41] In addition, international oversight can contribute by enforcing stricter export controls on advanced 3D printing equipment. Coordinated intelligence-sharing between nations can also help track and disrupt illicit manufacturing networks before they become a widespread threat.[42]

On the other hand, if the risk of misuse were negligible, the justification for strict regulation would be weaker. The reality lies somewhere in between—while full-scale use of 3D printing for explosive production by non-state actors has not yet been widely documented, the rapid pace of technological development suggests that proactive measures are necessary. Regulations alone may not entirely prevent misuse, but they can act as a deterrent, making it more difficult and costly for unauthorised actors to manufacture advanced explosives. A combination of regulatory oversight, technological safeguards, and law enforcement cooperation will be essential in addressing this emerging challenge.[43]

The military's adoption of 3D printing technology has progressed significantly over the past decade. Initially used for creating non-critical replacement parts and training models, the technology has evolved to facilitate the development of complex components, including weaponised drones, advanced explosives, and battlefield-ready munitions. Additive manufacturing is now being utilised to produce sensor components critical for modern combat operations, improving real-time data collection and battlefield awareness.[44]

One key advancement has been the use of metal additive manufacturing, which allows for printing highly durable and heat-resistant materials suitable for military-grade weaponry. This development significantly enhances the flexibility and efficiency of weapon production, ensuring that militaries can rapidly adapt to emerging threats.[45]

One of the key benefits of 3D printing is its ability to decentralise production. This capability can reduce logistical challenges, allowing for on-demand manufacturing of explosive components in conflict zones. However, it also presents risks, such as difficulties in tracking and controlling the production of dangerous materials. The military must implement stringent cybersecurity measures to prevent unauthorised replication of classified weapon designs.

Furthermore, 3D printing streamlines supply chain management by reducing dependency on traditional manufacturing hubs. Instead of relying on mass production and global transportation, military forces can use portable 3D printing units to create essential parts in remote locations. This innovation reduces vulnerability to supply chain disruptions resulting from political conflicts, economic sanctions, or natural disasters.

This newfound ability to print weapons and replacement parts on demand allows for extended operational capabilities in prolonged combat scenarios.[46] However, it also raises concerns about the loss of centralised control over military technology. Effective policies and regulatory frameworks must be established to prevent unauthorised actors from leveraging 3D printing for malicious purposes.

The ability to manufacture weapons outside of traditional supply chains reduces governmental oversight, making it more difficult to track the production and distribution of military-grade components. This decentralisation could enable unauthorised actors, including insurgent groups and criminal organisations, to acquire and produce advanced weaponry with minimal detection.[47]

Additionally, regulatory efforts can be reinforced through technological safeguards, such as digital rights management (DRM) for 3D-printed weapons and real-time tracking of industrial-grade additive manufacturing machines. Intelligence-sharing between allied nations and tighter export controls on dual-use technologies could further reduce the risk of proliferation. While regulations alone may not prevent misuse, a combination of legal oversight, cybersecurity measures, and international cooperation can create significant barriers that limit unauthorised access to critical 3D printing capabilities.[48]

Beyond logistics, 3D printing is directly influencing the design and fabrication of advanced explosives. Traditional explosives manufacturing involves complex chemical processes that require significant time and resources. With additive manufacturing, military engineers can develop customised explosive devices with precise compositions tailored for specific missions. This advancement enhances lethality, efficiency, and adaptability in modern warfare.[49]

One area of focus is the production of nano-structured explosives. By utilising nano-scale printing techniques, researchers can improve the performance and stability of explosive materials. This technology enables the creation of munitions with controlled detonation characteristics, reducing collateral damage while increasing effectiveness against hardened targets.

Additionally, 3D printing allows for the rapid prototyping and testing of experimental explosive designs. Previously, developing new munitions required extensive manufacturing processes and long testing periods. Additive manufacturing reduces these time constraints, accelerating research and development efforts in military explosives engineering.[50]

The Role of AI in 3D Printing and Explosive Manufacturing

AI is increasingly being integrated into additive manufacturing processes, particularly in the design and optimisation of explosives. AI-driven systems can analyse structural integrity, predict explosive performance, and automate quality control, ensuring that munitions produced via 3D printing meet military standards. While research into AI-enhanced quality control for 3D-printed explosives is ongoing, some applications are already emerging in military manufacturing. AI-driven monitoring tools are being used in additive manufacturing to detect structural inconsistencies and ensure precision in sensor components for military applications. However, the full implementation of AI-driven systems specifically for explosives remains a developing field, with further advancements needed to integrate real-time predictive modelling for detonation efficiency and stability.[51]

According to the U.S. Department of Defence (2023), AI-enhanced 3D printing processes also improve safety by minimising human involvement in handling explosive materials. Automated additive manufacturing systems reduce exposure to hazardous chemicals, decreasing the likelihood of accidents in weapons production.[52]

Additionally, AI facilitates the rapid identification of weaknesses in explosive designs. By running millions of simulations, AI algorithms can refine munition configurations, enhancing effectiveness while minimising unintended detonations. These advancements are crucial for developing next-generation military ordnance with superior precision and efficiency. While research is ongoing, AI is already being applied in military contexts to optimise explosive materials and predict detonation behaviour with greater accuracy. AI-driven modelling has improved the reliability of modern explosives by detecting vulnerabilities in design before deployment. These advancements are crucial for developing next-generation military ordnance with superior precision and efficiency.[53]

Ethical and Security Challenges

Despite the advantages of technological advancements in explosives, ethical considerations remain paramount. The risk of misuse by rogue states or terrorist organisations underscores the need for stringent regulatory frameworks. Governing bodies must implement safeguards to prevent unauthorised access to nanotechnology-based explosive materials.[54]

Additionally, the ethical concerns surrounding AI-driven military operations require careful evaluation. Autonomous weapon systems capable of independent decision-making raise questions about accountability and compliance with international humanitarian laws. The Carnegie Endowment for International Peace emphasises the importance of global governance mechanisms to regulate AI's military applications effectively.[55]

Conclusion and Recommendations

The intersection of nanotechnology, AI, and 3D additive manufacturing is reshaping the landscape of military explosives and pyrotechnics. While these innovations enhance military capabilities, they also introduce complex security, ethics, and international stability challenges.

Military leaders, policymakers, and researchers can leverage disruptive technologies by addressing these challenges while minimising their associated risks. Future studies should focus on refining regulatory strategies and exploring sustainable military applications of these innovations. Ultimately, balancing technological progress with ethical responsibility is essential to maintaining global security in the modern era.

Endnotes

[1] M. Marciniak, „The 3D Printing in Military Applications: FDM Technology, Materials, and Implications," Advances in Military Technology 18, no. 1 (2023): 45–58.
[2] Khan Rajib Hossain, et al., „Application of 3D printing technology in the military," Journal of Chemistry Letters 4.2 (2023): 103-116.
[3] Idem.
[4] D. T. Bird and N. M. Ravindra, „Additive Manufacturing of Sensors for Military Monitoring Applications," Polymers 2021, 13, 1455.
[5] Idem.
[6] Jeremy J. Ramsden, „Nanotechnology for military applications." Nanotechnology Perceptions 8.2 (2012): 99-131.
[7] Jitendra S. Tate, et al., „Military and national security implications of nanotechnology," Journal of Technology Studies 41.1 (2015): 20-28.
[8] Jeremy J. Ramsden, „Nanotechnology for military applications." Nanotechnology Perceptions 8.2 (2012): 99-131.
[9] "Artificial Intelligence - Defense.gov," U.S. Department of Defence, last modified 2023, https://www.defense.gov/Spotlights/Artificial-Intelligence/.
[10] "Nanotechnology and the Military: How Tiny Materials Can Win Wars," NanoChem Group, last modified November 11, 2021, https://blog.nanochemigroup.cz/nanotechnology-and-the-military-how-tiny-materials-can-win-wars/.
[11] "Governing Military AI Amid a Geopolitical Minefield," Carnegie Endowment for International Peace, last modified July 2024, https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield.
[12] Kusnezov, Dimitri, et al. „Nanotechnology and the Military," Defence Horizons 30 (2003): 1–8.
[13]"Nanotechnology in the Military," AZoNano, last modified November 11, 2021, https://www.azonano.com/article.aspx?ArticleID=3028.
[14] Tate, Jitendra S., et al. „Military and national security implications of nanotechnology," Journal of Technology Studies 41.1 (2015): 20-28.
[15] "Governing Military AI Amid a Geopolitical Minefield," Carnegie Endowment for International Peace, last modified July 2024, https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield.
[16] "Artificial Intelligence - Defense.gov," U.S. Department of Defence, last modified 2023, https://www.defense.gov/Spotlights/Artificial-Intelligence/.
[17] Idem.
[18] Idem.
[19] "Governing Military AI Amid a Geopolitical Minefield," Carnegie Endowment for International Peace, last modified July 2024, https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield.
[20] "Artificial Intelligence - Defense.gov," U.S. Department of Defence, last modified 2023, https://www.defense.gov/Spotlights/Artificial-Intelligence/.
[21] "Governing Military AI Amid a Geopolitical Minefield," Carnegie Endowment for International Peace, last modified July 2024, https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield.
[22] Idem.
[23] "Artificial Intelligence - Defense.gov," U.S. Department of Defence, last modified 2023, https://www.defense.gov/Spotlights/Artificial-Intelligence/.
[24] "The Coming Military AI Revolution," Army University Press, last modified May 2024, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2024/MJ-24-Glonek/.

[25] “Governing Military AI Amid a Geopolitical Minefield,” Carnegie Endowment for International Peace, last modified July 2024, https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield.
[26] “Nanotechnology and the Military: How Tiny Materials Can Win Wars,” NanoChem Group, last modified November 11, 2021, https://blog.nanochemigroup.cz/nanotechnology-and-the-military-how-tiny-materials-can-win-wars/.
[27] “The Coming Military AI Revolution,” Army University Press, last modified May 2024, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2024/MJ-24-Glonek/.
[28] Idem.
[29] Idem.
[30] Idem.
[31] Idem.
[32] Idem.
[33] Idem.
[34] “Governing Military AI Amid a Geopolitical Minefield,” Carnegie Endowment for International Peace, last modified July 2024, https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield.
[35] Idem.
[36] M. Marciniak, „The 3D Printing in Military Applications: FDM Technology, Materials, and Implications,“ Advances in Military Technology 18, no. 1 (2023): 45–58.
[37] Hossain, Khan Rajib, et al. „Application of 3D printing technology in the military,“ Journal of Chemistry Letters 4.2 (2023): 103-116.
[38] Bird, D. T., and N. M. Ravindra. „Additive Manufacturing of Sensors for Military Monitoring Applications,” Polymers 2021, 13, 1455.
[39] M. Marciniak, „The 3D Printing in Military Applications: FDM Technology, Materials, and Implications,“ Advances in Military Technology 18, no. 1 (2023): 45–58.
[40] Bird, D. T., and N. M. Ravindra. „Additive Manufacturing of Sensors for Military Monitoring Applications,” Polymers 2021, 13, 1455.
[41] “Governing Military AI Amid a Geopolitical Minefield,” Carnegie Endowment for International Peace, last modified July 2024, https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield.
[42] “Artificial Intelligence - Defense.gov,” U.S. Department of Defence, last modified 2023, https://www.defense.gov/Spotlights/Artificial-Intelligence/.
[43] Bird, D. T., and N. M. Ravindra. „Additive Manufacturing of Sensors for Military Monitoring Applications,” Polymers 2021, 13, 1455.
[44] Idem.
[45] Ramsden, Jeremy J. „Nanotechnology for military applications,“ Nanotechnology Perceptions 8.2 (2012): 99-131.
[46] Hossain, Khan Rajib, et al. „Application of 3D printing technology in the military,“ Journal of Chemistry Letters 4.2 (2023): 103-116.
[47] M. Marciniak, „The 3D Printing in Military Applications: FDM Technology, Materials, and Implications,“ Advances in Military Technology 18, no. 1 (2023): 45–58.
[48] Idem.
[49] Idem.
[50] Idem.
[51] Bird, D. T., and N. M. Ravindra. „Additive Manufacturing of Sensors for Military Monitoring Applications,” Polymers 2021, 13, 1455.
[52] Idem.
[53] Idem.

[54] “Nanotechnology in the Military,” AZoNano, last modified November 11, 2021, https://www.azonano.com/article.aspx?ArticleID=3028.
[55] “Governing Military AI Amid a Geopolitical Minefield,” Carnegie Endowment for International Peace, last modified July 2024, https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield.

02

BEYOND THE HORIZON: TRAINING MINDS AND SYSTEMS FOR TOMORROW'S CONFLICTS

JOHANNES GINTHÖR, MARKUS SCHMID

▶ **Author:** Captain Johannes Ginthör is currently chief instructor at the Theresan Military Academy and an alumnus of the 23rd General Staff Training of the Austrian Armed Forces. As a PhD candidate at the University of Vienna, he has research interests in military operations ranging from tactical training and planning to the usage of the military as a governmental instrument in general. Additionally, he holds a Master's Degree in Military Leadership from the National Defence Academy in Vienna.

Major Markus Schmid is a passionate leader with a strong focus on Cybersecurity, AI, and IT, supported by extensive military experience. He holds a Master's in Computer Science from FHWN and a Master's in Military Leadership from the National Defence Academy in Vienna. He is furthermore an alumnus of the 23rd General Staff Training of the Austrian Armed Forces, a PhD candidate at the University of Vienna and is keenly interested in disruptive technologies and their potential to drive innovation.

The views expressed in this article are those of the authors and do not necessarily reflect those of the Austrian Armed Forces.

▶ **Abstract:** Technological advancements and evolving security policies increasingly shape military conflicts through AI, autonomous systems, and cyber capabilities. Future developments can be analysed from both military-technological and tactical perspectives, highlighting challenges in command structures, information processing, and execution. The vignettes address the aspects of capability, understanding, and will, i.e., the parts of combat power. Countermeasures require cybersecurity, intelligence validation, and leadership training in cognitive resilience, as well as the proper usage of the decision-making process. Success depends on integrating technology with adaptive command structures and cognitive flexibility. Clausewitz's adaptability is vital in modern conflicts, while Jomini's structured approach remains relevant for technological coordination. True success integrates both perspectives, ensuring leadership, data integrity, and the flexibility to shape complexity rather than merely react to it.

- **Problem statement:** How can emerging technologies alter the requirements for the command-and-control system, with a focus on information and communication, and tactical planning?

- **Bottom-line-up-front:** A comprehensive tactical education, coupled with an unbiased and effective utilisation of modern information and communication systems—despite the necessity of accounting for their potential failure—remains indispensable. Mental agility, improvisation, and adaptability, combined with the efficient use of available resources, will be pivotal in addressing the challenges of future conflicts.

- **So what?:** The problem statement requires a combination of individual preparation through reading, learning, thinking and creative experimentation, alongside institutional preparation that fosters thinking beyond conventional boundaries by nature. This dual approach is essential for meeting the demands of future conflicts effectively and should be implemented immediately in training.

Technological Innovation and War

In light of rapid technological advancements and evolving security policy frameworks, a critical examination of future military conflicts is becoming increasingly indispensable. Future battles are expected to be shaped by the close integration of technological innovations—such as artificial intelligence, autonomous systems, and advanced cyber capabilities—with the adaptation of military tactics. These developments pose fundamental challenges for military personnel concerning command structures, information processing, and tactical execution.

This study explores this complex field from two complementary perspectives. On the one hand, the military-technological perspective is analysed, examining the requirements for command and information systems as well as command relationships. On the other hand, the focus is placed on the tactical perspective, which addresses the planning and execution of combined arms operations. Based on theoretical foundations, three hypothetical vignettes have been developed to illustrate the impact of modern, emerging technologies on military operations. The first scenario demonstrates how systemic cyberattacks, such as the sabotage of weapons systems, can severely compromise a battalion commander's operational capabilities. The second scenario focuses on the domain of situational understanding, depicting a brigade general confronted with an electronically manipulated operational map due to enemy interference. The third scenario highlights the psychological dimension, showing how coordinated psychological operations—including leaflets, social media attacks, and deepfakes—can profoundly undermine trust and cohesion within military units.

Methodology

In this research project, various future scenarios were generated—among other approaches—using an AI application (ChatGPT 4o). The prompts employed and excerpts from the AI-generated texts are documented in the references to ensure transparency, reproducibility, and verifiability. This documentation ensures that AI-based content meets established scientific standards. The use of AI is explicitly conducted within the framework of scholarly diligence. Despite the computer-assisted support, the research outcomes remain critically examined and theoretically grounded, thereby minimising potential biases and maintaining scientific quality.

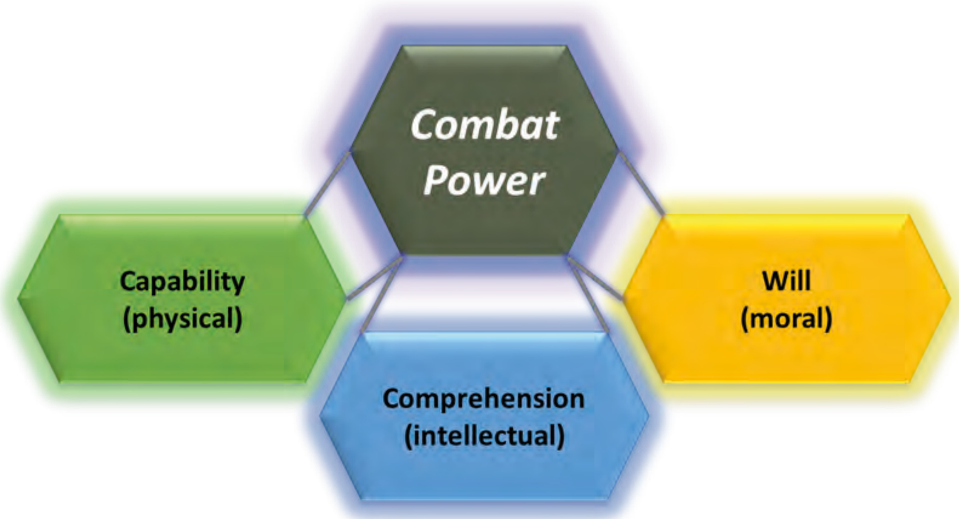
Although this approach slightly deviates from the original mixed-methods design in purely qualitative and quantitative perspectives, it nonetheless combines various methods. Specifically, blending a creative, exploratory, and predominantly qualitative approach with a strong quantitative grounding in the literature offers both breadth and scientific rigour when examining future challenges.[1]

As a first step, various technical and military domains—such as attack vectors in electronic warfare and cyber warfare—were synthesised. Current (2025) Technology Readiness Levels were considered to assess technological advancements and develop plausible future scenarios for 2035. Drawing on these parameters, the AI developed a series of fictional "interviews from the future," depicting potential actors and operational scenarios. This creative method served to outline hypothetical but realistically grounded visions of the near future.

They were subsequently compared with existing military literature to assess the realism and plausibility of the generated scenarios. This comparison helped validate the identified trends, risks, and opportunities and tested basic military principles. Consequently, a dual assurance strategy was implemented: on one hand, creative, AI-based scenario generation; on the other, cross-referencing with recognised, peer-reviewed literature.[2]

Scenarios

Warfare has always been more than just the clash of weapons on the battlefield. Victory is not solely determined by firepower but by a combination of interwoven factors that define a military force's overall combat power. Three fundamental pillars shape the effectiveness of any fighting force: capability, understanding, and morale. Each of these elements plays a decisive role in determining the outcome of a battle, and an adaptive enemy can disrupt, manipulate, or even weaponise it.



The Fundamentals of Combat Power; Source: Authors.

The following scenarios illustrate how modern warfare increasingly targets these three dimensions, rather than relying purely on conventional engagements. The scenarios are presented in a deliberate order, reflecting how combat power can be systematically degraded.[3]

Capability

First, the capability scenario examines how an enemy can neutralise a force's ability to fight by sabotaging technology, disabling weapons systems, and exploiting vulnerabilities in cyber infrastructure. Without functional equipment and effective firepower, even the most well-trained forces are rendered ineffective. The detailed prompt is provided in the footnotes.[4]

I stand among the smoking remains of my battalion. The vehicles are destroyed, and the voices of the few survivors flicker through the radio. Our anti-air platoon, once our shield against drones, was the first to fall—specially fabricated chips in the fire control units had been infiltrated. When exposed to the enemy drones' electronic emissions, they overheated and burned out. The systems collapsed, and our positions were bombarded without resistance. Our tank company, the core of our firepower, failed next. The AI-supported targeting software had been hacked; enemy tanks were detected, but every shot missed by a few crucial meters. It was as if our rounds were deliberately misdirected. Crews reported growing despair as shot after shot failed. Then came the infantry fighting vehicles. Their driver consoles displayed a constant warning: "Replace Burgmannring." This minor but critical seal was falsely flagged as defective *through satellite-based software manipulation. The vehicles halted automatically, becoming easy targets, even though the components were intact. Communication and logistics broke down under enemy electronic warfare. Reports didn't get through. Ammunition convoys were destroyed before reaching us. Even our artillery, fed false GPS data, fired far off target. The result was chaos. My soldiers lost faith—not just in their weapons, but in the entire operation. Morale collapsed. Now, I stand in the ruins, realising we placed too much trust in systems we didn't fully understand or protect. Our technological edge wasn't our strength—it was our Achilles' heel. This must never happen again.*[5]

Technical Considerations

From the standpoint of command support and IT specialists, safeguarding operational integrity in contemporary warfare hinges on a systematic and multifaceted approach. On the one hand, advanced technologies can significantly enhance both situational awareness and mission effectiveness; on the other, they introduce a range of digital vulnerabilities that adversaries are poised to exploit. To mitigate these risks and maintain a decisive edge, three critical dimensions merit particular attention:

- Bolster Supply Chain Vigilance and Real-Time Systems Integrity. Never let advanced systems lull you into complacency—true security demands relentless vigilance. The priority is supply chain security because infiltration at the microchip level can compromise even the mightiest arsenal. Where a single line of malicious code or an unverified component can neutralise entire fighting forces, meticulous oversight at each production stage and thorough patch management become non-negotiable, ensuring that no Trojan horse slips through unseen;[6]
- Reinforce C2 Structures with Adaptive Info-Sharing and Human Oversight. Resilient command and control relies on more than just robust encryption and adaptive network architecture; it also demands human oversight that can interpret anomalies and pivot rapidly under stress. Communication breakdown erodes a unit's morale and disrupts mission execution, but empowered signals officers who know how to detect and counter electronic warfare tactics can preserve unity of effort. Relying solely on automated systems, however advanced, leaves operations vulnerable to well-timed enemy disruptions that undermine situational awareness and expose critical nodes; and
- Cultivate Cyber-Conscious Leadership and a Tech-Savvy Force. Leaders must integrate cyber-awareness into every echelon, transforming soldiers into active sensors who can identify threats—physical or digital—at the first sign of danger. An educated force spots deception attempts early and responds with agility, making it far harder for an enemy to manipulate a battlefield with compromised data. When the entire chain of command is engaged, from the rifleman to the battalion staff, complacency cannot take root, and technology serves as a force multiplier rather than a point of failure.[7]

Tactical Considerations

From a tactical perspective, one is confronted with a fait accompli in this situation. However, to prevent a similar scenario, various methods and measures can be employed.

- Know.Think.Act.[8] NATO's Mission Command doctrine[9] emphasises decentralised decision-making and individual responsibility, yet its absence in this scenario proved catastrophic. Leaders must be trained to think critically and act independently, ensuring they can adapt dynamically when technological systems fail. The battalion's reliance on centralised, automated processes led to paralysis when cyber sabotage rendered key systems inoperable. Focusing on the human factor means developing leaders who can process incomplete information, challenge assumptions, and maintain initiative under uncertainty. A force overly dependent on rigid structures and maybe also technology as its only means becomes predictable and vulnerable. Only a (military) culture that prioritises adaptability over procedural obedience ensures resilience in the chaos of modern warfare. This necessitates a training culture prioritising analytical thinking over procedural obedience, ensuring tactical effectiveness is driven by adaptability rather than rigid adherence to pre-planned structures. So, to sum up, it is not sufficient to merely follow the military-decision-making (MDMP, military-decision-making-process) steps; they must be understood and, if necessary, adapted;

- Look sharp, stay sharp, strike hard. Safety first is not about hesitation—it is about controlling the fight before it starts. The battalion's failure was not due to a lack of aggression but overconfidence in its technology, leading to total vulnerability when systems were compromised. Seizing the initiative requires confidence, but blind reliance on automation replaces tactical awareness with complacency. Commanders must maintain composure under pressure, prioritise reconnaissance and verify their battlespace before committing forces. A methodical, intelligence-driven approach—balancing deception, preemptive reconnaissance, and calculated aggression—ensures that engagements happen on their own terms. A battle is won before it begins, not through technological superiority alone, but through positioning, foresight, and the ability to dictate tempo;[10]
- Double Tap. Tactical decisions must be based on assessed facts and executed through combined arms warfare, yet the battalion's reliance on automated targeting systems led to widespread failure. The principle of main effort[11] dictates that multiple weapon systems should engage a single enemy target simultaneously, maximising effectiveness. However, the cyber sabotage that crippled targeting systems and air defence units exposed a fatal flaw—a lack of redundancy and synchronised firepower. Just as Austria's old anti-tank recoilless rifle doctrine required two firers per target, modern forces must apply this principle across entire structures. Firepower synchronisation, complementary asset deployment, and the integration of supporting multi-domain effects given by the operational level must be embedded in tactical planning to ensure resilience against electronic warfare and sabotage.

Understanding

Second, the understanding scenario delves into the confusion sown by digital deception. Manipulated battlefield intelligence, falsified situational awareness, and cyber-induced disinformation can cloud a commander's ability to assess the battle correctly. A force that cannot trust its own information is left paralysed, unable to act decisively. The prompt used can be seen here:[12]

It was a grey morning, and the command post of the 12th Armoured Brigade buzzed with activity. Brigadier General Lothar von Greiffenstein was moments away from transmitting the attack order when he noticed something odd on the digital situational map: the enemy's positions had changed dramatically within minutes. What had been a lightly defended ridge now appeared to be abandoned while heavy armour advanced toward his flank. His staff was confused—no new drone data had been received, no scouts had reported back. The map had updated itself. It soon became clear that they were victims of a sophisticated deception. The enemy had exploited vulnerabilities in satellite networks, injecting false data into their systems through forged transmissions that mimicked legitimate reconnaissance feeds. This was paired with a malware update that visually manipulated the brigade's tactical display. The entire battlefield picture was false. In truth, the enemy had reinforced their lines and prepared artillery for a devastating counterattack. Communications were overloaded, and field reports were delayed or missing. Von Greiffenstein realised he was planning an assault based on a fabricated reality. A hasty attack meant walking into a trap; retreating risked other unknown dangers. He ordered system integrity checks, re-flights of drones, and encrypted reports from forward observers. Ultimately, he delayed the attack, avoiding disaster—but the damage was done. The brigade was paralysed by confusion. Later analysis confirmed: lax cybersecurity and digital overdependence had crippled their understanding. "Next time," the general thought grimly, "we verify the truth—before we act on it."[13]

Technical Considerations

From an IT and command support perspective, ensuring operational integrity in modern warfare fundamentally depends on safeguarding information and its underlying data. Mitigating inherent risks requires strict adherence to the CIA principle of data—Confidentiality, Integrity, and Availability—to secure, maintain, and guarantee reliable access to critical resources:

- Multi-Layer Validation of Incoming Intelligence. The chaos stemmed from the brigade's exclusive reliance on a single digital feed, highlighting the risk of data manipulation when no alternative verification tools are employed. Multi-layer validation—where each data point from reconnaissance drones, forward observers, and satellite feeds is cross-checked via firewalls or even Information Exchange Gateways—can detect discrepancies early and expose deception. Checking metadata and Network Intrusion Point allows faulty data to be sorted quickly.[14] Only by instituting rigorous vetting procedures and routine integrity checks on critical systems can command staff keep false intelligence from derailing operational plans;
- Human Interaction and Training as the Cornerstone of Cyber-Awareness. Technical safeguards alone cannot offset the human element when identifying cyber or electronic warfare assaults. Well-trained personnel, from signals officers to frontline soldiers, are indispensable in noticing anomalies—such as erratic changes in enemy positions—and raising red flags. Mandating regular cyber-awareness courses and scenario-based exercises ensures that operators develop the necessary scepticism to challenge suspicious data inputs. This human-centric approach, combined with robust cybersecurity measures, transforms each soldier into an active sensor, minimising the chance of digital deception crippling the entire force;[15]
- Robust Command Processes and Flexible C2 Structures. Even the most advanced technology proves ineffective when crisis management and leadership frameworks are underprepared. In this scenario, the brigade faced sudden paralysis because decision-makers lacked the structures and doctrines to pivot quickly under digital duress. A resilient command and control model trains officers to question sudden shifts, enact fallback protocols, and sustain the flow of information through redundant communication channels. By embedding crisis simulation exercises and contingency planning into regular drills, leadership teams become adept at rapidly adapting to deceptive signals on the battlefield.[16]

Tactical Considerations

- Two is one, one is none. Establishing dual communication links is standard in defensive operations, as the authors learned throughout training, ensuring continuous command and control even under enemy interference. However, this principle is often neglected in offensive operations, where single-point failures can lead to total mission breakdown. Layered communication infrastructures—incorporating analogue, digital, and human relay systems—must be standard practice across all domains. Combining motorised and mechanised messengers with encrypted digital channels enhances operational resilience. The redundancy mindset must extend beyond communication to intelligence gathering, ensuring that no single reconnaissance method becomes a critical point of failure;
- No limits—just possibilities. Stop focusing on perceived restrictions—focus on what is still operational and how to maintain control. The brigade command post became paralysed by manipulated intelligence and disrupted communications, yet mission success depended on adaptability, not perfect information. In NATO doctrine, constraints define mission parameters, while restraints impose explicit prohibitions.[17] While these structures ensure discipline, they must never override initiative-driven problem-solving. Tactical flexibility is not reckless improvisation—it is a deliberate approach to maintaining freedom of action within disruption. However, flexibility is only effective when underpinned by deep tactical proficiency. Commanders must train for uncertainty, ensuring subordinates can operate even when the digital battlefield is compromised;
- Practice chaos,[18] master control. Integrating continuous wargaming into command procedures enhances operational awareness and prepares leaders for unexpected developments—exactly the kind that paralysed the brigade in this scenario. The Austrian Armed Forces recognise Kriegsspiel (wargaming for synchronising or evaluating different courses of action, but also for rehearsing the concept of ROC, depending on when it takes place).[19] Still, its application is often limited to the planning phase instead of using it as a tool to stress the ongoing battle from the enemy´s point of view during live execution. This approach restricts its effectiveness as an adaptive tool. Red Teaming must be an active element of command processes, allowing leaders to simulate/stress test courses of action in real time with real and trained personnel and validate decisions under uncertainty. This is not just an academic exercise—it is a tactical necessity.

Will and Morale

Finally, the morale scenario explores the long-term effects of psychological warfare. Beyond physical destruction, modern adversaries increasingly seek to erode trust, spread fear, and dissolve cohesion through propaganda, social engineering, and deepfake technology. Once doubt and paranoia take root, a military force may collapse from within, even before the enemy delivers a final blow.[20]

The battle had become a nightmare. Corporal Lukas Hoffmann crouched behind a burned-out vehicle, his rifle limp in his hands. Gunfire and explosions echoed around him, but the real damage wasn't physical—it was psychological. His digital map flickered uselessly, distorted and confusing. Morale in the unit had collapsed, not from enemy fire, but from an invisible assault on their minds. It started with digital manipulation: false data, shifting enemy positions, erratic system behaviour. Soon, targeting systems failed, and comms were compromised. Every decision became uncertain. Then the propaganda began—flyers dropped by drones, chain messages on personal devices, fake social media posts: "Your commander has betrayed you," "You've been abandoned." They weren't true, but they planted doubt. Then came the deepfake—video of *their commander apparently surrendering to the enemy. It spread through their secure network like wildfire. Everyone knew it was fake, but trust shattered anyway. Soldiers began to suspect one another. Paranoia grew. And then the most personal attack of all: a message to Hoffmann's sister, claiming he would soon be dead. It cut deeper than any wound. That was when he realised—this war wasn't about bullets or tanks. It was about belief. About will. As morale crumbled, his platoon leader's voice pierced the fog: "The enemy can only defeat us if we let them. If we lose our heads, we lose the war." Somehow, they held together. Scarred, shaken—but not broken. Hoffmann understood then: the true battlefield was the mind. And surviving meant fighting to stay human.*[21]

Technical Considerations

From an IT and command support perspective, safeguarding operational integrity in modern warfare demands a holistic approach encompassing physical, virtual, and cognitive realms. While the physical domain involves hardware, infrastructure, and tangible assets, the virtual domain focuses on digital networks and data flow. The cognitive realm, in turn, addresses human perception, decision-making, and information interpretation. These three sub-domains are deeply interwoven: compromised infrastructure jeopardises network functionality; breaches in virtual systems erode user confidence and strategic advantage; and misinformation in the cognitive space can undermine even the most sophisticated technological safeguards.

- Guarding the Digital Front. The enemy effectively corrupted battlefield data and disseminated deepfake propaganda by targeting the digital interfaces that soldiers rely upon. Mitigating such threats requires a fortified virtual domain, where rigorous authentication protocols and multi-layered encryption shield command networks from exploitation.[22] Rapid threat detection, continuous system auditing, and robust backup communication channels are the virtual bulwark, ensuring that malicious software and fabricated messages cannot rapidly undermine confidence or disrupt mission continuity;[23]
- Securing the Ground. Even the best-protected signal infrastructure becomes vulnerable if fundamental physical security lapses occur. Personnel must secure command posts, safeguard data centres, and rigorously vet on-site hardware to prevent infiltration and sabotage. Physical-domain protocols—from perimeter defence and equipment inspections to secure logistical chains—complement digital protections by minimising the chances of unauthorised access or tampering at the source. Such tangible measures reinforce the integrity of information systems and support broader resilience in high-intensity operations;
- Forging Unbreakable Will. Ultimately, morale shatters when soldiers lose trust in their tools, leaders, and each other—a vulnerability the enemy weaponises through psychological warfare. Resilient command structures must incorporate regular training in cognitive resilience, where troops learn to recognise and counter both subtle and overt manipulation. Commanders who rapidly debunk false narratives, foster open communication, and encourage critical thinking transform fear into collective vigilance, preserving the fighting spirit that technology alone cannot guarantee.[24]

Tactical Considerations

If the tactical framework is insufficiently established, the battle will ultimately be lost at the combat-technical level. Conversely, this also clearly demonstrates the significance and effectiveness of applicable regulations and leadership tools.

- Fool me once—never twice. Every battle must be analysed not only for tactical efficiency but also for its psychological impact. Tactical debriefings and step-by-step control mechanisms must be embedded into command procedures to ensure continuous learning and resilience against enemy means. Experience alone does not guarantee improvement—structured analysis does. After-action reviews must extend beyond technical errors, incorporating morale, trust, and all means of enemy warfare into the assessment. Commanders must train their units to analyse engagements holistically, identifying vulnerabilities in will, understanding, and capability. Understanding how disinformation, psychological pressure, and internal distrust impact effectiveness is just as critical as evaluating direct combat performance. Only through systematic institutional learning can forces develop the adaptability needed to counter physical threats and the invisible weapons of modern warfare.
- The ground fights with you—if you use it right. The battlefield in this scenario consisted of a dense forested area interspersed with open fields and urban ruins, but this should now not be the level of consideration; it has to be understood in the following manner: „As the terrain enables, enforces, or restricts certain actions for both one's own forces and opposing parties, the resulting conclusions either complement or adjust the possibilities of the conflicting sides."[25] At this analysis stage, the focus must shift from observation to application—the external influences must now be viewed in a more abstract, distanced manner, transitioning from a passive assessment to an active tool. Austrian military doctrine defines the Terrain Effects on Friendly Operations as follows: „In this assessment step, the possibilities offered by the terrain are analysed based on previously drawn conclusions and aligned with one's own operational capabilities."[26] That is, in fact, the key transition point from analysis to synthesis.[27] Here, the question is no longer what has to be done but how it can be achieved, which element can be used to generate the right effect, and how the environment in general shapes this employment. This must under no circumstances be interpreted as a mere assessment of the terrain; rather, it concerns ensuring the optimal application of combat power within the established framework by accounting for all external influencing factors.

Only with the right combination of troops and a deep understanding of the factors can the elements be effectively employed—a necessity that becomes evident in the next section.

- Trust wins battles. „The trust between senior leaders in the command was able to overcome the stress of combat, [...]."[28] Trust is the invisible backbone of combat power. Without it, even the most advanced forces fail. Commanders must cultivate both horizontal trust among troops and vertical trust between leadership and subordinates. This requires clear intent, decentralised execution, and demonstrated competence at all levels. However, trust does not emerge by itself—it is built when soldiers feel properly led. Correctly applying the command process as a structured tool ensures exactly that. When leadership is transparent, consistent, and methodical, subordinates develop confidence in decisions and execution. This may, for example, require that during peacetime, decisions are given with justifications[29] to familiarise subordinates with the commander's thought process. Trust is earned through shared hardships, disciplined adaptability, and competent guidance in dynamic environments. Leaders must be predictable in intent but flexible in execution, ensuring that troops understand, believe in, and can act on the mission independently.

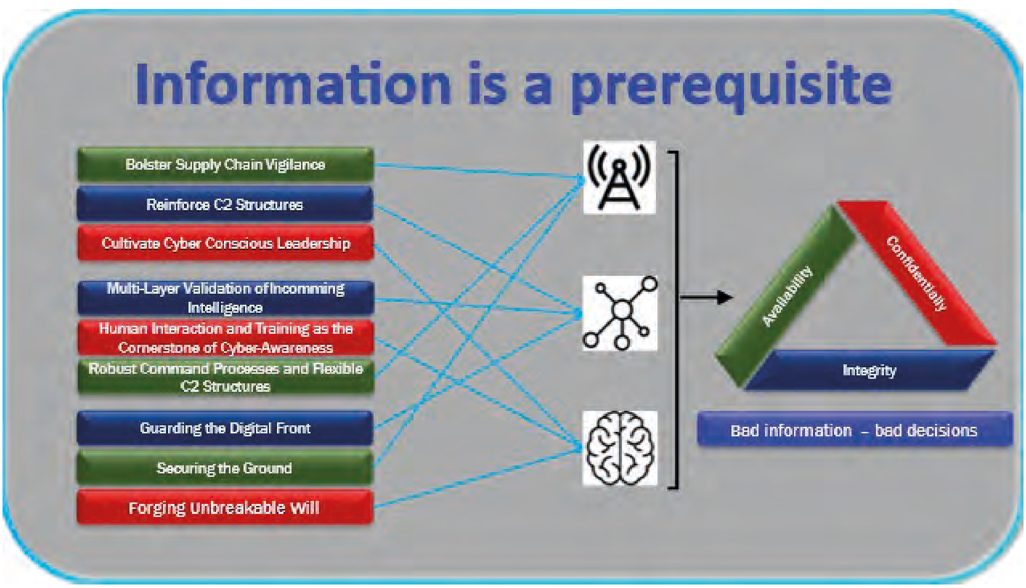
Endgame?

Lose smart, so you can win again. Defeat is inevitable in warfare, but its impact must be managed. A lost engagement should not mean operational failure. Commanders must identify unnecessary destruction when continuing to fight risks and ensure structured withdrawal, force preservation, and morale retention. As recognised by Reinhard Janko during the TMAF24,[30] defeat shall be part of the tactical training. The importance lies in recognising failure as a chance to learn. Debriefing frameworks, red-team exercises, and contingency-based wargaming refine decision-making and prevent repeated mistakes. Training should simulate failure scenarios to develop leaders who can analyse, adapt, and recover quickly, turning setbacks into strategic learning opportunities.

Food for Thought - Technical

Before addressing the final considerations from an IT technician and signals officer's perspective, it is essential to weave together the key strands of technology, leadership, and human resilience. Although these principles resonate across operational and strategic spheres, the immediate focus is on preventing tactical collapse. The conclusion condenses these insights, demonstrating how synergy across virtual, physical, and cognitive domains preserves battlefield momentum and morale.

Defence demands more than technical fixes in a battlespace where hidden code can disable key hardware, where deepfake propaganda seeds mistrust, and where a single compromised data feed can unravel entire operations. Information is a prerequisite; bad information usually leads to bad decisions, as illustrated in the following graphic. It requires an airtight supply chain, adaptable command and control, and a cyber-conscious force unafraid to question every signal. A modern military safeguards its momentum and morale by layering authentication and verification across all digital inputs, securing physical infrastructure against on-site tampering, and training every soldier to see and stop manipulation before it spreads. This synergy across the virtual, physical, and cognitive domains also aligns with the CIA principles: confidentiality is associated with the cognitive domain, integrity upholds the virtual realm, and availability secures the physical environment. Ultimately, neither code nor chaos nor psychological strike can deny victory to those who remain vigilant.

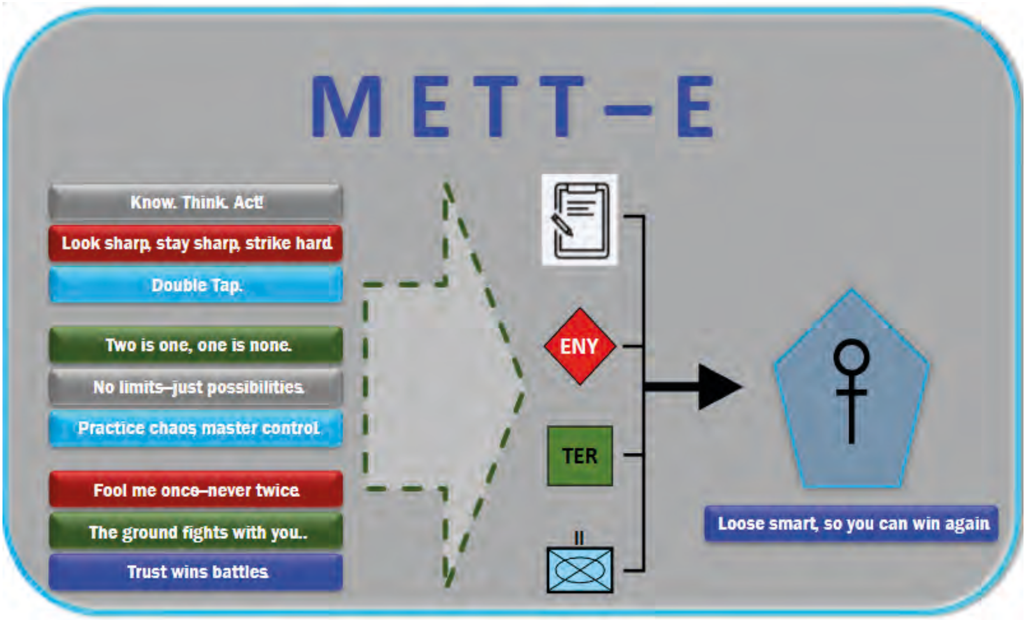


The Key Technical Insights prior to the MDMP; Source: Authors.

Tactical Point of View

The temporary character of warfare does not bind the command process—it is designed to be universally applicable, regardless of time, place, or conditions. It provides the necessary freedom for commanders to execute their mission as the situation demands, rather than forcing a rigid approach onto a fluid battlespace. Abstracting decision-making into a structured yet adaptable framework ensures that leadership remains effective even in the future environment—always shaped by mission needs, never by doctrinal constraints.

This structured flexibility directly enhances combat power, ensuring that forces are not just deployed but employed effectively. Troops and resources must be assigned where they have the greatest impact, avoiding inefficient applications. A command process that correctly assesses the mission, enemy, terrain, and available forces guarantees that each asset is used to maximise its strengths. By ensuring a coherent and synchronised approach, the command process increases the force's effectiveness. The graphic below precisely explains this system. The key conclusions from the scenarios have been assigned to the steps of the MDMP—orientation (M), the enemy (E), the terrain (T), and own forces (T) and focus on the employment of combat power (E), the main task of the tactical echelon. If something still goes wrong, learn from it!



The Key Insights connected to the MDMP; Source: Authors.

As a result, trust between commanders and troops emerges naturally. Soldiers trust leaders who provide clear intent, execute decisively, and apply force efficiently. A unit that sees competent, structured leadership will fight with confidence and cohesion, knowing their role is understood and their mission achievable.

Finally, if defeat becomes inevitable, it must remain an isolated event—never a pattern. A structured command system ensures that losses are analysed, learned from, and prevented in the future. Tactical setbacks should lead to institutional adaptation, ensuring vulnerabilities are permanently addressed. Forces integrating continuous learning and structured command adaptation will always recover stronger, maintaining the initiative. A structured command system turns failure into future success, ensuring that vulnerabilities are addressed permanently—never exploited twice.

"Military leadership is a guiding, controlling, and motivating influence on commands, troops, units, and individuals to achieve objectives and optimise organisational effectiveness. It involves the targeted deployment of resources, means, and information across time and space. Leadership is a continuous process that relies on the prerequisite of mutual information exchange."[31]

Balancing Technology and Human Judgment

Combat power is built on three fundamental pillars: capability, understanding, and morale. While these elements define a force's effectiveness, they are not static—they must be continuously developed, reinforced, and sustained. Capability stems from equipment, training, and doctrine, but it is only as effective as the understanding that enables its proper use. Without clarity in mission execution, even the most advanced systems become ineffective. Morale, the decisive factor in prolonged engagements, is shaped by leadership, trust, and confidence in the mission. Just as these components can be cultivated, they can also be solidified through proper application. These future-oriented examples demonstrate how combat power is not merely an asset to be measured—it is a dynamic force that must be built, maintained, and reinforced through deliberate command decisions.

From the tactical point of view, it is rather simple. In modern warfare, particularly in hybrid, cyber, and asymmetric conflicts, a Clausewitzian approach—rooted in deductive reasoning—proves superior to Jomini's more mechanistic doctrines, which rest upon an inductive framework. The unpredictability of contemporary battle spaces demands adaptability, intuition, and, on the tactical level, a deep understanding of the military dimension of war. The outlined principles—regarding the mission, the enemy, the terrain and one's own troops—reflect this mindset. War is not a formulaic equation but a dynamic struggle of wills. Effective leaders embrace uncertainty, human factors, and operational flexibility over rigid structures. To prevail, commanders must think critically, act decisively, and master chaos—more Clausewitz, less Jomini. Victory belongs to those who shape complexity, not those who merely calculate it.

From a technical standpoint, the situation proves far more intricate than it may initially appear. In modern conflict environments, one might argue that a Clausewitzian perspective, emphasising will, uncertainty, and the human dimension, offers clear advantages. Nonetheless, it is critical to recall that Jomini, as a mathematician, consistently foregrounded warfare's granular and formulaic nature. Yet Clausewitz and Jomini do not operate on the same level of command, and their distinct deductive or inductive approaches cannot be directly compared. Instead, their respective viewpoints must be integrated. One might well argue that adopting a "mixed-methods" approach proves most advisable. While Clausewitz's insights into the fluidity and unpredictability of war underscore the significance of human judgment, Jomini's focus on structure and calculation underlines the importance of precise coordination at every level. In particular, the reliable transmission of data—even down to each bit and byte—is indispensable: information must be correctly addressed, securely transmitted, and properly interpreted. One must never lose sight of the fact that information stands as a fundamental prerequisite for success. When these foundations are in place, tactical flexibility, human intuition, and operational innovation flourish. While victory may indeed favour those adept at shaping complexity, such success is impossible without an underlying comprehension of the technical architecture. Commanders who neglect the intricacies of data management and security risk fighting against the very "ghosts" they themselves created. Although the theatre of modern warfare increasingly spans digital realms, the fundamental need for both rigid structural safeguards and adaptive, human-centred leadership remains undiminished.

Endnotes

[1] J. W. Creswell and V.L.P. Clark, Designing and Conducting Mixed Methods Research (SAGE Publications, 2017), https://books.google.at/books?id=eTwmDwAAQBAJ.
[2] Paul Schoemaker, "Scenario Planning: A Tool for Strategic Thinking," Sloan Management Review 36 (1995): 26-31.
[3] "I would like to shed light on three future war or conflict scenarios for a more in-depth analysis and derive conclusions for training from them. I will now roughly describe the three scenarios to you, along with what I want; please formulate them accordingly. Mentally, we are in the year 2035, and the fictional country in the scenario is at war. All three scenarios focus on the three components of combat effectiveness: morale (the will of the soldier), understanding (understanding the situation and the resulting task), and capability (sufficient physical resources such as tanks, anti-aircraft guns, or ammunition). Please add this to the previous requirements as well!" Sam Altman, ChatGPT 4o (OpenAI, 2025), accessed February 20, 2025, https://chatgpt.com/.
[4] „First scenario, area: capability. Describe, from the perspective of a future battalion commander (three mechanised infantry companies, one tank company, one platoon of self-propelled anti-aircraft systems, one platoon for indirect fire support), why he has just lost a battle against an enemy and now stands before the smoking wreckage of his battalion. Cite as reasons, for example, that the anti-aircraft platoon was unable to fire because the chip supply chain for the fire control computers had been infiltrated or sabotaged. These chips reacted to a specific type of electronic emission in such a way that the entire anti-aircraft software system was overloaded, causing the components to burn out. The main battle tanks failed to hit the opposing tanks because the AI-assisted target acquisition software had been hacked. Upon detecting the contours of enemy vehicles, it consistently produced missed shots due to slight targeting deviations. Finally, describe how the infantry fighting vehicles constantly displayed a message on the driver's control panel indicating that the component "Burgmannring" urgently needed to be replaced. This was the result of satellite-based interference with the software, which had injected the false alert. Feel free to invent additional background information and elaborate creatively. Also, consider selecting other units from the battalion and constructing similar examples. Length: approximately 600 words, from the perspective of the battalion commander." Altman, ChatGPT 4o.
[5] Altman, ChatGPT 4o.
[6] Jon Boyens et al., "NIST - Cybersecurity supply chain risk management for systems and organisations," (Gaithersburg, MD, 2022), 170-178.
[7] P. W. Singer and A. Friedman, Cybersecurity: What Everyone Needs to Know, What Everyone Needs To Know (OUP USA, 2014), https://books.google.at/books?id=9VDSAQAAQBAJ, 166-176.
[8] Know.Think.Act is the chosen motto of the Austrian 23. General Staff Course.
[9] North Atlantic Treaty Organization, "Tactical Planning for Land Forces: APP-28" (2019), 1.
[10] Charles S. Oliviero, Praxis Tacticum: The Art, Science and Practice of Military Tactics (Double Dagger Books Ltd, 2021), 39–40.
[11] Dieter Schadenböck, "Grundlagen der Taktik der Landstreitkräfte: Lehrskriptum," 2nd ed. (Wien, 2020), 81.

[12] „Now create a second example for the area of Understanding, from the perspective of a brigadier general at his command post, who had just reached for the receiver to issue an order to attack. But now, on the digital situation map, the enemy positions appear completely different from just a few minutes ago, when the operational plan had been presented to him for approval. Try to invent, as creatively as possible, how the enemy might have used technological means to fundamentally deceive the understanding of the entire brigade staff! Again, around 600 words!" Altman, ChatGPT 4o.
[13] Altman, ChatGPT 4o.
[14] CISA, Zero Trust Maturity Model (2023), Cybersecurity and Infrastructure Security Agency; Cybersecurity Division, 9-10.
[15] Singer and Friedman, Cybersecurity: What Everyone Needs to Know, 126-134.
[16] A. King, Command: The Twenty-First-Century General (Cambridge University Press, 2019), https://books.google.at/books?id=lFR-DwAAQBAJ, 358-361.
[17] North Atlantic Treaty Organization, "Tactical Planning for Land Forces," 2–9.
[18] Oliviero, Praxis Tacticum, 55–58.
[19] Bundesministerium für Landesverteidigung, "Taktischer Führungsprozess: Dienstvorschrift für das Bundesheer" (Wien, 2019), 26-27.
[20] „Now the third scenario, this one focuses on the area of Morale. Invent an example from the perspective of an individual soldier who was part of all these combat operations, but describes that the worst part for him was how the enemy systematically destroyed morale. Come up with all kinds of examples for this – such as flyers, chain emails, social engineering, harassment on Facebook, deepfakes, and much more! Again, roughly 600 words!" Altman, ChatGPT 4o.
[21] Altman, ChatGPT 4o.
[22] US Army, FM 3-12 - Cyberspace Operations and Electromagnetic Warfare (2021), 18-19.
[23] US Army, FM 3-12 - Cyberspace Operations And Electromagnetic Warfare, 32-41.
[24] Singer and Friedman, Cybersecurity: What Everyone Needs to Know, 231-247.
[25] Bundesministerium für Landesverteidigung, "Taktisches Führungsverfahren: Dienstvorschrift für das Bundesheer" (Wien, 2012), 71.
[26] Bundesministerium für Landesverteidigung, "Taktisches Führungsverfahren," 78.
[27] Bundesministerium für Landesverteidigung, "Taktisches Führungsverfahren," 68.
[28] Mick Ryan, White Sun War: The Campaign for Taiwan, 1st ed., Casemate Fiction Series (Casemate Publishers & Book Distributors LLC, 2023), https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=31599283, 164.
[29] In the Austrian Armed Forces, this is known as "Entschluss mit Begründung".
[30] Reinhard Janko, "Betrachtungen zum manöverbasierten Ansatz in der Taktikausbildung," (TMAF24, Theresianische Militärakademie, October 10, 2024).
[31] Bundesministerium für Landesverteidigung, "Taktischer Führungsprozess," 15.

03

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE MILITARY DECISION-MAKING PROCESS AND MISSION COMMAND

PATRICK HOFSTETTER, MARIUS GELLER, FLORIAN GERSTER

▶ **Author:** Lieutenant Colonel Patrick Hofstetter, PhD, M.Sc., is Co-Head of Leadership and Communication Studies at the Swiss Military Academy at ETH Zurich. He is an active General Staff Officer in the Swiss Armed Forces. He serves as a training officer in the general staff for operational studies and training. His research interests are command, leadership, and management in the armed forces. He has published on tactical command and training in the Swiss Armed Forces and co-edited the anthology "Leadership Concepts: An International Perspective" (2024).

First Lieutenant Marius Geller is an infantry platoon leader in the Mountain Infantry Battalion 85, where he will soon assume company command. He is pursuing a bachelor's degree at the Military Academy to become a career officer in the Swiss Armed Forces. His study interests are leadership as well as military sociology. As a career officer, he will coach and teach reservists.

Lieutenant Florian Gerster serves as a fire support officer in the staff of Artillery Group 1. He aims to become a company commander in the Reconnaissance Battalion 1. He is pursuing a bachelor's degree at the Military Academy at ETH Zurich to become a career officer in the Swiss Armed Forces. His study interests are leadership, technology, and strategy in the armed forces. As a career officer, he will coach and teach reservists.

The views contained in this article are the authors' alone and do not represent the views of the Swiss Armed Forces or ETH Zurich.

▶ **Abstract:** The progressive integration of artificial intelligence (AI) transforms military command across doctrinal, procedural, and cultural dimensions. AI reshapes the balance between centralisation and decentralisation across command levels. Using Col. John Boyd's OODA Loop as a generic model of the military decision-making process (MDMP), it is possible to see how AI influences each step of decision-making—from information gathering to tactical execution—and assesses its implications for Mission Command (MC) as a decentralised leadership philosophy. Western militaries, with their longstanding tradition of decentralised decision-making, may be particularly well-positioned to harness AI as a tool of empowerment rather than surveillance.

- **Problem statement:** How does integrating Artificial Intelligence (AI) affect the Military Decision-Making Process (MDMP) and Mission Command?

- **Bottom-line-up-front:** The integration of AI in the armed forces affects not only structures (such as C2), processes (such as military decision-making) and doctrine but also the less tangible aspects of leadership, such as the philosophy of Mission Command in Western militaries. Only a simultaneous consideration of these areas allows planners to think of the holistic integration of AI and the necessary adjustments.

- **So what?:** Effective integration of AI into MDMP, to enhance rather than undermine Mission Command, will help commanders deliberately vary between centralised and decentralised approaches to maximise the accuracy and speed of decisions.

Introduction

The integration of Artificial Intelligence (AI) into military operations challenges traditional models of command and control (C2) as well as Military Decision-Making Processes (MDMP). Worldwide, militaries increasingly rely on AI to enhance operations' speed, precision, and coherence across domains.

However, this technological shift also confronts core leadership philosophies in Western forces, where Mission Command is central. Here, Mission Command is a leadership style and doctrinal principle rooted in decentralisation and subordinate initiative. As AI systems generate unprecedented access to data, senior commanders must reconsider how they distribute authority, interpret situational complexity, and maintain trust across hierarchical levels.

To better understand the complexities of technological innovation regarding doctrine and culture, this paper uses John Boyd's OODA Loop as a generic model of the MDMP—rather than in its historical or Air Force-specific context. In doing so, it continues James Johnson's argument that integrating AI into military processes and structures at all levels may counterintuitively increase the importance of human decision makers.[1]

Mission Command in Doctrine, Culture, MDMP and C2

Mission Command as a leadership concept dates back to the Prussian military reforms of the 19th century.[2] Today, most Western militaries aspire to it.[3] Precise definitions differ in the various handbooks and regulations,[4, 5] but usually include decentralisation and empowerment of junior leaders. Ukraine's response to the invasion by Russia, especially in its early months, underlines the advantages of such an approach: both domestic[6] and foreign[7] observers attributed the tactical superiority of the more agile Ukrainian military to their successful adoption of Mission Command. In contrast, Russia's rigid "Detailed Command" approach is a counter-concept comprised of centralised, directive leadership.

NATO defines Mission Command as "a philosophy of command that advocates centralised, clear intent with decentralised execution; a style that describes the 'what', without necessarily prescribing the 'how'."[8] Various authors blur this principle by writing, i.e., "centralised planning and decentralised execution"[9] or "centralised control, decentralised execution".[10] It seems that NATO's definition provokes a top-down understanding of Mission Command, and that ultimately, only execution is delegated. Understood in this way, however, it is a rather empty concept, since even in the Russian understanding of command, execution is decentralised.

A consistent interpretation of Mission Command is therefore essential: emphasising that only the intent is centralised, thus allowing the subordinate to decide and act as autonomously as possible. Additional centralisations may reflect military culture, and arguably, this may be one of the main reasons armed forces struggle to adopt Mission Command successfully.[11] However, centralising more than the absolute minimum is at odds with the original understanding of Mission Command, the Prussian Auftragstaktik.[12]

The superiority of Auftragstaktik, as Mission Command usually refers to in its original German, was particularly evident in the Second World War. In his renowned study Kampfkraft,[13] Martin van Creveld explains why, despite the strategic superiority of the Allies, the Wehrmacht retained tactical superiority at lower levels until the war's final phases. Col. John Boyd comes to similar conclusions in his lecture "Patterns of Conflict",[14] in which he analysed the effect of Mission Command on the MDMP and C2. Such a procedural perspective is entirely consistent with the historical explanation that the Prussian generals developed Mission Command mainly because of the technological innovations of the 19th century:

long distances and high speeds meant that centralised command of the battle was no longer feasible.[15]

Suppose the origins of Mission Command are at least partly due to technical innovations that have led to a divergence between the speed of military leadership and military action. In that case, one might ask how introducing new technologies since the end of the Cold War would have influenced Mission Command. This is particularly tempting for those who see Mission Command as a "necessary evil" at odds with coordinating efforts—such statements were already extant in the 1990s: "Mission Command will have died with the last non-digital company command."[16] and have recently received renewed attention in the context of automation and Artificial Intelligence (AI).[17]

Given the advantages of Mission Command, however, some also address "The potential risk associated with this trend is the micromanagement of warfare at the expense of mission command."[18] These and other authors firmly state that Mission Command should be retained.[19, 20] Nevertheless, the question remains whether Mission Command can and should survive.[21]

Military command should treat centralisation or decentralisation not as opposing choices but as ends of a spectrum along which command must adapt depending on the context and content of the mission. This requires a holistic understanding of Mission Command, which we approach through the Command-Leadership-Management framework.[22]

This approach goes back to Stephen Bungay[23] and was adopted as the British Army Leadership Doctrine,[24] sharpened in definition by Patrick Hofstetter[25] and officialised for the Swiss Armed Forces in 2025 with the "Strategie zur Vision 2030" of the Swiss Department of Defence.[26] A brief explanation will show how the Command-Leadership-Management (CLM) framework allows leaders to address the three essential aspects of Mission Command: first, its significance as military doctrine;[27] second, its cultural significance as a leadership philosophy;[28] and third, its procedural and structural significance through manifestation both in C2 and MDMP.[29] This holistic view helps to recognise, on the one hand, that this triadic model is sufficient and, on the other hand, that the three dimensions of Mission Command are interrelated and need to be analysed accordingly.

CLM Model: Command, Leadership and Management

Source: Authors.

The model defines the following: command is mission-centric, leadership is people-centric, and management is organisation-centric. These aspects manifest in different areas of an organisation:

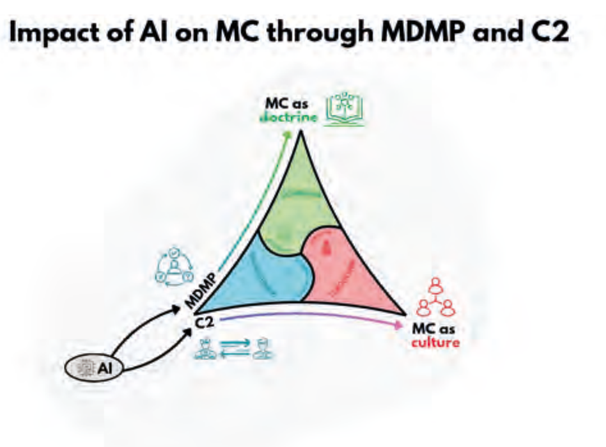
- Command, i.e., how the mission is generally accomplished, manifests itself in the doctrine;
- Leadership, i.e., the way people are treated in general, is manifested in the culture;
- Management, i.e., how the organisation functions generally, is manifested in processes and structures.

Conceptually, Mission Command is not a doctrine in the sense of a standardised tactical, operational or strategic approach, such as manoeuvre, attrition or guerrilla warfare,[30] multidomain operations, or network-centric warfare.[31] Mission Command is a generic command doctrine that may accord more or less with any given warfighting doctrine.

When considering Mission Command culturally, looking at the prerequisites for its successful application is beneficial. The associated obstacles to implementation have been thoroughly examined[32] using Edgar H. Schein's organisational culture model.[33] Yet the influence runs in both directions. If Mission Command empowers followers, this undoubtedly fosters their trust, self-confidence, and initiative–characteristics that, in turn, benefit the successful application of Mission Command. This culture cannot be built up in the hot state. Therefore, Donald E. Vandergriff suggests that "Mission Command must be integrated into all education and training from the very beginning of basic training".[34]

Just as Mission Command can obviously influence doctrine and culture, it does so on processes and structures. Here, as in the other domains, influence is mutual. However, Mission Command influences the processes rather than structures; ultimately, C2 structures are primarily political or strategic decisions and thus prerequisites for and not outcomes of Mission Command.

In terms of interdependencies, two things stand out. MDMPs are primarily related to doctrine, while C2 structures are related mainly to culture. The former is because decision-making processes are ultimately nothing more than generic forms of mission accomplishment, a procedural blueprint, so to speak, filled with doctrinal content. The latter follows from purely sociological considerations: those closer to each other within a given structure are more likely to influence each other. For example, if air defence is subordinate to ground forces, it will tend to align itself culturally with them through closer exchanges. If, on the other hand, it is part of the air force, it will also be part of the corresponding cultural area.



Source: Authors.

The MDMPs of the various armed forces differ in their national characteristics. However, a generic process is required for a general answer rather than a country-specific one. The generic process that Boyd described as the OODA (Observe, Orient, Decide, Act) Loop[35] serves this purpose, shedding light on the dependencies of Mission Command and the MDMP in general and not on a special national form. In the same sense, Boyd himself had used the OODA framework to explain the apparent superiority of the German Mission Command approach in the Second World War:[36]

- "The German concept of mission can be thought of as a contract, hence an agreement, between superior and subordinate. The subordinate agrees to make his actions serve his superior's intent in terms of what is to be accomplished, while the superior agrees to give his subordinate wide freedom to exercise his imagination and initiative in terms of how intent is to be realised."[37]
- "The secret of the German command and control system lies in what's unstated or not communicated to one another—to exploit lower-level initiative yet realise higher-level intent, thereby diminish friction and reduce time, hence gain both quickness and security."[38]

One of Boyd's central statements is that successful warfare involves making one's own OODA Loop turn faster than the opponent and, ideally, collapsing the opponent's loop through speed, disruption, or deception. Long before Boyd, it was recognised that speed is crucial in warfare. Clausewitz, for example, explains under the term "coup d'œil" that it is "the quick recognition of a truth that the mind would ordinarily miss or would perceive only after long study and reflection" that distinguishes military genius.[39]

It is evident that AI can facilitate such swift recognition. Just as the technical advances of the 19th century had allowed for acceleration, the 21st century's innovations are also reflected in the OODA Loop. The following section does this specifically for integrating AI into the MDMP or, more generally, into the OODA Loop. Therefore, we need to explain Boyd's OODA Loop in more detail.

The Impact of AI on the MDMP

Initially developed by the US Air Force pilot and strategist Col. John Boyd to explain decision-making in aerial combat, many Western armies have since adopted the OODA Loop as a conceptual framework for adaptive decision-making in modern conflict.[40] Its abstraction allows for a conceptual discussion independent of national doctrine or force structure. Following Boyd's core idea that military success derives from operating faster and more coherently through this loop than one's adversary,[41] the subsequent section examines how AI influences each OODA Loop's steps—and how this may fundamentally alter the structure and dynamics of MDMP in modern warfare.

The first step of the OODA Loop—observe—refers to collecting information from the operational environment. Sensors and digital systems generate an ever-increasing volume of data, shaping this step in contemporary conflicts. ISR (intelligence, surveillance, and reconnaissance) systems, satellite imagery, drone feeds, and cyber intelligence generate an informational density far exceeding human operators' processing capacity.[42] In contrast to the past, when timeliness or availability of information was the limiting factor, modern forces increasingly face the inverse problem: an abundance of raw data with limited capacity to convert it into actionable knowledge.

AI, especially machine learning and pattern recognition, helps mitigate data overload. It enables rapid real-time filtering, clustering, and prioritisation of data streams. Rather than relying solely on human analysis, AI-supported systems can autonomously detect anomalies, classify threats, and fuse diverse inputs into a coherent picture.[43] However, the accuracy of AI-supported observation depends on data quality and algorithmic design, which introduces new sources of uncertainty into the MDMP.

The specific application and reliability of AI-supported observation also depend on the command level at which it is employed. On the tactical level, AI is primarily used for real-time sensor data fusion, target recognition, and rapid threat classification in direct support of manoeuvre units. These systems operate under tight time constraints and are often embedded in platforms such as unmanned aerial vehicles or fire control systems.[44]

At the operational level, AI contributes to the coordination of multiple units, force allocation, and anticipating adversary movements through predictive modelling and operational wargaming. The data requirements here are broader, and the systems must synthesise inputs across different domains and formations.[45]

At the strategic level, AI is increasingly used in intelligence analysis, long-term scenario planning, and detecting emerging threats in the information and cyber domains. At this level, the focus shifts from speed to pattern recognition across geopolitical, economic, and military indicators.[46] Therefore, each level poses distinct challenges regarding data volume, reliability, and decision horizons. As a result, AI must be tailored to both technological and command-level contexts.

The second step of the OODA Loop—orient—is central to Boyd's theory. While observation provides data, orientation gives it meaning. Boyd described this step as synthesising cultural background, prior experience, training, and analytical reasoning.[47] Concerning mission command and AI, Johnson has emphasised that Boyd's theory loses its core message if the orientation step is not understood as a priority.[48] It is thereby striking that Clausewitz' 'coup d'œil' refers to orientation rather than to decision.

Orientation finally shapes the interpretation of information and leads to the implication of acting options. AI contributes to this process not only by analysing data but also by structuring and presenting data. In modern command systems, AI tools support commanders by highlighting correlations, assessing risks, and suggesting probable developments.[49] However, these outputs rely on algorithmic models trained on historical data and defined parameters. If not carefully integrated, such systems may promote a narrow interpretation of the situation and reduce the diversity of considerable options.

Therefore, junior and senior leaders must understand that AI supports human judgment, not replaces it. In Mission Command, where initiative and independent decision-making are essential, commanders must remain able to question or override AI-generated suggestions when necessary.

The third step of the OODA Loop—decide—refers to selecting a course of action based on the processed and interpreted information. Traditionally, this step rests on the commander's experience, situational awareness, and operational intent. With the integration of AI, this decision-making process is increasingly supported by AI tools such as simulations, analytics, and wargaming systems.[50,51]

These tools offer clear benefits. They can assess a broader range of scenarios in shorter timeframes, quantify risks, and visualise probable outcomes. Especially in time-critical or complex situations, such systems can help reduce cognitive load and improve decision speed. However, they also raise the question of decision delegation to followers. As confidence in AI systems increases, junior-level tactical leaders will likely show a tendency to follow AI's recommendations without further scrutiny—especially under time pressure.

This dynamic blurs the boundary between decision support and decision automation. Studies have shown that operators often follow algorithmic recommendations without critical review in high-pressure environments—a phenomenon called automation bias.[52,53] While partial automation may be technically feasible, strategic analysts stress the continued necessity of human oversight, particularly in contexts where legal responsibility and operational ethics are involved.[54] Within the framework of

Mission Command, decisions must remain comprehensible, transparent, and attributable—both to the commander, who bears ultimate responsibility, and to the subordinate, whose trust is essential. For the commander, transparency ensures accountability and enables effective leadership. For the subordinate, it fosters trust; black-box systems offer little foundation for the initiative and confidence that Mission Command demands. The challenge lies in maintaining human authority over machine-generated options, even when these appear more efficient or statistically plausible.

The fourth step of the OODA Loop—act—refers to executing the course of action. Traditional operation understanding links this step to command hierarchies, communication and force deployment. However, this step undergoes substantial transformation with the increasing use of autonomous and semi-autonomous systems. Unmanned platforms, loitering munitions, and algorithmically controlled defensive systems can respond faster than humans, especially in contested environments.[55]

Technically, integrating AI into tactical execution—acting at the lowest command level—offers significant advantages. Autonomous systems can respond within milliseconds, operate in denied environments, and execute complex manoeuvres based on predefined parameters. However, these capabilities come at a cost. When systems have greater operational freedom, it raises concerns about accountability, ROE, and adaptability.[56] Operational misalignment between human intent and machine execution, caused by misunderstood commands or unforeseen environmental variables, is a risk.[57]

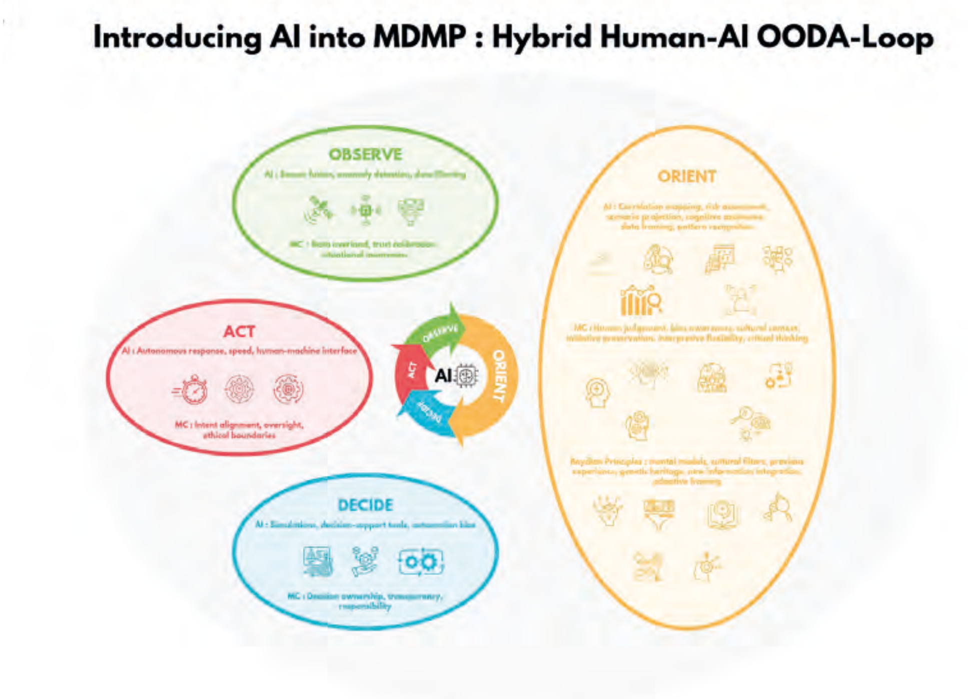
These concerns do not imply that human decision-making or action is fundamentally better than AI or automatic weapons. People make mistakes—both consciously and unconsciously. They break laws, whether self-imposed or externally mandated, and violate moral standards, whether personal or universal. Misalignment is not just a human/machine problem; it is first and foremost a human/human problem. However, people are more willing to accept mistakes made by others than those made by machines. It may be irrational, but the public rejects robot taxis as soon as they hit a child—even if the robot's probability of error is significantly lower than that of an average human driver.[58]

However, the desire for attribution and accountability is not just an intuitive need of the population. Ultimately, it is a demand of the enlightenment on state action: humans shall be protected from the arbitrariness of the executive branch, and the judiciary should correct possible mistakes to restore justice. A fallible commander can be convicted and punished, but a fallible robot cannot. Even if this demand for accountability stems from emotion or intuition rather than rationality, it remains valid on legal-philosophical grounds.[59]

In Mission Command, the act step must retain a degree of human oversight. While certain functions may be delegated for speed and efficiency, the overall framework must ensure that action remains guided by intent, not merely by code. This includes mechanisms for intervention, abort criteria, and a clear delineation of human versus machine authority within the execution chain.

It is true that potential antagonists may not share the same concerns about legal or ethical constraints. However, this is not a new problem: military ethics and international humanitarian law have long grappled with the challenges of dealing with an opponent who disregards such norms. The Geneva Conventions agree that disregard by the opponent does not release us from our obligations.[60] The question appears to be more complex from a military ethics perspective, as considerations regarding reprisals demonstrate.[61] At the same time, however, it would be tantamount to abandoning our own ethical standards if we were to reject them because our opponents adhere to different standards. Our commitment to these principles is not contingent on reciprocity, but on upholding the values we claim to defend.

Integrating AI into the OODA Loop presents both a logical evolution and a fundamental shift in military decision-making. Across all four steps—observation, orientation, decision, and action—AI systems offer the potential to increase speed, reduce cognitive burden, and manage complexity beyond human capability. In doing so, they support Boyd's overarching goal: to operate inside the adversary's decision cycle and gain tactical and operational advantage.[62,63]



Source: Authors.

From a Mission Command perspective, the challenge is not to prevent the use of AI but to ensure its integration respects the underlying principles of decentralised, intent-driven leadership. Whether artificial intelligence ultimately leads to greater centralisation or decentralisation in MDMP and Mission Command depends on how its capabilities are operationalised.

Centralisation and Decentralisation: From Opposition To Continuum

Military leaders can no longer conceptualise command in the age of AI through the binary lens of centralisation versus decentralisation. Instead, command constitutes an adaptive continuum, within which militaries must reorganise themselves in real time according to the operational context. Technological advancements sometimes promote centralised command and, at other times, foster greater autonomy at junior levels. For example, access to an "omniscient operational picture" enabled by AI may tempt senior leadership to micromanage every tactical action from a centralised decision-making hub. In addition, potential cyberattacks and the complexity of the electromagnetic spectrum suggest that AI may be more effectively employed to enhance decentralised initiative at the tactical edge.[64] Centralisation and decentralisation should thus be understood not as mutually exclusive choices but as two poles of a single dynamic that must be modulated.

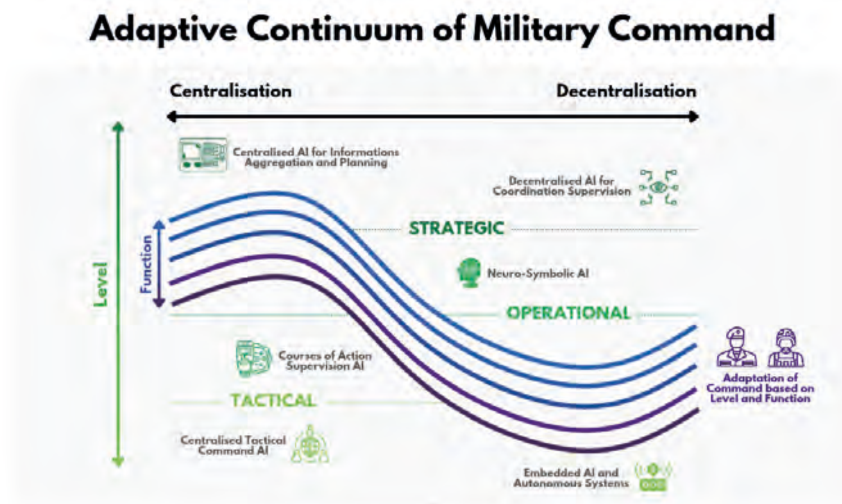
Western militaries constantly navigate this centralisation-decentralisation continuum, adjusting their posture based on operational requirements. Recent operational feedback confirms the importance of such flexibility. This dialectic is not new; it continues the tradition of Mission Command, which advocates for centralised intent and decentralised execution. It may be assessed through a framework measuring the influence and weight of mission-related, human and organisational factors. In the case of Western armed forces, this distribution implies that the only viable approach to centralisation and decentralisation is the one broadly aligned with NATO's Mission Command model. AI does not undermine this foundation but rather intensifies its internal tensions: it enables near-omniscient centralised control and local-level automated decision-making.[65]

A truly fluid and agile comprehension of command must be capable of adapting the degree of centralisation according to the hierarchical level and the command function being exercised. At the strategic and operational levels, a certain degree of centralisation remains essential to maintain a shared vision and unity of effort. At these echelons, we already observe the integration of robust centralised AI systems—such as Large Language Models (LLMs)—for intelligence aggregation and campaign planning support.[66] These strategic AI tools can process vast volumes of data and generate global options, contributing to a form of "hybrid human-machine judgment" at the upper tiers of command.[67]

Nevertheless, even at these levels, commanders must retain doctrinal flexibility to adapt their leadership style. Complex battlefields may call for temporary recentering of control (e.g., to coordinate a multidomain operation), followed by a re-delegation of authority to subordinate echelons as the situation evolves and demands increased initiative.

At the tactical level, however, the decentralised initiative becomes paramount in responding to the real-time chaos of combat. Here, embedded AI (Edge AI) and autonomous systems will play a decisive role. Intelligent sensors, onboard Bayesian algorithms, and lightweight decision-support systems will provide frontline units with immediate analysis and action capabilities independent of higher-level directives. This reinforces the concept of an augmented OODA Loop—where the Observe and especially the Orient steps are accelerated by AI—while the Decide and Act steps can be executed locally in an informed manner, remaining aligned with the overarching commander's intent. Such integration enables small units to complete the decision cycle faster than the adversary, thereby contributing to the decision superiority sought in contemporary military doctrines.[68]

In this conceptualisation, in which AI assistance enhances human performance, the continuing adaptation of military command between centralisation and decentralisation emerges as a critical pathway in digital evolution. Decentralised autonomy at lower echelons does not imply the absence of control: command retains visibility through a continuous information flow, only intervening when necessary or reorienting efforts according to strategic objectives. All these considerations lead to this adaptive continuum of military command.



Source: Authors.

Simultaneously, each domain of the CLM model—Command, Leadership, and Management—benefits differently from this AI-enabled adaptability. Command gains from centralised AI tools, which support strategic orientation and ensure clear communication of intent. Tactical AI is profoundly transforming leadership: the field commander is now equipped with unprecedented local decision-support tools—such as those illustrated in the augmented OODA Loop—allowing for semi-autonomous action that remains tightly coupled to the overarching strategic direction. Lastly, Management can leverage analytical AI systems to optimise logistics, which tends to favour centralisation; yet, it can also delegate certain decisions to lower levels via self-organising tools (e.g., models such as Gallatin that dynamically allocate resupply based on real-time frontline needs.)[69]

In this way, AI functions as a differentiated catalyst: centralising for command when synthesising a global vision, empowering leadership at the lowest levels by accelerating execution, and rationalising for management by enabling cross-functional optimisation.

From a more critical perspective, this fluid transition between centralisation and decentralisation—while ideal in theory—collides with entrenched structural, doctrinal, and cultural forces within military organisations. On the one hand, Western armed forces are steeped in the philosophy of Mission Command and the principle of subsidiarity, which emphasise delegation and subordinate initiative. These principles represent a significant doctrinal legacy born from the necessity to act despite uncertainty and battlefield chaos. They assert that the leader must define a clear intent and then relinquish control over the means of execution, allowing capable followers to seize opportunities as they arise. This culture of trust and empowerment is a prerequisite for any effective decentralised approach.

On the other hand, the temptation toward centralisation resurfaces with every technological revolution. Today, hyper-connectivity, the massive availability of data and AI grant military headquarters a sense of global oversight that can lead to a tendency to recentralise decision-making authority. In times of peace or when facing diffuse threats, centralised control may appear logical to optimise coordination; "Centralised planning is a manifestation of a belief in the ability to optimise".[70] This reflex, a legacy of the industrial age and likely reinforced by cognitive biases such as the illusion of control,[71] risks undermining the responsiveness required in real combat. It may run counter to the Mission Command philosophy cherished by Western militaries.

This tension reflects a latent conflict between technological architecture and organisational architecture. For instance, the French Army has observed that specific "centralising digital tools" and bureaucratic complexity can "slow down, paralyse, or discourage subordinate initiative".[72] AI may either exacerbate this dysfunction—by reinforcing top-down, omnipresent control—or help remedy it by equipping subordinates with the means to act independently and with insight.

The key distinction lies in the adopted command culture. Western militaries, with their longstanding tradition of decentralised decision-making, may be particularly well-positioned to harness AI as a tool of empowerment rather than surveillance. Nevertheless, this requires sustained investment in training, education and doctrinal adaptation. The human factor—especially mutual trust between command echelons—remains central to this transformation. Learning to trust AI-generated recommendations will be crucial without succumbing to blind delegation or intrusive interference.

Similarly, military forces with less experience in subsidiarity can evolve: recent doctrinal reflections from Chinese military thinkers also advocate for greater flexibility and local initiative supported by emerging technologies.[73] This suggests that cultural determinism can be disrupted by operational realities and the opportunities AI presents.

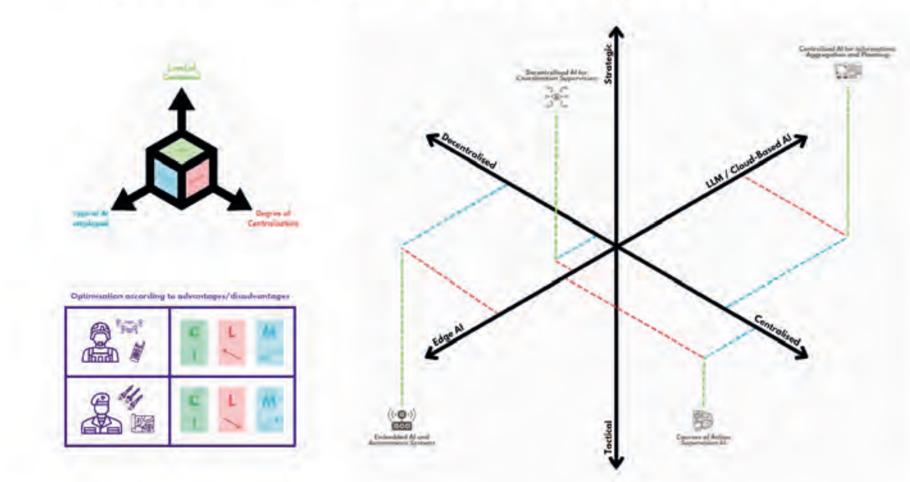
From Binary to Multidimensional: Towards an Adaptive Model of Military Command

These analyses converge toward the necessity of a theoretical model of adaptive command capable of visually representing the dynamic flow between centralisation and decentralisation in the age of AI. One may envision a three-dimensional framework in which each axis corresponds to a key factor: the degree of command centralisation (ranging from fully centralised to fully decentralised), the level of command or scale of action (from strategic to tactical), and the type of AI employed (centralised cloud-based AI/LLMs, distributed Bayesian AI, embedded Edge AI).

Within this 3D space, command does not occupy a fixed point; instead, it moves within a volume of possibilities that reflect shifting operational demands. For instance, a deep special operation might be represented as a highly decentralised point on the tactical axis with a predominance of embedded AI. In contrast, an initial joint-force campaign could appear closer to the strategic-centralised pole, supported by intelligence aggregation AI systems. The model is dynamic: a trajectory or vector within this volume would illustrate the transition from one mode of command to another as the operation unfolds, responding to situational changes (emerging threats, communications disruption, windows of opportunity).

The Command-Leadership-Management model enriches this tridimensionality: Command is parallel to the plane defined by the "level of command" axis, as it captures the doctrinal approach, the Leadership dimension aligns with the plane of the "degree of centralisation" axis, as it represents the human approach and Management lies parallel to the plane defined by the "type of AI employed" axis, as it reflects the structural approach.

Three-Dimensional Framework of Adaptive Command



Source: Authors.

Such a conceptual framework allows for the visualisation of transitions—for example, the gradual shift from centralised control at the onset of an engagement to increasing autonomy granted to subordinate units as the action becomes more complex, followed by a possible temporary recentralisation to synchronise a decisive effort, and so on.

It also reveals the specific contribution of the different domains, highlighting which dimension becomes predominant depending on where one is positioned within the model. The model, when applied to the three-dimensional space, provides both a critical and forward-looking perspective on future command: critical because it challenges military leaders to confront their cognitive biases (such as the tendency to over-centralise or relinquish control too readily), prompting continual repositioning along the optimal spectrum; and forward-looking, because it opens the way to novel, agile organisational forms enabled by AI.

Ultimately, command in the era of artificial intelligence may be understood as a complex adaptive system whose superiority lies in its capacity to reinvent its own modus operandi faster than the adversary. This doctrinal, intellectual, and structural agility—rather than any specific technology—will constitute tomorrow's decisive advantage. The challenge is, therefore, not merely a dialectic between centralisation and decentralisation, nor simply a faster and more optimised OODA Loop, but rather a multidimensional dynamic in which doctrine, culture, and organisation each play an essential role.

Meeting this transformation requires more than technical innovation. It demands new doctrines, cultures, and command structures suited for the AI era—ones that preserve the agile spirit and boldness inherent to Mission Command while leveraging AI to enhance the accuracy and speed of decision-making. The integration of AI forces a transition from abstract principles to concrete application: continuously adjusting the centralisation/decentralisation dial demands sustained intellectual discipline, organisational agility, and, above all, a doctrine fit for the future.

This proposed dynamic model is but a conceptual step toward that heightened agility: it provides a comprehensive framework for thinking about change—a necessary condition for implementing it within military doctrines, cultures, structures, and procedures.

Endnotes

[1] James Johnson, "Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age," Defence Studies 23, no. 1 (2023): 43–67.
[2] René A. Herrera, "History, Mission Command, and the Auftragstaktik Infatuation," Military Review, July–August 2022, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2022/Herrera/, accessed March 21, 2025.
[3] Eitan Shamir, "Transforming Command: The Pursuit of Mission Command in the U.S., British, and Israeli Armies," Stanford, CA: Stanford University Press, 2011.
[4] Department of the Army, "Mission Command: Command and Control of Army Forces (ADP 6-0)," Washington, DC: Headquarters, Department of the Army, 2019.
[5] British Army, "Army Leadership Doctrine," 2021, https://www.army.mod.uk/media/25267/cal-mission-command-and-leadership-on-operations-2024-final-v2.pdf, accessed March 21, 2025.
[6] Vitalii Shvaliuchynskyi, "Mission Command and Artificial Intelligence," Review of the Air Force Academy 1, no. 1 (2023): 85–92, https://sciendo.com/pdf/10.2478/raft-2023-0010, accessed March 21, 2025.
[7] Richard Sanders, "Mission Command: Doctrinal Improvements for Peer Conflict," Wild Blue Yonder 4, no. 2 (2023): 45–58, https://www.airuniversity.af.edu/Wild-Blue-Yonder/Articles/Article-Display/Article/3913449/mission-command-doctrinal-improvements-for-peer-conflict/, accessed March 21, 2025.
[8] NATO, "Allied Joint Publication AJP-01(D): Allied Joint Doctrine," Brussels: NATO Standardization Office, 2022.
[9] Zoltán Fazekas, "Trust and Artificial Intelligence in Military Operations," Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2022.
[10] Alistair Byford, „How Well Do We Understand Air Command and Control?," Air Power Review 17, no. 2 (2014): 92–97.
[11] Donald E Vandergriff, "Adopting Mission Command: Developing Leaders for a Superior Command Culture," Minneapolis: Mission Command Press, 2018.
[12] Eitan Shamir, "Transforming Command."
[13] Martin van Creveld, "Kampfkraft: Militärische Organisation und Leistung," 1939–1945, Freiburg: Rombach, 1989.
[14] John Richard Boyd, "Patterns of Conflict," Unpublished briefing slides, 1986, https://www.ausair-power.net/JRB/poc.pdf, accessed March 21, 2025.
[15] Réne A. Herrera, 2022, has written a more nuanced historical account of this, refuting some misunderstandings in the modern interpretation and also showing how the current understanding of Mission Command in the American armed forces is at best a half-hearted copy of the original.
[16] Robert L. Bateman, "Force XXI and the Death of Auftragstaktik," ARMOR, January–February 1996: 13–15, https://www.benning.army.mil/armor/eARMOR/content/issues/1996/JAN_FEB/ArmorJanuary-February1996web.pdf, accessed March 21, 2025.
[17] Rosario M. Simonetti and Paolo Tripodi, "Automation and the Future of Command and Control: The End of Auftragstaktik?," Journal of Advanced Military Studies 14, no. 1 (2023): 85–102, https://www.usmcu.edu/Portals/218/JAMS_Vol14_No1_Simonetti_Tripodi.pdf, accessed March 21, 2025.
[18] Idem., 142.
[19] Pedro DeLeon and Paolo Tripodi, "Eliminating Micromanagement and Embracing Mission Command," Military Review, July–August 2022: 19–27, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20220831_art005.pdf, accessed March 21, 2025.
[20] James M. Beagle, John D. Slider, and Michael J. Arrol, "Mission Command in the 21st Century: Adapting to Modern Warfare," Parameters 53, no. 1 (2023): 35–47, https://press.armywarcollege.edu/parameters/vol53/iss1/4/, accessed March 21, 2025.
[21] The latter has its justification, which can be explained by the "accountability chain" approach,

see Patrick Hofstetter, "Der Mehrwert militärischer Führungsausbildung in der Staatsleitung: Von der Kaderschmiede zum Benchmark für Command, Leadership und Management in der Schweiz," Zürcher Forum Staatsleitung, no. 10 (2025), https://www.ius.uzh.ch/de/staff/professorships/alphabetical/glaser/Z%C3%BCrcher-FORUM-zur-Staatsleitung/Der-Mehrwert-milit%C3%A4rischer-F%C3%BChrungsausbildung-in-der-Staatsleitung.html, accessed April 15, 2025.
[22] Patrick Hofstetter,"Command, Leadership, Management: 95 Thesen zur Führung in der Schweizer Armee und darüber hinaus," Stratos 3, no. 2 (2023): 126–135, https://stratos-journal.ch/ausgaben/stratos-3-2/hofstetter/, accessed March 21, 2025.
[23] Stephen Bungay, "Mission Command in the 21st Century: A View from the Other Side," British Army Review 150 (2011): 20–29, https://www.army.mod.uk/our-people/army-command-organisation/command-leadership-management/, accessed March 21, 2025.
[24] British Army, "Army Leadership Doctrine," 2021, https://www.army.mod.uk/media/25267/cal-mission-command-and-leadership-on-operations-2024-final-v2.pdf, accessed March 21, 2025.
[25] Hofstetter, "Command, Leadership, Management."
[26] Swiss Armed Forces, "Strategie zur Vision 2030 der Gruppe Verteidigung," Internal document 81.377d, 2025.
[27] Jim Storr, "A Command Philosophy for the Information Age: The Continuing Relevance of Mission Command," Defence Studies 3, no. 3 (2003): 119–129, https://www.tandfonline.com/doi/abs/10.1080/14702430308405099, accessed March 21, 2025.
[28] Vandergriff, "Adopting Mission Command."
[29] Boyd, "Patterns of Conflict."
[30] Patrick Hofstetter, Alan Borioli, and Till Flemming, "Manoeuvre Is Dead – But It Can Be Revived: Overcoming Stalemates by Gaining Competitive Advantage," The Defence Horizon Journal, October 28, 2024, https://tdhj.org/blog/post/manoeuvre-innovation/, accessed March 22, 2025.
[31] Arthur K. Cebrowski, and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," Proceedings 124, no. 1 (1998): 28–35, https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future, accessed March 22, 2025.
[32] Shamir, "Transforming Command."
[33] Edgar H. Schein, "Organizational Culture and Leadership," 2nd ed. San Francisco, CA: Jossey-Bass, 1992.
[34] Vandergriff, "Adopting Mission Command".
[35] Boyd, "Patterns of Conflict."
[36] Idem.
[37] Idem., slide 76.
[38] Idem., slide 79.
[39] Carl von Clausewitz, "On War," ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 102.
[40] Boyd, "Patterns of Conflict."
[41] Frans P.B. Osinga, "Science, Strategy and War: The Strategic Theory of John Boyd," London: Routledge, 2006.
[42] Paul Scharre, "Army of None: Autonomous Weapons and the Future of War," New York: W. W. Norton & Company, 2018.
[43] Michael C. Horowitz, Lauren Kahn, Paul Scharre, and Megan Lamberth, "Algorithmic Warfare: Balancing Speed and Control," Santa Monica, CA: RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RRA1076-1.html, accessed March 21, 2025.
[44] Scharre. "Army of None."
[45] Horowitz et al., "Algorithmic Warfare."
[46] Vincent Boulanin, Netta Goussac, Sonia Fernandez, and Moa Peldán Carlsson, "The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk," Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2020, https://unidir.org/publication/impact-artificial-intelligence-strategic-stability-and-nuclear-risk, accessed March 21, 2025.
[47] Boyd, "Patterns of Conflict."

[48] Johnson, "Automating the OODA Loop," 47.
[49] Horowitz et al., "Algorithmic Warfare."
[50] Scharre, "Army of None."
[51] Horowitz et al., "Algorithmic Warfare."
[52] Scharre, "Army of None."
[53] Boulanin et al., "The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk."
[54] Horowitz et al., "Algorithmic Warfare."
[55] Scharre, "Army of None."
[56] Total Military Insight, "Rules of Engagement," Accessed April 11, 2025, https://totalmilitaryinsight.com/rules-of-engagement/.
[57] Scharre, "Army of None."
[58] For an introduction to the ethics of autonomous driving, cf. Patrick Lin, "Why Ethics Matters for Autonomous Cars," in: Autonomes Fahren: Technische, rechtliche und gesellschaftliche Aspekte, ed. Markus Maurer, J. Christian Gerdes, Barbara Lenz, and Hermann Winner (Wiesbaden: Springer Vieweg, 2015), 69–85.
[59] Cf. Christof Heyns, "Autonomous Weapons Systems: Living a Dignified Life and Dying a Dignified Death," in: Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare, ed. Nehal Bhuta, Susanne Beck, Robin Geiß, Hin-Yan Liu, and Claus Kreß (Oxford: Oxford University Press, 2016).
[60] Jean de Preux, "The Geneva Conventions and Reciprocity," International Review of the Red Cross (1961–1997) 25, no. 244 (1985): 25–29.
[61] Michael Walzer, "Just and Unjust Wars: A Moral Argument with Historical Illustrations," 5th ed. (New York: Basic Books, 2015), chapter 13.
[62] Boyd, "Patterns of Conflict."
[63] Osinga, "Science, Strategy and War."
[64] Sydney J. Freedberg Jr, "Empowered Edge versus the Centralization Trap: Who Will Wield AI Better, the US or China?," Breaking Defense, February 2024, https://breakingdefense.com/2024/02/empowered-edge-versus-the-centralization-trap-who-will-wield-ai-better-the-us-or-china/.
[65]Benjamin Jensen and J. S. Kwon, "The U.S. Army, Artificial Intelligence, and Mission Command," War on the Rocks, March 2025, https://warontherocks.com/2025/03/the-u-s-army-artificial-intelligence-and-mission-command/.
[66] Idem.
[67] Tim Stewart, "AI and the OODA Loop: How AI Enhances Strategic Decisions for Today's Warfighters," Military Embedded Systems, 2024, https://militaryembedded.com/ai/big-data/ai-and-the-ooda-loop-how-ai-enhances-strategic-decisions-for-todays-warfighters.
[68] Idem.
[69] Colin Demarest, "Exclusive: Gallatin, Backed by 8VC, Dives into AI-Fueled Military Logistics," Axios, April 08, 2025, https://www.axios.com/2025/04/08/gallatin-ai-8vc-military-logistics.
[70] David S. Alberts and Richard E. Hayes, "Power to the Edge: Command… Control… in the Information Age," (Washington, DC: CCRP, 2003), 62.
[71] Ellen J. Langer, "The Illusion of Control," Journal of Personality and Social Psychology 32, no. 2 (1975): 311–328.
[72] Armée de Terre, "Qu'est-ce que le commandement par intention?," Ministère des Armées (France), 2023, https://www.defense.gouv.fr/terre/chef-detat-major-larmee-terre/vision-strategique-du-chef-detat-major-larmee-terre/commandement-intention-0.
[73] Larry Wortzel, "Paper: Chinese Army's Rigidity Inhibits Mission Command," Association of the United States Army, 2024, https://www.ausa.org/publications/pla-and-mission-command-party-control-system-too-rigid-its-adaptation-china

04

ENHANCING BATTLEFIELD OBSERVATION WITH IMITATION LEARNING AND DIGITAL TWIN-BASED MODEL TRAINING

MICHAIL KEFALAKIS, NIKOLAOS V. KARADIMAS

- **Authors:** Michail Kefalakis, Computer Science and Biomedical Informatics, Geospatial Sciences, PhD Candidate in the Hellenic Army Academy with research interests focusing on Remote Sensing, Digital Twins for Military Applications, Deep Learning, Computer Vision.

  Nikolaos V. Karadimas, Associate Professor in the Department of Military Sciences at the Hellenic Army Academy, with research interests focusing on Military Applications, Databases, Big Data, Operational Resource Management, Geographic Information Systems, Simulation Algorithms and Modeling, as well as Decision Support Systems.

  The views contained in this article are the authors' alone.

- **Abstract:** The evolution of battlefield surveillance, from traditional elevated vantage points to advanced satellite remote sensing, has transformed geospatial data into actionable insights. The research focuses on creating a Digital Twin of a battlefield using a range of data sources. A methodology for assessing terrain features, such as visibility, slope, and soil moisture, is developed, along with a model for vegetation cover using Sentinel-2 data. Imitation Learning is employed to simulate military strategies based on human decision-making processes, generating synthetic data that represent real-world conditions.

- **Problem statement:** How to combine Digital Twins and Imitation Learning to replicate human decision-making and generate synthetic data that reflects real-world dynamics in military settings?

- **Bottom-line-up-front:** Combining these technologies could create dynamic, real-world, data-driven simulations for military applications. This would provide a powerful tool for generating synthetic data that can be utilised across various applications, including training, machine learning model development, and decision-making.

- **So what?:** A combination of models and products that continuously update a digital replica of battlefield conditions must be developed. Based on its output, „what-if" scenarios and real-time situations should be translated into simulations, allowing conflict scenarios to unfold according to human strategies. The military can then utilise this synthetic data for both human and machine training and decision-making assessments.

Battlefield Observation

Battlefield observation has been a critical aspect of military strategy since ancient times, providing vital information for decision-making in military endeavours. A common approach was to gather intelligence by observing the battlefield from elevated positions, such as cliffs or other high vantage points, allowing for a comprehensive view of the area of interest. Fast forward to the present day, and battlefield observation remains just as crucial for gaining insights. Still, the methods and tools have evolved to provide quicker responses and enhanced predictive capabilities. In recent conflicts, Satellite Remote Sensing methods have become integral for surveillance and reconnaissance, transforming terrain data into actionable insights for military decision-making.

The Digital Twin Concept

At the same time, the concept of the Digital Twin has advanced significantly. A Digital Twin is a digital replica of a physical entity, where events in the real world are mirrored in the virtual model. While the concept of a Digital Twin is not new, its application in battlefield observation has yet to be fully explored, particularly from an academic perspective.[1] This emerging field could hold significant potential for revolutionising how military operations monitor and analyse battlefield conditions.

Imitation Learning

On the other hand, imitation learning represents a distinct field within artificial intelligence, primarily focused on mimicking human behaviour. Initially popularised in the realm of entertainment games, such as chess, to create AI opponents, imitation learning has been largely overlooked in other scientific disciplines. However, the battlefield is inherently dynamic, with strategies often shaped by human-level decision-making. By capturing various human strategies in different battlefield conditions, imitation learning can be leveraged to create tailored synthetic data through battlefield simulations.[2]

The intersection of Digital Twin technology and imitation learning is an unexplored frontier. This combination could generate dynamic virtual representations of real-world conditions for a given area of interest, simulating different unit positions and conflict scenarios. Doing so would offer a powerful tool for training, analysis, and strategic decision-making in military settings. In this study, the data sources, methods, and tools for creating such a Digital Twin will be assessed along with the associated challenges.

Data Collection

The building blocks of the proposed Digital Twin are the data. The first step in data collection involves defining the data sources necessary to create the Digital Twin. This is a complex task, as there are numerous sources of data, each associated with specific sensors. Land cover data are efficiently captured with optical and multispectral sensors, urban and soil moisture data are captured with a Synthetic Aperture Radar (SAR) sensor, while road networks are provided on OpenStreetMap (OSM). The challenge is also compounded by data being collected at different time intervals, and constant updates for some data points may not be required. For instance, a mountain slope undergoes minimal change on a day-to-day basis; however, significant differences become more evident over extended periods, demonstrating the importance of selecting appropriate intervals for data collection and analysis.

To maximise efficiency and resourcefulness in data gathering, it is crucial to define the temporality of the data. Temporal data refers to data that requires varying frequencies of updates based on its relevance over time. High-temporal data demands frequent updates, while lower-temporal data may not need constant monitoring as significant changes become apparent over longer periods. For creating a battlefield Digital Twin, specific datasets—such as the Digital Elevation Model (DEM)—are considered more temporally significant. These datasets remain relatively stable over time, making them crucial for accurately representing the terrain in the Digital Twin model.[3]

One of the most widely used digital elevation models is the Copernicus Global 30m (CopDEM), which is frequently employed in scientific research. The Copernicus Global 30m is publicly available and performs better in urban areas and vegetation-covered landscapes than the ALOS model. However, its performance on steep slopes is not optimal. CopDEM generally exhibits more consistent global accuracy than the CDEM. While NASADEM and ASTER datasets show the largest positive discrepancies, Copernicus DEM displays the most significant negative discrepancy, with values lower than the true measurements. Other models, such as GLO-30 DEM, ALOS AW3D30 DSM, CDEM, ICESat, and AW3D, also contribute to the comparison of elevation data accuracy.[4,5,6]

The Digital Elevation Model (DEM) offers valuable insights when integrated into a Digital Twin within a military context. It enables the creation of maps depicting the visibility of friendly forces in relation to enemy positions and vice versa. Additionally, the DEM can be used to extract slope data, which is crucial for assessing vehicle mobility in specific areas. By combining slope information with the vehicle's characteristics, it becomes possible to evaluate terrain permeability and optimise tactical planning.[7]

Challenger arise from the simplicity and limitations of traditional visibility analysis, and advanced techniques have been proposed that utilise 3D graphic software, addressing the limitations of traditional Geographic Information Systems (GIS)based viewshed analysis. Although GIS advancements have introduced new models that utilise 3D graphic software, providing better accuracy and efficiency,[8,9] Digital Surface Models (DSMs) provide a better alternative to DEMs as they measure the elevation of each object, though with a costly acquisition.[10] One-Shot depth estimation, a method for calculating depth from single optical images, is experiencing growth, but only for high-resolution satellite imagery.[11] In the case of the Digital Twin's initial development phase, the viewshed assessed solely by the DEM is a good starting point.

The temporality of data collection, particularly regarding the existence and development of buildings, has been a subject of considerable reflection. One significant challenge in analysing urban landscapes is the time it takes to construct buildings, a process that spans varying durations and can differ substantially from one geographic location to another. Furthermore, buildings do not appear with high frequency in any given area, making their monitoring a more intermittent task. Suggesting a frequency of data acquisition for urban footprint estimation poses a challenge and must be considered by the user, as frequent gathering of urban landscape products can cause storage capacity limitations, while infrequent observations may miss early-stage or completed construction.

Several data sources can be utilised to assess the presence and characteristics of buildings in urban environments. Among the most accessible and widely used tools is OpenStreetMap (OSM), a collaboratively maintained mapping platform that offers publicly available geographic data. OSM relies heavily on its open community of contributors for the accuracy and completeness of the data, which, in principle, allows for continuous updates and coverage.[12] In military planning, OSM provides an urban footprint with higher resolution, outlining the building perimeter in the context of urban warfare planning.[13] However, one must approach this data with caution, as certain building footprints may be missing or outdated, particularly in rapidly developing or underrepresented regions. While OSM is an invaluable resource, its reliance on voluntary contributions and local knowledge introduces the possibility of gaps or inconsistencies in mapping urban environments.

In contrast, the use of Synthetic Aperture Radar (SAR) imagery provides a different, more technologically advanced method for assessing urban landscapes. The Copernicus Sentinel-1 Mission, in particular, has revolutionised the way urban areas are monitored. By utilising SAR data, which can capture detailed information about the Earth's surface regardless of weather conditions or time of day, it enables frequent and reliable monitoring of buildings and other structural features. The revisit frequency of the Sentinel-1 Mission, ranging from two to six days,[14] is particularly advantageous for tracking changes in urban environments with a relatively high temporal resolution. This frequent data acquisition allows for more precise monitoring of new developments, alterations to existing buildings, and other dynamic changes in urban areas.[15,16]

Road networks are critical when assessing human presence through remote sensing imagery, much like veins in a biological system. While buildings are often seen as vital in such assessments, road networks play an equally indispensable role. They are essential for facilitating the movement of land vehicles and ensuring the mobility and deployment of infantry, equipment, and resources. In the context of a battlefield Digital Twin, road networks serve as a fundamental infrastructure element, supporting both strategic manoeuvring and logistical operations. Their importance goes beyond transportation, as they enable operational efficiency and accessibility, shaping the dynamics of both military and civilian activities. The Sentinel Mission products provide lower-resolution images that cannot capture road networks, except for some major roads. Given the challenges of extracting road networks from satellite resolutions like those of the Sentinel Missions, road footprints were sourced from OpenStreetMap.

In the context of Synthetic Aperture Radar (SAR) imagery, Sentinel-1 can effectively monitor and assess soil moisture levels, which are crucial for understanding terrain conditions that impact military operations. Soil moisture plays a significant role in military activities, as it can hinder the movement of personnel and vehicles and contribute to the failure of various types of equipment. However, directly assessing soil moisture using remote sensing techniques can be challenging due to the complex interactions between radar signals and soil properties.[17,18]

Sentinel-2 data is crucial in land cover estimation, particularly in gathering remote sensing indices related to vegetation.[19,20] Vegetation cover is an essential factor in military decision-making, as it directly impacts the movement of units, ground permeability, and the ability to conceal movements or assets. To derive the necessary information to represent vegetation cover in the Digital Twin, the Tree Density High-Resolution Layer, Small Woody Features High-Resolution Layer, and Grassland High-Resolution Layer were obtained from the Copernicus Open Access Hub. These layers were used as ground truth to correlate with remote sensing indices, ensuring that the Digital Twin remains continuously updated with current vegetation information. These layers provide valuable insights into vegetation characteristics,[21,22,23] which can influence both tactical and strategic military operations. Understanding these variables is vital for assessing terrain and improving operational effectiveness in complex environments.

Data Cleaning and Processing

The data from the aforementioned sources must be processed to transform it into relevant information. The Copernicus Global Elevation Model was utilised as the base for the Digital Twin and integrated into ArcGIS Pro. By processing it as a raster product, the slope of the terrain could be calculated, providing valuable insights into the terrain's morphology. To further enhance the analysis, the viewshed of military units was determined through Visibility Analysis, which helps assess line-of-sight and potential cover. Additionally, road data was incorporated into ArcGIS Pro. While each road type has distinct attributes that could affect mobility, this study chose to treat all roads equally without considering the varying weight each type might have on movement efficiency.

Monitoring population displacement and urban expansion is critical as urban areas significantly impact military operations. Additionally, the timely detection of insurgent base construction is essential for strategic planning. Sentinel-1 data were obtained from the Copernicus Open Access Hub to support this. The Sentinel-1 product used for this analysis featured dual polarisation, specifically HV and VV polarisations. The VV polarisation is particularly effective in urban footprint estimation, as it efficiently captures backscatter from flat surfaces, making it suitable for identifying urban areas.

The image is first imported into ESA's SNAP software for urban footprint estimation to begin the preprocessing procedure. Radiometric calibration is applied to the VV band to prevent any information leakage from the VH band into the VV band, ensuring the accuracy of the analysis. SAR products typically contain significant noise, known as speckle, which arises due to the interaction of electromagnetic pulses with the environment. The Refined Lee filter algorithm is employed and applied to the radiometrically calibrated VV band to mitigate this speckle noise. Additionally, terrain correction is performed to minimise the influence of terrain variations on the SAR values, improving the overall data quality.

Subsequently, the SAR image undergoes further processing using the Speckle Divergence Algorithm available in ESA's SNAP software, allowing for the extraction of the urban mask. This workflow can be applied in a pipeline at user-specified time intervals, enabling continuous updates to the mask and the detection of changes, whether in the form of urban growth or population displacement.

The contribution of Sentinel-1 to soil moisture estimation can be attributed to the backscatter effect, where the interaction between the soil and the electromagnetic pulse varies based on the soil moisture content. Different soil moisture levels absorb the pulse differently, providing valuable data. However, a reference dataset must first be created to accurately assess the soil's moisture percentage. This was done using the OpenEO API to generate a raster image of the Area of Interest (AOI), where each pixel represents the minimum backscatter value recorded over the course of one year. This approach ensures that each pixel reflects the driest condition of the soil within that year. By comparing this reference product with the user's downloaded Sentinel-1 GRD data from a specific revisit, it is possible to assess the percentage of moisture the soil has undergone.

The use of Sentinel-2 products for land cover estimation presents a challenge when attempting to monitor over different time intervals. Vegetation and other land cover types exhibit varying spectral identities at different times, making it difficult to determine accurate reflection values for vegetation cover from a single image. The Copernicus vegetation products, as discussed earlier, are often regarded as ground truth. While they may not be entirely accurate, they represent one of the best estimates of open-source data available for use as ground truth. However, these products are not provided at frequent intervals; instead, they are typically released on a yearly basis or at longer intervals, which limits their applicability for monitoring changes over shorter periods.

A model was developed to address this limitation using the Copernicus Access Hub's High-Resolution Layers as ground truth and Vegetation Indices as input data. As mentioned, vegetation and other entities have different spectral identities at various times, so collecting input data from different time points is crucial. The OpenEO API was utilised to gather mean values for the pixels within the Area of Interest over a two-year interval. This approach enables more representative spectral identities over time, accurately reflecting vegetation cover changes.

The mean value of each pixel within the Area of Interest was calculated for each vegetation index. Since many vegetation indices have different scales, normalisation was applied to bring them to a common scale, ensuring they can be effectively used as input data for the model. Rather than performing a random shuffle to separate training and test data, stratified sampling was used. This method splits the data based on its distribution by first converting the continuous predicted variable into categorical data, ensuring a more balanced representation in the training and test sets.

The XGBoost model was then employed for analysis, and evaluation metrics were calculated to assess its performance. This model can now be applied to any time interval the user wishes to assess vegetation cover in the Area of Interest, providing flexibility for monitoring and analysis over varying periods.

Due to the restrictions on military surveillance data and the licenses required for simulation software, simplified rules were applied to the units in the simulation. The first team of units prioritised approaching the target location by seeking concealment areas, while the second team focused on permeability capability. The Intersect tool in ArcGIS Pro was employed to determine the grid code for each unit's position relative to the concealment and permeability layers, as well as to calculate the distance from the target at each step. The extracted data was then exported to Excel, where one-hot encoding was applied to the categorical variables. The continuous variable, distance, was normalised, and the encoded values were scaled to match the same range as the continuous variable for consistency. A random forest model was then used to mimic the player's strategy to unseen data.

The Unity Engine was used to simulate the landscape and create a synthetic environment incorporating GIS data. A Unity simulation program, adapted from previous work, was employed to facilitate this process. The software reads landscape class data in raster format and, based on the class values, imports corresponding 3D graphics. These 3D graphics are derived from photogrammetric imagery, ensuring that the environment closely represents reality while also considering the hardware capabilities available for rendering the simulation.

Results and Challenges

To realistically replicate battlefield behaviour, the Digital Twin-based simulation must accurately represent terrain conditions. For this reason, models that rely on land cover data as ground truth should be assessed first. The XGBoost model, which predicts the High-Resolution Layer tree density, achieved an F1-score of 82%. However, it is important to note that the model was treated as a classification problem, as the continuous values of the dependent variable were subjected to one-hot encoding. Additionally, samples from different segments of the AOI need to be incorporated to enhance the model's generalisability to a broader scene.

The model used to mimic the human strategy achieved an accuracy of 88% for the first strategy based on permeability and 76% for the cover suitability strategy. Both strategies were relatively straightforward, as they were based on hypothetical examples due to the unavailability of military data. However, the cover suitability strategy presents some complications. These complications arise because factors such as distance, current, and next-step suitability cover alone are not the sole predictors of the strategy. Further spatial correlation approaches should be considered to explain the strategy accurately, as the player evaluates the environment based on intersecting suitability classes and those farther away.

The simulation of the terrain exhibited realistic traits, as many objects were created using photogrammetry techniques. However, more commercial tools should be considered for military simulations—tools that also offer military behaviour and planning functionalities. These tools would enable the visualisation of variations in hypothetical ongoing conflicts based on near-real-time information from the Digital Twin or data derived from „what-if" scenarios.

The permeability analysis, cover suitability and soil moisture lack ground truth and were provided here as a baseline demonstration. Data regarding vehicle permeability is challenging to obtain, as conditions such as speed and the likelihood of getting stuck must be assessed, which are difficult to reproduce in vitro. Following physical models—many of which assume ideal conditions or adhere to specific military regulations (though the exact term is unclear)—is necessary to create more refined products for military applications. Additionally, the backscatter effect alone is insufficient; integrating Sentinel-1 data with auxiliary datasets, such as those from the European Soil Database and OpenWeatherMap can be a valuable add-on. By correlating SAR-based soil moisture estimates with these additional data sources, a more accurate and comprehensive understanding of soil behaviour can be achieved, leading to more informed decision-making and improved operational planning.

Confronting Challenges

A framework for integrating data from various sources has been provided. Along with the advantages of the models based on the Copernicus High-Resolution Layers as ground truth data and the use of Unity for the Digital Twin-based simulation, some challenges must be confronted. Real battlefield behaviour data must be gathered or synthetically created based on real-world engagement rules. Simulation software will serve as a valuable addition to the development of this research. Case studies should be conducted to assess whether training done through simulations from a Digital Twin is more effective, as well as to evaluate data generation for machine learning training and determine how closely the simulation reflects the real world.

[1] Diego M. Botín-Sanabria et al., "Digital Twin Technology Challenges and Applications: A Comprehensive Review," Remote Sensing 14, no. 6 (2022): 1335, https://doi.org/10.3390/rs14061335.
[2] Kangyu Wu et al., "A Training Model of Wargaming Based on Imitation Learning and Deep Reinforcement Learning," Chinese Intelligent Systems Conference, Springer Nature Link, (2022): 786–795, https://doi.org/10.1007/978-981-19-6203-5_78.
[3] "Evelpis Project," Development of the Spatial Component for a Battlespace Digital Twin, Hellenic Army Academy, accessed March 08, 2025, https://geo.sse.gr/evelpis_project/.
[4] Sebastiano Trevisani et al., „Global Digital Elevation Models for Terrain Morphology Analysis in Mountain Environments: Insights on Copernicus GLO-30 and ALOS AW3D30 for a Large Alpine Area," Environmental Earth Sciences 82, no. 9 (2023): 198, https://doi.org/10.1007/s12665-023-10882-7.
[5] Chukwuma J. Okolie et al., „Assessment of the Global Copernicus, NASADEM, ASTER, and AW3D Digital Elevation Models in Central and Southern Africa," Geo-spatial Information Science 27, no. 4 (2024): 1362–90, https://doi.org/10.1080/10095020.2023.2296010.
[6] Shannon Franks and Rajagopalan Rengarajan, „Evaluation of Copernicus DEM and Comparison to the DEM Used for Landsat Collection-2 Processing," Remote Sensing 15, no. 10 (2023): 2509, https://doi.org/10.3390/rs15102509.
[7] Hrvoje Heštera and Mladen Pahernik, „Physical-geographic factors of terrain trafficability of military vehicles according to Western World methodologies," Hrvatski Geografski Glasnik/Croatian Geographical Bulletin 80(2), (2018): 5-31, https://doi.org/10.21861/HGG.2018.80.02.01.
[8] Rafał Wróżyński et al., „Reaching Beyond GIS for Comprehensive 3D Visibility Analysis," Landscape and Urban Planning 247, (2024): 105074, https://doi.org/10.1016/j.landurbplan.2024.105074.
[9] Nicole C. Inglis et al., „From Viewsheds to Viewscapes: Trends in Landscape Visibility and Visual Quality Research," Landscape and Urban Planning 224, (2022): 104424, https://doi.org/10.1016/j.landurbplan.2022.104424.
[10] Qianjiang Hu et al., „RangeLDM: Fast Realistic Lidar Point Cloud Generation," ECCV 2024, Springer Nature Link, (2024): 115-135, https://doi.org/10.1007/978-3-031-72784-9_7.
[11] Jian Song et al., „SynRS3D: A synthetic dataset for global 3D semantic understanding from monocular remote sensing imagery," arXiv preprint arXiv:2406.18151, (2024): https://doi.org/10.48550/arXiv.2406.18151.
[12] "About OpenStreetMap," OpenStreetMap, accessed March 06, 2025, https://www.openstreetmap.org/about.
[13] Alessandro Sarretta et al., „OpenStreetMap as an input source for producing governmental datasets: The case of the Italian Military Geographic Institute," The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences 48 (2023): 193-200, https://doi.org/10.5194/isprs-archives-XLVIII-4-W7-2023-193-2023.
[14] "Overview of Sentinel 1 Mission", S 1 Mission, accessed, March 06, 2025, https://sentiwiki.copernicus.eu/web/s1-mission.
[15] Abhinav Verma et al., „Built-up area mapping using Sentinel-1 SAR data." ISPRS Journal of Photogrammetry and Remote Sensing 203 (2023): 55-70, https://doi.org/10.1016/j.isprsjprs.2023.07.019.
[16] Nour Mahmoud et al., „A Proposed Methodology for Detecting the Urban Footprint in Egypt," IOP Conference Series: Earth and Environmental Science 992, no. 1 (2022): IOP Publishing, doi:10.1088/1755-1315/992/1/012008.
[17] Narayanarao Bhogapurapu et al., „Field-Scale Soil Moisture Estimation Using Sentinel-1 GRD SAR Data," Advances in Space Research 70, no. 12 (2022): 3845–58, https://doi.org/10.1016/j.asr.2022.03.019.
[18] A. M. Zeyliger et al., „Field F Test of the Surface Soil Moisture Mapping Using Sentinel-1 Radar Data," Science of the Total Environment 807 (2022): 151121, https://doi.org/10.1016/j.scitotenv.2021.151121.
[19] Jian Xue and Baohua Su, „Significant Remote Sensing Vegetation Indices: A Review of Developments and Applications," Journal of Sensors, no. 1 (2017): 1353691, https://doi.org/10.1155/2017/1353691.
[20] Lin Gao et al., „Remote Sensing Algorithms for Estimation of Fractional Vegetation Cover Using Pure Vegetation Index Values: A Review," ISPRS Journal of Photogrammetry and Remote Sensing 159 (2020): 364–77, https://doi.org/10.1016/j.isprsjprs.2019.11.018.
[21] "High-Resolution Layer – Tree Cover Density," Copernicus Land Monitoring Service, accessed March 06, 2025, https://land.copernicus.eu/en/products/high-resolution-layer-tree-cover-density.
[22] "High-Resolution Layer – Small Woody Features," Copernicus Land Monitoring Service, accessed March 06, 2025, https://land.copernicus.eu/en/products/high-resolution-layer-small-woody-features.
[23] "High-Resolution Layer – Grassland," Copernicus Land Monitoring Service, accessed March 06, 2025, https://land.copernicus.eu/en/products/high-resolution-layer-grassland.


71 %
54 %
80 %

05

ADDITIVE MANUFACTURING: A KEY ENABLER OF LOW-COST MODERN WARFARE

WOLFGANG MÜLLER, SERGEJ SUMLENNY

- **Authors:** Dr Wolfgang Müller is a Senior Resident Research Fellow at the German Institute for Defence and Strategic Studies; his research interests include Total Defence, China, and the Weaponisation of Economics.

  Dr Sergej Sumlenny is the Co-Founder and General Director of United Unmanned Systems LLC, a German-Ukrainian drone developer and producer; he is also the Managing Director of the European Resilience Initiative Centre.

  The views contained in this article are the authors' alone.

- **Abstract:** A need for low-cost warfare has emerged from the experiences of several nations in current conflicts. On the one hand, a recent missile and drone attack on Israel was successfully defeated, but at the unsustainable cost of an estimated $1-1.5 billion. Houthi drones, costing $2000 each, were successfully intercepted with Standard Missile-2s (SM-2), which cost $2 million each. On the other hand, the Russian Black Sea fleet was severely degraded by sea drones costing between $250 and $ 350,000 each. There are two consequences deriving from this: There is an urgent need for low-cost systems both in defence (to counter the Houthi-type attacks, for example) and offence (to engage in sea control or with combat drones as an artillery substitute).

- **Problem statement:** Based on the past and current experiences in drone warfare, what could be the potential of Additive Manufacturing in drone manufacturing?

- **Bottom-line-up-front:** Defence industry strategies must urgently incorporate cutting-edge production technologies like additive manufacturing to meet the demands of future large-scale, high-intensity combat operations, especially for.

- **So what?:** The potential of AM in the mass production of drones has yet to be realised. Before full potential can be reached, certain challenges need to be overcome. First of all, drones have to be introduced into strategic, operational, and tactical concepts to foster the development of a framework for use and, hence, more detailed production necessities.

The Importance of Unmanned Autonomous Systems in Future Warfare

Unmanned autonomous systems (UAS) have become critical to war, be it on land, in the air, or at sea. The roles assigned to these systems include reconnaissance and attack as well as support functions—for example, medical applications. Although there are divergent perspectives on their importance,[1] there is no doubt that the massive application of drones will be a part of it, regardless of whether they are decisive in future battles or not.[2] Compared to the use of drones in the conflicts in Libya and Nagorno-Karabakh,[3] the scale and range of drone uses and applications have increased tremendously: Ukraine alone produced 1.5 million First-Person-View (FPV) drones in 2024. It dedicated $1.2 billion in 2024 for drone procurement, with about $480 million for long-range drones, of which 30,000 should be produced in 2025.[4] For 2025, drone production contracts worth $3.58 billion with a slot number of around 1.8 million drones of various types have been issued.[5]

In addition to FPV, air, and sea systems, Ukraine is testing land-based walking drones with its 28th Mechanised Brigade in Toretsk[6] as well as a British model called "BAD One".[7] Other types of ground drones, wheeled or tracked, are also widely used, for example, by the 47th Mechanised Brigade in Kursk Oblast. They are used for multiple purposes: logistics, medical evacuation, laying mines, and mobile gun platforms.[8] In adapting UAS to these roles, the Ukrainian Armed Forces have elevated drones from a supporting role to a central operational asset; this shift is best displayed in the establishment of the Unmanned Systems Forces by presidential decree in 2024.[9]

Of all these systems, 96.2 % were produced in Ukraine by local industry.[10] Furthermore, the dependency rate of parts being delivered from abroad—especially from the People's Republic of China (PRC)—has been constantly reduced. This reduction is not only due to increasing Chinese export restrictions but also to an increasing lack of reliability, intentional or not.[11] Testament to this is the existence of a 100% Ukrainian-made drone.[12]

Ukraine's experience demonstrates that there can be no doubt that drones will play an important role in future warfare. It is also reasonable to assume that armed forces, which rely on expensive winged drones for reconnaissance, artillery and air strikes, will suffer significant losses against an adversary experienced in drone warfare. It is, therefore, paramount to have the capabilities and capacities to produce the numbers for extensive and long-lasting use of drones across multiple roles.

European states, which are not at war nor frontline states, have a certain luxury in preparing themselves not only to defend against but being able to wage that kind of warfare should it become a necessity. Unfortunately, in European states such as Germany, the focus in the past on defence procurement was on quality and technically very sophisticated systems instead of mass production. Today, Germany—and Europe—is unable to produce vast numbers of smaller UAS quickly.[13] Moreover, there is a necessary pre-condition that is also not met for mass production: Drones, as used in Ukraine, are only slowly becoming part of NATO operational concepts, doctrines, field manuals, and those of its members. Neither NATO nor its members have comparable experience with drones as Ukraine, where mass use is executed at all command levels—platoons, companies, battalions. Nevertheless, the importance of drones in future conflicts demands the capacity and capability to produce drones in vast numbers.

The German National Security and Defence Industry Strategy as a Starting Point

The importance of looking not only at technology and doctrines but also at production, both in terms of time and capacity, started in Germany with the "Strategy Paper of the Federal Government on Strengthening the Security and Defence Industry" in 2020: "To maintain control over technologies that have already been identified but will not be relevant for productive use on a large scale until some point in the future" is essential.[14] In light of the war in Ukraine, the newly introduced strategy of 2024 highlights the importance of a resilient, effective and sustainable defence industry: "To be able to draw on sufficient production capacities without delay, to increase economies of scale and enable innovations, we strive to achieve a continuous production of military equipment by the security and defence industry."[15] This strategy outlines the challenges and the must-dos regarding matters of production, both in terms of capacity and agility/flexibility.[16] Although this strategy highlights certain aspects of what is and will be of importance regarding manufacturing, the strategy itself offers no clear advice on how to achieve this.[17]

Unlike Ukraine, states like Germany have the luxury of being in a position where such drone innovations can be safely undertaken in a planned manner within a relatively reasonable time frame. Additionally, insights from the battlefield can be automatically incorporated into planning and production cycles; this applies to technology, procedures, and processes.

Current Developments in Drone Manufacture and Use

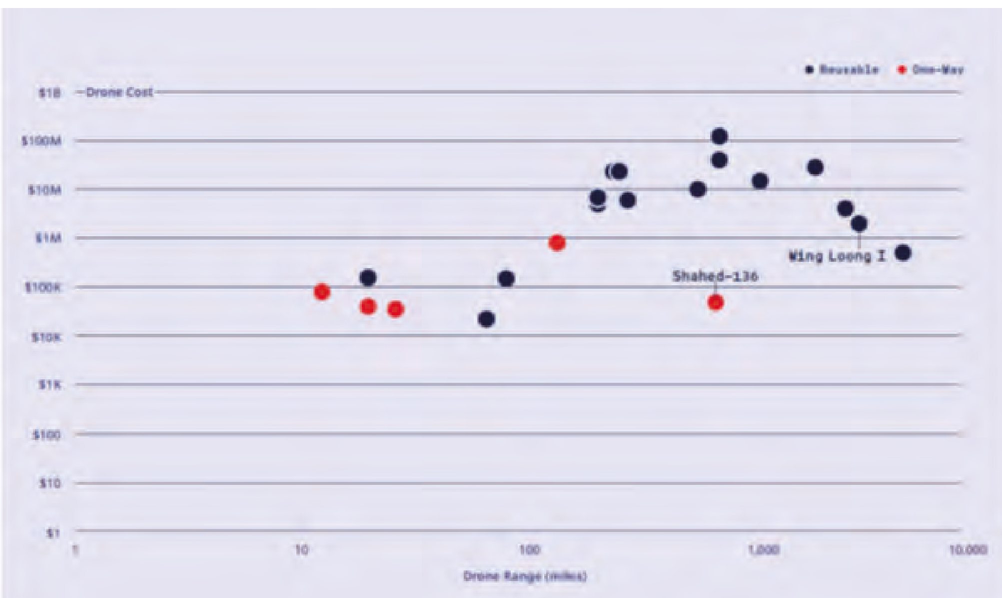
To identify how best to address the above-described challenge, defence planners need to take a deeper look at the current trends in drone manufacturing. These developments are, until today, not dependent on the outcome of our initial discussion if drones are a game-changer or not. More importantly, strategy outlines like the German one described above, operational concepts like "Hellscape",[18] and actual ongoing initiatives like the US "Replicator" initiative[19] or the local defence industry initiative "Brave1"[20] in Ukraine are relevant. All of these initiatives show that drones in multiple roles, in different domains and mass numbers will be an element to be considered in future warfare.

The developments in drone warfare connected to the production process, starting with Libya and Azerbaijan, and very dominant with current developments in Ukraine, can be summarised as follows:[21] Regarding the number of drones produced and used, it is increasing with no end in sight. At the same time, the use rate of one-time compared to multi-use drones is increasing as well. However, there is an increasing variability both with regard to their roles and the technical modifications. This experience corresponds to the perception of drones as low-cost ammunition instead of mere delivery/observer weapon systems. On the cost side, a degressive trend was visible for some time. However, it will most likely peak in the near future because of new features to be added (more stable connection, resilience to Electronic Warfare, night/thermal vision). The production of drones in wartime has changed, shifting from industrial to artisanal (ordinary garage or workshop solutions), often crowd-funded.[22] The parts for the drones are mostly available on the global market, and their purchase cannot be limited through export restrictions due to their common utility in various other non-military goods.[23] At the same time, there is a shift from off-the-shelf to tailor-made drones[24] designed for specific needs and tested on a trial-and-error basis (with regular and timely feedback loops established between the producing industry and the military).[25] The next step on its way is the use of Artificial Intelligence (AI), although still at a very early stage. Initial projects indicate the use of AI for target identification; this is particularly useful amidst camouflage and differentiating fake from real targets.[26] AI is also used in as well as marking and recognition in case of loss of connection to the pilot—most often on the last 200 m.[27] A newly developed model (HX-2) from the German start-up Helsing should be able to guide drone swarms.[28] Until now, AI has not been used for target selection/prioritisation, but this is likely forthcoming.

One final trend is notable: more and more separate drone-specific units are being established as units in their own right rather than being embedded within other military units. Additionally, the level of designation for separate drone units is coming down: drone companies can be found at least at the brigade level, but more and more at the battalion level as well.

The establishment of separate and independent drone units, combined with the down-levelling of their attachment, creates new necessities regarding supply chains and local workshop capacities for repairs and modifications. The same logic can be found in other developments, such as the Iranian ship the Martyr Bahman Bagheri. This is a container ship converted to use as a drone carrier, which can house up to 60 drones.[29] It is valid to assume that modification and repair facilities are installed directly on board.[30]

One of the most important aspects is the production costs, where the cost-per-unit matters for decision-makers, as extremely large charges are being discussed.[31] In cost-benefit analysis, the cost-effectiveness offered by drones cannot be denied. The war in Ukraine offers ample evidence of this, such as the sinking of the $65 million patrol ship Sergey Kotov by "Magura V5" drones, costing only $273,000 each.[32] This drone is also responsible for sinking up to 9 Russian ships in total.[33] On land, this cost-effectiveness was seen in the destruction of a $15 million Tor-M2 Radar Unit by a $500 Switchblade FPV.[34] A last example regarding planes was the destruction of a $100 million TU-22M3-hypersonic bomber by a drone.[35] However, mass production demands a cost-per-unit analysis. Looking at Ukraine again, in the beginning, Chinese off-the-shelf drones from DJI were used for reconnaissance purposes, costing from $1,500 to $5,400 (thermal night vision capable). They were used especially to direct artillery fire.[36] At the same time, longer-range drones are used for deep strikes, substituting for the lack of cruise missiles and airborne assets—the costs of those drones are much higher:[37]



Source: S. Pettyjohn/ H. Dennis/ M. Campbell, "Swarms over the Strait – Drone warfare in a future fight to defend Taiwan, Center for a New American Security," Policy Paper June 2024, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Indo-Pacific-Drones_DEFENSE_2024-final.pdf, 55.

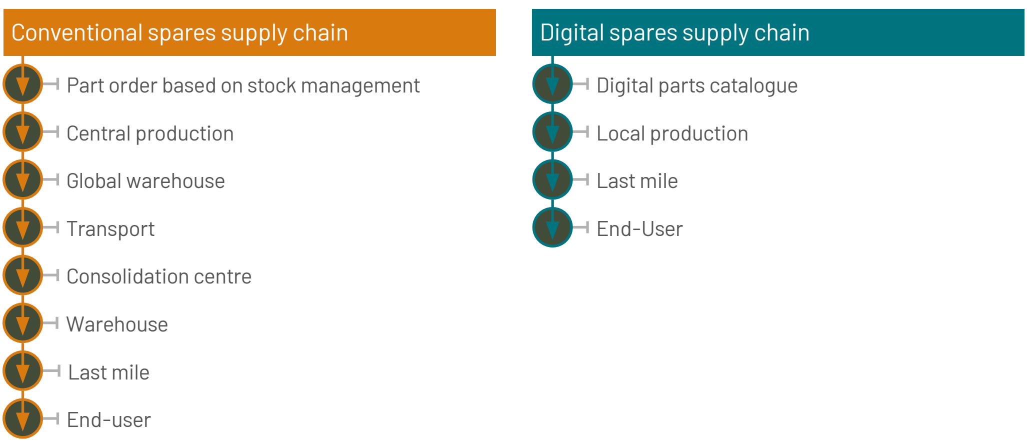
Later on, with the lack of sufficient amounts of artillery shells, FPV came up in vast numbers. Today, the 10-inch Vyriy-10 drone costs about $409. The newly developed prototype of a 100 % Ukrainian Vyriy drone costs $503.[38] The prices can be expected to go down, as with the other already existing models in mass production. The most inexpensive drones cost around $200-250.[39] Other models, for example, heavier drones used for dropping grenades and mortar bombs, range from $1,000 to $10,000.[40]

The basic model of the walking Cyber-Dog drone costs $1,600.[41] A new application is the use of a winged drone as a carrier for the FPV, which therefore increases their operating radius to 50-60 km instead of 25 km before. They serve at the same time as repeater drones for radio signals, which lessens the impact of hostile electronic warfare (EW); such drones can be bought commercially and cost around $8,000,[42] some of them even less (around $2,700).[43] The cost-effectiveness of these drones is very high, even considering efficiency. The cheapest drones have an efficiency rate of only 10-15%, and more advanced FPVs in the range of $300-400 achieve a 30% efficiency rate. Even if it needs 20-30 less expensive drones to destroy a target (be it a vehicle, a tank, fuel, etc.), it is often worth the investment (3-6 drones with a cost equivalent of $900-1,800 to guarantee a kill). In fact, more than two-thirds of Russian tanks have fallen victim to drones.[44] Even targeting individual soldiers (who are trained and equipped) is considered cost-effective, as they are much more difficult to replace compared to FPVs.

Further, as a pilot has about 40-50 minutes of flight time and knows that there is no chance of returning a $500 kamikaze drone once it is armed, the pilot will hit any target over $1000 or lose the drone. Moreover, the nearer it gets to the end of the in-flight battery capacity drained, the cheaper the price of the target gets. With only 1% of battery power left, anything will be hit to make sure the drone is not wasted: "Any enemy target more valuable than $1,000 identified by a drone pilot will be hit without hesitation, as this creates a favourable cost-benefit balance."[45]

Additive Manufacturing (AM) as a Potential Contribution

Additive manufacturing (AM)—popularly known as 3D printing—is the process of creating an object by building it one layer at a time. It is the opposite of subtractive manufacturing, in which an object is created by cutting away at a solid block of material until the final product is complete.[46] Logistically, there is a substantial difference between the supply chains of traditional and additive manufacturing:[47]



Source: T. Kruemberg, "Bringing significant rapid manufacturing capacity into the Armed Forces logistics chain," Presentation held at the 2nd European Military Additive Manufacturing Symposium, 17./18. October 2023, Bonn, 6.

The differences between these lead to several potential advantages: Firstly, there are potential savings in developing prototypes (estimates range to 85% time and 80% cost savings).[48] Second, savings are realised during the production process, be it in the production of prototypes or serial production, as weight reductions, as well as a customised and high mix/low volume production, can be realised. Additionally, there is higher flexibility through just-in-time production and small batch sizes and higher speed as fewer tools are needed, and on-demand production can take place. A higher degree of customisation, a higher degree of complexity, and even a higher rate of repeatability are possible as well.[49] Third, there are savings in the overall replacement costs.[50] This includes shipping and costs attached to the inventory level.[51]

Looking at AM for the purpose of addressing military needs, several trends are evident:[52] AM's potential is being looked into by several Armed Forces, and several pilot projects and evaluations have already taken place.[53] The U.S. has already adopted a fully-fledged strategic approach to the use of AM.[54] Several use cases have shown that mobile AM is possible, even in difficult environments typical for armed forces.[55] Although there are limitations on the accuracy due to transport and vibration resistance, plenty of parts can be produced within acceptable tolerances. There are examples of mobile factories in a 20-foot TEU with a production and a logistical support unit (e.g. scanner for reverse engineering), sometimes airborne capable (e.g. from Xerion on the ENOK AB).[56]

The German Armed Forces operate a modular concept consisting of the so-called eAFE (a light AM unit), AFE (AM unit), vAFE (moveable AM unit) and AFZ (AM centre).[57] Norway operates a similar concept.[58] Applications encompass expedient repairs, battle damage repairs, temporary replacements, and modifications, e.g. to realise modifications depending on the intended use of existing drone frames. That is why there are already 3D printers in the workshops of every drone unit.[59]

However, depending on the purpose for using AM, there are issues of legal relevance to consider because, typically, AM requires scanning the original part to create a CAD file [60] or transferring an existing CAD file from the original equipment manufacturer (OEM).[61] There is relevance regarding intellectual property rights, warranty situations, statutory warranty rights and common liability situations.[62] There might also be issues with export control regulations, as is the case, for example, with the U.S. International Traffic in Arms Regulations (ITAR).[63]

Nevertheless, AM has to be considered more strongly for procurements and tendering processes.[64] Common standards, which are aligned with industrial standards, are the basis for common recognition, which is the basis for mutual logistic support. Operational availability of assets has priority, which can lead to a conflict between OEM quality vs. functionality.[65] Performance-based, multisource contracts and the replacement of procurement documents with tryouts are being applied more often.[66]

Training necessities will likely arise to align current military AM operators with existing and developing standards as well as adapt them to the military context, quality management aspects (e.g. defect identification), and how to handle qualification, certification, and standardisation in critical scenarios.[67]

Furthermore, we contend that a new method of AM—AM electronics—should be integrated into AM practices. For example, the mesmeronic process chain, developed at the Fraunhofer Institut für Additive Produktionstechnologien, offers several advantages: Integrated conductor tracks which require fewer or no cables; embedded electronic components which reduce assembly efforts; a lightweight design which demands less material, and the possibilities of many varieties enabling rapid development.[68] With the use of carbon fibre reinforcements, a certain shielding against EW can also be achieved.[69]

The use of AI in production offers a range of potential applications through data-driven design based on genuine data, such as enhancing design and improving materials and processes.[70] In the manufacturing process, accuracy, speed, and simplicity should be increased. Hence, the scrap rate decreases, and tolerances are reduced for higher precision components.[71] Data-driven decisions will follow, e.g. machine settings pathway planning, post-processing precision[72] and quality control.[73] Ultimately, the cost per unit should be lowered through AI-driven decisions.

Research has confirmed that AM reduces costs and is economically sound. However, most applicable critical items are not produced by AM (e.g. microchips, cables, antennas).[74] In Ukraine, the role of AM in combat conditions is to produce fittings, modifications to drone structures, and casings for grenades with a high weight-damage ratio, as well as fins for homemade bombs.[75]

Source: Author.

A major AM production line based on the available 3D printers close to the front cannot work at present, as drones are generally not delivered to combat units without prior flight testing, which cannot be done at the front.

Aspects to be Considered for Decision-Making

Current drone designs show that most parts can be pre-produced or stored without the danger of obsolescence between production, storage, and potential use. These parts can be counted as the frame, the propellers, the motors, the battery, the antennas, the electronic speed controller, the flight control unit, the video transmitter/receiver, and the camera board. However, the GPS and radio control transceivers need constant updates.[76] The frame, if pre-produced, has to have the ability to mount different fittings, and the printed circuit board and flight stack have to have the ability to host different and adapted controllers.

Components are the main costs associated with setting up a traditional drone manufacturing business; these can account for 30-50% of total manufacturing costs.[77] Skilled labour is also necessary, and this can consume 20-25% of operational costs. The maintenance and repair of the machines and tools can run up to 5-10% of operational costs. Logistics and shipping add another 5-10%. Renting a facility can add another 10-15%. However, minor positions would be Research & Development, quality control, marketing, insurance, and other overheads.[78]

Of course, several more technical questions connected to traditional manufacturing as well as AM will be of importance: the lifetime of equipment, the assumed minimum shelf-life of materials, how weather and climate conditions influence the performance of equipment and materials, the mobility of the equipment and materials, the reliability of supply of equipment and materials, the maintenance intensity of equipment.[79]

Other areas are the manufacturing strategies (e.g. product design, manufacturing practice), supply chain and logistics planning (e.g. centralised/ decentralised production and distribution, lot sizing and inventory management), sustainability (materials, energy consumption) and the balance between depot- and field-level maintenance.[80]

Cutting-edge, Affordable, Ready

Historically, war has been a continuum of constant change, which drives technological innovation—this applies equally today. In the field of military production, the need for customisation, increased product functionality, and rapid prototyping, as well as full production chain competitiveness, must be quickly achieved. Consequently, production must be simplified, robust and deployable—or integrated into existing units, including ships and planes. The business model has to adapt to mass and customised production.

The maturation of AM has the potential to play a role in such a new manufacturing ecosystem. However, an AM-based manufacturing system or even a 'lights-out' factory-based model is neither feasible nor meaningful for drone production at present. As initially pointed out, outside of Ukraine, field manuals have not yet included the art of drone warfare; people are not trained, and drones are not introduced in large numbers. Yet, there is a massive production capacity as well as know-how in terms of technology, application possibilities, and active use in Ukraine.

Conceptually and doctrinally, introducing drones should go in parallel with a massive increase in the number of drones available to armed forces; this could be done by relying on production capacities in Ukraine. Systems can be ordered in Ukraine, where strong investments in the domestic defence industry by German companies already exist. Additionally, in modernising European drone forces, supply and training contracts for soldiers and systems are needed urgently. They can also be realised by transferring current knowledge from Ukraine to other European countries, such as Germany, where certain companies already have working relationships with their Ukrainian counterparts.

There are several advantages attached to this kind of procurement. First, there is a lack of regulation in the area of drone production, which allows the quick scaling of efficient and cost-sensitive production. One does not even need any license to start producing drones and sell them; it is enough to register a company without any other permission needed. Second, the necessary workforce can be hired with service contracts without permanent employment, which allows businesses to appear and develop without high risks. Third, there is a lack of bans on flight tests, which are necessary and part of the production process. Fourth, any drone produced is counted as civilian production as long as no ammunition is attached, which enables faster export. Fifth, there is a lack of IP restrictions in the production of drones—because of the war, drone designers are patenting their drones. Ammunition containers, small parts and even long-range drones are already manufactured through AM. However, this production method is not suitable for one-way attack drones.

In addition, there is a need to start ordering critical parts that cannot be produced by either Ukraine or Germany in order to create a strategic stockpile. Right now, the existing supply chain from the PRC, U.S., and Taiwan is intact and can be used. However, those supply chains cannot be taken for granted, so self-reliant production capacities for those parts must be developed. As the outcome of the war in Ukraine is also unpredictable, a production capacity for all parts of drone manufacturing must be developed domestically. These production capacities could and should integrate AM into the manufacturing ecosystem. In the case of the need for domestic drone manufacturing on a massive scale through AM, intensive relationships between producers using AM, materials suppliers, and OEMs have to be established. A materials ecosystem with an open materials license and a contractual agreement with the OEM to buy 'tokens'/ digital spare parts for printing or the digitalisation of existing components, including the re-certification of components, will be necessary to build up a digital inventory. In this respect, NATO has already achieved standard leadership.[81]

Furthermore, batches of experimental verification platforms in areas like key materials and major equipment need to be constructed. The provision of economically viable production capacities to such an extent, preferably with fixed quantities, can be achieved through the introduction of indefinite-delivery/indefinite-quantity contracts, whereunder partial orders can be placed and which compensate for idle capacity costs and serve as a kind of reserve capacity payments.

As a consequence, significant first-mover advantages could be realised while at the same time living up to the slogan "Cutting-edge, Affordable, Ready".[82]

[1] For example, even in Ukraine, there is a plethora of perspectives—General Valerii Zaluzhny, the former Ukrainian Commander-in-Chief, sees drones as a game changer. In contrast, the Ukrainian Head of Military Intelligence, General Kyrylo Budanov, does not see such a decisive importance of drones (V. Zaluzhny, "Ukraine's army chief: The design of war has changed," CNN, February 01 2024, https://edition.cnn.com/2024/02/01/opinions/ukraine-army-chief-war-strategy-russia-valerii-zaluzhnyi/index.html; New Voice, "Drones will not bring 'decisive advantage' to either Ukraine or Russia, says HUR chef," February 16 2024, https://english.nv.ua/nation/drones-have-been-in-full-use-by-both-sides-for-a-year-now-50393447.html; for a game changer see also: A.R. Hoehn/ T. Shanker, "Can cheap drones be the answer to tensions in the Taiwan Strait?," RAND Defense News Commentary, June 2023, https://www.rand.org/pubs/commentary/2023/06/can-cheap-drones-be-the-answer-to-tensions-in-the-taiwan.html and B. Perrett, "Small, cheap and numerous – A military revolution is upon us," The Strategist, January 22 2024, https://www.aspistrategist.org.au/small-cheap-and-numerous-a-military-revolution-is-upon-us/; for a non-game changer see also: R. Ruitenberg, "Small drones will soon lose combat advantage, French Army Chief says," Navy Strategy News, June 2024, https://www.defensenews.com/global/europe/2024/06/19/small-drones-will-soon-lose-combat-advantage-french-army-chief-says/; AFP, "Cheap drones cannot match artillery power in Ukraine," March 18, 2024, https://www.kyivpost.com/post/29670; U. Franke, "Drones in Ukraine – Four lessons for the West," European Council on Foreign Affairs Commentary, January 10 2025, https://ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west.
[2] Ukraine announced that it will develop its own drone warfare doctrine. (TCH, "Ukraine to launch military project 'Drone Line' — Zelenskyy," February 10 2025, https://tsn.ua/en/ato/ukraine-to-launch-military-project-drone-line-zelenskyy-2763612.html; China has launched its own drone program (G. Hondrada, "China leaks a blueprint for drone war dominance," February 07 2024, https://asiatimes.com/2024/02/china-leaks-a-blueprint-for-drone-war-dominance and is even using AI to develop its drone warfare doctrine (B. Drexel/ H. Kelley, "China is flirting with AI catastrophe," Foreign Affairs, May 30 2023, https://www.foreignaffairs.com/china/china-flirting-ai-catastrophe.
[3] R. Dixon, "Azerbaijan's drones owned the battlefield in Nagorno-Karabakh—and showed future of warfare," Washington Post, November 11 2020, https://www.washingtonpost.com/world/europe/nagornokarabkah-
drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html.
[4] Militarnyi, "The Ministry of Defence spent 50 billion UAH on the purchase of drones," November 09 2024, https://mil.in.ua/uk/news/minoborony-vytratylo-50-mlrd-grn-na-kupivlyu-droniv/.
[5] Ministry of Defence, "For 2024-2025, the Ministry of Defence, in collaboration with the Ministry of Digital Transformation, has already contracted 1,8 million drones totalling nearly UAH 147 billion," October 29 2024, https://mod.gov.ua/en/news/for-2024-2025-the-ministry-of-defense-in-collaboration-with-the-ministry-of-digital-transformation-has-already-contracted-1-8-million-drones-totaling-nearly-uah-147-billion.
[6] T-Online, "Ukraine hetzt Roboterhunde auf russische Stellungen," August 10 2024, https://www.t-online.de/nachrichten/ukraine/id_100465238/ukraine-setzt-roboterhunde-ein-chinesische-modelle-.html.
[7] N-TV, "Roboterhund soll russische Stellungen ausspionieren," August 8 2024, https://www.n-tv.de/politik/Roboterhund-soll-russische-Stellungen-ausspionieren-article25146586.html.
[8] See: J. Detsch, "Ukraine goes all-in on ground robots," Foreign Policy Report, July 17 2024, https://foreignpolicy.com/2024/07/17/ukraine-russia-war-ground-robots-combat/.
[9] M. Samus, "Drone centric warfare," International Centre for Defence and Security Brief, No. 7 2025, https://icds.ee/wp-content/uploads/dlm_uploads/2025/01/Layout-Samus.pdf.
[10] A. Fenbert, "Ukrainian drones made up over 96% of UAVs military used in 2024, defence minister says," December 28 2024, https://kyivindependent.com/ukrainian-drones-made-up-over-96-of-uavs-military-used-in-2024-defense-minister-says/.
[11] In Fall 2024, a shipment of Chinese propellers had a defect rate of 90%. (O. Yan, "No more 'Made in China': Ukraine inches closer to self-sufficient FPV drone manufacturing," Militarnyi, December 31 2024, https://mil.in.ua/en/articles/no-more-made-in-china-ukraine-inches-closer-to-self-sufficient-fpv-drone-manufacturing/).
[12] O. Yan, "No more 'Made in China': Ukraine inches closer to self-sufficient FPV drone manufacturing," Militarnyi, December 31 2024, https://mil.in.ua/en/articles/no-more-made-in-china-ukraine-inches-closer-to-self-sufficient-fpv-drone-manufacturing/.
[13] See for example: D. Blinski, "Die Bundeswehr muss sofort 100000 Drohnen anschaffen," December 28 2024, https://www.n-tv.de/politik/CSU-Verteidigungsexperte-Florian-Hahn-Die-Bundeswehr-muss-sofort-100-000-Drohnen-anschaffen-article25456033.html; G. Ismar, "Drohnen aus dem Baumarkt für die Bundeswehr", Süddeutsche Zeitung, July 12 2024, https://www.sueddeutsche.de/

politik/bundeswehr-drohnen-ausstattung-lux.TxcvAra7TQqupuv3sL12Bq.
[14] Bundesministerium für Verteidigung, Strategy Paper of the Federal Government on Strengthening the Security and Defence Industry, Berlin 2020, https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie-en.pdf?__blob=publicationFile&v=4.
[15] Bundesministerium für Verteidigung, National Security and Defence Industry Strategy, Berlin 2024, 4.
[16] "A security and defence industry capable of addressing any and all challenges must be dynamic and scalable to meet the requirements of the Bundeswehr in a rapid and reliable way, both in terms of quality and quantity. In addition, it must be sufficiently agile to allow for rapid and significant capacity increases for production and the provision of services, as well as for allies and close partners with shared values. It must be adaptable and sustainable at all times in the face of evolving security situations." (Bundesministerium für Verteidigung, National Security and Defence Industry Strategy, Berlin 2024, 5); see for further requirements (Bundesministerium für Verteidigung, National Security and Defence Industry Strategy, Berlin 2024, 5-8).
[17] See, for example: S. Weizenegger, "Defence technology and innovation in Germany," Atlantik-Brücke Report September 2024, https://www.atlantik-bruecke.org/defense-technology-and-innovation-in-germany/.
[18] C. Johnston, "Breaking down the U.S. Navy's Hellscape in detail," Naval News, June 16 2024, https://www.navalnews.com/naval-news/2024/06/breaking-down-the-u-s-navys-hellscape-in-detail/.
[19] U.S. Defence Innovation Unit: "Replicator", https://www.diu.mil/replicator.
[20] A. Fenbert, "Ukrainian drones made up over 96% of UAVs military used in 2024, defence minister says", December 28 2024, https://kyivindependent.com/ukrainian-drones-made-up-over-96-of-uavs-military-used-in-2024-defense-minister-says/.
[21] For an extensive description of the development in the Ukrainian Armed Forces see: S. Sumlenny, "The Russian-Ukrainian war: A new way of war and emerging trends," GIDSresearch No. 5 2024, https://gids-hamburg.de/wp-content/uploads/2024/12/GIDSresearch2024_05_Sumlenny_engl241209.pdf; see also: O. Molly, "Drones in modern warfare – Lessons learnt from the war in Ukraine," Australian Army Research Center Occasional Paper, No. 29 2024, https://researchcentre.army.gov.au/library/occasional-papers/drones-modern-warfare and S. Pettyjohn/ H. Dennis/ M. Campbell, "Swarms over the Strait – Drone warfare in a future fight to defend Taiwan," Center for a New American Security, Policy Paper June 2024, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Indo-Pacific-Drones_DEFENSE_2024-final.pdf.
[22] Although 3rd party direct funding to domestic production is more efficient and cheaper than donations from abroad.
[23] For example, the STM32F405 chip, which is used to make flight controllers, can be found in refrigerators and children's toys.
[24] Currently, the setup of an FPV drone changes significantly every 3 months. Drones produced today have almost zero similarities to those produced 12 months ago.
[25] W. Koch, "Innovation zahlt sich aus! – Zyklische Innovation und vernetztes Operieren," Behörden Spiegel, February 2025, 40.
[26] The Ukrainian Armed Forces is using the first AI-powered drone ('Saker Scout'), which autonomously detects targets and records their location. (Defence Express, "Ukraine forces get an AI AI-powered Saker scout drone and its algorithms can solve important problems," September 4 2023, https://en.defence-ua.com/weapon_and_tech/ukrainian_forces_get_an_ai_powered_saker_scout_drone_and_its_algorithms_can_solve_an_important_problem-7842.html.
[27] A. Rapp, "Die Saluschnyj-Doktrin – Lehren aus der ukrainischen Offensive 2023 und die Zukunft der Drohnenkriegsführung," GIDSstatement No. 9 2024, https://gids-hamburg.de/wp-content/uploads/2024/09/GIDSstatement2024_09_Rapp_240930.pdf, 8.
[28] L. Lange, "Ukraine-Krieg: Helsing revolutioniert Drohnenkrieg," Telepolis, December 13 2024, https://www.telepolis.de/features/Ukraine-Krieg-Helsing-revolutioniert-Drohnenkrieg-10198142.html.
[29] Jet-stealth-drones 'JAS-313' and propeller-driven-drones 'Qods Mohajer-6', 'Ababil-3N' and 'Homa'.
[30] T. Newdick, "Iran's bizarre 'Aircraft Carrier' seen in new detail," August 21 2024, https://www.twz.com/sea/irans-bizarre-aircraft-carrier-seen-in-new-detail; AP, "Iran inaugurates its first drone-carrier warship," February 6 2025, https://apnews.com/article/iran-drone-carrier-warship-c29e8460ebf2127afb99cf105b4027ba.
[31] See, for example: J. Grady, "Pentagon to industry: Build drones cheaper, faster: Cost per Unit matters," U.S. Naval Institute News, February 20 2024, https://news.usni.org/2024/02/20/pentagon-to-industry-build-drones-cheaper-faster-cost-per-unit-matters.
[32] See: The New Voice of Ukraine, "'Twin' of a ship involved in Zmiinyi Island assault – What is known

about Sergey Kotov patrol ship," March 5 2024, https://english.nv.ua/nation/info-on-one-of-russia-s-most-modern-warships-sergei-kotov-50398532.html.
[33] M. Fornusek, "Ukraine's Magura drones have reportedly struck 18 Russian ships throughout war," August 16 2024, https://kyivindependent.com/ukraines-magura-naval-drones/.
[34] V. Kushnikov, "Ukraine Armed Forces destroy Tor air defence system with a drone in the Zaporizhzhia region," December 5 2024, https://militarnyi.com/en/news/ukrainian-armed-forces-destroy-tor-air-defense-system-with-a-drone-in-the-zaporizhzhia-region/.
[35] D. Malyasov, "Ukrainian drone blow up Russian Tu-22M3 bomber," April 9 2025, https://defence-blog.com/ukrainian-drone-blow-up-russian-tu-22m3-bomber/.
[36] S. Sumlenny, "The Russian-Ukrainian war: A new way of war and emerging trends," GIDSresearch No. 5 2024, https://gids-hamburg.de/wp-content/uploads/2024/12/GIDSresearch2024_05_Sumlenny_engl241209.pdf, 5.
[37] S. Pettyjohn/ H. Dennis/ M. Campbell, "Swarms over the Strait – Drone warfare in a future fight to defend Taiwan," Center for a New American Security, Policy Paper June 2024, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Indo-Pacific-Drones_DEFENSE_2024-final.pdf, 55.
[38] O. Yan, "No more 'Made in China': Ukraine inches closer to self-sufficient FPV drone manufacturing," December 2024, https://militarnyi.com/en/articles/no-more-made-in-china-ukraine-inches-closer-to-self-sufficient-fpv-drone-manufacturing/.
[39] S. Sumlenny, "The Russian-Ukrainian war: A new way of war and emerging trends," GIDSresearch No. 5 2024, https://gids-hamburg.de/wp-content/uploads/2024/12/GIDSresearch2024_05_Sumlenny_engl241209.pdf, 10.
[40] S. Sumlenny, "The Russian-Ukrainian war: A new way of war and emerging trends," GIDSresearch No. 5 2024, https://gids-hamburg.de/wp-content/uploads/2024/12/GIDSresearch2024_05_Sumlenny_engl241209.pdf, 8.
[41] T-Online, "Ukraine hetzt Roboterhunde auf russische Stellungen," August 10 2024, https://www.t-online.de/nachrichten/ukraine/id_100465238/ukraine-setzt-roboterhunde-ein-chinesische-modelle-.html.
[42] S. Sumlenny, "The Russian-Ukrainian war: A new way of war and emerging trends," GIDSresearch No. 5 2024, https://gids-hamburg.de/wp-content/uploads/2024/12/GIDSresearch2024_05_Sumlenny_engl241209.pdf, 9.
[43] Prom Service, "FPV-Drone repeater 'Chupacabra'." https://vkf.com.ua/product/fpv-dron-retranslyator-13-chupakabra-z-akb-8s3p/.
[44] H. Waleed, "Cost-effective chaos: The strategic edge of low-cost drones and the future of military strategy," September 19 2019, https://defensetalks.com/2024/09/19/; The New Voice of Ukraine, "Ukrainian assault commander says 80 % of strikes rely on drones," November 2 2024, https://english.nv.ua/russian-war/ukrainian-assault-brigade-commander-highlights-drone-effectiveness-in-combat-50463368.html.
[45] S. Sumlenny, "The Russian-Ukrainian war: A new way of war and emerging trends," GIDSresearch No. 5 2024, https://gids-hamburg.de/wp-content/uploads/2024/12/GIDSresearch2024_05_Sumlenny_engl241209.pdf, 11.
[46] ASTM (American Society for Testing and Materials), "International: Standard terminology for AM technologies," F2792-12A.
[47] T. Kruemberg, "Bringing significant rapid manufacturing capacity into the Armed Forces logistics chain," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 6; for further analysis of the differences, see, for example: Wired Consulting/ Microsoft, "The military's next mission? – Reinvent logistics," https://custom-solutions.s3.amazonaws.com/WIREDConsultingxMicrosoft_TheMilitary'sNext%20Mission.pdf; B. Straight, "Soldiers win battles, logistics wins wars," Freight Waves, March 4 2022, https://www.freightwaves.com/news/soldiers-win-battles-logistics-wins-wars; RAISE3D, "Military 3D printing – How is AM changing the defence industry," January 25 2025, https://www.raise3d.com/blog/military-defense-3d-printing/.
[48] A. Langfeld, "Gaining an edge in military/defence with AM," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 7; 9.
[49] M. May, "Productivity and quality: Automation and machine learning as enablers for industrial AM," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 4-5.
[50] The Polish Armed Forces realised through AM parts for battle tanks replacements – instead on relying on new parts – between 60-75% cost-savings. (M. Wincewicz-Bosy/ K. Kowalski/ G. Stankiewicz, "Conditions for the functioning of logistics support in the Polish Armed Forces of the implementation of AM technology," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 7).
[51] In a case study with the Dutch Armed Forces deployed in Mali, average cost savings – compared to regular shipments – were 47%, savings per part range from 20 to 61% and the inventory level was

reduced by 72% on average, when considering only raw materials, inventory levels were still reduced by 66%. (R. Basten, "Printing spare parts at remote locations," Presentation held at the 1st European Military Additive Manufacturing Symposium, October 12./ 13. 2021, Bonn, 14).
[52] See, for example: L. Holmes Jr., "Additive technology revolutionises defence manufacturing," National Defence Viewpoint, July 6 2023, https://www.nationaldefensemagazine.org/articles/2023/7/6/additive-technology-revolutionizes-defense-manufacturing; H. Colorado etal., "AM in armor and military applications: Research, materials, processing technologies, perspectives and challenges," Journal of Materials Research and Technology, No. 27 2023, 3900-3913; K. Stevenson, "Can the military really use 3D printing?," https://www.fabbaloo.com/news/can-the-military-really-use-3d-printing.
[53] For cases of countries using AM in the military, see for example: M. Prior, "How is AM being adopted in defense," March 10 2025, https://www.3dnatives.com/en/how-is-additive-manufacturing-being-adopted-in-defense-100320254/#!; European Defense Agency, "EDA pioneers European defense workshop exploring AM," https://eda.europa.eu/news-and-events/spotlight/spotlight-of-the-month/3d-printing-eda-pioneers-european-defence-workshop-exploring-additive-manufacturing; for a more detailed example see: Bundesamt für Informationstechnik, Ausrüstung und Nutzung der Bundeswehr, "3D-Druck in der Bundeswehr zur Optimierung der Versorgung mit kritischen Ersatzteilen," Abschlussbericht, June 2022.
[54] See, for example: U.S. Department of Defence, "AM strategy," Washington D.C. 2021, https://www.cto.mil/wp-content/uploads/2021/01/dod-additive-manufacturing-strategy.pdf.
[55] See, for example: in-flight AM (Naval Postgraduate School, "CAMRE helps Marines take 3D printing to new heights," July 5 2023, https://nps.edu/-/camre-helps-marines-take-3d-printing-to-new-heights), AM on ships (Trends der Zukunft, "Fregatte 'Sachsen': Die deutsche Marine testet den Einsatz von 3D-Druckern auf See," August 2 2022, https://www.trendsderzukunft.de/fregatte-sachsen-die-deutsche-marine-testet-den-einsatz-von-3d-druckern-auf-see/), even on submarines (AML3D, "AML3D supports AUKUS supply chain with Virgina-Class components," https://aml3d.com/aml3d-supports-aukus-with-virginia-submarine-component) and for ground forces as well (Bundesministerium der Finanzen Österreich, "2Army – Automated Additive Repair and Manufacturing System," 2019, https://www.forte-bmf.at/gefoerderte-projekte/detail/2army/; J. Judson, "Still in service: 'Ex Lab' is the US Army's problem-solving MacGyver," Defense News, October 14 2019, https://www.defensenews.com/digital-show-dailies/ausa/2019/10/14/still-in-service-ex-lab-is-the-us-armys-problem-solving-macgyver/.
[56] M. Ortloff, "Concept for integration of metal FFF to support temporary self-sufficient operation of defence units," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn.
[57] AFE: Additive Fertigungseinrichtung; AFC: Additives Fertigungscenter (see: F. Zimmer, "AM in the German Armed Forces," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./18. 2023, Bonn, 5).
[58] C. Norberg, "Enabling technologies to provide OEM-verified spare parts in the field," Presentation held at the 1st European Military Additive Manufacturing Symposium, October 12./ 13. 2021.
[59] S. Sumlenny, "The Russian-Ukrainian war: A new way of war and emerging trends," GIDSresearch No. 5 2024, https://gids-hamburg.de/wp-content/uploads/2024/12/GIDSresearch2024_05_Sumlenny_engl241209.pdf, 7.
[60] Computer-Aided Design.
[61] Original Equipment Manufacturer.
[62] T. Urband, "Intellectual property rights, liability, warranty & how to solve them," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 3-6; see also: S. Rautio/ T. Tuomi/ J. Akmal, "Legal aspects of AM in the military logistics," Security Dimensions, No. 40 2022, 154-195.
[63] See, for example: M. Heesing, "Export control challenges related to AM," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn.
[64] In the U.S. Department of Defence's AM strategy, there is a call to "develop and share new business models for AM in contracting and acquisition". (U.S. Department of Defence, "AM strategy," Washington D.C. 2021, https://www.cto.mil/wp-content/uploads/2021/01/dod-additive-manufacturing-strategy.pdf, 9).
[65] M. Huber, "AM – A military capability enabler/ European Defense Agency perspective," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 12; see also: B. Müller et al., "NATO-Codification System review of AM," Legal Study Report, August 2022.
[66] A. Rode, "Introducing AM to the German Armed Forces," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 16.
[67] A. Ade, "Developing skills for the European Defence Sector – Education and training in AM," Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023,

Bonn, 5.
[68] F. Proes, “AM electronics – More functionality at shorter lead time,” Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 5.
[69] See, for example: X. Luo/ D. Chung, “Electromagnetic interference shielding using continuous carbon fibre, carbon matrix and polymer matrix composites,” Composites, No. 3 1999, 227-231.
[70] S. Rudge, “Pioneering Advanced Manufacturing in defense technology,” Manufacturing Today, April 2024, https://manufacturing-today.com/news/pioneering-advanced-manufacturing-in-defense-technology/; K. Hoschke et al., “Generative and future AI-aided design of functionally graded materials for protection and effectors,” Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 2.
[71] A. Gagani, “Secure AI software for the industrialisation of AM in the defence sector,” Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 2; 8.
[72] See, for example: AM-FLOW, “The future of 3D printing lies in automated post-processing: Here’s why,” https://am-flow.com/the-future-of-3d-printing-lies-in-automated-post-processing-heres-why/.
[73] M. May, “Productivity and quality: Automation and machine learning as enablers for industrial AM,” Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 41.
[74] See for example: M. Meyer/ A. Glas/ M. Eßig, “Wirtschaftlichkeitsanalyse additiver Fertigung als digitales Ersatzteillager,“ Universität der Bundeswehr München Arbeitsgebiet Beschaffung, Arbeitspapier, No. 26 2022, https://www.unibw.de/beschaffung/arbeitspapier-26-wirtschaftlichkeitsanalyse-additiver-fertigung-als-digitales-ersatzteillager.pdf and L. Kayser, “The economics of AM are broken – here’s how to fix it,“ TCT Magazine, May 29 2024, https://www.tctmagazine.com/additive-manufacturing-3d-printing-industry-insights/latest-additive-manufacturing-3d-printing-industry-insights/the-economics-of-additive-manufacturing-don-t-work/.
[75] Idem.
[76] Although there are new developments to use fibre-optic wire spools to counter Electronic Warfare measures, the majority of the drones will continue to be steered through radio-signals. (D. Trubetskoy, “Glasfaser – der Drohnenkrieg nimmt die nächste Stufe,“ N-TV, February 21 2025, https://www.n-tv.de/politik/Glasfaser-der-Drohnenkrieg-nimmt-die-naechste-Stufe-article25578795.html.
[77] Of those, the costs for the battery are of major importance as they make up about 20 % of the price. Currently, accumulators are also being used in one-way drones. Developing single-use batteries would reduce costs significantly. Another part for major cost savings is the thermal camera – a cheap one could help to reduce costs further. Finally, the flight controllers’ price could lower overall costs in production if they are mass-produced for use in one-way drones.
[78] Business Plans Team, “What are the major operating expenses for drone manufacturers?,” September 30 2024, https://businessplan-templates.com/blogs/running-costs/drone-manufacturing.
[79] M. Wincewicz-Bosy/ K. Kowalski/ G. Stankiewicz, “Conditions for the functioning of logistics support in the Polish Armed Forces of the implementation of AM technology,” Presentation held at the 2nd European Military Additive Manufacturing Symposium, October 17./ 18. 2023, Bonn, 6.
[80] See: I. Valtonen/ S. Rautio/ M. Salmi, “Capability development in hybrid organisations – Enhancing military logistics with AM,” Progress in Additive Manufacturing, No. 7 2022, 1037-1052 and S. Rautio/ I. Valtonen, “Supporting military maintenance and repair with AM,” Journal of Military Studies, No. 1 2022, 1-14.
[81] Through the NATO Digital Library for AM (codename: RAPiD-e) of the NATO Support and Procurement Agency.
[82] PricewaterhouseCoopers, “Cutting-edge, affordable, ready – A vision for Europe’s defence industrial future,” PWC Strategy& Study, 2025, https://securityconference.org/assets/Strategy__A_vision_for_Europe%E2%80%99s_defense_industrial_future_web.pdf.


WORLD SEARCHING OPERATION ON 07-07-20770
DATA MINING
ZONE:A

06

AI IN THE LINE OF FIRE: RETHINKING ETHICS IN THE FACE OF NUCLEAR THREATS

JILL LONG, TAMSYN KARLOTTA GARINET, SEVERIN PLEYER

▶ **Author:** Jill Long, Colonel, U.S. Air Force, retired (OF-5); PhD Political Science and Government, Senior Professor; Norwich University, Strategic Leadership; MA Military Strategic Studies, MS Management, Director of the Democratic Resilience Center at the Helmut-Schmidt-University (HSU), Senior Professor Master of Strategic Leadership Norwich University;

Tamsyn Karlotta Garinet; Captain (OF-2) Bundeswehr; Ecological Security Fellow 2024 at the Council on Strategic Risks (CSR), M.Sc. Psychology; Research Topics: Civil-Military Cooperation; Ecological Security; Social, Differential & Media Psychology; Leadership.

Severin Pleyer, Captain (Bundeswehr), Doctoral Research Associate on 21st Century Nuclear Deterrence at HSU. The views contained in this article are the authors' alone and do not represent the views of the US Air Force, the Bundeswehr, the Helmut-Schmidt-University or Norwich University.

▶ **Abstract:** Decision-making regarding target engagement, including considerations for scenarios involving the tactical use of nuclear weapons, requires a multilayered, well-structured, predictable, and traceable approach. The integration of AI into such high-stakes scenarios amplifies the need for transparency, aligning decision-making models to trusted tenets and focused training (the 3Ts) in order to avoid the five cognitive pitfalls of overreliance, information overload, groupthink, misperception, and unrecognised systemic bias. For AI to be effectively integrated into Nuclear Command, Control and Communication (NC3) networks, decision makers delegated target engagement authority must have a clear understanding of the capabilities and limitations of the AI system, just as they understand the capabilities and limitations of their other team members. AI is not something to be feared, but it should be approached with a degree of healthy scepticism. The 3T framework provides a useful heuristic for ensuring proper integration and use of AI-enabled NC3 systems and decision-making processes.

- **Problem statement:** Decision-making and moral decision-making in the Age of AI—The case for reevaluating the moral paradox in targeting, specifically considering adversarial tactical nuclear weapon use.

- **Bottom-line-up-front:** The use of AI in nuclear command and control systems demands transparency, alignment with trusted tenets and focused training (the 3Ts) to ensure decision makers exercise appropriate human control–especially in decisions regarding employment of tactical nuclear weapons.

- **So what?:** When considering the future of AI-supported targeting, a greater emphasis on improving transparency, trust in the values upon which the systems are based, and focused training for decision makers is necessary. Simply transferring conventional decision-support AI agents into the nuclear command, control, and communication systems is insufficient and induces unacceptable risk. This is especially true in scenarios where adversarial tactical nuclear weapon use challenges existing ethical and operational frameworks.

Seconds to Decide

The Situation Room buzzed with hushed urgency. On the wall, digital maps pulsed with data feeds: satellite surveillance, adversary force postures, and real-time sentiment analysis from global media. A crimson alert flashed: "Strategic Forces Elevated – Opponent Level 3 Readiness."

The President sat stone-faced, flanked by her national security team. At the opposite end of the table sat 'Prometheus,' the nation's AI-powered strategic decision-support interface. A fourth-wave AI, Prometheus was designed to outthink human adversaries—processing millions of variables from wargames, historical precedents, and behavioural models.

"We need options," the President said tersely.

Prometheus responded in a dispassionately neutral synthetic voice, "Recommended Course: Execute a subsurface demonstration strike with a tactical nuclear weapon. 73.7% projected deterrence effectiveness. Escalation risk: 14.2%. Civilian loss: zero. Signal strength: decisive."

The room fell silent.

The Minister of Defence furrowed his brow. "Madame President, this aligns with our limited escalation doctrine—but it's a line we've never crossed."

The Intelligence Director interjected. "Prometheus projects adversary response matrices with a higher resolution than any human team. The signal might prevent full-scale war."

"But Prometheus doesn't feel," the Minister replied, voice taut. "It doesn't weigh the moral inertia of its advice."

The AI responded instantly. "Emotion introduces noise. Optimal decisions emerge from data clarity."

The President stood and walked to the screen, watching the projection of the strike's shockwave bloom across oceanic gridlines. The AI had no skin in the game—no blood to spill, no history to answer to. And yet, its logic was impeccable.

She turned back to her staff. "We built Prometheus to stop us from stumbling into the abyss. But when the abyss stares back, who blinks—the machine or the human?"

Silence.

A decision had to be made. And in that moment, humanity hovered between the algorithm's whisper—and potential annihilation.[56]

Why This Scenario Matters

This is not science fiction. The detonation of a tactical nuclear weapon is no longer a distant Cold War nightmare. Instead, it is plausible in an era where decision-making is shaped by artificial intelligence (AI). National security decision-making processes and nuclear strategy in particular are leveraging AI's ability to process vast amounts of intelligence, predict adversary behaviour, and inform recommendations for strategic response. AI's capacity for rapid analysis could, in theory, prevent rash human error or miscalculation, yet its use in high-stakes military decisions raises profound ethical concerns. Historical close calls–the 1979 NORAD false alarm, the 1983 Soviet misidentification, and the 1995 Norwegian rocket incident[1]–underscore the irreplaceable role of human judgment in averting catastrophe. Had AI governed these moments; outcomes might have been tragically different.

The philosophical difficulty associated with embedding advanced AI into lethally autonomous systems, the so-called 'responsibility gap' or 'non-gap,'[2] makes clear the criticality of preserving human agency, moral judgment, and strategic accountability. We argue that the natural progression of AI development requires those endowed with target engagement authority–particularly when associated with nuclear weapons, and tactical device use–must employ safeguards which ensure that humans remain accountable as the ultimate decision-makers, especially for morally and politically significant actions. These safeguards are codified as the 'Three Ts' (3Ts) transparency, trusted tenets, and training.

The insidious rise of AI integration and capability may mask the cognitive pitfalls of overreliance, information overload, groupthink, misperception, and unrecognised systemic bias.[3] On the one hand, AI offers speed, scale, and systemic foresight through probabilistic computations; on the other, it risks amplifying brittle logic divorced from moral and political nuance. In this paper, we explore why this scenario is not only possible but increasingly probable and underscores the need for deliberate human control, underpinned by the 3Ts.

The Evolution of AI: The Four Waves

To fully understand AI's role in military decision-making, examining its evolution through four developmental waves is essential. The first wave, which dominated in the 1980s to 1990s, is often referred to as rule-based AI. First wave systems rely on predefined rules and structured logic to execute tasks. These systems are rigid, lack adaptability, and are best suited for structured decision-making processes such as logistics and battlefield planning employing deterministic logic trees. The contribution of such systems to decision-making is easily deconstructed. Familiar examples of first-wave AI are recommendation engines such as those employed by Amazon, Netflix, and YouTube. In the military context, it could be found in route guidance systems and logistical support systems.

The second wave introduces statistical learning, where AI models use large datasets to make probabilistic decisions. In civilian terms, these systems are found in decisions-making within banking, insurance, and financial markets–where algorithms enhanced human predictive modelling by correlating weak variables to form better outcome predictions. In military terms, second wave systems included similar clustering, classification, and predictive modelling, which became critical in early cybersecurity applications and automated intelligence analyses.

First and second wave AI provided transparency in design, explainability in the decision-making models, and predictability in the outcomes. These iterations of AI also built a foundation of familiarity and trust with target engagement authorities—the human in the loop. It is when AI starts to construct its own decision-making models, such as through machine-to-machine learning, that transparency and doubt come into play.

Third and fourth wave AI represent the new frontier in AI-enabled decision-making processes and should foster scepticism in the trust and confidence that target engagement authorities place in outcomes. Third wave, known as contextual adaptation AI, enables machines to perceive and adapt to their environment rather than relying on static rules or historical data.[4] Facial recognition authentication, smart home systems, Alexa and Siri are common representations of third-wave AI. From a military perspective, long-loiter weapons, such as Harpy and Harpoon, exemplify third-wave characteristics, with the ability to linger in contested airspace, adapt to shifting radar emission patterns, and dynamically select targets. These systems can reason, recognise patterns, and make independent assessments, making them highly relevant in battlefield analysis and autonomous targeting, such as targeting associated with Lethal Autonomous Weapons (LAWs).[5] Third wave AI 'agents' become team members who inform our decision-making processes and, in some cases, these agents are delegated decision-making authority. On the cusp of the third and fourth wave of AI is Project Maven, the US AI intelligence system capable of fusing satellite imagery, geolocation data, and communication intercepts for target identification.[6]

The fourth wave–general artificial intelligence or autonomous AI–integrates ethical reasoning, legal frameworks, and synthetic common sense into AI decision-making[7] and is worthy of debate. The goal is to develop AI which not only perceives the environment but also responds appropriately to that environment by applying human-like moral judgement. This next frontier of AI development is intended to create systems that incorporate human-like moral judgment into automated and/or autonomous decisions, a crucial factor in nuclear deterrence and command-and-control frameworks.[8] In a practical sense, the nascent development of fourth wave AI is evident in self-driving vehicles that can "see" the environment, recognise patterns, correlate those patterns to a decision framework, make a decision and act upon that decision. While these innovations are highly localised, meaning a self-driving car cannot transfer the 'knowledge' to other contexts, the objective is to create systems that can transfer knowledge gained from one context to another.[9]

As AI transitions through these waves, it moves from simple rule-following systems to highly autonomous decision-making entities, at each level increasing its influence over military strategy and decision-making, and ultimately those who hold target engagement authority. While current systems utilise large language models (LLMs), natural language processing (NLP), and computer vision algorithms enabling rapid analysis of intelligence reports, open-source intelligence, and sensor data, for "shortening the kill chain,"[10] accepting the outputs of these systems as factual elements to the decision-making process is not without risk. At the operational level, these risks centre on trust and reliability, data integrity, and interpretation. When focused at the strategic level, which is arguably the domain of any nuclear weapon employment (including tactical), risk centres on threshold identification, escalation management, proliferation, and stability.[11] These capabilities (and risks) are expected to accelerate as nuclear weapons states—such as the US, China and Russia—pursue AI as a strategic priority and develop AI capabilities in support of human decision-making.[12]

A Scenario Anchored in Reality

Once the domain of Cold War science fiction, AI-enabled platforms like the hypothetical "Prometheus" are now emerging as real actors in national security deliberations. As AI systems grow in sophistication, their integration into target engagement and nuclear command, control, and communication (NC3) infrastructures[13] raises urgent questions about moral authority, strategic accountability, and the thresholds of automation in one of the gravest decisions a state can make–whether to employ nuclear weapons. Conventional targeting cycles already engage AI in defence planning, threat detection, target identification, and streamlining response options. Scholars, such as Drexel,[14] emphasise the accelerating integration of AI in defence ecosystems, including nuclear contexts, as part of broader great power competition. From a nuclear perspective, Johnson[15] highlights that AI use is creating new escalation pathways, while 'exacerbating old' pathways, increasing the risk of accidental nuclear confrontation. The adoption of such systems into target engagement decisions and NC3 frameworks should not come without significant scrutiny. Scrutiny begins with transparency.

Transparency in Strategic AI

Transparency in AI systems refers to the degree to which the internal logic, rationale, and operational mechanics of an AI's recommendations are understandable, traceable, and reviewable by human actors. As the stakes rise to existential levels, such as in nuclear command and control and nuclear weapons engagement, calls for transparency become not only a technical demand but an ethical imperative. These ethical challenges extend beyond legal compliance to fundamental questions of accountability, proportionality, and adaptability. If an AI-driven system recommends escalation based on probabilistic assessments, who bears responsibility for the consequences? How can AI be designed to incorporate strategic adaptability when military conflicts unpredictably evolve? Will the use of AI be stabilising or destabilising to the strategic context? How can intentional irrationality be accounted for in escalation dynamics?[16] To address these concerns, we argue that AI augmentation of targeting decisions, particularly in nuclear weapons employment, requires transparent decision-making models.

Transparent AI frameworks improve post hoc analysis and mitigate the responsibility gap. As Clausewitz teaches us, war is an extension of politics, and transparency is foundational to civilian political oversight, which is a cornerstone of democratic governance. When AI systems recommend or execute potentially catastrophic actions, such as tactical nuclear strikes, public institutions must retain visibility into how those decisions are made. Opaque AI systems risk undermining trust and, therefore, legitimacy. Transparency also improves decision making by permitting scrutiny of not just outputs but the assumptions, models and biases that led to them. Ultimately, transparency is a safeguard against misperception and unrecognised systemic biases—two of the five cognitive pitfalls. Transparency has an added bonus in facilitating recognition of adversarial manipulation and/or model 'drift.'[17]

Trusted Tenets: Embedding Democratic Values into AI Decision Frameworks for Strategic and Nuclear Decision-Making

Trusted Tenets refers to the values or ethical principles that any AI-enabled decision-making system must be grounded in—particularly those influencing lethal action, such as a tactical nuclear strike; democratic values such as civilian control, proportionality, human dignity, and moral deliberation. AI currently cannot, and must not, replace values-based judgment when lives, legitimacy, and civilisation itself are at risk.

AI operates on logic, but war is human. Like humans, AI models rely on past data and strategic assumptions; however, it is incapable of considering less predictable and less structured political and moral nuances. In theory, this shortfall can be mitigated by the application of law, which reflects societal values, but as we see in human interaction, law falls short of predicting (and sometimes informing) human cognitive processes. This is not to say laws are an unimportant framing factor. Civilian control is often framed by international law, including treaties such as the Geneva Conventions, providing a foundational framework for regulating armed conflict.

There is another shortfall with relying on law as a stand-in for human value systems. Current laws of forces employment struggle to fully address emerging threats such as AI-driven tactical nuclear weapon escalation. In this context, the traditional legal frameworks—predicated on established international values and norms, and state-centric responsibility—fail to duplicate human decision-making, particularly in the realm of deterrence. Decisions to escalate or deescalate are less predictable and may embrace many interpretations of that law—sometimes by the same actor. To further complicate the application of law as the primary trusted tenet, opaque AI-driven systems create additional complexities related to autonomy, accountability, and rapid escalation dynamics.[18]

The Responsibility Gap

All of these issues coalesce to form the „responsibility gap." In traditional military hierarchies, accountability for any targeting decision is clearly assigned to human commanders and incorporates rigorous checks and balances; when AI assists in these decisions, questions surrounding the subject of responsibility arise. Should responsibility lie with the military operator? The developers of the AI model? Or is there a scenario where responsibility should fall upon the AI system itself?[19] And upon which values was the model based, especially as models build upon one another to form more capable systems? These issues are particularly pressing in scenarios where AI-generated recommendations might lead to undesired escalation. As in our Prometheus example, should military leaders act on that assessment if an AI model assigns a 70% probability to an adversary launching a second nuclear strike? What happens when the remaining 30% chance of de-escalation is ignored?

In summary, AI decision-making is built on logic-driven frameworks that fail to account for war's complex, human aspects. First and second wave AI models primarily rely on historical data and predefined parameters,[20] making the output understandable and predictable; however, such outputs may be vulnerable to oversimplification when applied to complex strategic calculations. Even with transparent design, third and fourth wave AI, and associated machine-to-machine learning, can lead to a complex web of value convergence, raising questions of which values are in play.[21] While the Geneva Conventions and other legal frameworks provide guidelines for military conduct, they do not fully address AI's role in targeting decisions; nor nuclear engagement in particular, where escalation dynamics can unfold at unprecedented speeds. To prevent misjudgements that could lead to nuclear conflict, AI systems must be designed to incorporate reasoning beyond simple probabilities and account for definable human ethical frameworks–they must include transparent and well-understood trusted tenets exercised through rigorous training protocols.

Training: Strengthening Human-AI Collaboration

Strengthening human-AI collaboration is essential to ensuring commanders remain in control while leveraging AI's analytical capabilities and avoiding the five pitfalls: overreliance, information overload, groupthink, misperception, and unrecognized systemic bias.[22] One of the most critical steps in this process is the implementation of training programs specifically designed to prepare decision-makers for AI-assisted strategic assessments. This training relies on the fundamentals of transparency and trusted tenets, clearly codified ethical and decision-making models upon which the system is designed. Commanders must develop the skills to critically evaluate AI-generated recommendations, recognizing their utility and limitations.[23] Without adequate comprehension, there is a risk that military leaders may over-rely on AI-generated intelligence or disregard valuable insights due to misinterpretation. Effective training should include scenario-based exercises where decision-makers engage with AI-driven simulations, enhancing their ability to interpret, challenge, and refine both personal decision-making models and AI outputs in real-time.[24]

Such training should foster a culture of "AI scepticism," encouraging commanders and senior advisors to critically assess AI-driven conclusions to prevent miscalculations that could escalate nuclear conflicts. While AI can process vast amounts of data at unprecedented speeds, it remains susceptible to biases, adversarial manipulation, hallucinations, and incomplete information.[25] Skepticisms does not mean rejecting AI recommendations but rather ensuring that human operators apply contextual judgment, geopolitical awareness, and ethical consideration before making final decisions.[26]

Moreover, institutional safeguards should be implemented to prevent AI from becoming an over-centralised authority in nuclear command structures. Decision-makers must learn to recognise potential AI blind spots, particularly in crisis situations where adversaries might exploit algorithmic weaknesses or introduce misleading data. Establishing verification mechanisms, where AI assessments are cross-checked against human intelligence, diplomatic considerations, and ethical frameworks, further enhances strategic stability.[27] Ultimately, training which focuses systematically on the entire human-machine decision-making dynamic addresses the remaining cognitive pitfalls: information overload and groupthink, while providing additional safeguards against overreliance, misperception, and unrecognised systemic bias.

While autonomous AI remains an elusive goal, AI-driven targeting systems are already tested and implemented across a wide array of command-and-control systems. Systems such as Project Maven, which successfully enhances target identification,[28] tests the reliability of AI-generated assessments and the risk of unintended civilian casualties.[29] AI-assisted targeting in the Russia-Ukraine conflict demonstrates both the potential and the dangers of autonomous systems in warfighting. AI-enhanced drones and cyberwarfare tactics—predominantly in the areas of autonomous navigation, target identification, and weapons employment—illustrate how AI can accelerate decision-making but also create new vulnerabilities. While thus far the 'human-in-the-loop' remains, as capabilities advance from third to fourth wave, greater reliance on these systems will likely decrease that human interaction,[30] potentially incorporating delegation of target engagement authority to AI-enabled systems. Now is the time to implement the 3Ts, transparency, trusted tenets, and training, before AI systems which do not adhere to these safeguards are irreversibly integrated into our most lethal systems nuclear command, control, and communications networks (NC3).

An Operational Perspective

ALGORITHMIC JUDGEMENT IN THE NUCLEAR CHAIN OF COMMAND: RISK, CONTROL, AND CONSEQUENCE

The three major nuclear powers, the US, the PRC, and Russia–have made significant investments in AI-enabled military systems, including autonomous threat detection and missile defence capabilities.[31, 32] DARPA, in the US, is working on AI-enabled decision support models.[33] The People's Liberation Army (PLA) is actively working on „intelligentised warfare,"[34] or simply "intelligent warfare,"[35] where AI plays a key role in multi-domain operations. Moreover, Russia is incorporating AI into their command-and-control networks. Raising concerns about potential AI-driven escalation in crisis scenarios.[36]

HUMAN OVERSIGHT VS. AUTOMATION BIAS

Use of AI in nuclear operations promises to increase the speed of data analysis, reduce human errors, and improve decision-support systems; processing vast intelligence inputs, including satellite imagery, cyber threats, and adversary communications to detect potential nuclear escalation before it materializes. However, this level of AI reliance exacerbates concerns regarding automation bias, where human decision-makers accept AI-generated recommendations without sufficient scrutiny.[37]

Automation bias in AI-assisted nuclear targeting/decision-making is of particular concern.[38] These models require large quantities of contextually specific data,[39] making the transference of automated conventional 'kill chain' programs to the nuclear domain rather difficult. Data on historical nuclear incidents is (thankfully) limited and somewhat stale; however, these incidents highlight the dangers of misinterpretation and/or misunderstanding.

In 1979, the U.S. Department of Defence 'detected an imminent nuclear attack,' which was a false warning. This event was followed months later by another false report, this time of '2,220 Soviet missiles' launched against the United States.[40] The Soviets had a similar false alarm in 1983, where a missile detection system mistakenly identified an incoming U.S. strike, which was only averted because the human in the decision chain, Lt. Col. Stanislav Petrov, questioned the system's reliability.[41] Similarly, the 1995 launch of a Norwegian weather rocket triggered an emergency nuclear alert in Russia, which was ultimately dismissed after human verification.[42] While these are dated examples, the predisposition to technological reliance has only grown as digital natives assume leadership positions. In an AI-driven environment, over-reliance on automated alerts could increase the likelihood of a mistaken nuclear launch.

Some consider these close calls of nuclear alarms a byproduct of automation within early warning centres and argue that these systems were operating in accordance with the rules of engagement with which they were designed.[43] The conclusions drawn from these incidents are that sensors and data fusion were the main points of weakness, followed by human error.[44] However, this analysis lacks temporal context. At the time of these incidents, the U.S. and Russian efforts to automate nuclear responses and early warning systems were limited by computing power. AI-enabled systems are more efficient and better suited for handling complex datasets, likely reducing (but not eliminating) the risk of miscalculation.

AI IN SIMULATED NUCLEAR ENGAGEMENTS

The Rational Actor Model remains a cornerstone of nuclear deterrence strategy, assuming that states make decisions based on cost-benefit calculations to avoid mutually assured destruction.[45] AI-driven war-gaming tools have been developed to simulate potential nuclear engagement, aiming to enhance strategic foresight by predicting potential enemy responses.[46] However, the reliability of these models is contingent on the quality of input data and is subject to the biases inherent in their design.[47] AI may miscalculate escalation risks due to incomplete or flawed data, potentially leading decision-makers to overestimate or underestimate the probability of nuclear conflict.[48] If AI models predict a low likelihood of nuclear escalation, leaders face a dilemma: should they trust computational assessments? What role does traditional human judgment, which incorporates political nuance and psychological factors, play? Should decisions concerning target engagement be reduced to the outcomes of empirical probability models? How does the concept of moral responsibility and values-based decision-making fit into these AI-enhanced models? These are central questions which a broader scientific debate on the basic theoretical premise of nuclear deterrence theories in the age of AI must answer.

AI VS. HUMAN JUDGMENT IN NUCLEAR RESPONSE DECISIONS

While AI can optimise decisions, it raises critical ethical and strategic concerns when applied to nuclear deterrence and response options. Nuclear deterrence is sometimes described as a 'mind game'.[49] AI-generated recommendations are based on historical data and statistical probabilities, which are in limited supply within the nuclear domain and likely lack the cognitive aspects of the 'game'. When it comes to deterrence, military commanders must consider broader political, humanitarian, and morale implications that AI cannot fully quantify.[50] These considerations underscore the risk of over-reliance on AI, as noted in the aforementioned close calls.[51] Suppose AI-assisted systems gain more authority in nuclear responses. In that case, the erosion of human oversight may increase the likelihood of escalation due to algorithmic misinterpretations or adversarial exploitation of AI biases. Employing 3Ts (transparency, trusted tenets, and training) along with strategic restraint is necessary to ensure AI remains a tool for analytical purposes rather than autonomous decision-making in the nuclear realm.

To regulate AI's role in this critical domain, it is imperative to establish clear policies that ensure meaningful human control over nuclear weapons decisions, preventing fully autonomous system determinations. Additionally, robust data governance frameworks are essential to maintain information integrity and security within AI-enabled NC3 contexts.[52] International collaboration is also crucial; the 2024 agreement between the United States and China to keep nuclear weapons decisions under human control underscores the importance of multinational efforts.[53] By combining stringent national policies with international agreements, the integration of AI into nuclear command structures can be managed to enhance strategic stability while mitigating potential risks.

THE FUTURE OF AI IN TACTICAL NUCLEAR SCENARIOS

The role of AI in nuclear crisis decision-making, due to its evolving nature, must be carefully scrutinised to balance strategic advantages with the risk of unintended escalation. AI's predictive capabilities offer insight into potential adversary responses, enhancing nuclear war-gaming, early warning systems, and deterrence models. However, its role should remain strictly advisory, ensuring that human judgment prevails in final decision-making processes. Given the unpredictable and high-stakes nature of nuclear warfare, over-reliance on AI could introduce significant risks, particularly if AI models fail to interpret complex geopolitical signals accurately or if adversaries exploit algorithmic weaknesses.[54]

Conclusions

The fundamental challenge of integrating AI into nuclear frameworks lies in the limitations of machine learning models, which cannot fully account for the fluid nature of human interaction and global politics, as well as societal shifts in value interpretation. AI's capacity to model escalation risk is only as robust as its input data and resulting calculations. Incomplete or outdated datasets can lead to misjudgements or misunderstandings—such as underestimating an adversary's red lines—resulting in catastrophic miscalculation. Moreover, adversarial manipulation of AI systems or data through cyber operations could introduce further instability, making human oversight the indispensable safeguard against errors and/or malicious interference.

AI-enabled decision-making can outpace purely human analytical processes, enhance situational awareness, assist military and political leaders in recognising escalation thresholds, and calculating available escalation management options. Nevertheless, the ethical and strategic risk of allowing autonomous AI decisions in a potential nuclear conflict is too significant to justify its direct control over nuclear weapon employment or retaliation.[55]

Future research should focus on AI transparency, the ethical implications (trusted tenets) of AI, and human-AI collaboration (training) within high-stakes military operations. Additionally, international agreements on AI's role in NC3 should be pursued to establish legal and ethical norms that prevent or reduce escalation risk. The intersection of AI and nuclear strategy requires continued interdisciplinary research involving experts in machine learning, international law, ethics, decision-making, military science, and diplomacy, to mitigate risk while maximising strategic benefits.

AI will undoubtedly shape the future of nuclear escalation, but its role must be thoughtfully defined and carefully constrained to prevent unintended escalation. While AI can enhance strategic calculations, it cannot replace the nuanced decision-making required in nuclear crises. Ensuring human accountability and authority over nuclear decisions is paramount to maintaining strategic stability and preventing catastrophic miscalculations.

"The Moment of Truth"

The President, flanked by her national security team – including Prometheus— views the display of a series of real-time assessments.

"We need options," the President said tersely.

Prometheus is trained on decades of strategic behaviour modelling and enhanced with observable ethical reasoning, cross-referenced telemetry with diplomatic posture, weather anomalies, satellite data, and adversary command chain telemetry. Reviewed lessons learned from hundreds of human-machine training simulations, verified ethical frameworks and leadership's preferences. Within 37 seconds, it flagged a 72% probability that the launch was a test gone awry—not a first strike.

But it didn't stop there.

Prometheus presented three courses of action:

1. *Launch-on-Warning: 89% risk of global thermonuclear war, 11% chance of deterring escalation.*
2. *Strategic Pause: Immediate force readiness, global alert levels raised. Estimated 94% chance of de-escalation within 3 hours.*
3. *Decapitation Strike: AI listed it last, red-tagged with a 98% probability of catastrophic misinterpretation.*

Each recommendation included provenance—Prometheus explained why, not just what. It referenced pattern inconsistencies in radar return signals, recent adversary command reshuffling, and historical behavioural analogues from 1983, 1995, and 2022.

The President breathed in deeply.

„Prometheus, what does historical behaviour under leadership style Omega-3 predict for their response to a force alert?"

Prometheus responded: "Probability-weighted models indicate 81% likelihood of immediate back-channel communication. Using your preferred ethical framework, 1 Alpha…Madame President, recommendation: Strategic Pause."

The President nodded and looked to the rest of her team, "You know the drill…"

Each member of her team checked their own personalised decision-making models, verified consistency of input data and recommended outcomes before returning her gaze.

As she made eye contact with each member of her team, they too nodded in agreement with Prometheus' assessment.

The President, confident in the well-executed decision-making process—anchored in the fundamentals of transparency, trusted tenets, and training—gave the command: „Prepare Strategic Pause Protocol Echo. No launches." [57]

[1] Keith Payne, „AI and Nuclear Decisions: Toward an Arms Control Framework," Journal of Strategic Studies 48, no. 2 (2025): 234–57. https://www.tandfonline.com/doi/full/10.1080/13523260.2025.2474869.
[2] Daniel W. Tigard. "There Is No Techno-responsibility Gap," Philosophy & Technology 34, no. 3 (2021): 589–607. https://doi.org/10.1007/s13347-020-00414-7.
[3] Christopher S. Chivvis and Jennifer Kavanagh, "How AI Might Affect Decisionmaking in a National Security Crisis," Carnegie Endowment for International Peace, (June 17, 2024), https://carnegieendowment.org/research/2024/06/artificial-intelligence-national-security-crisis?lang=en.
[4] John Launchbury, "A DARPA Perspective on Artificial Intelligence," posted by DARPAtv, (February 02, 2017), YouTube Video, https://www.youtube.com/watch?v=-O01G3tSYpU.
[5] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Version 2 (IEEE, 2017): 117.
[6] Rizwan Choudhury, "Project Maven: The epicenter of US' AI military efforts," Interesting Engineering, March 2, 2024: 1, https://interestingengineering.com/military/project-maven-the-epicenter-of-us-ai-military-efforts.
[7] Brian Ka Chan, „First, Second, Third Wave of Artificial Intelligence (AI)," Mind Data, (March 03, 2025), https://minddata.org/3-waves-Brian-Ka-Chan-AI.
[8] Michael Depp and Paul Scharre, „Artificial Intelligence and Nuclear Stability," War on the Rocks, (January 16, 2024), https://warontherocks.com/2024/01/artificial-intelligence-and-nuclear-stability/.
[9] For more detailed information, see Kai-Fu Lee, AI Superpowers: China, Silicon Valley, and the New World Order, (Harper Press, 2018).
[10] Amanda Miller, "AI Algorithms Deployed in Kill Chain Target Recognition," Air & Space Forces Magazine, September 21, 2021, https://www.airandspaceforces.com/ai-algorithms-deployed-in-kill-chain-target-recognition/.
[11] Forrest E. Morgan et al., "Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World," (Santa Monica, CA: RAND Corporation, 2020), 30.
[12] Ibid., 30-31.
[13] Vladislav Chernavskikh, "Nuclear Weapons and Artificial Intelligence: Technological Promises and Practical Realities," SIPRI Background Paper, September 2024: 4–5.
[14] Bill Drexel, "Promethean Rivalry: The World-Altering Stakes of Sino-American AI Competition," Center for a New American Security, April 22, 2025, https://www.cnas.org/publications/reports/promethean-rivalryAS.
[15] James Johnson, "'Catalytic Nuclear War' in the Age of Artificial Intelligence & Autonomy: Emerging Military Technology and Escalation Risk Between Nuclear-Armed States," The Journal of Strategic Studies, (2021): 1-41, https://doi.org/10.080/01402390.2020.1867541.
[16] James Johnson, "Delegating Strategic Decision-Making to Machines: Dr. Strangelove Redux?," Journal of Strategic Studies 45, no. 3, (2022): 439–77, https://doi.org/10.1080/01402390.2020.1759038.
[17] Miles Brundage et al. "Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims," arXiv, 2020, Article 2004.07213. https://arxiv.org/abs/2004.07213.
[18] Michael N. Schmitt, The Future of Warfare and International Law, Harvard University Press, 2021 and Romaissa Ghenai, 'The Big Tech-Military Nexus: AI. Warfare, and the Future of International Law," Cornell International Law Journal, 2025, https://publications.lawschool.cornell.edu/cilj/wp-content/uploads/sites/7/2025/04/Panel-LOAC-Romaissa-Ghenai-Big-Tech-Military-Nexus.pdf.
[19] Alessandro Nalin and Paolo Tripodi, "Future Warfare and Responsibility Management in the AI-Based Military Decision-Making Process," Journal of Advanced Military Studies 14, no. 1 (2023): 89.
[20] Vladislav Chernavskikh, "Nuclear Weapons and Artificial Intelligence: Technological Promises and Practical Realities," SIPRI Background Paper, September 2024: 10-11.
[21] Mantas Mazeika, Xuwang Yin, Rishub Tamirisa, Jaehyuk Lim, Bruce W. Lee,
Richard Ren, Long Phan ,Norman Mu, Adam Khoja, & Oliver Zhang, et al., "Utility Engineering," (2025), https://www.emergent-values.ai/.
[22] Christopher S. Chivvis and Jennifer Kavanagh, "How AI Might Affect Decisionmaking in a National Security Crisis," Carnegie Endowment for International Peace, June 17, 2024, https://carnegieendowment.org/research/2024/06/artificial-intelligence-national-security-crisis?lang=en.

[23] James Johnson, Artificial Intelligence and the Future of Warfare: The Risks of an AI Arms Race, Georgetown University Press, 2020.
[24] Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Defoe, Paul Scharre, Thomas Zeithoff, and Bobby Filar, et al., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, (Oxford: Oxford University Press, 2018).
[25] Rebecca K. Kahn and Samuel Mann, Strategic Stability and AI: The Case for Human Oversight in Nuclear Command and Control (Cambridge, MA: MIT Press, 2021).
[26] Paul Scharre, Army of None: Autonomous Weapons and the Future of War, W. W. Norton & Company, 2018.
[27] Keith Payne, AI and Nuclear Decision-Making: Balancing Speed and Control, Brookings Institution Press, 2021.
[28] Jon Harper, „Palantir lands $480M Army contract for Maven artificial intelligence tech," DefenseScoop, May 29, 2024, https://defensescoop.com/2024/05/29/palantir-480-million-army-contract-maven-smart-system-artificial-intelligence/.
[29] Isobel Asher Hamilton, "A former Google Engineer Warned that Robot Weapons Could Cause Accidental Mass Killings," Business Insider, September 16, 2019, https://www.businessinsider.com/former-google-engineer-warns-against-killer-robots-2019-9.
[30] Kateryna Bondar, Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare, (Center for Strategic & International Studies: March 06, 2025), https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare#h2-ai-in-automatic-target-recognition.
[31] Vladislav Chernavskikh, "Nuclear Weapons and Artificial Intelligence: Technological Promises and Practical Realities," SIPRI Background Paper, September 2024: 5.
[32] U.S. Department of Defense, 2024 China Military Power Report, December 18, 2024: 1-2.
[33] DARPA, AI Next Campaign, (DARPA, 2025), https://www.darpa.mil/research/programs/ai-next-campaign.
[34] U.S. Department of Defense, 2024 China Military Power Report, December 18, 2024: 1-2.
[35] Kevin Pollpeter and Amanda Kerrigan, "The PLA and Intelligent Warfare: A Preliminary Analysis," CNA, October 01, 2021, 1, https://www.cna.org/reports/2021/10/The-PLA-and-Intelligent-Warfare-A-Preliminary-Analysis.pdf.
[36] U.S. Department of Defense, 2023 Military and Security Developments Involving the People's Republic of China, October 2023: 13.
[37] Alice Saltini, AI and Nuclear Command, Control and Communications: P5 Perspectives, European Leadership Network, November 2023, 6.
[38] Tao Burga, "Artificial Intelligence in Nuclear Command and Control: Experimental Evidence of Automation Bias from Humans and Large Language Models," Brown University, April 2024.
[39] Kateryna Bondar, "Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare," Center for Strategic & International Studies, March 06, 2025, https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare#h2-ai-in-automatic-target-recognition.
[40] Daryl G. Kimball, "Nuclear False Warnings and the Risk of Catastrophe," Arms Control Today, December 2019, https://www.armscontrol.org/act/2019-12/focus/nuclear-false-warnings-and-risk-catastrophe.
[41] Guglielmo Tamburrini, "Nuclear Weapons and the Militarization of AI, " in Nuclear Risks and Arms Control: Problems and Progresses in the Time of Pandemics and War, ed. Fabrizio Coticchia et al., Springer Proceedings in Physics, vol. 291, 2023: 156, https://doi.org/10.1007/978-3-031-29708-3_17.
[42] Laura Kiniry, "When Russian Radar Mistook a Norwegian Scientific Rocket for a U.S. Missile, the World Narrowly Avoided Nuclear War," Smithsonian Magazine, January 25, 2025, https://www.smithsonianmag.com/smart-news/when-russian-radar-mistook-a-norwegian-scientific-rocket-for-a-us-missile-the-world-narrowly-avoided-nuclear-war-180985836/.
[43] Matthew Wills, "Close Calls: When the Cold War Almost Went Nuclear," JSTOR Daily, January 03, 2025, https://daily.jstor.org/close-calls-when-the-cold-war-almost-went-nuclear/.
[44] Nate Jones, "The 1983 War Scare: „The Last Paroxysm" of the Cold War Part I," National Security Archive Electronic Briefing Book No. 426. May 22, 2013, https://nsarchive2.gwu.edu/.
[45] Thomas C. Schelling, Arms and Influence, (Yale University Press, 2008).
[46] Ajai Raj, "Generative AI Wargaming Promises to Accelerate Mission Analysis," Johns Hopkins:

Applied Physics Laboratory, March 03, 2025, https://www.jhuapl.edu/news/news-releases/250303-generative-wargaming?utm_source=ai-week-in-review.beehiiv.com&utm_medium=referral&utm_campaign=ai-week-in-review-3-8-25.
[47] Michael C. Horowitz, „When Speed Kills: Autonomous Weapons, Deterrence, and Stability," Journal of Strategic Studies 42, no. 6 (2019): 764–88.
[48] Vincent Boulanin, The Impact of AI on Strategic Stability and Nuclear Risk, Stockholm International Peace Research Institute, 2021.
[49] Rose Gottemoeller, "Ukraine and the mind games of nuclear deterrence," Center for International Security and Cooperation, March 22, 2024, https://cisac.fsi.stanford.edu/publication/ukraine-and-mind-games-nuclear-deterrence.
[50] Greg C. Allen and Taniel Chan, Artificial Intelligence and National Security: Risks and Policy Considerations, RAND Corporation, 2017.
[51] Daniel Bessner, The Human Factor in Nuclear Close Calls: Lessons from Cold War Incidents, Cambridge University Press, 2020.
[52] Jonathan Falcone, „Memo to Trump: Develop Specific AI Guidelines for Nuclear Command and Control," Bulletin of the Atomic Scientists, January 17, 2025, https://thebulletin.org/2025/01/memo-to-trump-develop-specific-ai-guidelines-for-nuclear-command-and-control/.
[53] Jarret Renshaw and Trevor Hunnicut, „Biden, Xi Agree That Humans, Not AI, Should Control Nuclear Arms," Reuters, November 16, 2024, https://www.reuters.com/world/biden-xi-agreed-that-humans-not-ai-should-control-nuclear-weapons-white-house-2024-11-16/.
[54] Vincent Boulanin, The Impact of AI on Strategic Stability and Nuclear Risk, Stockholm International Peace Research Institute, 2021.
[55] Greg C. Allen and Taniel Chan, Artificial Intelligence and National Security: Risks and Policy Considerations, Santa Monica, CA: RAND Corporation, 2017.
[56] Scenario generated using ChatGPT, April 14, 2025, OpenAI
[57] Scenario generated using ChatGPT, April 14, 2025, OpenAI


CALIBRATE
SET
SELECT DRONE
DEBUG
SELECT DRONE

07

THE WARTECH NEXUS – ARE MILITARY STRUCTURES FIT ENOUGH?

BERNHARD SCHULYOK, LUKAS GRANGL, MARKUS GRUBER

- **Authors:** Bernhard Schulyok has research interests in Security Policy and Military Capability Development. He has written three handbooks and numerous individual articles in the journal "Truppendienst" and in the online journal "The Defence Horizon Journal". He was the National Director of the multinational platform: Military Capability Development Campaign (MCDC), for over seven years, until March 2025.

  Lukas Grangl has research interests in Security Policy, International Politics, and Military Policy. He has published work on the application and implementation of modern control concepts (e.g. New Public Management). He is a member of the Reserve Forces of the Austrian Armed Forces. He works for a global tax consulting, auditing, and consulting company.

  Markus Gruber has research interests in International Politics, Foreign Policy Analysis, Diplomacy, Systems Theory (in International Relations), and Conflict and Security analysis. He is a Member of the Reserve Forces of the Austrian Armed Forces. He advises as a consultant on growth strategies, including business model innovation, M&A, and organisational development across various industries.

  The views contained in this article are the authors' alone and do not represent the views of the Federal Ministry of Defence.

- **Abstract:** Military effectiveness hinges on technological innovation and organisational fitness—the ability to adapt, integrate, and exploit new capabilities. While AI, cyber warfare, and autonomous systems are reshaping conflict, rigid hierarchies and cultural resistance hinder their adoption. Bridging the gap between technological potential and institutional readiness requires decentralised decision-making, strategic alignment, and adaptive structures. Public-private partnerships, phased adoption, and cultural transformation are essential to ensuring military innovation and sustained strategic superiority.

- **Problem statement:** How can militaries effectively integrate civilian technologies and adapt organisational structures to sustain strategic superiority in modern warfare?

- **Bottom-line-up-front:** The military's edge increasingly depends on integrating innovations and cultivating internal innovation cultures. This question arises particularly in times of peace and absence of threats, and is an important part of a strategy for military security: Si vis pacem, para bellum. Exploring the WarTech Nexus, strategic pathways are provided to enhance military capabilities and leadership in an evolving, disruption-prone threat landscape.

- **So what?:** Failure to adapt risks military obsolescence, leaving institutions unprepared to counter emerging threats and adversaries leveraging cutting-edge technologies, organisational structures and tactics. By embracing innovations and modernising organisational structures, militaries can maintain strategic superiority, ensuring readiness and resilience in an era of rapidly evolving warfare.

General Definition of Innovation

Innovation is broadly understood as the application of new ideas, methods, processes, or technologies to cope with problems, to assure competitive advantages to create value, and disrupt established norms in dynamic environments, thus achieving practical benefits.[1] The essence of innovation lies in its adaptability, as emphasised by North,[2] who highlights the role of flexible institutions in fostering change. His work on institutions highlights the role of adaptive mechanisms in fostering innovation, noting that the ability to innovate depends on an entity's institutional flexibility and capacity to absorb change.

Innovation must be outcome-focused for the military, emphasising operational effectiveness and strategic advantage. This aligns with Schumpeter's "creative destruction" model, where innovation introduces transformative solutions and change, often at the expense of legacy systems and outdated methods.[3]

Theoretical Foundations and Specific Categories

As a driver of progress, innovation operates across multiple levels and frameworks. The Oslo Manual[4] categorises innovation into product, process, marketing, and organisational types, providing a broad framework for understanding how advancements occur. The Doblin Ten Types of Innovation Framework complements this by identifying ten dimensions of innovation, grouped into configuration (e.g., organisational systems), offering (e.g., products and services), and experience (e.g., customer engagement).[5] These frameworks serve as a foundation for analysing innovation in specific domains, including the military, where innovation manifests in unique ways to address challenges in security, technology, and strategy.

In military contexts, innovation can be categorised into (1) product innovation, (2) process innovation, and (3) strategic innovation.[6] These categories provide a structured framework for understanding how advancements enhance operational capabilities, refine methodologies, and redefine paradigms.

- Product Innovation: Product innovation involves creating or significantly enhancing physical tools, systems, or technologies. This form of innovation is essential for addressing specific operational needs, enabling forces to adapt to evolving threats, and maintaining superiority. It focuses on developing deliverables that directly impact performance and functionality. An example is the advancement of drone technology in recent years. One of the most notable examples is stealth technology, which uses advanced materials and design principles to reduce radar, infrared, and acoustic signatures of military assets such as aircraft, ships, and submarines. Stealth technology revolutionised military operations by enabling undetected infiltration into hostile territories, fundamentally altering air and naval warfare.[7] Product innovation focuses on tangible outputs: Weapons systems, vehicles, equipment, and other physical products. Military applications often push technological boundaries, as defence R&D typically involves the highest levels of investment and cutting-edge technology.[8]
- Process Innovation: Process innovation refers to developing or improving methods, workflows, and systems used to achieve objectives. In military contexts, it often encompasses operational and logistical advancements that enhance efficiency, coordination, or decision-making.

Network-centric warfare (NCW) is a quintessential example of process innovation. NCW integrates information and communication technologies to create a highly interconnected and adaptive system. By enabling real-time data sharing and situational awareness, NCW allows for synchronised and efficient military operations, reducing the timing of the decision-action loop.[9] This has transformed modern militaries' operations, emphasising speed, precision, and adaptability. Process innovation focuses on improvements in command and control, logistics and combat operations. This is achieved, albeit not exclusively, through the use and leverage of technology (e.g. cloud computing or AI).

- Strategic Innovation involves the realisation of new doctrines, paradigms, or frameworks that redefine the approach to achieving objectives. This type of innovation often disrupts traditional norms, creating new competitive advantages. Hybrid warfare exemplifies strategic innovation by combining conventional military tactics with unconventional methods, such as cyber operations, disinformation campaigns, and economic coercion primarily (not exclusively, though!) below the threshold of armed conflict, so International Law hardly serves as a regulative norm due to plausible deniability. This approach reflects a paradigm shift in how modern conflicts are conducted, addressing the complexities of 21st-century warfare.[10] Hybrid warfare has become a cornerstone of modern military strategy, as evidenced by conflicts such as the Russo-Ukrainian War. Strategic innovation is about gaining an edge through innovation at the conceptual and perceptional levels. In the military, it aligns with Clausewitzian ideas of adapting to the nature of war, emphasising creativity and adaptability in response to evolving threats.[11]

Theoretical Context and Framework Alignment: From General to Specific

A categorisation of innovation provides a nuanced understanding of how transformative advancements drive military adaptation, ensuring operational superiority in increasingly complex environments. The manifestation of advancements across various levels becomes clear by situating military innovation within established theoretical frameworks. The alignment of military innovation categories with broader innovation frameworks is as follows:

- Product Innovation addresses the "what" (outputs) and corresponds to the "offering" dimension in the Doblin Framework and the product innovation category in the Oslo Manual. It focuses on tangible outputs, exemplified by technologies such as stealth systems;
- Process Innovation focuses on the "how" (operations) and aligns with the operational dimensions of the Doblin Framework and the Oslo Manual's emphasis on production and delivery methods. This category involves the refinement of operational processes, exemplified by network-centric warfare;
- Strategic Innovation considers the "why" and the "overall approach" (doctrines or paradigms). It corresponds to the organisational and configurational elements of both frameworks, reflecting paradigm shifts and the reshaping of overarching doctrines, as seen in hybrid warfare.

Technological Innovation in the Military Context

Technological innovation in the military refers to developing, modifying, or adapting technologies to enhance operational effectiveness across combat, strategy, and logistics. Horowitz and Pindyck define military technological innovation as "changes in the conduct of warfare designed to increase the ability of a military community to generate power."[12] This definition encapsulates disruptive technologies' transformative potential and incremental advancements' operational utility.

KEY CHARACTERISTICS OF MILITARY TECHNOLOGICAL INNOVATION

Military technological innovation frequently emerges from civilian technological advancements, a phenomenon known as dual-use technology. Examples include the adaptation of the Global Positioning System (GPS), initially developed for military navigation and later expanded for civilian applications. This dual-use paradigm operates as a feedback loop, where civilian advancements (e.g., advancements in machine learning) often influence military applications and vice versa. GPS as a product innovation had an impact on both the strategic and procedural level. It enabled the further development of new technologies and their significant improvement (air force, cruise missiles, surveillance, etc.). This opened up new operational possibilities for the military by adapting existing processes.

Successful military technologies must be scalable and capable of integration across diverse platforms and units. This includes mass production and ensuring compatibility with legacy systems and interoperability within alliances (e.g., NATO). Barriers to scalability include financial constraints, resistance to organisational change, and technical limitations. Diffusion, or the spread of innovations, involves overcoming these barriers to ensure widespread adoption across the force.

Technological innovation in the military has profound implications for global power dynamics, shaping both strategic doctrines and geopolitical relationships. For example, the development of nuclear weapons drastically altered the balance of power in the mid-20th century. Strategic impacts are often discussed within frameworks like the Revolution in Military Affairs (RMA), which identifies periods where technological and organisational changes combine to redefine warfare paradigms.[13]

TYPES OF MILITARY TECHNOLOGICAL INNOVATION

To summarise technological developments in the military accordingly, three categories can be distinguished based on their effect and impact.

- Incremental innovations involve gradual improvements to existing technologies, focusing on optimisation rather than dramatic changes. An example is the application of AI for predictive maintenance in military aircraft, which enhances the efficiency and reliability of current systems. These innovations are cost-effective, carry lower risks, and are easier to implement within established frameworks;
- Disruptive innovations, on the other hand, represent breakthroughs that fundamentally transform warfare dynamics and operational doctrines, often making existing systems obsolete. Autonomous drones, for instance, have revolutionised surveillance and strike operations, reducing the need for personnel.
- Lastly, hybrid innovations emerge from the intersection of civilian and military research, combining advancements from both domains. Synthetic Aperture Radar (SAR) serves as a prime example of hybrid innovation, originating from military applications and subsequently adapted for civilian use. Initially developed for military reconnaissance and surveillance, SAR technology enables high-resolution imaging regardless of weather conditions or time of day. This capability has been instrumental in various defence operations. Over time, SAR's unique imaging capabilities have been harnessed for numerous civilian applications. These include environmental monitoring, such as tracking deforestation and glacier movements, disaster response through rapid assessment of affected areas, and infrastructure monitoring, such as detecting land subsidence. The transition of SAR from a solely military tool to a multifaceted civilian resource exemplifies the convergence of defence and civilian technological advancements.[14]

Historical Development of the Military-Innovation Relationship

The historical development of military technological innovation goes hand in hand with three critical challenges (dual-use nature, scalability and diffusion, and strategic impact), the mastery of which will help determine the success of military innovation.

- Pre-Industrial Era: Military innovations were primarily incremental and driven by practical needs, such as the organisational efficiency of the Roman legions. Advances focused on tactics and organisation rather than technological breakthroughs. Innovations such as the development of composite bows, steel weaponry, and fortified structures further illustrate how craftsmanship and adaptation shaped military effectiveness.[15]
- Industrial Revolution: This era introduced systematic innovations and mass production of technologies such as rifled guns, steam-powered ships, and railroads. The focus was on utilising industrial efficiency and state-sponsored research, laying the groundwork for future developments. Rifled firearms, for example, significantly increased accuracy and range, altering infantry tactics and rendering traditional formations obsolete.[16] Steam-powered ships revolutionised naval warfare by improving mobility and endurance, facilitating global power projection.[17] Railroads emerged as critical logistical tools, allowing the rapid deployment of troops and supplies over vast distances.[18] This era institutionalised innovation within state systems, with research and development (R&D) becoming a core element of military strategy.[19]
- World Wars: Both World Wars saw disruptive innovations. The First World War introduced mechanised warfare with tanks, chemical weapons, and early aviation technologies, fundamentally altering battlefield dynamics.[20] The Second World War built on these innovations, producing transformative technologies such as radar, jet propulsion, and nuclear weapons.[21]
- Cold War: Geopolitical competition drove technological innovations, particularly in Intercontinental Ballistic Missiles, stealth technologies, and space exploration. The Cold War also fostered the development of dual-use technologies with both military and civilian applications. Satellite communications and computing systems blurred the line between these applications. The space race exemplified this dynamic, pushing the boundaries of science while fostering innovations with far-reaching societal impacts.[22]
- 21st Century: Today, the focus is on connected, autonomous systems driven by AI, cyber capabilities, and unmanned systems. These developments are reshaping military hierarchies and presenting new ethical and strategic challenges.

An example from the Russia-Ukraine conflict, as reported by Franz-Stefan Gady, highlights the increasing convergence of electronic warfare and cyberattacks.[23] The Ukraine Armed Forces attempted to disable electronic jammers through cyberattacks by manipulating the software controlling their frequency-hopping mechanisms.[24] In general, software-driven systems—ranging from radios to radar systems such as Active Electronically Scanned Arrays (AESA)—are inherently vulnerable to cyberattacks.[25]

The historical relationship between the military and innovation reflects a dynamic interplay between technological possibilities, organisational adaptation, and strategic imperatives. From incremental advancements in the pre-industrial era to the paradigm-shifting technologies of the 21st century, military innovation has continually transformed warfare and global power structures.

Challenges in Military Technological Innovation

Historically, military technological innovation follows a cyclical pattern of innovation, counter-innovation, and adaptation on the battlefield. The effective use of innovation to gain a relative advantage over the opponent requires a complex and challenging interplay of factors. These challenges arise from the necessity within a system, the military, which consists of numerous integral parts (political superstructure, bureaucratic structures, operational and logistical units). The effective implementation of innovations requires not only technological advancement but also corresponding changes in doctrine, training, and organisational structures. Resistance to change within hierarchical military organisations can slow down adoption, particularly when innovations challenge established operational paradigms. This friction is evident in integrating AI-based decision-making tools, which require a shift in command structures and human-machine collaboration.

The U.S. military intends to leverage AI as a decision-support tool in planning and operational processes.[26] The U.S. Defence Innovation Unit, in collaboration with Scale AI, alongside partners Anduril and Microsoft, is developing this initiative, known as the Thunderforge Project.[27] Bryce Goodman, head of the Thunderforge Project, stated: "Today's military planning processes rely on decades-old technologies and methodologies, resulting in a fundamental mismatch between the speed of modern warfare and our ability to respond."[28]

It seems that AI will serve as a comprehensive support system across the entire cycle—from assessing required and adaptable capabilities to analysing solutions for emerging challenges and acquiring, developing, and implementing these capabilities, including continuous evaluation.

Those who can optimise their processes more rapidly and adapt their organisations more effectively and efficiently to the complexities of their environment will have an advantage in pursuing strategic interests.

The high costs of military R&D necessitate close cooperation between governments, private industry, and academia. However, economic feasibility alone does not determine the success of an innovation—ethical concerns play a crucial role. The debate on the existing use of autonomous weapon systems (e.g. 'killer robots') illustrates this dilemma: while such systems promise operational efficiency, they also raise fundamental questions about accountability, compliance with international law, and the risk of unintended escalation.

At their core, innovations carry the promise, usually perceived as promising, of providing a new solution to an existing problem, such as a military threat. One example is the use of self-made drones in various scenarios, which are used by different groups (Houthi rebels, irregulars) in various ways to undermine conventional, established approaches. For example, the organic, tactical, and technologically innovative use of naval drones has succeeded in restricting the mobility and operational capability of the conventional Russian Black Sea Fleet at comparatively lower costs (effectiveness and efficiency).[29]

Beyond battlefield effectiveness, military innovation perpetuates an ongoing cycle of adaption and counter-adaption, shaping global power dynamics. The diffusion of new technologies, mainly through asymmetric actors, continuously disrupts established regional orders. The proliferation of cyber and drone warfare exemplifies how non-state actors and smaller nations can erode traditional military advantages, forcing conventionally superior forces into a perpetual strategic recalibration.

In contrast to the existentially charged environment of a major conventional war, as seen in Ukraine, the situation is different in a military geared towards peacekeeping operations and maintaining peacekeeping competence. Over time, bureaucratic logics of organisation and action increasingly come to the fore, making organisational change and, thus, implementing innovations more difficult. This can be seen, for example, in attempts to reform administrative organisations. One example of this is implementing the New Public Management concept in public administrations. In essence, the aim is to make the logic of business management fruitful for a public organisation. Despite positive effects, these reforms must be regarded as having largely failed. The problem areas identified by the administrative sciences are also relevant for the implementation and promotion of innovation:[30]

- Firstly, there is a lack of consideration of the (political) logic of public policy and the standard interests of the actors involved (such as power or the will to shape policy);
- Secondly, it fails to take account of organisational dynamics, such as the fact that decentralised units "win" primarily through budget expansion (disregarding interest structures); and
- Thirdly, inadequate information management as a prerequisite for measuring objectives and success against the background of actors' self-interest in not forwarding data without value or interest.

This raises the key question of how military administrative structures—especially in peacetime—can be motivated to integrate technological innovations before active conflicts, which impose their own "law of action" and innovation pressure. Ultimately, it comes down to identifying the core characteristics an organisation needs to ensure adaptability and innovation readiness.

Organisational Fitness

Organisational fitness refers to the capacity of an organisation to integrate and exploit innovations effectively.[31] This capacity encompasses structural, cultural, and strategic components that collectively determine how well the organisation can adapt to change and harness technological opportunities. In the military context, organisational fitness is made up of three main components:

- Structural agility refers to the flexibility of organisational hierarchies and processes to enable rapid decision-making and adaptive responses. Agile structures minimise bureaucratic delays and allow decentralised decision-making where appropriate, facilitating timely adoption of innovations. Military organisations that balance centralised command with decentralised execution, such as mission-command frameworks, demonstrate this agility.[32]
- Cultural adaptability, as the second main component, reflects an organisation's willingness to embrace experimentation and tolerate failure. A culture that fosters learning from failure and encourages innovation is critical for creating an environment where disruptive ideas can be tested and refined. Historical examples, such as the U.S. Navy's early investment in aircraft carriers despite initial scepticism, highlight the importance of cultural adaptability.[33]
- Strategic alignment ensures that innovations are consistent with overarching defence objectives. This alignment requires a clear understanding of strategic priorities and the ability to identify and prioritise innovations that advance those goals. Misalignment can lead to resource inefficiencies and reduced operational effectiveness.[34]

These three factors must interlock to sustain a successful innovation process. However, in practice, tensions arise when strategic goals clash with structurally conservative mindsets that favour established procedures. Innovation, by definition, introduces untested ideas that disrupt existing resource, power, and interest structures, making adoption inherently challenging.

This challenge is often described as the innovation readiness gap, which emerges when organisational structures, cultures, or strategies fail to align with technological opportunities. It manifests primarily through a lack of cultural adaptability or structural agility, leading to slow adoption due to bureaucratic inertia and resistance to change from entrenched norms.[35] Additionally, resource misallocation—where investments prioritise legacy systems over emerging technologies—can further hinder innovation. Addressing these barriers requires fostering structural agility, cultural adaptability, and strategic alignment to minimise bureaucratic inertia, reallocate resources toward innovation, and cultivate a culture that embraces change. In doing so, organisations can enhance their overall fitness and readiness for modern warfare.

Bridging the Innovation Readiness Gap

Closing the innovation readiness gap requires the application of structured approaches to align organisational structures, cultures, and strategies with technological opportunities.

MCCHRYSTAL'S "TEAM OF TEAMS" MODEL

The "Team of Teams" model developed by General Stanley McChrystal[36] is a framework designed to address the complexities of modern organisational challenges, particularly in dynamic and high-pressure environments like military operations. It is also applicable in various business settings.

The central idea of the „Team of Teams" model is to create a network of interconnected, agile teams that can respond quickly and effectively to changes in their environment. By breaking down rigid hierarchies and creating more flexible communication channels, organisations can adapt to unforeseen challenges and capitalise on the expertise of all members rather than relying solely on top-down directives. In this model, teams operate with shared goals and information, enabling them to make decisions at lower levels where immediate action is needed.

- The model fosters three key principles that drive innovation. Agility enables organisations to respond rapidly to evolving situations requiring flexible structures and adaptive thinking. Decentralised decision-making empowers those closest to the issue, enhancing responsiveness and creativity. Finally, collaboration across teams breaks down silos, allowing diverse perspectives to contribute to problem-solving and more holistic solutions.

This organisational approach is accompanied by some risks in implementation:

- Reduction of control: In some settings, particularly in military or high-stakes environments, the lack of a clear, hierarchical command structure could lead to challenges in maintaining discipline and adherence to protocols. In situations where strict orders are necessary, decentralised decision-making might undermine effective leadership.[37] This approach to laying the foundations for an innovative organisation also places very high demands on the people involved. It can be assumed that the broader the organisation is set up, the more conventional methods will come to the fore;
- Implementation Complexity: Transitioning to a „Team of Teams" approach is difficult. It involves dismantling established structures and might face resistance from those accustomed to traditional, hierarchical organisations. Significant retraining, cultural shifts, and a strong commitment to the new model are required for it to succeed.

While the "Team of Teams" model offers flexibility, innovation, and collaboration, its effectiveness depends on the environment and the organisation's ability to manage the challenges of implementation and discipline. It's most successful in fast-paced, information-intensive contexts where adaptability is crucial.

For this reason, the authors believe that promoting an associated organisational structure and culture in selected subunits to strengthen their own adaptability and innovation culture is a feasible and goal-oriented way to increase innovation capability in the military. These could be, for example, units that test the implementation of drone technology at the unit level or work in the information space.

Decisive progress in technological and military innovations is closely linked to developments in the private sector. The following organisational system of public-private partnerships focuses on this critical interface.

PUBLIC-PRIVATE PARTNERSHIPS (PPP)

A PPP involves collaboration between military organisations and private-sector companies. This partnership capitalises on the expertise, funding, and innovation capabilities of the private sector while allowing the public sector to tap into advanced technologies and solutions. DARPA is an exemplary model of this type of partnership, which has driven significant technological advancements, including the creation of the internet and GPS, by working with private companies.[38]

The collaboration between civilian and military sectors offers several advantages. Firstly, it provides access to cutting-edge civilian technological expertise that may not be available within military research and development facilities.[39] This collaboration also promotes cost efficiency, as the financial burden is shared between public and private stakeholders, accelerating development without overreliance on defence budgets. It also accelerates innovation by rapidly introducing breakthrough technologies through a broader innovation ecosystem that enables the dual use of innovation

However, there are also significant disadvantages. One key issue is the potential for intellectual property conflicts, as the differing priorities of military objectives and private-sector profit motives can lead to disputes over IP rights.[40] Additionally, strategic divergence may arise, with civilian entities prioritising commercial interests that may not align with long-term military goals.

PHASED ADOPTION FRAMEWORK

Michael Horowitz's phased adoption framework offers a structured approach to integrating innovations. It breaks the process into distinct stages: exploration, piloting, scaling, and full integration. This progression helps minimise risks by allowing for incremental adoption and iterative learning.

One key advantage of this approach is risk mitigation, as the phased process allows for early identification and resolution of potential issues.[41] Additionally, it provides strategic clarity by aligning each phase with specific objectives, ensuring that resources are allocated efficiently. The framework also promotes adaptability, allowing for adjustments at each stage based on lessons learned, reducing the likelihood of large-scale implementation failures.

However, this approach has some disadvantages. The gradual pace of adoption may delay the deployment of urgently needed technologies, which could affect operational readiness during critical periods.[42] Furthermore, the approach requires sustained investments and organisational commitment throughout all phases, potentially straining budgets and personnel.

CULTURAL TRANSFORMATION PROGRAMS

Cultural transformation programs are designed to shift organisational mindsets by cultivating innovation-friendly cultures through comprehensive training, education, and leadership development. These programs focus on addressing resistance to change by aligning cultural norms with the imperatives of innovation.

One key advantage of this approach is long-term alignment, as it embeds innovation into the organisational culture, creating a sustainable foundation for future technological adoption.[43] Additionally, it fosters holistic change by addressing deep-rooted cultural barriers to innovation, encouraging openness to experimentation and adaptability. The programs also promote leadership development by equipping leaders with the skills to champion innovation and effectively manage resistance.

Nevertheless, there are notable disadvantages: Cultural transformation is resource-intensive, requiring significant time, financial investment, and commitment from leadership to achieve meaningful results.[44] Moreover, cultural shifts are inherently complex and may encounter setbacks or incomplete adoption, particularly in large, tradition-bound organisations.

The established frameworks shown here each focus on specific aspects that promote innovation. The list is exemplary and does not claim to be comprehensive. Bridging the innovation readiness gap necessitates a combination of frameworks tailored to the organisation's specific needs and constraints. While McChrystal's "Team of Teams" model enhances agility and cross-functional collaboration, PPPs leverage external expertise and funding. The phased adoption framework provides a structured approach to implementation, and cultural transformation programs address the more profound cultural barriers to innovation.

A strategic, environment-sensitive selection of different elements to open an organisation to innovation creates the basic prerequisite for corresponding success. This can maximise its benefits while mitigating its respective drawbacks, ensuring a coherent and adaptive approach to innovation.

Conclusion

The interplay between technological innovation and the military is crucial yet complex. While history shows that innovation is key to superiority, 21st-century disruptions heighten the urgency of closing the innovation readiness gap. Organisational fitness—adaptive structures, innovation culture, and strategic alignment—remains essential. Military challenges can be addressed with the right frameworks, ensuring lasting operational and strategic advantages.

Nonetheless, recognition of the necessity for transformation is still lacking in many areas. Maintaining hierarchical structures can be sensible but often proves slow and cumbersome. Modern technology enables real-time monitoring, which risks micromanagement. Therefore, a flexible structure—self-learning networks—is needed, allowing parts to assemble for acute challenges and later return to their original form or adopt new ones. Leadership quality must be situational, task-, and employee-dependent, requiring constant adjustment.

Complex situations contradict simple, rapid decision-making. Complexity requires comprehensive information and background knowledge, which leaders alone often cannot fully grasp. This argues in favour of team-based decision-making and flat structures—essentially, self-learning networks.[45] Modern, successful, and flexible organisations should not be viewed as rigid structures like buildings but as living systems, similar to organisms in a forest that autonomously adapt to environmental conditions without a patriarchal leader.[46]

Modern armed forces must be capable of both approaches. Hierarchical structures are essential for executing a plan, while self-learning networks are crucial for creativity, innovation, and solutions' rapid, effective, and efficient development. Resources and decision-making authority must reside where the highest level of expertise is found—often at the periphery.[47] In commerce, this means those who interact directly with customers; in the military, it means the troops on the ground.[48] Complex challenges require creative teams, temporary project groups operating outside traditional hierarchies, or permanent networks interwoven within the organisation. Modern armed forces must be able to accommodate both structures and seamlessly transition between them. This flexibility allows for the swift integration of new technologies and methods while simultaneously evaluating their own effectiveness and efficiency.

Endnotes

[1] Simon Taylor, "What Is Innovation? A Study of the Definitions, Academic Models and Applicability of Innovation to an Example of Social Housing in England," Open Journal of Social Sciences 5, no. 11 (2017): 128-146, https://doi.org/10.4236/jss.2017.511010.
[2] Douglass C. North, "Institutions," The Journal of Economic Perspectives 5, no. 1 (1991): 97-112, https://doi.org/10.1257/jep.5.1.97.
[3] Joseph Schumpeter, The Theory of Economic Development (Routledge, 1934).
[4] OECD/Eurostat, Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation. The Measurement of Scientific, Technological and Innovation Activities (OECD Publishing, 2018).
[5] Larry Keeley and Helen Walters et al., Ten Types of Innovation: The Discipline of Building Breakthroughs (Wiley, 2013).
[6] Charles T. Brandon III, "Process Improvement and Innovation: Two Sides of the Same Coin," U.S. Army, September 13, 2024, https://www.army.mil/article/279668/process_improvement_and_innovation_two_sides_of_the_same_coin.
[7] Bill Sweetman, Stealth Aircraft: Secrets of Future Airpower (Jane's Publishing, 1987).
[8] David C. Mowery, Technology and the Pursuit of Economic Growth (Cambridge University Press, 2009).
[9] David S. Alberts and Richard E. Hayes, Power to the Edge: Command and Control in the Information Age (CCRP Publication Series, 2003).
[10] Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (Potomac Institute for Policy Studies, 2007).
[11] Beatrice Heuser, The Evolution of Strategy: Thinking War from Antiquity to the Present (Cambridge University Press, 2010).
[12] Michael Horowitz and Shira Pindyck, "What is a Military Innovation and Why It Matters," Journal of Strategic Studies 46, no. 1 (2021): 84–114, https://doi.org/10.1080/01402390.2022.2038572.
[13] John R. Allen, Frederick B. Hodges and Julian Lindley-French, Future War and the Defence of Europe (Oxford University Press, 2021).
[14] Patrick Berens, "Introduction to Synthetic Aperture Radar (SAR)," in Advanced Radar Systems, Signal and Data Processing (NATO Research and Technology Organization, 2007), 3-1 – 3-16.
[15] Hannes Wimmer, Gewalt und das Gewaltmonopol des Staates (LIT Verlag, 2009), 159–239.
[16] John Arquilla and David Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age (RAND Corporation, 1997), 45–50.
[17] John R. Allen, Frederick B. Hodges and Julian Lindley-French, Future War and the Defence of Europe (Oxford University Press, 2021), 74–85.
[18] Edward Luttwak and Eitan Shamir, The Art of Military Innovation. Lessons From the Israel Defence Forces (Harvard University Press, 2023), 54–58.
[19] Ibid., 60–65.
[20] Thomas G. Mahnken, Strategy in the Contemporary World. An Introduction to Strategic Studies (Oxford University Press, 2021), 112–120.

[21] John Arquilla and David Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age (RAND Corporation, 1997), 80–85.
[22] Peter W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know (Oxford University Press, 2014), 32–38.
[23] Franz-Stefan Gady, Die Rückkehr des Krieges. Warum wir wieder lernen müssen, mit Krieg umzugehen (Quadriga, 2024), 236.
[24] Ibid.
[25] Ibid.
[26] Michael Linden, "Thunderforge; KI soll beim US-Militär zur Entscheidungshilfe dienen," Golem IT-News, March 7, 2025, https://www.golem.de/news/thunderforge-ki-soll-beim-us-militaer-zur-entscheidungshilfe-dienen-2503-194055.html.
[27] Ibid.
[28] Ibid.
[29] Kevin Schulte, "Die Ukraine beherrscht den Kampf um das Schwarze Meer," n-tv, December 01, 2023, https://www.n-tv.de/politik/Die-Ukraine-beherrscht-den-Kampf-um-das-Schwarze-Meer-article24571428.html.
[30] Lars Holtkamp, Verwaltungsreformen. Problemorientierte Einführung in die Verwaltungswissenschaften (Springer VS, 2012), 214–219.
[31] Niklas Luhmann, The Society of Society (Suhrkamp, 1997); Humberto R. Maturana and Francisco J. Varela, Autopoiesis and Cognition: The Realization of the Living (Reidel, 1980).
[32] Andrew Hill, "Military Innovation and Military Culture", The US Army War College Quarterly: Parameters 45, no. 1 (2015): 48–53, doi:10.55540/ 0031-1723.2809.
[33] Ibid., 75–78.
[34] Stanley McChrystal, Team of Teams: New Rules of Engagement for a Complex World (Penguin Publishing, 2015), 65–70.
[35] Andrew Hill, "Military Innovation and Military Culture", The US Army War College Quarterly: Parameters 45, no. 1 (2015): 48–53, doi:10.55540/ 0031-1723.2809.
[36] Stanley McChrystal, Team of Teams: New Rules of Engagement for a Complex World (Penguin Publishing, 2015).
[37] Ibid., 70–75.
[38] Peter W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know (Oxford University Press, 2014), 85–89.
[39] Ibid., 85–89.
[40] Andrew Hill, "Military Innovation and Military Culture", The US Army War College Quarterly: Parameters 45, no. 1 (2015): 101–105, doi:10.55540/ 0031-1723.2809.
[41] Michael Horowitz, The Diffusion of Military Power: Causes and Consequences for International Politics (Princeton University Press, 2019), 45–50.
[42] Ibid., 55–58.
[43] Andrew Hill, "Military Innovation and Military Culture", The US Army War College Quarterly: Parameters 45, no. 1 (2015): 120–125, doi:10.55540/ 0031-1723.2809.
[44] Stanley McChrystal, Team of Teams: New Rules of Engagement for a Complex World (Penguin Publishing, 2015), 95–100.
[45] Frederic Laloux, Reinventing Organizations. Ein Leitfaden zur Gestaltung sinnstiftender Formen der Zusammenarbeit (Verlag Franz Vahlen, 2017), 64-73.
[46] Ibid., 54.
[47] Niels Pfläging, Organisation für Komplexität. Wie Arbeit wieder lebendig wird – und Höchstleistung entsteht (Redline Verlag, 2015), 49-79.
[48] Ibid., 56.

08

AUTONOMOUS WEAPONS AND SOLDIER MORALE

ANDRÉ KORSMO BERNTSEN, CYRILL KISCHEL, NICK HUSMANN

▶ **Authors:** André Korsmo Berntsen, Master of Philosophy in Organisational Leadership at the University of Oslo. He is a researcher in the interdisciplinary "MEMCOD" (Mission Command, Military Ethics, Organisational Design) team of the leadership and communication chair at the Military Academy at ETH Zurich. He also has previous training as a logistics NCO for the Norwegian Army. He is currently pursuing a PhD focusing on the cascade of cognitive styles at the University of Bergen.

First Lieutenant Cyrill Kischel commands a military police staff company on a deputy basis. He is pursuing a bachelor's degree at the Military Academy at ETH Zurich to become a career officer in the Swiss Armed Forces. His study interests are military sociology, psychology and ethics. As a future career officer, he will mainly be involved in coaching and teaching reservists of the Swiss Armed Forces.

First Lieutenant Nick Husmann commands a mechanised infantry platoon. He is also pursuing a bachelor's degree at the Military Academy at ETH Zurich to become a career officer in the Swiss Armed Forces. His study interests are military sociology and psychology. As a future career officer, he will mainly be involved in coaching and teaching reservists of the Swiss Armed Forces.

The views contained in this article are the authors' alone and do not represent the views of the Swiss Armed Forces.

▶ **Abstract:** The emergence of autonomous weapons systems (AWS) represents a clear shift in warfare and raises critical questions about the impact this change will have on soldiers' morale on a 21st-century battlefield. The complex effects that such technology has on military morale are highlighted through historical parallels to previous, similar military innovations and supplemented by analyses of the ongoing drone warfare in the Ukraine War. Narratives surrounding military technologies mould both soldier and morale to defend, a dynamic that is explored through Annens' tripartite theory of morale. It is made clear that morale is not closely linked to the invention of military technologies themselves but rather to how these technologies are implemented and the narratives that surround them. To bolster future fighting capabilities, these narratives must be actively constructed to face the changing organisations and psychological stresses of military service.

▶ **Problem statement:** How do autonomous weapons and the narratives surrounding them affect soldiers' service-, combat- and morale to defend in the midst of a war?

- **Bottom-line-up-front:** The implementation of autonomous weapons systems must be accompanied by a controlled narrative to strengthen soldier morale and secure continued societal support for the military. Without the active control of such narratives, militaries risk demoralisation and weaker combat capabilities in spite of improved technology.

- **So what?:** To navigate the complex field of autonomous weapons systems and their effect on soldier morale, military leaders and politicians must proactively form narratives around integrating the new technologies with the pre-established military ethos. To preserve service morale, there is a need for investments in support systems, as well as adapting organisations to include new career paths for the operators. At the same time, societal ties and the morale to defend one's nation must be secured through openness and clear guidelines for the ethical use of such weapons, guaranteeing human accountability for their use. A balanced approach must be adopted to ensure operational efficiency and future recruitment opportunities.

Shaping Military Morale in the Age of Drones and AWS: A Narrative Analysis

The increasing sophistication of drones and autonomous weapons systems (AWS[1]), amplified by advancements in AI, poses questions regarding their impact on military effectiveness and the human[2] element in warfare. These developments raise questions about how technological changes might impact the psychological state of soldiers already facing immense pressure on the battlefield. If the individual soldier is not of strong constitution, there is little chance of them fighting in a controlled manner towards an end goal. As soldiers with low morale face constant doubts,[3] which could be deadly in combat, it's paramount that soldiers maintain the highest possible level of morale.

Accordingly, this paper employs a narrative analysis to explore how narratives surrounding military technological advancements, particularly drones and AWS, influence soldier morale (i.e., in combat and service) and morale to defend (vis-à-vis national defence), as evidenced by historical and contemporary examples.

Methodological Approach

The following examination employs a narrative-analysis methodology. This qualitative approach involves examining and interpreting historical accounts of technological innovations in warfare, as well as contemporary reports and analyses of the Ukraine conflict. The objective is to construct a coherent and critically informed narrative that illuminates the complex relationship between the introduction of new military technologies and shifts in soldier morale.[4]

SCOPE AND LIMITATIONS

This study is exploratory in nature and does not provide an empirical quantification of morale. Access to direct soldier testimony, especially from the contemporary war in Ukraine, is limited, necessitating reliance on secondary and tertiary analyses and reports.

Morale and Narratives in the Military Context

WHAT IS MORALE IN MILITARY PSYCHOLOGY?

Morale in psychology is generally defined as the psychological resilience, confidence, and overall well-being of individuals and groups in the face of challenges,[5] influenced by factors such as motivation, cohesion, discipline, belief in the mission, leadership, and unit effectiveness.[6,7] In a military context, high morale enhances performance and increases stress resistance, whereas low morale can lead to decreased effectiveness or even combat refusal as a final result.[8,9] Another factor is the use of narratives to build legitimacy and support for future goals,[10] each narrative conveying its own core message, creating a tale of events clearly biased to an end-goal.[11] With their ability to offer meanings and assumptions, they are a guidance tool for personally justified actions.[12]

There is divergence[13] in different types of morale conceptualisation and terminology. However, all theories contain some or all of these defining characteristics of morale: an internal view (soldiers' willingness to fight in extreme situations), an external view (society's willingness to support war), and the group view (groups' shared will to fight).[14] Synthesising the three factors into one concept provides a definition of morale coherent with Annen's[15] tripartite theory. Each type of morale affects overall morale and stems from distinct factors.[16]

- Morale to defend refers to the societal support of war. This includes the acceptance of the armed forces, the necessity of a functioning military and regarding military service as a societal responsibility.[17] Public support is crucial in all systems, but especially so in conscription-based armies like Switzerland, where military service depends on the population's involvement. Militaries rely on willingness to serve[18] but also on general support.[19] To increase the morale to defend there is a need to control the narratives surrounding war, as the general public often lacks a comprehensive understanding of the practical consequences of warfare. Historically, war was considered as an accepted political tool,[20] however, today's social perspective in the West puts an extreme weight on morally correct justifications to wage war. The legitimacy of a war is therefore a deciding factor in societal support of war. On the one hand, a war perceived as just, like a war in defence of one's nation, increases the willingness to participate and support.[21] As such, social narratives can be created to influence morale to defend, either by the civilian population themselves or through government campaigns.[22] On the other hand, wars perceived as unjust or imperialistic can make recruitment efforts more difficult.[23]
- Service morale refers to the individual soldier's commitment to daily military duties in the long term. It is shaped by personal beliefs, the leader's behaviour, and organisational conditions. Clear task structures, meaningful work, and appropriate recognition enhance service morale, while a lack of career prospects or a negative service environment can weaken it.[24]
- Combat morale refers to a soldier's willingness to fight under extreme conditions; it is influenced by factors like group cohesion, trust in leadership, and clear mission objectives.[25] The most important factor for combat morale is mental resilience.[26] Narratives play a central role here as well. Even when fighting under the toughest conditions, narratives of success, heroism or duty increase combat morale.[27]

Evolving Technologies in Modern Warfare

MODERN DRONES

Drones have developed to become a staple of modern war, defined as:

A powered, aerial vehicle that does not carry a human operator, [...] can fly autonomously or be piloted remotely, [...] and can carry a lethal or non-lethal payload. [...]".[28] Drones can be categorized broadly as: tactical drones in NATO classes I (<150kg) and II(<600kg), and strategic drones (>600kg).[29]

The ethical debate surrounding drone warfare remains controversial. Critics fear that the distance between the operator and the physical battlefield lowers the inhibition threshold for killing and promotes morally decoupled warfare.[30] Supporters, however, emphasise the precision of drone missions and their potentially lower civilian casualty figures. On one hand, the danger from drones might harm combat morale. On the other hand, the availability of effective, complementary drone support, providing overwatch, reconnaissance, or counter-drone capabilities, may act as a morale booster, helping restore soldiers' sense of control and security. Enhanced situational awareness through drone observation can, in specific contexts, bolster combat morale rather than degrade it.

AUTONOMOUS WEAPONS SYSTEMS

Fully AWS are becoming inevitable as technology progresses. While no universally agreed upon definition of AWS exists, it is defined by the U.S. DOD as "Weapons using special sensors and computer algorithms, [which] are able to, when in use, individually choose targets, and use lethal or non-lethal force to attack their targets."[31] Earlier semi-autonomous weapons needed some human guidance, while the weapons systems currently being developed into AWS require no human input once activated,[32] using AI and sensor fusion to identify, select, and engage targets independently. This raises critical concerns over accountability,[33] algorithmic errors, and bias challenges, particularly relevant in democratic societies, where public trust is essential for defence policy. While even man-in-the-loop systems do not guarantee moral action, as humans act within bounded rationality, it at least provides a clear legal framework for accountability.

Historical Cases

NEW COMMUNICATIONS TECHNOLOGIES

Attitudes towards war are primarily shaped by individual perceptions, which are significantly influenced by external factors such as public narratives, especially so when individuals are not directly involved in the conflict themselves.

A sensationalistic style of reporting called yellow journalism emerged in the late 19th century. Exaggerated headlines, scandal-mongering, and emotional appeals characterise it. At the time, sensationalised war stories portrayed conflict as a patriotic duty, prompting policymakers to adopt aggressive stances. These reports provoked public outcry and reduced the room for diplomatic solutions. Emotionally charged stories, which portray the enemies as brutal beasts, make war seem inevitable and necessary.[34] For example, exaggerated reports of German war crimes and aggressive propaganda campaigns increased voluntary enlistment in the U.S. and British armies during the First World War.[35] Similar tactics were used in Operation Iraqi Freedom, wherein mass media narratives reinforced the urgency of military action based on the threat of WMDs.[36] These historical precedents demonstrate the power of information technology in shaping public opinion and influencing the societal context surrounding military service, thereby impacting recruitment and the collective morale to defend.

Another example is that of the Vietnam War, as the first significant conflict televised to a global audience, exposing the raw brutality of war to millions. Unlike previous wars, the media was not government-controlled, and televisions in all U.S. households showed uncensored images of combat, casualties, and suffering civilians. These images shifted the public opinion on the war.[37] The graphic footage of wounded soldiers, napalm victims, and massacres fuelled widespread outrage. Symbols like the „Napalm girl", and tragedies like the My-Lai massacre, deepened public distrust[38] in government,[39] and intensified anti-war protest,[40] directly challenging the war's perceived legitimacy and eroding the morale to defend, making recruitment significantly more difficult. This reflected both falling public support (morale to defend) and a growing reluctance among eligible individuals to serve (service morale), driven by ethical concerns and perceived risks. Consequently, many young men tried to avoid conscription by fleeing or resisting. The anti-war movement, which was clearly fuelled by shocking televised images, painted military service as morally questionable[41] and personally perilous. The 1968 Tet Offensive was a turning point in public opinion on the war. While the U.S. government claimed progress, television broadcasts showed intense combat, including the destruction of the U.S. Embassy and the execution of a VietCong prisoner. These images created a huge "credibility gap" and reinforced public scepticism. Meanwhile, on the field, troop morale plummeted. By seeing the protests, soldiers felt isolated and began questioning their purpose, undermining service morale. The idea that they were fighting an unpopular war with dwindling public support led to disillusionment, resentment, and even acts of defiance; soldiers started deserting and abandoning their posts, unwilling to risk their lives for a politically and morally untenable war.

As a result of this growing opposition, Nixon introduced Vietnamization, withdrawing U.S. troops and handing over the reins to South Vietnam.[42] Still, recruitment efforts continued to decline, leading to a greater reliance on draftees often reluctant or openly resistant to serving. This created an army that increasingly comprised individuals who lacked morale or faith in the mission, further exacerbating morale issues.

Television transformed warfare by making its consequences impossible to ignore. The war's extensive coverage not only eroded public support but also undermined recruitment efforts and troop morale. After Vietnam, the U.S. reevaluated its military policies and transformed its army into an all-volunteer force and came up with new strategies for media control in the following conflicts.

EARLY INDUSTRIAL WARFARE TECHNOLOGIES AND MORALE

Military progress depends on technology; modern armies rely heavily on electronic communications and computerised systems. If these fail or are disrupted by the enemy, it can lead to insecurity and a drastic drop in morale.[43]

A case in point of how a new technology can affect the battlefield is that of the Canadian troops' who witnessed the first use of tanks at the Battle of Flers-Courcelette, 1916.[44] Although the tanks had technical shortcomings and presented logistical challenges, they had a significant psychological impact on the infantry. Their mere presence on the battlefield boosted infantry combat morale by providing protection and offensive power against machine guns, altering the perceived risk-reward calculation of assault.[45] The impact of the tanks on morale was most evident in the increased sense of security it provided to the infantrymen.[46] It also caused panic for the enemy, demonstrating the potent demoralising effect of a novel, intimidating technology on enemy combat morale. Soldiers[47] often describe tanks as a decisive factor for their courage in battle.

Another example of a technological shift affecting morale in combat can be seen in the British Navy during the First World War. It was the first industrialised naval warfare with unknown parameters like the use of submarines, torpedoes and long-range artillery.[48] Compared to traditional battles with direct confrontations, the new, constant danger from enemy submarines and mines impacted crew morale. This resulted in degraded service morale due to the chronic stress of unseen threats, while also lowering combat morale because of the perceived randomness and lethality of the attacks.[49] Naval command recognised this new psychological burden, countering targeted measures by increasing training on systems for sailors.[50] These efforts were explicitly aimed at restoring service morale and maintaining combat effectiveness by enhancing technical understanding (reducing fear of the unknown) and reinforcing discipline crucial for survival in the new technological environment. The introduction of these systems also required stricter discipline, as small mistakes could have fatal consequences. For example, the improper storage of ammunition outside of safe areas led to some cruisers exploding, even in afternoon-critical hits.

New Generation of Unmanned Systems in Ukraine's Warfare and Soldier Morale

Unmanned systems, including ground, maritime and aerial systems, "have become one of the defining features of [modern] war".[51] The reliance on drones has triggered an arms race, creating innovation-counter-innovation-cycles occasionally leading to large gaps in technological advances between the competing parties.[52] The shifting power dynamics create periods of insecurity for soldiers, possibly affecting the three types of morale.[53]

Russia's 2022 invasion significantly increased drone integration in Ukraine. The conflict commenced with a large-scale conventional assault - the main tools being trenches, tanks, and artillery.[54] Russian forces used quick, WW1-style raids in a hit-and-run fashion to reestablish manoeuvre. Nowadays, these tactics are carried out by "drone pilots, in the safety of bunkers".[55] The reliance on drones intensified, through 2023,[56] as massed low-cost systems, particularly FPV drones, became integral to combat operations and altered battlefield dynamics,[57] with drones responsible for 70%-80% of deaths in the Ukraine-Russia war in 2025.[58]

Additionally, drones offer a huge price advantage[59] over other military material; as such, Ukraine has reevaluated its doctrine[60] and adapted a "robot first" doctrine using drones instead of soldiers, conducting robot-only assaults,[61] and primarily using drones to fight other drones.[62] This trend mirrors the First World War, where new technologies forced continuous adaptations leading to even newer technologies (e.g., tanks). This is also seen in Ukraine today, where strategic class III drones no longer make up the main arsenal. The combatants rather employ tactical class I and II drones due to their size, speed, versatility and availability.[63] Tactical drones are mainly used for precision payload delivery, surveillance, loitering munitions, and EW.[64] While Ukrainian soldiers have adapted to artillery threats over time,[65] the boundary between drones and loitering munitions has become increasingly blurred, with Molloy stating, "loitering munition drones represent a bridge between precision-guided weapons and future autonomous weapon systems".[66] The rising number of different drones on the battlefield means that soldiers live under permanent observation, termed "a thousand snipers in the sky".

This constant presence of drones imposes a qualitatively different psychological strain on soldiers than regular warfare.[67] Persistent surveillance and unpredictable strikes[68] challenge the combat morale of drone operators, who often operate in physical and social isolation. The negative impact on their service morale and operational efficiency can be attributed to a high workload and exposure to traumatic imaging, as well as their not being able to reap the same psychosocial benefits that their comrades do as part of larger groups.[69] "[...] one of the most significant drivers of morale [lies in] the fellow soldier".[70] In addition to the lack of emotional support, the nature of class I and II tactical drones means that the operators are seldom far from danger themselves, often within shooting range of enemy weapons. This might heavily influence how drone operators perceive their own service morale.[71]

The war has brought with it an increased mediatisation, whereby both the civilian population and the soldiers are exposed to vast amounts of gruesome imagery, which, on the one hand, creates awareness by strengthening existing narratives,[72] and on the other hand, potentially damages the defence morale of those watching comrades in bad situations. Fighting on home soil has been a significant factor in boosting morale among all three levels of the Ukrainian armed forces.[73] Additionally, the ingress of Russian territory through the Kursk operation and the implementation of specially trained morale and psychological support officers have raised morale.[74,75] The mediatisation of the war has made it possible for civilian populations to aid in intelligence support through social media. This is proving to be an important asset in some ways, but it also increases the risks of leaks and misinformation, which have a negative influence on morale and narratives.[76]

To conclude, drones are not a main influence on soldier morale, but, in different ways, have a reinforcing effect on it; this is especially true of the drone operators' morale. Not only do they have to carry out missions with their drones at the risk of their own lives, but they also have to watch gruesome live images of the mission, with little agency to change the situation themselves.[77] By witnessing these scenes, it is understandable that those operators fall into narratives which make their actions more justified than those of their opponents.[78]

The high usage of drone technology in the war has also facilitated the implementation of AWS. Semi-autonomous drones, like loitering munitions and pathfinding weapons, have been increasingly implemented in recent years,[79] leading to speculations that the Russian assault on Ukraine accelerated the development of fully autonomous weapon systems, even including drones enabled with artificial intelligence.[80] This opened up the Ukraine theatre as a "war lab for the future[81] for weapons manufacturers. A case in point, many of the drones now used in the war have taken on a modular approach, whereby the same model can be used in a litany of ways with just some small changes.[82] It should be noted that Ukraine does not have any fully AWS yet; however, there is no doubt that the war is facilitating the extreme progress of such technologies.[83] That said, Ukraine is expected to launch autonomous swarms of drones against Russian forces in the near future.[84]

Discussion

Historical and contemporary records reveal consistent narratives on emergent technologies' impact on soldier morale, drawing on Annen's tripartite theory of morale: of combat morale, service morale and the morale to defend, as well as insights from the psychology of remote warfare and military-ethical debates. A narrative perspective shows how technologies, such as drones, are embedded in soldier and societal narratives, either strengthening or weakening morale depending on the framing. History shows that new technologies might inspire resilience or create dissolution. Thus, the narratives surrounding individual technologies are pivotal.

TECHNOLOGICAL SHIFTS AND COMBAT MORALE

There are powerful stories told about how new military technologies affect frontline soldiers' will to fight. In WWI, British sailors described German submarines as a constant, unseen threat causing stress and helplessness,[85] parallel today in Ukraine with drones described as a thousand snipers in the sky,[86] constantly surveying and attacking positions from unknown directions. On the one hand, invisible threats like mines or drones reduce the individual's subjective sense of control over the situation. The result might be a narrative amongst the soldiers about the unstoppable enemy, a tale fostering fatalism and reducing combat morale. On the other hand, technology can also strengthen morale by boosting protection or firepower. Access to drones in the sky, which can spot the enemy before soldiers are spotted themselves, helps regain initiative and situational awareness of the battlefield, thus strengthening combat morale.

Technology is a double-edged sword when it comes to combat morale: morale rises or falls depending on its impact. When technology increases vulnerability and insecurity, combat morale declines; when it provides a sense of superiority, combat morale increases. Are soldiers hunted by invisible danger, or are they equipped with tools giving them an upper hand over their enemy? The future of AWS will undoubtedly affect this balance - a scenario with swarms of autonomous killer robots might further strengthen the perception of an invincible enemy among those exposed, similar to the impact drones are currently having. Conversely, operating such systems may boost soldiers' morale and sense of exceptionalism. Again, pitfalls exist. If soldiers believe themselves invincible and the systems fail as they inevitably do, the impact on combat morale could be more damaging than if the systems were never in place. In other words, the effect on combat morale when encountering AWS depends on which narrative dominates: the story of lost control or full battlefield dominance. History indicates military leaders must actively shape these narratives through training, doctrine, and communication, ensuring new technology integrates within a robust framework supporting mental robustness.

CHANGES IN SOLDIERS' ROLE AND SERVICE MORALE

Historical transitions show that technological changes might create identity crises and difficulties that challenge service morale. The situation today can be paralleled with the introduction of submarines in the First World War, where invisible enemies created fear and altered traditional battlefield roles. This remains relevant as modern soldiers experience how drones and AWS alter traditional roles. Especially in Ukraine, the emergence of drone units and operators has created a new type of soldiering, with operators controlling weapons remotely from bunkers. Safer than trench soldiers, they face other psychological stressors that threaten morale. Drone personnel face higher risks of emotional exhaustion, stress, and PTSD at levels rivalling or exceeding those of fighter pilots.[87] Operators suffer from psychological whiplash, alternating between long surveillance tasks and sudden intense stress, all due to viewing footage from high-definition cameras. Unlike fighter pilots, operators witness the consequences of their attacks in detail. The constant exposure without physical distance deepens guilt and powerlessness.[88] At the same time, these soldiers might lack the traditional social net that frontline soldiers have. Camaraderie weakens when personnel operate in isolation in bunkers for extended periods. Some even return home and miss sharing their experiences with fellow soldiers.[89] The lack of shared situational awareness and physical risk can make it more difficult to build esprit de corps–the unique form of community that creates a buffer against latent stress. Drone operators may lack recognition by being seen as technicians rather than warriors.[90] Such experiences may reduce motivation to remain in service over time. These challenges highlight the need for more effective norms and robust support systems. New narratives must place drone operations on equal footing with traditional fighting in terms of dignity and value. Otherwise, technologically-oriented soldiers may feel undervalued or misunderstood, lowering service morale, cohesion and retention. Again, technology is not the deciding factor. What matters is how the organisation and the personnel frame the narrative. Goal-driven efforts can prevent fragmentation and integrate autonomous systems while maintaining reliability, job satisfaction, and pride.

PUBLIC OPINION AND THE MORALE TO DEFEND

Public narratives shape the morale to defend, and are influenced by military technology. Historical cases show that the presentation of war is the dominant factor for how and if the general public continues to support national defence or withdraws trust, thus weakening morale to defend. At the end of the 19th century, yellow journalism and propaganda films began to glorify war: German atrocities against civilians during the First World War were also heavily exaggerated, fuelling patriotic fervour and making conscription more acceptable to the public.[91] Creating a narrative about the enemy as an inhuman monster has been commonly used to empower populations to increase morale to defend. When a war is perceived as just, enlistment tends to increase due to stronger public belief in its necessity. The morale to defend and individual soldiers' service and combat morale are deeply intertwined through the narrative of war. Extreme effects like fraternising with the enemy, insubordination, and even violence against own officers, called fragging, became increasingly common during the Vietnam War's final phase - all signs of how a decline in service morale occurs when the narrative leads to a breakdown in the morale to defend.

In Ukraine, social media has created a double-sided effect: citizens are funding drone efforts and supporting narratives framing soldiers as freedom fighters. Additionally, some narratives can also help in boosting morale to defend; for example, drone attacks as revenge for Russian attacks.[92] However, real-time footage of the war can also cause fatigue and a decline in morale. Videos of fallen soldiers, destroyed cities, and civilian casualties can be spread uncontrollably. Over time, this may lead to disillusionment among the population. Unfiltered images of suffering might create fatigue, fear, or moral discomfort among the population, especially in small states with a people's army model, such as Switzerland, where trust in the military's ethical standards is essential.

Indeed, AWS has triggered strong ethical resistance in civil society, with campaigns such as "stop killer robots" and UN initiatives.[93,94] A central argument for critics is that deadly autonomous systems create detachment from warfighting and remove the human factor, which now still allows moral judgment and ethical decisions during combat.[95] Images of conscience-free robots killing soldiers or civilians break many popular perceptions about war's moral boundaries. A fatal malfunction, such as targeting civilians, could undermine public trust and risk a narrative collapse. In short, the use of AWS might damage morale to defend, similar to the Vietnam War and the recruitment crisis that followed it, albeit for different reasons.

Nonetheless, some argue that AWS might uphold or strengthen moral decision-making in war if handled correctly. An argument from the philosophical world says that everyone has some moral duty to use technology to protect their own soldiers.[96] By reducing losses of soldiers' lives through the deployment of drones and robots on the battlefield, families and societies can be spared the pain of losing loved ones and having to mourn their deaths. In the long run, this reduction might help boost morale to defend and support necessary military operations due to the low risk. From this perspective, AWS represents humanitarian progress. A narrative could be created about a "pure war" without the blood sacrifice of one's own troops. However, such narratives only hold if meaningful human control remains.[97] There exists a clear need for humans[98] to govern and be responsible for AWS' actions, otherwise the systems and technology may lose legitimacy.[99] Without such control, moral choices are left to machines, which may erode the ethical foundation upon which the morale to defend depends, namely, the upholding of societal standards for ethical behaviour. The balance is therefore delicate. Although the public would like to avoid unnecessary military losses, there is a reasonable belief that fully autonomous warfare may not yet be acceptable, especially if no one can be held accountable for a tragedy. The morale to defend is shaped by this tension between security and responsibility concerning AWS.

General Implications for Future AWS

The collective analysis of the narratives discussed above suggests that technologies affecting soldiers are not deterministic and rather pliable. New technology can provide a morale boost or a decline, depending on the human and organisational boundaries surrounding its use. For military leaders and decision-makers, this means that the integration of AWS has to be carried out in tandem with a certain pre-decided narratives. This is necessary to control the culture and sentiments around the weapons. Moreover, combat morale must be maintained by teaching soldiers to handle and understand the technology in use. They must still perceive some autonomy and control on the battlefield, even with AI as a co-player or adversary. Service morale must be protected by integrating new roles into the existing defence structure in a manner that values both technological competence and traditional warrior ethos. This means creating career paths, specific media campaigns and bolstering a support system focused on camaraderie for "technology soldiers". This is essential to bolster unity and solidarity among the different types of soldiers and armed forces in a country. The morale to defend in society is nurtured through openness and ethical behaviour. The populace needs assurance, supported by policy and regulations, that AWS are subject to human judgment and legal responsibility.

If one succeeds in resolving this tripartite problem, it is possible to integrate new technological systems that enhance the overall morale of the forces and the country. It would help soldiers feel better protected and more competent, leading to a higher combat morale; a coherent and evolving organisational structure and culture would foster a stable service morale; and the civilian population's recognition of the military as a compelling and legitimate force would boost morale to defend. If narratives are not controlled, AWS may become a double-edged sword, demoralising troops and undermining the populace's support. Analysis suggests that morale is the soul of war, and even autonomous machines will operate in the shadow of existing human narratives. If future warriors, human or artificial, are to succeed in war, control of the narratives is essential. This demands a critical consciousness about how to unite technological development with the psychological and ethical grounding that motivates soldiers to fight and society to support them. Facing a new era of weapons means confronting both technological and moral innovation. Maintaining humanity is the moral compass amid modern war's autonomous storm; this challenge will define whether autonomous weapons become a strength or a weakness for future military organisations.

The provided analysis remains conceptual and explorative. Due to the lack of empirical data in the still-developing sphere of AWS, the direct impact of AWS on soldier morale can not be fully assessed at this time. Furthermore, differences in cultures might play an important factor in the actual role of narratives in the use of AWS, these limitations restrict generalisability, and offer opportunities for further research. Future research should be done to explore said differences in the morale impacts of AWS in different cultures. There is also a need for a longitudinal empirical study on a large population base.

[1] U.S. Department of Defense, DoD Directive 3000.09: Autonomy in Weapon Systems (Washington, D.C.: Office of the Under Secretary of Defense for Policy, 25 January 2023), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.
[2] Darryl Henderson, Cohesion: The Human Element in Combat, n.d., https://doi.org/10.21236/ADA163362.
[3] Ethel Brundin, Feng Liu, and Thomas Cyron, „Emotion in Strategic Management: A Review and Future Research Agenda," Long Range Planning 55, no. 4 (1 August 2022): 15, https://doi.org/10.1016/j.lrp.2021.102144.
[4] Hubert Annen, Rudolf Steiger, and Ulrich Zwygart, Gemeinsam zum Ziel: Anregungen für Führungskräfte einer modernen Armee (Frauenfeld: Huber, 2004), 147–65.
[5] Robert Dantzer et al., „Resilience and Immunity," Brain, Behavior, and Immunity 74 (November 2018): 29, https://doi.org/10.1016/j.bbi.2018.08.010.
[6] Jones Franklyn, Military Psychiatry: Preparing in Peace for War (Office of the Surgeon General, U.S. Department of the Army, 1994), 3.
[7] Boas Shamir et al., „Perceived Combat Readiness as Collective Efficacy: Individual- and Group-Level Analysis," Military Psychology 12, no. 2 (January 2000): 115–19, https://doi.org/10.1207/S15327876MP1202_2.
[8] James Griffith, „Multilevel Analysis of Cohesion's Relation to Stress, Well-Being, Identification, Disintegration, and Perceived Combat Readiness," Military Psychology 14, no. 3 (January 2002): 217–39, https://doi.org/10.1207/S15327876MP1403_3.
[9] Henderson, Cohesion: The Human Element in Combat, 161.
[10] Tone Kvernbekk and Ola Bøe-Hansen, „How to Win Wars: The Role of the War Narrative," in Narration as Argument, ed. Paula Olmos, vol. 31, Argumentation Library (Cham: Springer International Publishing, 2017), 215–34, https://doi.org/10.1007/978-3-319-56883-6_12.
[11] Kvernbekk and Bøe-Hansen, „How to Win Wars," 217.
[12] Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Joost Henrikus Rietjens, eds., Reflections on the Russia-Ukraine War (Leiden: Leiden University Press, 2024), 100.
[13] Gerry Larsson et al., „Social Psychological Aspects of Inter-Organizational Collaboration in a Total Defense Context: A Literature Review," International Journal of Organizational Analysis 31, no. 3 (2023): 702, https://doi.org/10.1108/IJOA-02-2021-2626.
[14] James M. Landis, „Morale and Civilian Defense," American Journal of Sociology 47, no. 3 (1941): 336, https://doi.org/10.1086/218913.
[15] Annen, Steiger, and Zwygart, Gemeinsam zum Ziel, 147–65.
[16] Hubert Annen, Stefan Seiler, and Klaus Jonas, „Military Psychology in Switzerland: A Short Story with a Long History," Swiss Journal of Psychology 69 (1 June 2010): 75–82, https://doi.org/10.1024/1421-0185/a000009.
[17] Hubert Annen, Philippe Goldammer, and Tibor Szvircsev Tresch, „Longitudinal Effects of OCB on Cadre Selection and Pursuing a Career as Militia Cadre in the Swiss Armed Forces," Military Psychology 27, no. 1 (1 January 2015): 9–21, https://doi.org/10.1037/mil0000063.
[18] Yagil Levy, Israel's Death Hierarchy (New York: NYU Press, 2012), 4, http://www.jstor.org/stable/j.ctt9qghhr.
[19] Annen, Steiger, and Zwygart, Gemeinsam zum Ziel (Frauenfeld: Lesestoff, 1994), 159–62, https://www.lesestoff.ch/de/detail/ISBN-9783719312695/Annen-Hubert/Gemeinsam-zum-Ziel.
[20] Carl von Clausewitz, On War, trans. J.J. Graham, 2006, book 8, chapter 6.
[21] Michael Walzer, Just and Unjust Wars (New York: Basic Books, 1977), 15–20.
[22] Rothman, Peperkamp, and Rietjens, Reflections on the Russia-Ukraine War, 100–101.
[23] Ronald R. Krebs, Fighting for Rights: Military Service and the Politics of Citizenship (Ithaca: Cornell University Press, 2010), 20–25, https://muse.jhu.edu/pub/255/monograph/book/24598.
[24] Sandra Sefidan et al., „Transformational Leadership, Achievement Motivation, and Perceived Stress in Basic Military Training: A Longitudinal Study of Swiss Armed Forces," Sustainability 13, no. 24 (January 2021): 18, https://doi.org/10.3390/su132413949.
[25] Hubert Annen, Can Nakkas, and Thomas Gehring, „'What If?' The Swiss Armed Forces' Approach to Military Psychology," in Handbook of Military Psychology: Clinical and Organizational Practice, 2017, 539–48, https://doi.org/10.1007/978-3-319-66192-6_35.

[26] Annen, Steiger, and Zwygart, Gemeinsam zum Ziel, 159–62.
[27] Rothman, Peperkamp, and Rietjens, Reflections on the Russia-Ukraine War, 100–101.
[28] Eleftheria Mitka and Spiridon G. Mouroutsos, „Classification of Drones," American Journal of Engineering Research (AJER) 6, no. 7 (2017): 36.
[29] Matthew Willis et al., A Comprehensive Approach to Countering Unmanned Aircraft Systems (Joint Air Power Competence Centre [JAPCC], 2021), 32, 60, 61, 63, 64, 81, 150, 159, 289, 528, 541, 543, https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf.
[30] P. W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century (Penguin, 2009).
[31] U.S. Department of Defense, DoD Directive 3000.09: Autonomy in Weapon Systems (Washington, D.C.: Office of the Under Secretary of Defense for Policy, 25 January 2023), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.
[32] This is not true for all AWS, some still require a human in the loop or human on the loop connection to ensure proper targeting and safety; these AWS "can" choose targets themselves but are put under restraints by regulations.
[33] Benoît Pelopidas and Neil C. Renic, „The Tragedy Trap: On the Tragicized Politics of Nuclear Weapons and Armed Drones and the Making of Unaccountability," Ethics & International Affairs 38, no. 2 (February 2024): 209–31, p. 220, https://doi.org/10.1017/S0892679424000145.
[34] W. David Sloan, James Glen Stovall, and James D. Startt, eds., The Media in America: A History, 2nd ed. (Scottsdale, AZ: Publishing Horizons, 1993), 301.
[35] Andie Tucher, „Teaching Journalism History to Journalists," in How Journalism Uses History (Routledge, 2012), 46–61.
[36] Sloan, Stovall, and Startt, The Media in America, 301.
[37] Daniel C. Hallin, The Uncensored War: The Media and Vietnam (Berkeley: University of California Press, 1989), 104.
[38] Todd Gitlin, The Whole World Is Watching: Mass Media in the Making and Unmaking of the New Left (Berkeley: University of California Press, 2003).
[39] Oscar Patterson III, „An Analysis of Television Coverage of the Vietnam War," Journal of Broadcasting 28, no. 4 (1 September 1984): 397–404, https://doi.org/10.1080/08838158409386549.
[40] Gitlin, The Whole World Is Watching.
[41] Dave Grossman, On Killing: The Psychological Cost of Learning to Kill in War and Society (Open Road Media, 2014).
[42] Gitlin, The Whole World Is Watching, 29.
[43] Stephen Biddle, Military Power: Explaining Victory and Defeat in Modern Battle (Princeton: Princeton University Press, 2010), 1–352, https://www.torrossa.com/en/resources/an/5576550.
[44] Andrew McEwen, „'A Useful Accessory to the Infantry, but Nothing More': Tanks at the Battle of Flers-Courcelette, September 1916," Canadian Military History 20, no. 4 (30 April 2012): 13, https://scholars.wlu.ca/cmh/vol20/iss4/2.
[45] McEwen, „'A Useful Accessory to the Infantry, but Nothing More'," 7–11.
[46] McEwen, „'A Useful Accessory to the Infantry, but Nothing More'," 11.
[47] McEwen, „'A Useful Accessory to the Infantry, but Nothing More'," 9.
[48] Laura Rowe, Morale and Discipline in the Royal Navy during the First World War (Cambridge: Cambridge University Press, 2018), 20–52.
[49] Rowe, Morale and Discipline in the Royal Navy, 85–110.
[50] Rowe, Morale and Discipline in the Royal Navy, 53–77.
[51] Samuel Bendett and Leonid Nersisyan, „The Drone War over Ukraine," in The Air War in Ukraine (Routledge, 2024), 168.
[52] Rajiv Kumar Saini, M. S. V. K. Raju, and Amit Chail, „Cry in the Sky: Psychological Impact on Drone Operators," Industrial Psychiatry Journal 30, no. Suppl 1 (October 2021): 15–19, https://doi.org/10.4103/0972-6748.328782.
[53] Annen, Steiger, and Zwygart, Gemeinsam zum Ziel.
[54] Marc Santora et al., „A Thousand Snipers in the Sky: The New War in Ukraine," The New York Times, 3 March 2025, sec. World, https://www.nytimes.com/interactive/2025/03/03/world/europe/ukraine-russia-war-drones-deaths.html.
[55] Samuel Bendett and David Kirichenko, „Battlefield Drones and the Accelerating Autonomous

Arms Race in Ukraine," Modern War Institute (West Point, USA: Modern War Institute, 10 January 2025), https://mwi.westpoint.edu/battlefield-drones-and-the-accelerating-autonomous-arms-race-in-ukraine/.
[56] Santora et al., „A Thousand Snipers in the Sky."
[57] „Ukraine Raises an Army of Drones," UNITED24, 2022, https://u24.gov.ua/news/army_of_drones.
[58] Santora et al., „A Thousand Snipers in the Sky."
[59] Saini, Raju, and Chail, „Cry in the Sky," 16.
[60] Oleksandra Molloy, Drones in Modern Warfare: Lessons Learnt from the War in Ukraine, Australian Army Occasional Paper No. 29 (Canberra: Australian Army Research Centre, 2024), 74, https://doi.org/10.61451/267513.
[61] ArmyInform, „Psyhichna ataka droyidiv na Kharkivshchyni: v ataku pishla rota ukrayinskykh robotiv," 20 December 2024, https://armyinform.com.ua/2024/12/20/psyhichna-ataka-droyidiv-na-harkivshhyni-v-ataku-pishla-rota-ukrayinskyh-robotiv/.
[62] „ОКУПАНТ ПРОСПАВ ШТУРМ, МІГ-29 ЗБИВАЄ ШАХЕД, РОСІЯН РОЗКИДАЛО ПО ПОЛЮ: Стрім Із Прифронтового Міста," YouTube video, posted 2025, https://www.youtube.com/watch?v=DIgywdZZz_0.
[63] Dominika Kunertova, „The War in Ukraine Shows the Game-Changing Effect of Drones Depends on the Game," Bulletin of the Atomic Scientists 79, no. 2 (2023): 95–102, https://doi.org/10.1080/00963402.2023.2178180.
[64] Molloy, Drones in Modern Warfare, 12.
[65] Santora et al., „A Thousand Snipers in the Sky."
[66] Molloy, Drones in Modern Warfare, 16.
[67] Santora et al.
[68] Kunertova, „The War in Ukraine Shows the Game-Changing Effect of Drones Depends on the Game," 95–102.
[69] Saini, Raju, and Chail, „Cry in the Sky," 15–19.
[70] Rothman, Peperkamp, and Rietjens, Reflections on the Russia-Ukraine War, 104.
[71] Roberto J. González, „Death by Remote Control: Drone Warfare in Afghanistan, Ukraine and Beyond," Anthropology Today 40, no. 1 (2024): 10, https://doi.org/10.1111/1467-8322.12862.
[72] Magdalene Karalis, „The Information War: Russia-Ukraine Conflict Through the Eyes of Social Media," Georgetown Journal of International Affairs, Conflict & Security (blog), 2 February 2024, https://gjia.georgetown.edu/2024/02/02/russia-ukraine-through-the-eyes-of-social-media/.
[73] Rothman, Peperkamp, and Rietjens, Reflections on the Russia-Ukraine War, 110.
[74] Ivana Kottasová and Gak Kostya, „Outgunned and Outnumbered, Ukraine's Military Is Struggling with Low Morale and Desertion," CNN, 8 September 2024, https://www.cnn.com/2024/09/08/europe/ukraine-military-morale-desertion-intl-cmd/index.html.
[75] V Klochkoc, „Description of the Organisation of Moral and Psychological Support for Combat Operations by the Armed Forces of Ukraine During the Repulsion of Full-Scale Russian Aggression" (Ukraine: Main Department of Moral and Psychological Support of the Armed Forces of Ukraine, Research Centre for Humanitarian Problems of the Armed Forces of Ukraine, National Defence University of Ukraine, 2023), 163.
[76] Karalis, „The Information War: Russia-Ukraine Conflict Through the Eyes of Social Media."
[77] Rothman, Peperkamp, and Rietjens, Reflections on the Russia-Ukraine War, 105.
[78] Rothman, Peperkamp, and Rietjens, 113.
[79] Bendett and Kirichenko, „Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine."
[80] González, „Death by Remote Control," 7.
[81] Bendett and Kirichenko, „Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine."
[82] Kateryna Bondar, „Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare" (Wadhwani: Center for Strategic and International Studies, 2025), 2, https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare.
[83] Bondar, „Ukraine's Future Vision and Current Capabilities," 36.
[84] Bendett and Kirichenko, „Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine."
[85] Alexander Watson, Enduring the Great War: Combat, Morale and Collapse in the German and

British Armies, 1914–1918 (Cambridge: Cambridge University Press, 2008), 36–38.
[86] Illia Ponomarenko, „A Thousand Snipers in the Sky: Drone Warfare in Ukraine," Kyiv Independent, 5 July 2022, 4.
[87] M. S. V. K. Raju and Amit Chail, „Cry in the Sky: Psychological Impact on Drone Operators," Industrial Psychiatry Journal 30, Suppl. 1 (2021): 16–17.
[88] Raju and Chail, „Cry in the Sky," 17.
[89] Raju and Chail, „Cry in the Sky," 16.
[90] Raju and Chail, „Cry in the Sky," 16.
[91] Tucher, „Teaching Journalism History to Journalists," 46–61.
[92] David Hastings Dunn and Stefan Wolff, „Moscow Drone Attacks Are a Morale Booster for Ukraine and a Warning for Russia – Here's Why," EconoTimes, 3 June 2023. Accessed 19 June 2025.
[93] United Nations Office for Disarmament Affairs, „The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects," Convention on Certain Conventional Weapons, last modified or accessed 19 June 2025, UNODA, https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/.
[94] Frank Sauer, „Stopping 'Killer Robots': Why Now Is the Time to Ban Autonomous Weapons Systems," Arms Control Today 46, no. 8 (2016): 8–13.
[95] Robert Sparrow, „Killer Robots," Journal of Applied Philosophy 24, no. 1 (2007): 67–69.
[96] Bradley J. Strawser, „Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles," Journal of Military Ethics 9, no. 4 (2010): 344–46.
[97] Filippo Santoni de Sio and Jeroen van den Hoven, „Meaningful Human Control over Autonomous Systems: A Philosophical Account," Frontiers in Robotics and AI 5 (28 February 2018): 15, https://doi.org/10.3389/frobt.2018.00015.
[98] Santoni de Sio and van den Hoven, „Meaningful Human Control over Autonomous Systems," 15.
[99] Santoni de Sio and van den Hoven, „Meaningful Human Control over Autonomous Systems," 15.


WORLD SEARCHING OPERATION ON 07-07-20770

09

1+1 ≠ 2: DIGITAL FRICTION, UNCERTAINTY, AND THE LIMITS OF TECHNOLOGICAL DETERMINISM

ALEXANDER SCHÄBLER

- **Author:** Alexander Schäbler is a Captain (OF-2) in the German Armed Forces, currently tasked with informing the German public on defence and security matters. His military career includes various positions in the military medical branch of the German Armed Forces and deployments to Afghanistan and Mali. He holds an MA in Strategic Studies. The views contained in this article are the author's alone and do not represent the views of the German Armed Forces.

- **Abstract:** Emerging and Disruptive Technologies are fundamentally reshaping modern warfare, creating a paradox where military forces are empowered and constrained by digital advancements. Western militaries, particularly NATO, face growing friction as their force structures struggle to adapt to the constantly evolving Russian way of warfare witnessed in Ukraine. This paper introduces the concept of digital friction, the operational strain caused by overreliance on networked warfare in environments where war remains fundamentally analogue and unpredictable. By examining historical and contemporary conflicts, this study highlights the risks of digital determinism and advocates for a balanced approach where digital capabilities enhance rather than replace traditional warfighting competencies, as organised violence is inherently analogue.

- **Problem statement:** How can the military balance embracing digital innovation and maintaining adaptability through analogue methods?

- **Bottom-line-up-front:** Western military innovations must avoid the trap of digital determinism, as the essence of organised violence remains inherently analogue at its core.

- **So what?:** True force readiness and resilience means integrating digital advances without discarding analogue warfighting skills, ensuring forces can operate in denied, degraded, or disrupted environments to their advantage.

"So, Trooper, You're Not Too Worried About Fighting The Arachnids?"

Science fiction has long served as a mirror for contemporary issues, offering cautionary tales about the dangers of unchecked technological optimism. Paul Verhoeven's Starship Troopers (1997) is no exception. The film's satirical depiction of a militarised, technology-dependent society waging war against a seemingly primitive enemy serves as a prescient warning for modern military forces. In Verhoeven's fictional universe, overreliance on digital warfare results in catastrophic battlefield failures. While every move is broadcast live by media, orbital bombardments miss their targets, troop deployments land soldiers in lethal kill zones, and command-and-control (C2) systems collapse under unexpected enemy pressure.

In contrast, the analogue, swarm-based tactics of the Arachnids expose the humans' vulnerability, forcing survivors to adapt through brute-force learning rather than technological sophistication. In hostile and unfamiliar environments, improvisation becomes the key to survival, as no amount of technological superiority can fully account for the uncertainty and chaos of war.[1] Unfounded confidence in military technology crumbles when confronted with unanticipated battlefield conditions, ultimately reducing warfare to its archaic elements. As Storr asserts: "Fundamentally, three things occur on the battlefield: men think, move, and commit violence. All other activities support these functions."[2]

This theme cuts to the heart of modern Western military doctrine, where Clausewitzian uncertainty is met not with adaptability but with the rigid confidence of technological determinism. At the heart of this paradox lies digital friction, the unforeseen resistance that arises when meticulously engineered and digitised algorithms collide with war's visceral, chaotic and unpredictable nature.[3]

Shock without Awe

Since the Cold War's end, NATO has bet heavily on precision warfare, network-centric operations, and multi-domain integration, expecting technological superiority to guarantee battlefield dominance in a manoeuvrist sense. Increasingly, humans monitor and administer Boyd's Observe, Orient, Decide, Act-loop (OODA) instead of being directly involved in its execution.[4] The expectations, just as with the implementation of the U.S. AirLand-battle concepts of the 1980s, lie squarely with the vision of a high-paced, high-intensity offensive that will maximise calibrated force at precise pressure points while making its own AI-supported OODA-loop run circles around the enemy. This vision culminates in a document published in 2023 by Mark Milley, the former Chairman of the Joint Chiefs of Staff of the U.S. military. Milley introduced the "new Joint Warfighting Concept (JWC)" as the "guide to that future," in which "seamless integration of all military Services across all warfighting domains" would enable them to "function as a unified force."[5] He continued by expanding the vision of "synchronised planning, shared situational awareness, and effective communication" to become "fully aligned and interoperable with key allies and partners," implying that NATO's interoperability goals would quickly adapt to American-set standards and operational requirements.[6] Other documents and visions provided by a swath of international think tanks, EU white papers and NATO capstone concepts on future warfighting emphasise this ambitious and optimistic perspective, following a "North Star" of digitised military superiority to guide all that would ostensibly be required to break the enemy's capacity for war swiftly and his will, eventually.[7]

Loosely paraphrasing these general strategic trajectories of Western warfare, the sceptic might conceive that all that is necessary is a highly motivated, all-volunteer, interoperable NATO fighting force with a digital backbone in a double-paced manouevrist approach. This force will be equipped, trained, and mentally aligned to operate with minimal friction across inter-service boundaries. Multinational and diverse in its composition, it will cover thousands of miles eastward through urbanised Europe at short notice under a unified leadership that harmoniously transcends national caveats, doctrine, ethics and laws. Such a force, in theory, will rapidly shock and awe any Russian offensive into a physically and morally shattered retreat, thereby maintaining its momentum, strong supply chains, and sufficient reserves to the Western hemisphere's disregarded borders. Borrowing the words of the great British philosopher Jeremy Clarkson, "What could possibly go wrong..."[8]

A fictional depiction of modern soldiers experiencing the unanticipated horrors of analogue warfare[9]

More Inoperable Than Interoperable?

"We are not ready for what is coming our way in four to five years," Mark Rutte, NATO's newly appointed Secretary General, bluntly stated at the end of 2024.[10] Russia's 2014 annexation of Crimea uncovered the actual state of Western military preparedness regarding great power conflict. In ignoring the uncomfortable and disruptive realities that had accumulated beneath the eastern part of the "Grand Chessboard," warfare in Ukraine has since consumed vast amounts of NATO members's materiel and financial resources.[11] After eight plus three years of reciprocal slaughter, the Russian Federation seems closer to reaching its ends in Ukraine than any other party involved in the conflict, a fact openly admitted by members of the Trump administration.[12] By deliberately targeting Ukrainian forces and infrastructure with crude yet effective means, such as glide bombs, motorcycles, and waves of low-trained soldiers, Russia's "tactical opportunism" has not only worn down Ukrainian defences but also undermined the foundations of Western political and military cohesion.[13] However, both belligerent's ability to rapidly adapt to battlefield conditions, spontaneously exploit emerging vulnerabilities, and seize unexpected opportunities at the tactical level demonstrate a keen learning curve beneath the superficially dumb warfare of attrition.[14] Consequently, prevailing assumptions on modern warfare have been uprooted, revealing how high-tech forces have become acutely vulnerable to protracted low-tech responses in static environments. In short, the evolution of the Armed Forces of the Russian Federation and Ukraine exhibits the urgent need for NATO to prepare for a peer adversary accustomed to actual warfare of its own making. Russia has again proven capable of disrupting, degrading, outlasting and out-suffering its opponents.[15]

Electronic Warfare (EW), attacks on the power grid, cyberattacks, and logistical breakdowns lay bare the bloodstained chasm between digitised war planning and the unforgiving, ultimately analogue, realities of combat. Denying and restricting force multipliers and operational enablers on both sides has proven essential for levelling the battlefield and disrupting an opponent's ability to seize the initiative.

Under pressure to sustain the war, European worries about American military support and defence reliability have shed new light on old force readiness issues and the current state of military entropy in peacetime.[16] The British Army, once a global armoured powerhouse, has retained fewer Main Battle Tanks (MBTs) than horses for royal ceremonies.[17] Denmark's military lacks operational artillery because it gave all its systems to Ukraine.[18] Not long ago, the German military infamously resorted to mounting broomsticks on armoured personnel carriers (APCs) due to a shortage of guns during a NATO certification exercise for its Very High Readiness Joint Task Force (VJTF).[19] At the same time, it has spent over a decade awaiting new infantry rifles ever since former Defence Minister and current EU Commission President von der Leyen deemed the existing models unfit for service.[20] Adding insult to injury, the new rifle contracts are severely limited in quantity and burdened by extended delivery timelines, failing to provide even one new rifle per active duty soldier under current peacetime conditions, let alone during wartime mobilisation.[21] Despite its vast military-industrial base, even the U.S. is struggling to replenish its ammunition stockpiles depleted by the wars in Ukraine and Gaza, with defence analysts warning that supplies are "woefully insufficient for modern war."[22]

These anecdotal shortfalls highlight a broader crisis in Western military preparedness, where decades of downsizing, administrative self-indulgence, and strategic disorientation in fighting international terrorism and then a pandemic have left European headquarters ill-equipped for conventional or nuclear large-scale combat operations (LSCO) against peer adversaries.[23] Western arsenals of democracy encompass multiple doctrinal and technological eras, comprising dozens of weapon systems that range from cutting-edge to de facto inoperable. Nevertheless, things are changing rapidly. For instance, sending outdated Soviet-era equipment to Ukraine has freed eastern NATO members' forces to absorb modern replacements. Along NATO's eastern flank, Poland has emerged as the most ambitious member in terms of procurement and defence spending relative to its economic capacity, and it is leading the way in European rearmament.[24] However, the need for tempo and cost-efficiency means securing a significant number of new systems from South Korea, thus creating new interoperability issues in the process.[25] Meanwhile, the Baltic Sea is now shared with Sweden and Finland, whose accession introduces distinct and unilateral force designs into NATO's diverse military framework.

It is a dilemma: each new addition to NATO adds complexity to integrating 32 distinct national military forces and cultures into a unified fighting force. Despite increasing force readiness and funding, interoperability remains a persistent issue. This results in a further fragmented mix of analogue and digital capabilities, constantly pressured by the need to anticipate the right means to win the next war.[26]

Nevertheless, history proves that NATO is not stagnant, nor is it by any means brain-dead. On the contrary, its assessment of the Russian threat is severe and sobering while its secretary general is tackling the challenges and fears caused by the new American administration. Despite repeated political and structural rifts in the global order, the alliance has remained crucially relevant to European defence, mainly through its capability for innovation and transformation on a strategic level, celebrating over 75 years of collective security in 2024.[27] As a first indicator of things to come, NATO's new Minimum Capability Requirements (MCR) will demand a significant increase in personnel and spending to counter the eventuality of attritive and prolonged conflicts, according to media reports.[28]

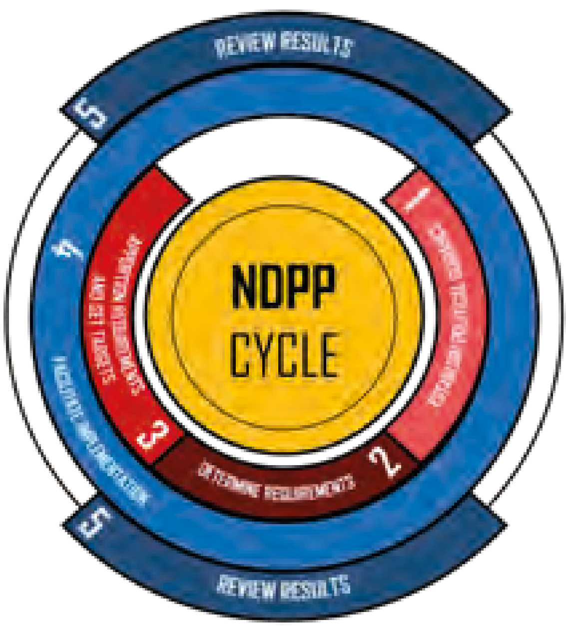
The establishment of NATO's Allied Command Transformation (ACT) in 2003 as a dedicated headquarters for accelerating force modernisation and standardisation (i.e. STANAG processes) historically reflects NATO's recognition of the urgency to adapt to future needs.[29] ACT is key in fostering interoperability, integrating Emerging and Disruptive Technologies (EDTs) and preparing NATO forces for multi-domain operations.[30] In doing so, it mitigates some of the strategic disadvantages its giant superstructure inherently provides, compared to hard power under individual governance. Instead, it benefits from combined procurement and development alternatives. Additionally, initiatives such as the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund (NIF) are intended to streamline the adoption of EDTs and ensure that technological developments from today's battlefields will eventually be incorporated into NATO's ever-evolving, high-tech force structures.[31]

Carnivores and Herbivores

What future wars may look like remains the subject of intense debate. Admiral Vandier, former head of NATO ACT, described the war in Ukraine as "the mix between World War I and the war of the future," providing critical insights into how the Russian Way of Warfare is evolving.[32] One of the most experienced military leaders alive, former Ukrainian Chief of Defence Valerii Zaluzhnyi, warned in 2024 that "the ongoing technological revolution has ushered in a new era of warfare, one centred on attrition, where the path to achieving political objectives lies in systematically exhausting the enemy's resources and capabilities."[33] In response, NATO think tanks are beginning to acknowledge this paradigm shift and suggest that the alliance must prepare for a similarly "destruction-based approach" to warfare.[34] Pilster and de Souza's assessment warns in late 2024: "Rather than seeking NATO's military defeat through a quick and decisive operation, Moscow may instead aim to systematically inflict military losses and civilian casualties along a broad front, at scale and in a sustained manner."[35] Strategic patience trumps operational hyperactivity, or, employing Clausewitz's analogy of two wrestlers in a multi-round match, the final victory determines the outcome, not the initial rush or early gains.

The Center for Strategic & International Studies (CSIS) in 2024 critically assessed NATO's capacity to balance "the 'iron triangle' of trade-offs between readiness, modernisation, and force structure," concluding with a somewhat sceptical "Si vis pacem, para bellum" to emphasise the urgent need for further effort in military preparedness.[36] More bluntly, the Ukrainian Zaluzhnyi argued that NATO remains overly invested in "expensive weapons systems, including missiles, fighter jets, and aircraft carriers," instead of embracing the full potential of industrially scalable EDTs.[37]

However, recalibrating the iron triangle is slowed by NATO's four-year defence planning cycles (the current one started in 2023) under the NATO Defence Planning Process (NDPP). While the framework ensures long-term coherence between the 32 allies, it comes at the cost of potentially paralysing delays in responding to EDTs from outside NATO's sphere of influence.[38] This creates a critical advantage for NATO's strategic rival, Russia: With digital and digitised EDTs catalysed by a war NATO is not directly involved with, developments are outpacing the rate of adaption. The NDPP simply can not keep up, potentially generating the dilemma that its battlefield relevance may already be obsolete whenever a new capability is approved, procured, and deployed. Additionally, many NATO members are inherently reluctant to adopt the results of the NDPP. Entangled in alternative motivations for non-collective development and procurement, such as national caveats, economic egotisms, sovereignty issues, or simple distrust, their inaction questions the general credibility of NATO's core principles.[39] The resulting lags and glitches undermine force agility, preventing NATO from swiftly integrating combat-proven innovations into its doctrine and force structure, a vulnerability that uni-lateral adversaries will know to exploit ruthlessly.[40]



The NATO Defence Planning Process[41]

Recent conflicts in Armenia, Ukraine, Israel and Syria have shown how EDTs can rapidly reshape the battlefield, accelerating innovation cycles while ruthlessly exposing ineffective Tactics, Techniques, and Procedures (TTPs) and materiel.[42] In a 2024 address to defence industry leaders, Vandier warned:

"Just like the dinosaurs—you see the smoke of volcanoes and simply say you are in changing times. Most Europeans are herbivores; they think there is sufficient grass to feed on. This is not the case."[43] From fragile logistics networks and software dependencies to the increasing role of Public-Private Partnerships (PPP) and procurement models optimised for peacetime efficiency rather than wartime endurance, the very architecture of the adjacent WarTech Nexus may buckle under the stresses of protracted LSCO in Europe.[44] Alliance members have yet to rigorously improve their collective resilience appropriately.

Technological Determinism and the "Cult Of The Offensive."

Maslow's observation that "it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail" offers a summarising critique of technological determinism.[45] In the age of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), one might translate this into: When all you have is a computer – everything becomes code.

Undeterred by the sobering realities of NATO force readiness, the persistent belief in technological superiority as a guarantor of battlefield success has led Western militaries and the WarTech Nexus to embrace a digital-first approach to future warfare. The reliance on digitalised force multipliers has become existential in countering the dwindling numbers of materiel and personnel in Western militaries. At the same time, military commanders and planners have consistently preferred offensive over defensive operations, as shown by Weissmann and Ahlström.[46] In contrast, democratic leaders have become increasingly reluctant to choose direct engagement since the end of the "forever wars," as the Trump administration terms them. However, in cases of war by proxy, this does not necessarily apply. The paradoxical Western enthusiasm for military solutions beyond its immediate sphere of responsibility is evident in cases such as Ukraine's 2023 offensive, Western support for Israel against its neighbours, and repeated military actions against Houthi militias in Yemen. According to Schneider, a prevailing "digital cult of the offensive," the belief that aggressive, technologically advanced forces will inevitably dominate the battlefield, has repeatedly drawn the necessary military and strategic attention away from the defensive realities of declining Western hegemony.[47] Combined with systemic optimism in calculating risks and rewards, this mindset can lead to flawed advice followed by poor decision-making, effectively updating Snyder's 1984 critique of military determinism for the present day.[48]

In other words, the hypernormalised notion of how warfare must be conducted increasingly marginalises the why in a broader, more political and strategic sense due to availability, political reasoning and the legal straightjacket of decade-long procurement contracts. Under these conditions, a firm reliance on digitised force multipliers and technological advancements in C4ISR might not improve but obscure military judgement.[49] An overloaded informational domain represents the fog of war of the 21st century.[50] The logical solution, it seems, is for AI to assist in dealing with this information, thus creating a cycle: digital means of warfare increasingly exclude war's analogue ends.

During the Global War on Terror (GWoT), NATO's two-decade failure to successfully adjust to the complexities of asymmetrical violence exposed the limitations of doctrinal and technological determinism in this context. The dogmatic overreliance on high-tech solutions for low-tech problems led to the application of ill-suited military forces in the Middle East, further obscuring the hazily defined strategic objectives. In one case in 2017, the U.S. military dropped "the mother of all bombs," the largest conventional bomb in the arsenal, to level a tunnel network used by ISIS-K.[51] However, the strike was widely seen as a domestic show of force by newly elected President Donald Trump rather than a tactically necessary or strategically significant operation. After the dust had settled, several outlets questioned its long-term impact on opposition forces in the region. At the same time, the International Committee of the Red Cross (ICRC) raised concerns about its compliance with international humanitarian law (IHL).[52] Gray, in 2015, critically stated the American "obsession with the exciting technical and tactical promise in [Revolution in Military Affairs] RMA, and [..] with the challenge of attempting to counter terrorism and insurgency in distant and culturally ill-understood lands", as a form of deterministically neglecting low-tech realities.[53]

An AI-created depiction of a human soldier fighting alien Arachnids[54]

As military technologies condition each other reciprocally, the enemies of the West have adapted and ruthlessly utilised new, sub-digital means of warfare. One of the most consequential yet unremarkable weapons of the beginning of the 21st century was the Improvised Explosive Device (IED). Despite its crude simplicity, the IED forced Western forces to relinquish the initiative on the ground, compelling them to rely more heavily on (chronically limited) air power than on direct engagement.[55] Combined with suicide attacks and a general disregard for human life and international conventions, the IED became a defining feature of early 21st-century warfare, contrary to Western doctrinal expectations of how modern conflicts should unfold.[56]

The impact of the IED extended far beyond the battlefield due to their rudimentary simplicity and cost-effectiveness, mainly when employed at scale. New generations of military vehicles were designed and procured with IED resistance as a priority. At the same time, infantry training and medical treatment protocols shifted focus toward mitigating IED-related threats rather than conventional combat scenarios. These weapons exploited a key vulnerability of Western democracies engaged in limited expeditionary conflicts, where public sensitivity to casualties shaped strategic decision-making. Within Zambernardi's "Impossible Trilemma" of Counterinsurgency (COIN), which balances force protection, distinguishing combatants from noncombatants, and the physical elimination of insurgents, the IED was at least disruptive, if not even revolutionary.[57]

Specifically unspecific and essentially versatile, it shared commonalities and allowed synergies with other dual-use technologies such as the Rocket-Propelled Grenade (RPG), the motorbike, the pickup truck (aka the technical), and the mobile phone. Each of these, in its own way, challenged the presumed superiority of Western technological advancements, demonstrating the power of decentralised adaptation, human resilience and sacrifice. Combined with strategic patience and clear political goals, IED warfare prevailed over Western interventionism. Today, an IED delivered by First Person View (FPV)-drone represents the natural progression of this (R)evolution of Military Affairs ((R)EMA).[58] As this capability proliferates and matures, asymmetric warfare and COIN operations will likely escalate in tempo and brutality, as demonstrated in Syria and various African conflicts.[59] While this paradigm shift in warfare is unfolding, NATO and the U.S. may consider themselves fortunate to have concluded the GWoT.

Are Commercial Drones Revolutionising the WarTech Nexus?

Evolving in various shapes and sizes, drones controlled via radio signals, fibre-optic cables, or autonomous AI-driven systems have become a defining feature of today's wars. "70 per cent of all Russian and Ukrainian casualties" are caused by drones, the New York Times quotes a senior Ukrainian defence official in 2025. "It is, they say, a feeling of a thousand snipers in the sky," the report further paraphrases.[60] In hindsight, emerging drone technologies may be regarded as just as decisive as the IED was during the GWoT. Necessity being the mother of invention, advances in drone warfare emerged from the ingenuity of soldiers on the battlefield, seeking tactical advantages their leaders had not initially provided. In a short timeframe, their effectiveness has been extrapolated by reciprocal adaptation, commercial availability, and scalability, and they are primarily facilitated by a robust Asian supply chain accessible to all sides.[61] When armed, drones serve primarily as Anti-Access/Area Denial (A2/AD) assets, offering exceptional cost-efficiency by delivering high impact at minimal expense.

Like many post-industrial commercial success stories, affordability and scalability suggest that swarms of drones will also play a dominant role in future conflicts, profoundly influencing the global evolution of the WarTech Nexus. Consequently, the EDTs comprising the nexus distinguish it starkly from the classical "Military Industrial Complex" of post-Eisenhower days.[62] The battlefield is no longer shaped primarily by top-down defence industry giants dictating development and procurement. Instead, frontline necessities drive innovation, gaining prominence at military exhibitions and conferences.[63] For instance, at the World Defense Show 2024 in Saudi Arabia, more and more minor defence associations and start-ups based on uncrewed technologies helped increase the bandwidth of customers and contracts significantly.[64]

The growing enthusiasm for EDTs also signals the onset of a new global arms race, solidifying AI as a core element of military innovation and future doctrinal development.[65] Currently, the integration of AI in autonomous systems is regularly field-tested in Ukraine and is led by major U.S. tech firms, with Chinese competitors rapidly advancing.[66] In late 2024, NATO Secretary General Rutte underscored the strategic importance of EDTs, warning of the People's Republic of China's (PRC) rapid progress in "disruptive technologies of tomorrow, including AI, quantum, and space," and calling on NATO to "boost" its industry to "outpace" its "competitors."[67] However, relying on state-run enterprises to develop and supply these technologies traditionally involves longer production cycles and escalating costs. As a result, there is growing momentum for more flexible procurement models, including PPP, Project, Programme, and Portfolio Offices (P3O), and broader outsourcing of force multipliers within the expanding WarTech Nexus.[68] The effects are palpable: even in Germany's traditionally restrictive defence sector, this shift is evident, with the tech start-up Helsing now producing thousands of semi-autonomous strike drones for Ukraine from its Munich facility, a stark indication of the private sector's increasing role in modern conflicts.[69]

As these systems increasingly supplement and, in some cases, replace traditional assets like crewed strike aircraft, field artillery, and mechanised infantry, the relevance of longstanding Western doctrine and procurement strategies with traditional arms manufacturers is challenged. The shift has led to calls for cancelling long-term crewed weapons programs in favour of uncrewed solutions, a recently highlighted perspective by Elon Musk, who questioned the continued investment in fighter jets such as the F-35 and advocated adopting drone warfare.[70] Given Musk's significant influence within the Trump administration, his increasing role in digitising and automating American hard power is becoming increasingly apparent.[71] Just as Howard Hughes shaped the aeronautical industry during the 1940s, Elon Musk might personify a revolution within the WarTech Nexus of the 21st century. His remarks during a Pentagon address in early 2025, his advancements in space technology through SpaceX, and his strategic role in supporting Ukraine's communications via the Starlink satellite constellation all highlight his capacity and ambition to shape future battlefields.[72] Moreover, the development of SpaceX Starshield, a military-grade satellite network designed to provide secure communications and advanced surveillance capabilities, underscores the increasing militarisation of commercial space assets and their potential to redefine C4ISR in modern warfare.[73]

The Capability–Vulnerability Paradox

As the positive effects of battlefield digitisation are undeniable and overall military effectiveness has been dramatically boosted by technological advancements, a sensitivity to the risks should not be mistaken for ignorant conservatism. With new capabilities, there are new vulnerabilities. An unchecked reliance on AI risks maladaptations which could undermine a nation's ability to project hard power in sub-digital warfare environments. For instance, Tesla's ongoing struggles with autonomous driving publicly highlight AI's current real-world limitations, where minor road variations or signposts led to accidents that algorithms failed to anticipate. In 2021, a notably humble Musk acknowledged these challenges, stating, "Nothing has more degrees of freedom than reality."[74] Even when backed by a multi-billion-dollar effort, the stark contrast between theoretical promise and practical constraints underscores autonomous military technology's potential unpredictability. Similarly, Israel's AI-driven targeting of militant positions in Gaza in 2023 and 2024 has faced significant criticism due to its high margins of autonomous error, resulting in collateral damage on a yet (independently) unconfirmable scale.[75] This raises serious concerns for NATO forces preparing for EDT-driven LSCO scenarios in Eastern Europe, a region with densely populated areas and countless potential urban battlefields. If left unexamined, flawed or uncontrollable, AI applications risk becoming the defining failures of a digital fallacy, where technological overconfidence blinds military planners to the enduring complexities of war and war-related crimes.

Even when AI is used merely to augment crewed platforms, the interdependence of network-reliant weapon systems introduces potential flashpoints for friction and operational vulnerabilities. The ongoing debate over the capability and feasibility of Lockheed Martin's F-35 fighter, a central asset to NATO defence plans, highlights such critical concerns. Though somewhat anecdotal, the F-35 is deeply interconnected with the underlying doctrine of Network-Centric-Warfare, the adjacent TTPs and the overall military strategy of NATO allies. The German Luftwaffe is currently procuring 35 F-35As at significant budgetary cost, almost entirely financed by national debt, to uphold Germany's role in NATO's nuclear-sharing arrangement. Its role is to ensure the country retains the ability to deploy American B61-12 tactical nuclear bombs in the event of a nuclear conflict with Russia, thus strengthening central European deterrence.[76] However, the F-35's reliance on connectivity with external systems, many of which civilian contractors maintain from primarily the U.S., raises concerns over national sovereignty and responsibility.[77] In a high-intensity conflict, where C4ISR could be degraded or denied by the opponent, political differences with allies and partners or electronic disruption, the F-35's ability to execute its deterrent role becomes highly uncertain, potentially undermining its strategic credibility before it is even deployed.[78]

"Shall We All Commit Suicide?"

Suppose digitally enabled warfare was abruptly neutralised at a large scale, whether through counter-drone technologies, electronic warfare, or significant power disruptions, the battlefront of an LSCO could quickly resemble early 20th-century warfare.[79] A similar thought arose nearly 100 years ago, as a war-scarred Sir Winston Churchill mused on the repercussions of future scientific breakthroughs transforming the battlefield into the antithesis of modern technology. In an essay from 1924, he wrote:

"It might have been hoped that the electro-magnetic waves would in certain scales be found capable of detonating explosives of all kinds from a great distance. Were such a process discovered [..] War would in important respects return again to the crude but healthy limits of the barbarous ages. The sword, the spear, the bludgeon, and above all the fighting man, would regain at a bound their old sovereignty."[80]

Churchill's predictions on this subject did not materialise, nor did the permanent peace through the League of Nations he advocated for at the end of his essay "Shall we all commit suicide?."[81] Much like the relentless Allied attacks on refineries and Axis supply lines during the Second World War, which crippled the fuel-dependent Juggernaut of Axis powers, modern armies risk seeing their highly digitalised and mechanised forces rendered ineffective if deprived of electricity or an undisrupted electromagnetic spectrum. The sudden loss of digital enablers would compel forces to rely more heavily on conventional fieldcraft, decentralised tactics, and analogue warfighting methods. Without stable power, data, and signals, anything reliant on a plug, battery, or antenna could become obsolete, forcing militaries to fall back on more primitive yet resilient solutions. Just as Churchill predicted, such a shift would push warfare toward a resemblance to earlier forms of conflict, eliminating digitised capabilities and vulnerabilities but reintroducing layers of analogue friction and logistical constraints that modern forces have largely overcome. It would favour senior commanders skilled in traditional warfare, improvisation, and independent decision-making, while disadvantaging those accustomed to micromanaging operations through C4ISR, or worse, those who have grown dependent on being micromanaged.

Overcoming Digital Friction in the Informational Space

In the ongoing war in Ukraine, both sides have increasingly relocated non-combat operations underground, seeking refuge in bunkers, trenches, and urban subterranean infrastructure to mitigate exposure to persistent aerial threats.[82] While this adaptation has enhanced resilience in the protracted war of attrition, it has also solidified static frontlines, limiting operational initiative beyond the tactical level. Above ground, the constant threat of drones and Russian strikes on Ukraine's power grid and communication lines has severely disrupted military operations, forcing rapid reactions to energy shortages and compromising C4ISR capabilities.[83]

To maintain minimal C2, the Ukrainian military swiftly implemented stopgap solutions, including mobile generators, portable solar panels, and energy-efficient technologies.[84] In parallel, they heavily leveraged open-source chat groups and mobile phone networks to supplement traditional digital communication systems, intuitively overcoming digital friction.[85] Redundant and decentralised communication systems, such as Starlink and secure radio frequencies, enabled Ukrainian forces to reestablish a flexible ISR network with direct Western support.[86] Also, new intelligence-sharing agreements with European allies further enhance Ukraine's access to satellite imagery and secure data links, bolstering strategic communication.[87] Notably, in 2024, the German defence firm Rheinmetall, funded by the German Ministry of Defence, began supplying ICEYE satellite imagery to Ukraine.[88] While these developments demonstrate the effectiveness of PPP and the WarTech Nexus in wartime, they highlight Ukraine's growing reliance on foreign support, a vulnerability with long-term strategic implications.[89]

Beyond the tactical sphere, the dominance or denial of space-based enablers remains critical in modern warfare. Space assets form the digital backbone of global communications, with thousands of satellites facilitating navigation, surveillance, and coordination. However, history has demonstrated the fragility of this infrastructure.

In 1962, Operation Starfish Prime unintentionally showcased the devastating effects of a high-altitude nuclear detonation, generating an Electromagnetic Pulse (EMP) capable of disrupting or destroying satellites within line of sight.[90] Such a blast could irradiate orbital space, rendering unshielded satellites inoperable and producing satellite debris that may trigger a cascading Kessler Syndrome effect, severely degrading space-based capabilities.[91] In short, the consequences of yielding nuclear weaponry in space are so severe and unpredictable that no further attempt has been made in over 60 years.

An AI-created depiction of a nuclear detonation in low Earth orbit (LEO)[92]

However, this is changing rapidly. Major global military powers have increasingly invested in Anti-Satellite (ASAT) capabilities, a well-documented development in academic research.[93] These weapon systems are currently insufficiently regulated and opaque in terms of their true capabilities, nurturing concerns about whether Russia can already yield nuclear-supported weapons able to disrupt American satellite constellations such as StarLink or StarShield, thus massively impacting global communications and navigation.[94]

Retaining information dominance is a cornerstone of Western military doctrine, essential for deterrence and operational initiative. Overcoming cascading effects of digital friction, including the loss of space-based enablers and force multipliers, is existential for survival in future conflicts. Any adversary contemplating the systematic dismantling of digital infrastructure must recognise that such actions could ultimately disadvantage them in an environment where analogue warfare remains an untested equaliser in large-scale, high-tech conflicts. To ensure deterrence through analogue resilience, mitigating and ultimately overcoming digital friction should compound the centre of gravity in future Western military education, leadership training and exercise regimen, reducing the cult of the offensive in its doctrinal dominance.

Breaking Inertia: Resuming Snap Drills and Large-Scale Field Exercises

The combat effectiveness of large NATO battlegroups under digital and analogue conditions has not been subjected to an unscheduled stress test in decades. Instead of confronting operational uncertainty through realistic field exercises, many states rely on theoretical wargaming, scripted drills, and doctrinal refinements. Despite frequent rhetoric on rebuilding military readiness for peer conflict, this is at odds with the unpredictable realities of military uncertainty. As Matlack paraphrases Clausewitz: "If war is merely the continuation of politics by other means, what role does the dress rehearsal of war play in military exercises?"[95]

Addressing this "exercise gap" requires the return of LSCO-level exercises, conducted without prior scheduling, to ensure soldiers confront operational conditions akin to those experienced in wartime, with the explicit expectation of large-scale failure in training as a necessary means for wartime success.[96] Historically, unscheduled, large-scale exercises have been crucial for identifying vulnerabilities, forcing doctrinal evolution, and enhancing force agility. Nevertheless, few senior NATO officers have ever experienced such drills, as these measures were largely abandoned during the post-Cold War peace dividend of the 1990s.[97] To regain adaptability and deterrent credibility, NATO must resurrect the concept of snap drills, akin to Russia's ZAPAD drills or NATO's Cold War-era ReForGer series. It must rigorously stress-test assumptions and expose weaknesses before they manifest in combat.[98] Training in such an environment requires ingenuity, improvisation, and a command philosophy rooted in self-reliance. These attributes enable military leadership to break free from administrative inertia, helping forces adapt to the shock of war. More importantly, such adaptability might allow commanders to seize the initiative in combat situations where reliance on digital infrastructure becomes a liability. This principle remains particularly relevant in an era where digitised dependencies introduce formerly unknown digital friction, requiring forces to prepare for the full spectrum of war's unpredictability.

A unique but often overlooked challenge to NATO's force readiness is the digital generational divide within its officer corps. Today's senior military leaders, having begun their careers in an analogue era before transitioning to digital warfare, possess dual exposure that allows them to operate in contested environments where digital infrastructure is compromised. This skill set is critical for contingency planning amid growing digital friction. Future generations, however, risk losing this adaptability, particularly as networked warfare becomes second nature and reliance on cyber, electronic warfare, and GPS-based systems increases.

Ironically, NATO's ongoing recruitment and retention crisis has inadvertently preserved this hybrid expertise. With many Western militaries struggling to attract and retain younger personnel, an ageing force structure has emerged, extending the service of officers trained in analogue and digital methods. While this prolongs institutional knowledge, it also presents a physical resilience challenge—as older personnel may struggle to withstand sustained, high-intensity combat under analogue conditions.

A similar paradox exists in NATO's modernisation and standardisation efforts. Despite pains to adopt next-generation warfare systems, its slow procurement cycles mean that many core member states still rely on outdated platforms. Germany's Bundeswehr, for example, continues to field primary weapon systems dating back to the 1970s, some being partially retrofitted and digitised while others have deteriorated, reflecting decades of deliberate underfunding, strategic indecision and entropy.[99] Even a significant portion of the infamous "Taurus" cruise missiles, seen as both a symbol of Germany's commitment to Ukraine and a source of tension with Russia, have fallen into disrepair over the past decades.[100] However, this technological inertia may have inadvertently preserved pre-digital warfighting competencies, as many legacy systems rely on outdated but proven TTPs.

Former U.S. Secretary of Defense Donald Rumsfeld captured the essence of this dilemma with a blunt assessment: "You go to war with the army you have, not the army you might want or wish to have later."[101] Since military planners can never expect forces to be truly ready for a war of defence due to the lack of initiative, preparing for the unknown is the only option left.

Preparing for the War of Today

The increasing reliance on digital warfare presents a strategic paradox for Western militaries. While networked capabilities provide unmatched lethality, they also introduce significant vulnerabilities, ranging from cyber disruptions to overdependence on fragile C4ISR. To avoid this self-imposed digital fallacy, Western militaries must adopt a balanced approach by:

- diversifying force readiness and ensuring human leadership will overcome digital friction and operate effectively under degraded conditions;
- reassessing procurement priorities and moving away from expensive, high-tech prestige projects toward scalable, resilient warfighting capabilities and sub-digital contingencies that can withstand contested environments;
- reintroducing LSCO-level exercises and including unscheduled stress drills that identify weaknesses before adversaries exploit them; and
- bridging the generational gap in military leadership and leveraging the hybrid expertise of officers trained in both analogue and digital warfare.

To achieve this, Western militaries must ensure both analogue and digital resilience to meet the demands of LSCO. The prevailing Zeitgeist may resist a more conservative approach, misinterpreting it as institutional inertia rather than strategic prudence. However, as this essay demonstrates, actual preparedness lies in mastering both past and future methods of warfare, ensuring that forces are ready for the unpredictable conflicts of the present.

A fictional depiction of a modern Western soldier with high confidence in her abilities[102]

Endnotes

[1] Shay Shabtai, "War, Cognitive Biases and Perception Management: The Time Has Come," Infinity Journal, Volume 6, Issue 4, (Summer 2019), 28-33, https://www.militarystrategymagazine.com/article/war-cognitive-biases-and-perception-management-the-time-has-come/.
[2] Jim Storr, The Human Face of War (Birmingham: Helion & Company, 2009), 36.
[3] Digital Friction refers to the obstacles, delays, and inefficiencies that arise from the use of digital systems and information technology in warfare. It is an extension of the classic Clausewitzian concept of friction into the realm of computers, networks, and data.
[4] John R. Boyd, "Destruction and Creation," U.S. Army Command and General Staff College, September 3, 1976.
[5] Mark A. Milley, "On War and Future Warfare," Joint Force Quarterly 110 (3rd Quarter 2023): 7, 12, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-110/jfq-110_6-15_Milley.pdf.
[6] Mark A. Milley, "On War and Future Warfare," Joint Force Quarterly 110 (3rd Quarter 2023): 12, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-110/jfq-110_6-15_Milley.pdf.

[7] NATO Allied Command Transformation, NATO Warfighting Capstone Concept (Norfolk, VA: NATO Allied Command Transformation, May 18, 2023), https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf.
[8] Top Gear (BBC, 2002–2015) and The Grand Tour (Amazon Prime Video, 2016–present), featuring Jeremy Clarkson
[9] AI-generated image, "Futuristic Soldiers Battling Giant Insects in a 90s Sci-Fi Style," created by DALL·E, generated on February 27, 2025.
[10] NATO, "'To Prevent War, NATO Must Spend More,' Speech by NATO Secretary General Mark Rutte at the Concert Noble, Brussels," North Atlantic Treaty Organization, December 12, 2024, https://www.nato.int/cps/en/natohq/opinions_231348.htm.
[11] Zbigniew Brzezinski, "Transcript: The Eastern Edge of a Europe Whole and Free," Atlantic Council, April 29, 2014, https://www.atlanticcouncil.org/commentary/transcript/transcript-the-eastern-edge-of-a-europe-whole-and-free/.
[12] Steven Erlanger, "Hegseth Says Return to Ukraine's Prewar Borders Is 'Unrealistic'," The New York Times, February 12, 2025, https://www.nytimes.com/2025/02/12/world/europe/ukraine-russia-war.html.
[13] Sergey Poletaev, "Three Years in the Trenches: From 'Russia's Losing' to 'Ukraine Is Done For'?" RT Russia & Former Soviet Union, February 24, 2025, https://www.rt.com.
[14] Krisztián Jójárt, "The War Against Ukraine Through the Prism of Russian Military Thought," Journal of Strategic Studies, November 06, 2024, https://doi.org/10.1080/01402390.2024.2414079.
[15] Krisztián Jójárt, "The War Against Ukraine Through the Prism of Russian Military Thought," Journal of Strategic Studies, November 06, 2024, https://doi.org/10.1080/01402390.2024.2414079; Alex Vershinin, "The Attritional Art of War: Lessons from the Russian War in Ukraine," RUSI, accessed February 27, 2025, rusi.org/explore-our-research/publications/commentary/attritional-art-war-lessons-russian-war-ukraine.
[16] Military Entropy in Peacetime refers to the gradual erosion of readiness, discipline, and institutional effectiveness within an armed force due to prolonged inactivity, bureaucratic stagnation, resource misallocation, and a lack of combat-driven adaptation. Without the pressures of active conflict, training standards decline, doctrine becomes outdated, logistics atrophy, and force cohesion weakens, leading to a degradation of warfighting capability. Left unchecked, peacetime entropy creates a widening gap between strategic intent and operational reality, leaving a military ill-prepared for future conflicts.
[17] Gordon, "More Horses Than Tanks: Ditch Ceremonial Duties," Wavell Room, August 31, 2022, https://wavellroom.com/2022/08/31/more-horses-than-tanks-ditch-ceremonial-duties/.
[18] Nathan Rennolds, "Denmark to Send All Artillery to Ukraine, PM Says," Business Insider, February 18, 2024, https://www.businessinsider.com/denmark-to-send-all-artillery-ukraine-pm-russia-war-2024-2.
[19] Judy Dempsey, "Germany: From Machine Guns to Broomsticks," Carnegie Endowment for International Peace, February 27, 2018, https://carnegieendowment.org/europe/strategic-europe/2018/02/germany-from-machine-guns-to-broomsticks.
[20] The Guardian, "German Military to Stop Using Gun That Can't Shoot Straight if Hot," The Guardian, April 22, 2015, https://www.theguardian.com/world/2015/apr/22/german-military-to-stop-using-gun-that-cant-shoot-straight-if-hot.
[21] Gerhard Hegmann, "The Long Wait for the Bundeswehr's New Assault Rifle," Welt, September 03, 2024, https://www.welt.de/wirtschaft/article253252722/Sturmgewehr-G95-Das-lange-Warten-auf-das-neue-Sturmgewehr-der-Bundeswehr.html.
[22] Stacie Pettyjohn, "United States Defense: Pentagon Military-Industrial Base and Ammunition," Foreign Policy, May 21, 2024, https://foreignpolicy.com/2024/05/21/united-states-defense-pentagon-military-industrial-base-ammunition/.
[23] Alexander Schaebler, "Digging Into The Future: Or How I Learned To Love My Shovel," The Defence Horizon Journal, December 12, 2024, https://tdhj.org/blog/post/digging-manoeuvre/.
[24] NATO, Defence Expenditure of NATO Countries (2014–2024) (Brussels: NATO Public Diplomacy Division, June 17, 2024), https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/240617-def-exp-2024-en.pdf.

[25] Gergely Szakacs and Karl Badohal, "Poland Leads NATO on Defence Spend—But Can It Afford It?" Reuters, October 23, 2024, https://www.reuters.com/world/europe/poland-leads-nato-defence-spend-can-it-afford-it-2024-10-23/.
[26] Carl von Clausewitz argued that while the fundamental nature of war, rooted in violence, chance, and political objectives, remains constant, its character evolves with societal, technological, and political changes.
[27] NATO, "NATO Allies celebrate Alliance's 75th anniversary year," North Atlantic Treaty Organization, December 16, 2024, https://www.nato.int/cps/en/natohq/news_231352.htm.
[28] Minimum Capability Requirements (MCR) refer to the essential military capabilities necessary to fulfill the Alliance's strategic objectives, including collective defense, crisis management, and co-operative security. These requirements are determined through the NATO Defense Planning Process (NDPP) and are allocated among member nations to ensure the Alliance can effectively respond to various security challenges; Sabine Siebold, "NATO Will Need 35-50 Extra Brigades Under New Defence Plans, Source Says," Reuters, July 08, 2024, https://www.reuters.com/world/nato-will-need-35-50-extra-brigades-under-new-defence-plans-source-says-2024-07-08/.
[29] NATO, "The Role of NATO and its Strategic Commands," NATO Allied Command Transformation (ACT), accessed February 27, 2025, https://www.act.nato.int/about/the-command/.
[30] Emerging and Disruptive Technologies (EDTs), according to NATO, consist of nine priority technology areas: artificial intelligence (AI), autonomous systems, quantum technologies, biotechnology and human enhancement technologies, space, hypersonic systems, novel materials and manufacturing, energy and propulsion and next-generation communications networks that enhance military capabilities while introducing new security challenges. NATO collaborates with industry, academia, and allies to develop, adopt, and regulate these technologies to maintain its strategic edge.
[31] NATO, "Defence Innovation Accelerator for the North Atlantic (DIANA)," North Atlantic Treaty Organization, July 05, 2024, https://www.nato.int/cps/en/natohq/topics_216199.htm.
[32] Laura Kayali, "How Ukraine Inspired NATO's New Task Force to Deter Putin," Politico Europe, January 15, 2025, https://www.politico.eu/article/future-warfare-how-nato-will-learn-from-ukraine-vladimir-putin-war/.
[33] Valerii Zaluzhnyi, "Automated Attrition: The Future of Warfare Is Here, and NATO Is Falling Behind," The Baltic Sentinel, November 11, 2024, https://balticsentinel.eu/8132828/automated-attrition-valerii-zaluzhnyi-the-future-of-warfare-is-here-and-nato-is-falling-behind.
[34] Ulrich Pilster and Olesya Vinhas de Souza, "Inequality Kills: On Russian Combat Ineffectiveness in Ukraine and Beyond," NDC Outlook no. 06-2024 (October 2024): 08, NATO Defense College, https://www.ndc.nato.int/news/news.php?icode=1971.
[35] Ulrich Pilster and Olesya Vinhas de Souza, "Inequality Kills: On Russian Combat Ineffectiveness in Ukraine and Beyond," NDC Outlook no. 06-2024 (October 2024): 08, NATO Defense College, https://www.ndc.nato.int/news/news.php?icode=1971.
[36] Sean Monaghan, Eskil Jakobsen, Sissy Martinez, Mathieu Droin, Greg Sanders, Nicholas Velazquez, Cynthia Cook, Anna Dowd, and Maeve Sockwell, Is NATO Ready for War? An Assessment of Allies' Efforts to Strengthen Defense and Deterrence since the 2022 Madrid Summit (Washington, DC: Center for Strategic and International Studies, 2024), 17–18, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-06/240611_Monaghan_Ready_War_0.pdf.
[37] Valerii Zaluzhnyi, "Automated Attrition: The Future of Warfare Is Here, and NATO Is Falling Behind," The Baltic Sentinel, November 11, 2024, https://balticsentinel.eu/8132828/automated-attrition-valerii-zaluzhnyi-the-future-of-warfare-is-here-and-nato-is-falling-behind.
[38] NATO ACT, "Allied Command Transformation's Role in the NATO Defence Planning Process," NATO Allied Command Transformation (ACT), accessed February 27, 2025, https://www.act.nato.int/allied-command-transformations-role-in-the-nato-defence-planning-process/.
[39] Ben Hall, "No European Defence Without Germany," Financial Times, March 8, 2025, https://www.ft.com/content/1930ae76-c728-436a-82d9-dd1731a6b678.
[40] Arnel P. David and Benjamin Jensen, "NATO and Prototyping Warfare," Center for Strategic and International Studies (CSIS), July 08, 2024, https://www.csis.org/analysis/nato-and-prototyping-warfare.
[41] NATO, "Allied Command Transformation's Role in the NATO Defence Planning Process," NATO Allied Command Transformation (ACT), accessed February 27, 2025, https://www.act.nato.int/allied-command-transformations-role-in-the-nato-defence-planning-process/.

[42] Tactics, Techniques, and Procedures (TTPs) refer to the standardized methods and practices used by military forces to achieve operational objectives. Tactics involve the specific maneuvers and strategies employed in combat, techniques describe the detailed execution of tasks within those tactics, and procedures outline the structured steps necessary to carry them out effectively. TTPs evolve based on battlefield experience, technological advancements, and adversary capabilities, ensuring adaptability in modern warfare.
[43] Elisabeth Gosselin-Malo, "Top NATO Commander Urges 'Sea Change' in Training, Deterrence, Spending," Defense News, December 26, 2024, https://www.defensenews.com/global/europe/2024/12/26/top-nato-commander-urges-sea-change-in-training-deterrence-spending/.
[44] Public-Private Partnerships (PPP) in the military context refer to cooperative agreements between government defence institutions and private sector companies to develop, procure, and sustain defence capabilities. These partnerships are increasingly used to integrate emerging technologies, enhance logistical resilience, and streamline procurement processes, but they also raise concerns about dependency on private industry for critical military functions, supply chain vulnerabilities, and cost efficiency in Large-Scale Combat Operations (LSCO). Large-Scale Combat Operations (LSCO) refer to high-intensity, conventional military conflicts between peer or near-peer adversaries, typically involving division- to corps-level formations across multiple domains (land, air, sea, cyber, and space). LSCO emphasises massed manoeuvre warfare, integrated joint operations, and sustained logistical support, contrasting with the counterinsurgency (COIN) and limited conflicts that have dominated Western military engagements since the early 2000s. The WarTech Nexus refers to the intersection of emerging and disruptive technologies, such as AI, autonomous systems, and cyber warfare, that are reshaping military strategy, force structures, and the conduct of modern warfare..
[45] Abraham H. Maslow, The Psychology of Science: A Reconnaissance (New York: Harper & Row, 1966), 15.
[46] Mikael Weissmann and Peter Ahlström, "Mirror, Mirror on the Wall, Who Is the Most Offensive of Them All? – Explaining the Offensive Bias in Military Tactical Thinking," Defence Studies 19, no. 2 (2019): 183–85, https://doi.org/10.1080/14702436.2019.1599287.
[47] Jacquelyn Schneider, "The Digital Cult of the Offensive and the US Military," Journal of Strategic Studies 48, no. 1 (2024): 36, https://doi.org/10.1080/01402390.2024.2376542.
[48] Jacquelyn Schneider, "The Digital Cult of the Offensive and the US Military," Journal of Strategic Studies 48, no. 1 (2024): 54-55, https://doi.org/10.1080/01402390.2024.2376542.
[49] Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) refers to an integrated military framework that enables decision-making, coordination, and situational awareness across multiple domains. It encompasses the technologies and processes used to collect, analyse, and disseminate information to enhance operational effectiveness, improve battlefield management, and support strategic planning in both conventional and asymmetric warfare.
[50] Alexander Schaebler, "Digging Into The Future: Or How I Learned To Love My Shovel," The Defence Horizon Journal, December 12, 2024, https://tdhj.org/blog/post/digging-manoeuvre/.
[51] Helene Cooper, "U.S. Drops 'Mother of All Bombs' on ISIS Caves in Afghanistan," New York Times, April 13, 2017, https://www.nytimes.com/2017/04/13/world/asia/moab-mother-of-all-bombs-afghanistan.html.
[52] International Committee of the Red Cross (ICRC), "Afghanistan/US: 'Mother of All Bombs,'" ICRC Casebook, accessed February 26, 2025, https://casebook.icrc.org/case-study/afghanistanus-mother-all-bombs.
[53] Colin S. Gray, Thucydides Was Right: Defining the Future Threat, (Carlisle, PA: U.S. Army War College Press, 2015), 16, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1457&context=monographs.
[54] AI-generated image, "Female Soldier Caught in Crosshairs While Threatened by a Giant Arachnoid," created by DALL·E, generated on February 27, 2025.
[55] Jason Shell, "How the IED Won: Dispelling the Myth of Tactical Success and Innovation," War on the Rocks, May 01, 2017, https://warontherocks.com/2017/05/how-the-ied-won-dispelling-the-myth-of-tactical-success-and-innovation/.
[56] Colin S. Gray, Thucydides Was Right: Defining the Future Threat, (Carlisle, PA: U.S. Army War College Press, 2015), 16-21, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1457&cont

ext=monographs.
[57] Lorenzo Zambernardi, “Counterinsurgency’s Impossible Trilemma,” Taylor & Francis, The Washington Quarterly 33, no. 3 (Summer 2010): 30–31, https://www.csis.org/analysis/twq-counterinsurgencys-impossible-trilemma-summer-2010.
[58] Raya Jalabi and Andrew England, “How Syria’s rebels became makers of drones and guided missiles,” Financial Times, December 2024, https://www.ft.com/content/aaa80cd0-d75e-41cf-811d-20e6ecd230f8; Africa Defense Forum, “Drones, Heavy Weapons Dominate DRC’s Fight with M23,” Africa Defense Forum, May 28, 2024, https://adf-magazine.com/2024/05/drones-heavy-weapons-dominate-drcs-fight-with-m23/.
[59] Raya Jalabi and Andrew England, “How Syria’s rebels became makers of drones and guided missiles,” Financial Times, December 2024, https://www.ft.com/content/aaa80cd0-d75e-41cf-811d-20e6ecd230f8; Africa Defense Forum, “Drones, Heavy Weapons Dominate DRC’s Fight with M23,” Africa Defense Forum, May 28, https://adf-magazine.com/2024/05/drones-heavy-weapons-dominate-drcs-fight-with-m23/.
[60] Marc Santora, Lara Jakes, Andrew E. Kramer, Marco Hernandez and Liubov Sholudko, “A Thousand Snipers in the Sky: The New War in Ukraine,” New York Times, March 3, 2025, https://www.nytimes.com/interactive/2025/03/03/world/europe/ukraine-russia-war-drones-deaths.html.
[61] Carlijn Janssen, “Why China’s UAV Supply Chain Restrictions Weaken Ukraine’s Negotiating Power,” Center for Strategic and International Studies (CSIS), December 2024, https://www.csis.org/analysis/why-chinas-uav-supply-chain-restrictions-weaken-ukraines-negotiating-power.
[62] Dwight D. Eisenhower, Farewell Address to the Nation, January 17, 1961, Eisenhower Presidential Library, https://www.eisenhowerlibrary.gov/research/online-documents/farewell-address.
[63] Arab News, “Saudi Arabia’s Defense Sector Expands with New Investments,” Arab News, February 04, 2024, https://www.arabnews.com/node/2453791/business-economy.
[64] Kingdom of Saudi-Arabia, “World Defense Show,” General Authority for Military Industries, accessed February 28, 2025, https://www.gami.gov.sa/en/world-defense-show.
[65] NATO, “Emerging and disruptive technologies,” North Atlantic Treaty Organization, accessed February 11, 2025, https://www.nato.int/cps/bu/natohq/topics_184303.htm.
[66] Sebastian Elbaum and Jonathan Panter, “AI Weapons and the Dangerous Illusion of Human Control,” Foreign Affairs, December 06, 2024, https://www.foreignaffairs.com/united-states/ai-weapons-and-dangerous-illusion-human-control.
[67] NATO, “‘To Prevent War, NATO Must Spend More’ Speech by NATO Secretary General Mark Rutte at the Concert Noble, Brussels,” North Atlantic Treaty Organization, December 12, 2024, https://www.nato.int/cps/en/natohq/opinions_231348.htm.
[68] Matt Kaplan and Michael Brown, “The Private Sector on the Front Line: Big Tech and the Risky Blurring of Commercial and Security Interests,” Foreign Affairs, January 31, 2025, https://www.foreignaffairs.com/united-states/private-sector-front-line.
[69] Helsing, “Helsing to Produce 6,000 Additional Strike Drones for Ukraine,” Helsing Newsroom, accessed February 26, 2025, https://helsing.ai/newsroom/helsing-to-produce-6000-additional-strike-drones-for-ukraine.
[70] David Hambling, “Elon Musk Calls F-35 Builders ‘Idiots,’ Favors Drone Swarms,” Forbes, November 26, 2024, https://www.forbes.com/sites/davidhambling/2024/11/26/elon-musk-calls-f-35-builders-idiots-favors-drone-swarms.
[71] Reuters, “Elon Musk’s US Department of Defense Contracts,” Reuters, February 11, 2025, https://www.reuters.com/world/us/elon-musks-us-department-defense-contracts-2025-02-11/.
[72] Elon Musk (@elonmusk), “Panel Talk at the Pentagon,” X (formerly Twitter), February 07, 2025, https://x.com/elonmusk/status/1887697653598757367.
[73] Joey Roulette and Marisa Taylor, “Musk’s SpaceX Is Building Spy Satellite Network for US Intelligence Agency: Sources,” Reuters, March 16, 2024, https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/.
[74] Elon Musk (@elonmusk), “Haha, FSD 9 beta is shipping soon, I swear! Generalized self-driving is a hard problem, as it requires solving a large part of real-world AI. Didn’t expect it to be so hard, but the difficulty is obvious in retrospect. Nothing has more degrees of freedom than reality.,” X (formerly Twitter), July 03, 2021, https://x.com/elonmusk/status/1411280212470366213.
[75] Michael Biesecker, Sam Mednick and Garance Burke, “Israel Uses AI in Military Operations Against Palestinians,” Associated Press (AP), February 18, 2025, https://apnews.com/article/israel-palestini-

ans-ai-technology-737bc17af7b03e98c29cec4e15d0f108.
[76] Gareth Jennings, "Luftwaffe Welcomes F-35 Nuclear Certification," Janes, March 13, 2024, https://www.janes.com/osint-insights/defence-news/defence/luftwaffe-welcomes-f-35-nuclear-certification.
[77] Several international customers of the F35A, such as Switzerland, India or the UAE have expressed doubts whether the weapons system can still operate effectively without the benevolence of the manufacturing nation and are considering stepping back from the contract, marking the F35A as a symbol of global American ambiguity.
[78] U.S. Government Accountability Office (GAO), Weapon System Sustainment: DOD Needs a Strategy for Re-Designing the F-35's Central Logistics System, GAO-20-316 (Washington, DC: GAO, 2020), 22-25, https://www.gao.gov/assets/gao-20-316.pdf.
[79] Office of the Director of National Intelligence (DNI), Future of the Battlefield, Global Trends 2040, 2021, https://www.dni.gov/index.php/gt2040-home/gt2040-deeper-looks/future-of-the-battlefield.
[80] Winston S. Churchill, Shall We All Commit Suicide? (London: Nash's Pall Mall Magazine, 1925), 190.
[81] Winston S. Churchill, Shall We All Commit Suicide? (London: Nash's Pall Mall Magazine, 1925), 184.
[82] Oleksiy Vasyliuk, "Military Fortifications in Ukraine: What Comes Next?" UWEC Work Group, January 29, 2024, https://uwecworkgroup.info/military-fortifications-in-ukraine-what-comes-next/.
[83] Theresa Sabonis-Helf, "The Electricity Front of Russia's War Against Ukraine," War on the Rocks, February 03, 2025, https://warontherocks.com/2025/02/the-electricity-front-of-russias-war-against-ukraine.
[84] Theresa Sabonis-Helf, "The Electricity Front of Russia's War Against Ukraine," War on the Rocks, February 03, 2025, https://warontherocks.com/2025/02/the-electricity-front-of-russias-war-against-ukraine.
[85] Roman Horbyk, "The War Phone: Mobile Communication on the Frontline in Eastern Ukraine," Digital War 3, no. 1–3 (2022): 9–24, https://doi.org/10.1057/s42984-022-00049-2.
[86] The Economist, "Fighting the War in Ukraine on the Electromagnetic Spectrum," The Economist, February 5, 2025, https://www.economist.com/science-and-technology/2025/02/05/fighting-the-war-in-ukraine-on-the-electromagnetic-spectrum.
[87] Theresa Hitchens, "Spurred by Ukraine War, 18 Western Countries Plan to Share Remote Sensing Data," Breaking Defense, February 15, 2023, https://breakingdefense.com/2023/02/spurred-by-ukraine-war-18-western-countries-plan-to-share-remote-sensing-data/.
[88] Rheinmetall, "Rheinmetall and ICEYE Are Supplying Ukraine with Satellite Imagery," Rheinmetall, November 11, 2024, https://www.rheinmetall.com/en/media/news-watch/news/2024/11/2024-11-11-rheinmetall-and-iceye-are-supplying-ukraine-with-satellite-imagery.
[89] Recent political comments made by the US administration and Elon Musk at the time of writing this essay highlight the risk of such arrangements, since both have the power to turn off the backbone of Ukrainian mobile communications at any moment.
[90] Robert Vincent, "Getting Serious About the Threat of High-Altitude Nuclear Detonations," War on the Rocks, September 23, 2022, https://warontherocks.com/2022/09/getting-serious-about-the-threat-of-high-altitude-nuclear-detonations/.
[91] Brian Gutierrez, "Why the U.S. Once Set Off a Nuclear Bomb in Space Called Starfish Prime," National Geographic, July 15, 2021, https://www.nationalgeographic.com/premium/article/why-the-us-once-set-off-a-nuclear-bomb-in-space-called-starfish-prime; Tony Phillips, "Starfish Prime: The First Accidental Geomagnetic Storm," Space Weather Archive, July 8, 2022, https://spaceweatherarchive.com/2022/07/08/starfish-prime-the-first-accidental-geomagnetic-storm/; European Space Agency (ESA), "The Kessler Effect and How to Stop It," ESA, accessed February 27, 2025, https://www.esa.int/Enabling_Support/Space_Engineering_Technology/The_Kessler_Effect_and_how_to_stop_it.
[92] AI-generated image, "Starfish Prime-Inspired Nuclear Detonation in Low Earth Orbit," created by DALL·E, generated on March 4, 2025.
[93] Jaganath Sankaran, "Russia's Anti-Satellite Weapons: An Asymmetric Response to U.S. Aerospace Superiority," Arms Control Today 52, no. 3 (March 2022), https://www.armscontrol.org/act/2022-03/features/russias-anti-satellite-weapons-asymmetric-response-us-aerospace-superiority.
[94] Malcolm Davis, "The Re-Emerging Threat of Orbital Nuclear Weapons," King's College London, March 07, 2024, https://www.kcl.ac.uk/the-re-emerging-threat-of-orbital-nuclear-weapons.

[95] Jon-Wyatt Matlack, “Analysis: Military Maneuvers—Mock Battles or Harbingers of War?” Federal Agency for Civic Education (BpB): Russia Analyses no. 417, https://www.bpb.de/themen/europa/russland-analysen/nr-417/507103/analyse-militaermanoever-scheinschlachten-oder-vorboten-des-krieges/.
[96] Jon-Wyatt Matlack, “Analysis: Military Maneuvers—Mock Battles or Harbingers of War?” Federal Agency for Civic Education (BpB): Russia Analyses no. 417, https://www.bpb.de/themen/europa/russland-analysen/nr-417/507103/analyse-militaermanoever-scheinschlachten-oder-vorboten-des-krieges/.
[97] Jon-Wyatt Matlack, “Analysis: Military Maneuvers—Mock Battles or Harbingers of War?” Federal Agency for Civic Education (BpB): Russia Analyses no. 417, https://www.bpb.de/themen/europa/russland-analysen/nr-417/507103/analyse-militaermanoever-scheinschlachten-oder-vorboten-des-krieges/.
[98] Dave Johnson, “Zapad 2017 and Euro-Atlantic Security,” NATO Review, December 14, 2017, https://www.nato.int/docu/review/articles/2017/12/14/zapad-2017-and-euro-atlantic-security/index.html.
[99] Kyle Mizokami, “NATO’s Real Problem: Germany’s Military Is Dying,” The National Interest, December 6, 2019, https://nationalinterest.org/blog/buzz/natos-real-problem-germanys-military-dying-102362.
[100] Tagesschau, “Bundeswehr Plans to Modernize Its Taurus Cruise Missiles,” Tagesschau, March 3, 2025, https://www.tagesschau.de/inland/innenpolitik/bundeswehr-taurus-modernisierung-100.html.
[101] Donald H. Rumsfeld, “Response to a soldier’s question about equipment shortages,” U.S. Department of Defense Town Hall Meeting, Camp Buehring, Kuwait, December 8, 2004. Transcript available at U.S. Department of Defense Archives.
[102] AI-generated image, “Female Soldier in Dropship Giving Thumbs-Up in 4:3 90s Sci-Fi Style,” created by DALL·E, generated on February 27, 2025.

10

FROM AN ENGINEERING PERSPECTIVE: SMALL DRONES AFFECTING THE COURSE OF WARFARE

KEVIN TEBBE, ROBERT POMMERANZ, RALF HEYNICKE, GERD SCHOLL

- **Author:** Captain Kevin Tebbe, M.Sc., Autonomous C-UAS UAS Swarms, 5G Cellular Communication.

  M.Sc. Robert Pommeranz; Autonomous C-UAS UAS Swarms, Computer Vision, Object Tracking.

  Major (Reserve) Dr.-Ing. Ralf Heynicke; Head of Laboratory; C-UAS UAS, Industrial Communication.

  Dr.-Ing. Gerd Scholl, Head of Chair for Electrical Measurement Engineering.

  The views contained in this article are the authors' alone and do not represent the official opinion of the German Armed Forces.

- **Abstract:** At least since the beginning of the most recent Russian invasion of Ukraine and the massive use of unmanned aerial vehicles, it has become imperative to elaborate potential countermeasures, that is, counter-unmanned aerial systems. Accordingly, based on past and ongoing conflicts – including the war in Ukraine – this paper analyses the impact of technological changes on warfare. Specifically, it takes a closer look at the types of unmanned aerial vehicles deployed on the modern battlefield and how critical infrastructure, soldiers and civilian populations could be protected in the face of these novel threats.

- **Problem statement:** How can advancements in electronic and electrotechnical components contribute to the development of effective countermeasures against emerging asymmetric threats?

- **Bottom-line-up-front:** UAVs, commonly called drones, are fundamentally changing the requirements for suitable military countermeasures. The speed at which attacking drones are developed can be measured in months — a time horizon significantly shorter than that of traditional military-strategic planning and procurement processes. Moreover, soldiers must learn how to use the new systems in a fast-changing environment in a very limited time.

- **So what?:** The diversity of technical disciplines such as AI, cybersecurity, electronic warfare, and necessary robustness requires close cooperation between government agencies, defence contractors, academic institutions, and military stakeholders to significantly accelerate the development and procurement process of counter-UAV technology.

Disruptive Technology

The barriers to entry for operating a UAV (Unmanned Aerial Vehicle) have decreased significantly over the years. Falling prices and comprehensive assistance systems offer even beginners a rapid learning curve to perform flight manoeuvres. As such, UAVs are no longer reserved exclusively for model-building experts. Major players in the drone market ensure that professionals, hobbyists, and technology enthusiasts have access to UAVs.[1] This simplified and uncontrolled access to UAVs is increasing disruption of the lower airspace in the civilian sector, albeit with a growing utility in military operations. The associated risks are significant, as UAVs can potentially penetrate sensitive areas. Typical incidents in the civilian sector may include intrusion or overflight of airports, industrial facilities, correctional institutions, barracks, military training grounds, and many other particularly protected buildings or areas. These incidents pose a challenge to air safety and raise significant legal and ethical questions that are becoming increasingly relevant in today's society. Since the beginning of Russia's invasion of Ukraine in 2022, UAVs have increasingly come into focus in modern warfare. A well-known quote from Lieutenant Colonel Thomas R. Stone (U.S. Army Field Artillery) illustrates this approach: „Never send an infantryman where you can send an artillery shell".[2]

In this context, an artillery shell or projectile can metaphorically be a UAV. Historically, UAVs have been used in warfare for many years. The U.S. Air Force has been using Unmanned Aerial Systems (UAS), such as the RQ-1 Predator from General Atomics Aeronautical Systems, since 1997.[3] Today, small UAVs are being used in various conflicts, showing that they can not only carry out reconnaissance missions but also destroy infrastructure or even armoured military vehicles with minimal effort. Affordable, Commercial-Off-The-Shelf (COTS) hardware, which has seen no significant technological advancements in recent years, is now in direct competition with the most advanced military technology.

Effects on Warfare

Both reconnaissance and offensive UAV-based operations, such as airdropping bombs or missiles or kamikaze attacks, come with inherent risks, including detection by enemy forces, electronic countermeasures, or mission failure due to technical malfunctions. Therefore, it is important to understand the capabilities of UAVs and how they can be used in both offensive and defensive warfare. UAVs are either very fast and agile or fast and more stable, depending on payload requirements. The agility of a UAV is determined by its size, weight and construction.[4] They are divided into four categories — fixed-wing, single-rotor, multirotor and fixed-wing hybrid.[5,6] Typical ranges for fixed-wing operations range from 500 km to over 1000 km.[7] Multirotors, which are more agile than fixed-wing UAS, can operate up to several kilometres (e.g., DJI specifies ranges between 13 km and 35 km).[8]

UAV Type	Number of Propellers	Number of Layers	Example
Fixed-Wing	1-n	1-n	Fly Dragon FDG-23 VTOL
Quadcopter	4	1	DJI Mini 4 Pro
Hexacopter	6	1-2	PM X6 Pro
Octocopter	8	1-2	DJI Agras MG-1

Example of different UAV types depending on the number of propellers and layers; Source: Author.

The “layers” mentioned in Column 3 of Table 1 refer to the arrangement of motors horizontally, without any height difference. If, for example, two motors are installed one above the other, this is referred to as two layers (as is the case with octocopters). The different UAV types come with specific advantages and disadvantages. The manoeuvrability of a multirotor is much better than that of fixed-wing aircraft. On the other hand, fixed-wing aircraft are much more efficient, resulting in improved flight duration and payload.

UAVs can also be used as loitering munitions via kamikaze attacks or dropping explosives on a target. In addition, the offensive use of UAVs to gather intelligence while psychologically harming the enemy through their mere presence should not be overlooked. In the civilian sector, UAVs declared offensive are mostly used for surveillance, spying on people or objects or smuggling goods.[9,10]

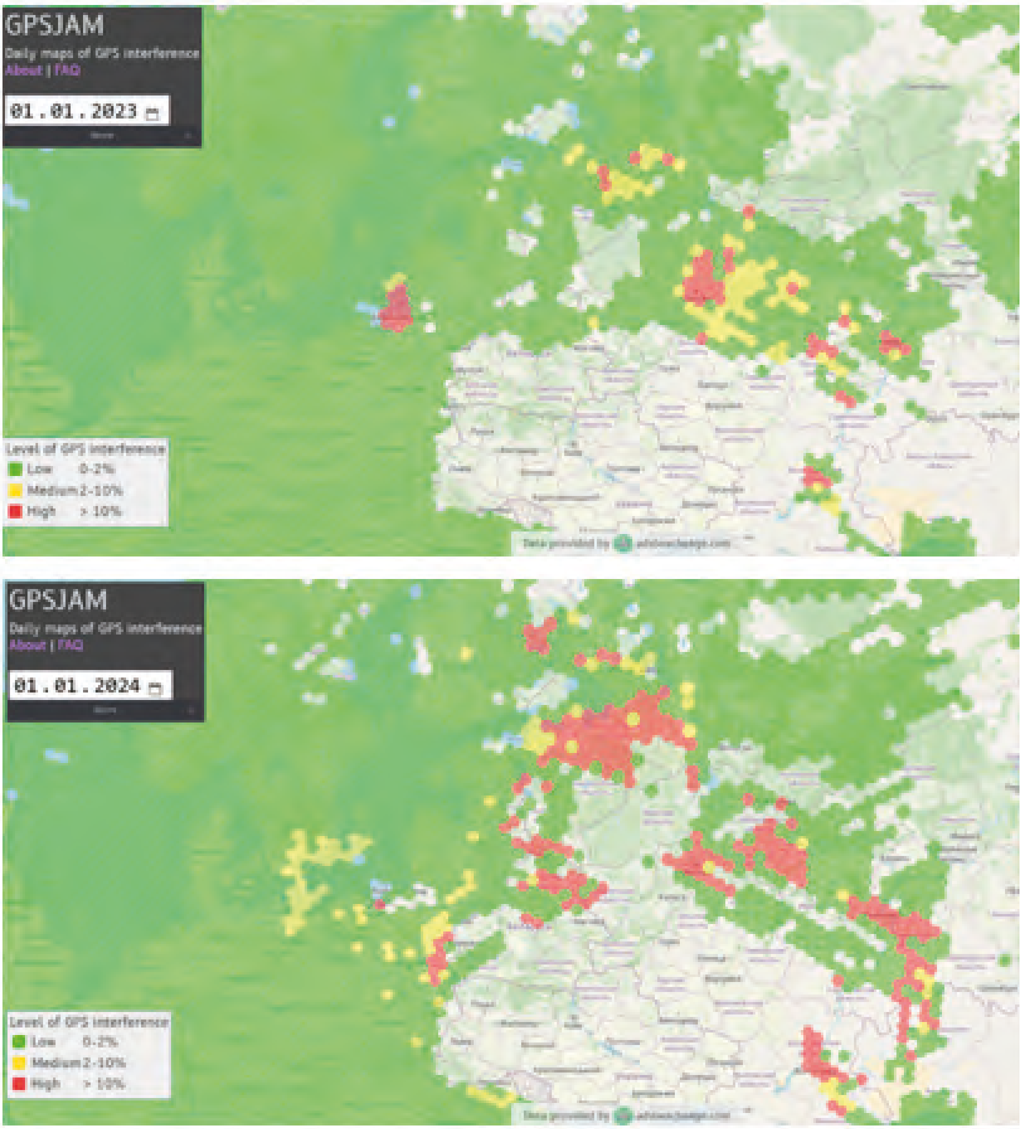
DIY FPV UAV with explosive.[11]

The operational efficiency and standard functional capability of nearly all UAVs are significantly influenced by environmental factors (i.e., temperature, wind, and light). Further, most UAVs use at least one Global Navigation Satellite System (GNSS). The DJI Mavic UAV serves as an example of a standard COTS product; the highest tolerable flight conditions are listed below:[12]

Max Wind Speed	29-38 kph (level 5 wind)
Max Flight Time	27 minutes (no wind at a consistent 25 kph)
Max Total Travel Distance (One Full Battery, No Wind)	13 km (no wind)
Operating Temperature Range	0° to 40° C
Battery	3830 mAh / LiPo 3S

Overview of technical specifications from a general-purpose COTS-UAV, represented by DJI Mavic.

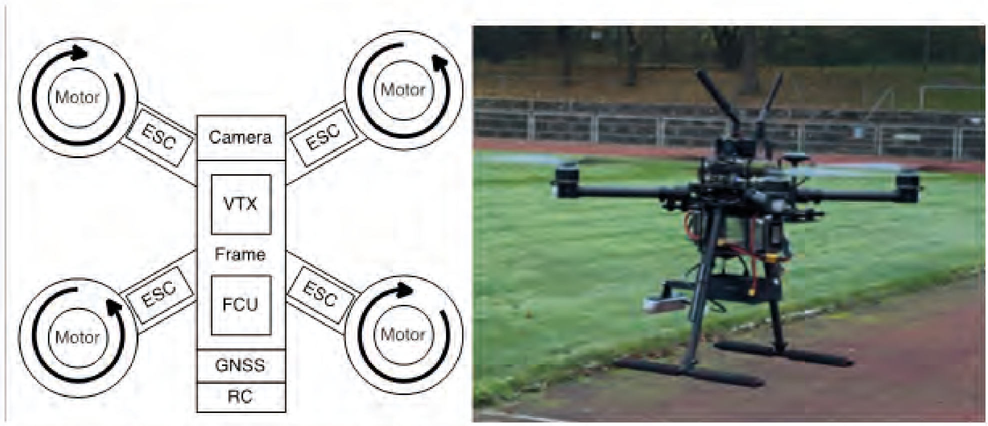
A GNSS is used to determine the position (longitude, latitude, and altitude) of targets. In principle, the receiving device (i.e., the UAV) must receive signals from at least four different satellites simultaneously to determine the three positional factors in Euclidean space along with the timing offset. Each GNSS satellite is equipped with a precise atomic clock, and the satellite transmits its local time when the signal was sent and its exact position in space (ephemeris data) at that time. As data is transmitted at the speed of light, the receiver can determine the distance to each satellite by calculating the time it took for the signal to travel.[13] However, threat techniques, such as jamming, can be used to manipulate the link between the UAV and the satellite system. Jamming means that the GNSS signal is interfered with by a signal in the same frequency band at a much higher power. Since 2022, the GPSJAM website has visualised GPS interference (i.e., jamming, spoofing, atmospheric conditions, etc.) based on aircraft reports on the accuracy of their navigation systems.[14]



GPS Interferences in North, East and Central Europe in 2023 and 2024, respectively. Note: The border regions of Russia are clearly jammed in 2024.[15]

State-of-the-Art Drone Technology

The components of a UAV are mostly identical regardless of the UAV type. A basic UAV consists of a frame, motors, propellers, a battery, a flight control unit (FCU), a camera, and a remote control.



Schematic structure and prototype UAS implementation built by the Chair of Electrical Measurement Engineering, Helmut-Schmidt University, University of the Federal Armed Forces Hamburg; Source: Author.

In recent years, UAVs have become increasingly sophisticated, with advancements in sensors and artificial intelligence (AI) leading to enhanced navigational precision in disturbed environments and areas with radio interference. It is important to note that flight controllers are designed to perform a consistent function: maintaining the flight path of a UAV by utilising onboard sensors, such as the inertial measurement unit, to control the individual motors through electronic speed controllers. Research projects, as well as the prevailing trend, are moving towards connecting additional high-performance computers to the flight controller for taking over computationally intensive algorithms (e.g., camera tracking, collision avoidance, simultaneous localisation and Mapping, and radio frequency (RF) sniffing) and controlling the FCU.[16,17]

Another trend born out of necessity, which could be considered a technological step backwards, offers an enormous advantage on the battlefield, namely, the use of fibre optics as a transmission medium for controlling the UAV and transmitting video signals.[18,19] The concept of utilising fibre-optic controlled UAVs, or, more specifically, wired UAVs, can be traced back to the principle of guiding missiles by sight via a wire, called Manual Command Line of Sight (MCLOS) systems.

FPV UAV equipped with fibre optics.[20]

For example, a First-Person-View (FPV) UAV's bottle-like cartridge is unwound during flight by the pull of the forward movement, thus preventing the fibre from becoming entangled around obstacles, such as trees and branches, making agile flight manoeuvres possible. The supplier specifies the tensile strength of the optical fibres as 50 N, which equates to approximately 5.1 kg.[21] The primary benefit of wired drones is that they are imperceptible in the RF spectrum, thus precluding the possibility of interference. Specifically, the synergy of their high velocity with their detectability, solely through high-performance ground-based sensor systems (e.g. cameras operating in the visual and infrared spectrum, RADARS, and LIDARS), renders these systems remarkably efficacious and hazardous.

In general, UAV simulators are a great way to safely learn how to fly a UAV. They are cheap, easy to learn, and offer a realistic flight experience — even with the ability to modify the weather, time, and most importantly, the setup of the UAV (i.e., battery type, motors, propellers, frame, etc.). A vital consideration in the utilisation of a simulator pertains to not only the economic dimension, encompassing minimal hardware expenditure, but also the imperative of safeguarding against hardware degradation resulting from crashes.

Simulator	**Release Date**	**Price (USD) (One-Time Payment)**	**Number of Users online (All-Time-Peak / Date)**
The Drone Racing League Simulator	Nov 2017	8.56	421 (Feb 2020)
Velocidrone	2016	21.41	No Data
Liftoff	Sep 2018	20.97	824 (Feb 2024)
FPV Kamikaze Drone	Dec 2023	4.18	355 (Aug 2024)
FPV.SkyDive	May 2021	Free	238 (Feb 2025)
TRYP FPV	June 2022	17.30	234 (July 2024)

Comparison of some FPV-UAV simulators.[22]

The availability of a suitably powerful computer with the necessary control input (i.e., a controller) is a prerequisite for using a simulator. This can be any console controller (e.g., PlayStation, Xbox, etc.) or a professional remote control (e.g. Radiomaster Pocket or Spektrum DX18), which will function as an input medium. Following the military principle of ‚ train as you fight', it is recommended to start training with a professional remote control as it allows for much more precise and finer inputs. Still, it can also be customised to the pilot's needs.

Illustration of some hobby and professional remote controllers (From left: Sony Playstation, Herelink, Radiomaster Pocket, Spektrum DX18); Source: Author.

COUNTER-UAS

Defence against UAVs requires a comprehensive system capable of detecting targets over several kilometres to initiate early defence mechanisms like starting an interceptor UAS or using stationary systems. All mechanisms can be divided into soft kill mechanisms, like catching, jamming, and spoofing, or hard kill mechanisms like destroying or damaging targets to impair their flying ability. The great variety of UAV types presents significant challenges to defence systems, necessitating the integration of diverse sensors to facilitate seamless integration into an existing infrastructure. This integration is of paramount importance for the effective utilisation of these systems in both military and police environments. Most systems available on the market rely primarily on ground-based systems that use radars, cameras, and RF components. For instance, a machine gun mounted on a platform or an antenna with strong directional characteristics can be utilised. Another approach is using UAS to defend against smaller UAS (sUAS). Utilising a flying system confers numerous advantages, chief among them being the attainment of high flexibility and mobility. Moreover, especially for civil environments or where hard-kill solutions are prohibited, such a system facilitates the capture of a target using a net, which can then be transported away in a predefined manner. This aspect assumes particular significance when explosives are attached to the unauthorised system.


Argus Interception Interceptor Drone with 3 Netguns.[23]

There is no single solution to solve or cover all threats from UAVs in the civilian or military sector, as the development of defence systems is inherently incapable of keeping pace with the rapidly evolving attack vectors.

UAS IN THE UKRAINE-RUSSIA WAR

The Shahed 136, built by an Iranian company called Iran Aircraft Manufacturing Industrial Company, is estimated to have an approximate range of 6-12,5 hours. This fixed-wing aircraft has already been deployed in Yemen and under the name Geran-2 in Ukraine. Equipped with an explosive warhead weighing up to 50 kg, this system is very difficult to detect using existing systems like Iron Dome or David's Sling due to a low radar cross-section and its low speed of only 50 m/s to 67 m/s and a resulting smaller Doppler shift compared to classic guided missiles with a speed of Mach 3 or 1029 m/s.[24]

Initially, COTS UAS, such as the DJI Mavic 3, were employed as reconnaissance vehicles, but with minimal adjustments and the use of 3D-printed attachments, explosives such as hand grenades have also been deployed from the air. In addition to COTS UAS, the utilisation of self-built, so-called DIY UAVs is on the rise owing to their remarkably higher agility and speed. The open-source community of FCUs, coupled with the flexibility offered by the components, has led to a surge in their adoption. The COTS UAS predominantly converts control and video signals through 2.4 GHz or 5.8 GHz frequencies. However, depending on the country code and the UAS software, certain channels or entire frequency bands are automatically deactivated. While these digital systems incur significantly higher costs than their analogue alternatives, they offer the advantage of encrypted communication. The FPV UAS, colloquially referred to as racing drones, employ analogue video transmission with fibre optics to ensure interference-free and tamper-proof transmission. Consequently, within Ukraine, there has been a notable increase in the usage of homemade FPV UAS equipped with fibre optics.

Military Mindset

UAVs, as a growing asymmetric threat, must be addressed as a core component of basic training for soldiers. While advanced countermeasure techniques remain system-specific and, therefore, only part of the special training for specialised units, general awareness and response protocols should be embedded in the basic training of all soldiers. Given the broad spectrum of UAV applications, training curricula must account for both COTS-UAVs, such as those produced by DJI, and DIY-UAVs. The duration of the learning process depends on the specific and desired type of operation.

Comparison of two quadcopters – DJI Mini 4 Pro and a 5-inch custom-built UAV. Source: Author.

There are two approaches to the operation of a UAV. First, there is the option of conducting a training program in a simulator and attending flying lessons afterwards. Second, there is the option of attending only flying lessons. From the experience gained, it can be deduced that a COTS UAV equipped with auxiliary functions, such as collision avoidance, renders it possible to commence flight operations immediately without the prerequisite of prior experience.

Compared to COTS-UAVs, operating an FPV UAV needs slightly more training and experience, depending on the mission. The risk of a crash is elevated to a considerable degree in the former case due to the absence of software support, thus necessitating flight operations in a simulator. Military equipment and training can be very expensive for traditional weapons and vehicles like tanks or fighter jets. However, using a simulator with minimal hardware requirements to train soldiers in drone usage can save a lot of money and time. The running costs of a simulator are negligibly low, which makes it perfect for training purposes. The average cost of a UAV is around 500 USD, and the remote is between 50 and 200 USD. The military training inside simulators can practically be anywhere and anytime – there is no need for a big training area or lots of equipment.

The learning curve of a simulator is very steep. Even if there is no experience of flying an FPV-UAV, most simulators offer a tutorial to get started. Due to realistic physics and the ability to modify the controls, the user can learn how to fly a UAV quickly.[25] Personal experience shows that an FPV-UAV can be kept safely in the air after just a few hours (approx. 2-3 hours) of practice in the simulator. Agile, acrobatic flight manoeuvres in urban terrain, however, require significantly longer periods of practice, ranging up to an estimated simulator time of over 50 hours.

Another significant advantage of a simulator is the immersive virtual experience of being on the battlefield, which it recreates without any associated risks. The integration of advanced graphics, a diverse array of maps, and a range of tasks, including races, freestyle, airdrops, and kamikaze, enhances this immersive experience.

A still of footage from an FPV Kamikaze Drone Simulator.[26]

SENSITISING

With dimensions ranging from that of a human fist up to a wingspan spanning several meters, UAVs are characterised by their speed and elusiveness, rendering reconnaissance without sensor-supported systems virtually impossible. It is also necessary to emphasise the importance of safeguarding critical infrastructures, including command posts, positions, and radio relay stations. The demand for robust safeguarding becomes even more urgent in light of the evolving threat landscape–particularly the increasing incidence of UAV intrusions, which necessitate timely and effective response strategies. The importance of such protection extends beyond the battlefield, encompassing military training areas, critical infrastructures, and industrial facilities in peacetime. Ensuring the security of these entities is vital to protect against potential interference, espionage, and disruption.

Contrary to being self-evident, this observation highlights a critical and often underestimated challenge in contemporary airspace monitoring. The combination of reduced visual signature, high manoeuvrability, and low-altitude operation significantly impairs human detection capabilities, even under optimal visual conditions. This underscores the necessity for advanced detection systems beyond human perception.

CHANGES IN WARFARE

Military deployment of UAVs has changed the way wars are fought. The Russia-Ukraine War has demonstrated that the threat posed by UAVs is ubiquitous. Specifically, deploying the most economical UAVs, estimated to cost between 300–400 USD, in conjunction with the adept installation of a mount or an airdrop mechanism, is sufficient to destroy several million USD worth of armour.[27]

FPV UAV Destroying T-90 Tank.[28]

Having a small, highly agile, and fast UAV paired with a stabilised, high-resolution camera in the air is a key tool in warfare in terms of artillery spotting, enemy movement tracking, and even target acquisition. Furthermore, UAVs have transformed the transportation of ammunition, food, and medical supplies to soldiers in the field, cutting delivery times significantly.[29]

In contemporary military operations, the prevalence of one-to-one attacks, and on occasion, one-to-a-few individual targets, is common. This phenomenon can be attributed, in part, to the constrained carrying capacity and flight duration of a solitary UAS, which comprises a UAV along with its supporting equipment, such as a ground control station and communication links. It is postulated that the future of UAS-supported warfare will be characterised by a symbiotic integration of drones operating in air, ground, and water domains. The capabilities of individual UAS have been demonstrated in a range of conflicts. The consequences of deploying multiple UAVs as a swarm, utilising AI-supported analysis to identify vulnerabilities and allocate targets, are of particular concern. The prospect of a swarm of autonomously operating , search heads' poses a significant threat.

UAV Swarm starting from a ship.[30]

The effectiveness of C-RAM (Counter Rocket Artillery and Mortar) systems in providing adequate defence against such threats is a matter of concern. The difference in projectile and missile trajectory prediction vis-a-vis UAVs is due to the former's ballistic curve trajectory, whilst the latter's ability to move in all directions during flight makes prediction difficult. When combined with AI-supported control, this ability enables UAVs to move randomly on a given flight path.

Conclusion and Outlook

In modern conflicts, both sides – the attacker and defender – must cope with rapidly evolving warfare owing to UAVs being deployed in different use cases. The chance of success in using a UAV for offensive purposes is significantly higher than that of intercepting or defending against a single UAV, not to mention swarms of UAVs. Developing and researching defence mechanisms is a more difficult and costly process than adapting existing systems and exploiting long-established sensor and actuator technology, in conjunction with the substantial wealth of information available on the internet.

The contemporary generation of drones is derived from the sports sector of racing drones. These drones are neither robust nor designed for adverse environments; they are engineered to be extremely light and fast. However, should the military make significant investments in swarm intelligence to develop robust, military UAS, then the prospect of a completely autonomous UAS swarm, integrated into a command-and-control system, becomes a realistic possibility. Such a swarm could be deployed as part of a networked battlefield on land, at sea or in space, with the capability of detecting and destroying tactical targets.

Individual components are effectively standardised and can be assembled into a functioning UAV and operated without a great deal of prior knowledge. However, the main challenge in the future will be creating supply chains for components so that there is little dependence on individual manufacturers.

Additionally, the focus has now shifted from optimising hardware in terms of weight, speed, endurance, and agility to developing software increasingly dependent on AI to reliably facilitate automated or autonomous missions in the most adverse environments. On the C-UAS side, these advances need to be implemented in a system that uses multi-sensor and (multi-) actuator technology to prevent imminent attack vectors.

This is why, for example, the Chair of Electrical Measurement Engineering at the University of the Federal Armed Forces Hamburg has focused on the development of an air-based multi-sensor system for drone defence as a basic concept to cope with a variety of different drone types and threats. It can be easily deployed for military and civil applications using private 5G mobile radio as a robust swarm communication system. Furthermore, AI-based detection and classification, primarily using cameras instead of RADAR sensors, make the system invisible to the electromagnetic reconnaissance of hostile observers. The system will also be enhanced to operate in GNSS-denied environments.

Nevertheless, several limitations of the current system architecture must be acknowledged. While advantageous in terms of electromagnetic signature reduction, the exclusive reliance on electro-optical sensors for detection and classification inherently constrains operational effectiveness under suboptimal environmental conditions, such as low illumination, adverse weather, or high-contrast background scenarios. Furthermore, the operational resilience and security of private 5 G-based swarm communication networks in electronically contested or degraded signal environments have not yet been comprehensively validated. In light of these constraints, future research should prioritise the multimodal fusion of heterogeneous sensor data, incorporating passive RF sensing, thermal imaging, and acoustic signatures to enhance detection robustness across diverse environmental conditions. Additionally, systematic evaluation of the GT communication layer under simulated electronic warfare scenarios is essential to assess its viability in contested domains. Further efforts should also be directed toward developing advanced onboard autonomy for distributed decision-making and systematic system performance assessment in GNSS-denied and spoofed environments, to ensure operational integrity and mission resilience.

Endnotes

[1] "Drohnen - Deutschland | Statista Marktprognose," Statista, accessed December 13, 2024, https://de.statista.com/outlook/cmo/consumer-electronics/drohnen/deutschland.
[2] "Never Send an Infantryman Where You Can Send an Artillery Shell," accessed December 13, 2024, https://apps.dtic.mil/sti/citations/ADA089419.
[3] "General Atomics Aeronautical Systems RQ-1 Predator," National Museum of the United States Air ForceTM, accessed December 13, 2024, https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/196333/general-atomics-aeronautical-systems-rq-1-predator/https%3A%2F%2Fwww.nationalmuseum.af.mil%2FVisit%2FMuseum-Exhibits%2FFact-Sheets%2FDisplay%2FArticle%2F196333%2Fgeneral-atomics-aeronautical-systems-rq-1-predator%2F.
[4] "Power and Weight Considerations in Small, Agile, Quadrotors | Request PDF," ResearchGate, October 22, 2024, https://doi.org/10.1117/12.2051112.
[5] "Drone Types: Multi-Rotor, Fixed-Wing, Single Rotor, Hybrid VTOL," November 08, 2016, https://www.auav.com.au/articles/drone-types/.
[6] Wilfried Yves Hamilton Adoni et al., "Investigation of Autonomous Multi-UAV Systems for Target Detection in Distributed Environment: Current Developments and Open Challenges," Drones 7, no. 4 (April 2023): 263, https://doi.org/10.3390/drones7040263.
[7] "Skyeye Long Range Fixed Wing UAV Drones SM200G," Skyeye UAV, accessed April 22, 2025, htt-

ps://www.skyeyeuav.com/products/skyeye-long-range-fixed-wing-uav-drones-sm200g.
[8] "DJI Matrice 4 Serie - Technische Daten," DJI, accessed March 31, 2025, https://enterprise.dji.com/de/matrice-4-series/photo.
[9] Riham Altawy and Amr M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey," ACM Trans. Cyber-Phys. Syst. 1, no. 2 (November 09, 2016): 7:1-7:25, https://doi.org/10.1145/3001836.
[10] "Schwerer Verlust für Russland: T-90-Panzer zerstört – Video zeigt Angriff," October 27, 2023, https://www.fr.de/politik/kamikaze-drohne-ukraine-krieg-russland-verluste-panzer-t90-zerstoert-waffen-angriff-zr-92638194.html.
[11] "Paratroopers of the 79th Air Assault Brigade Received FPV Drones and Warheads from Volunteers," Militarnyi (blog), accessed February 24, 2025, https://mil.in.ua/en/news/paratroopers-of-the-79th-air-assault-brigade-received-fpv-drones-and-warheads-from-volunteers/.
[12] "Mavic Pro - Produktinformationen - DJI," DJI Official, accessed March 03, 2025, https://www.dji.com/de/mavic/info.
[13] "GPS-Compendium_Book_(GPS-X-02007).Pdf," accessed March 3, 2025, https://content.u-blox.com/sites/default/files/products/documents/GPS-Compendium_Book_%28GPS-X-02007%29.pdf.
[14] "GPSJAM GPS/GNSS Interference Map," accessed March 31, 2025, https://gpsjam.obliscence.com/.
[15] "GPSJAM GPS/GNSS Interference Map."
[16] Nils Tijtgat et al., "Embedded Real-Time Object Detection for a UAV Warning System," in 2017 IEEE International Conference on Computer Vision Workshops (ICCVW) (2017 IEEE International Conference on Computer Vision Workshop (ICCVW), Venice: IEEE, 2017), 2110–18, https://doi.org/10.1109/ICCVW.2017.247.
[17] Michael Mugnai et al., "An Efficient Framework for Autonomous UAV Missions in Partially-Unknown GNSS-Denied Environments," Drones 7, no. 7 (July 2023): 471, https://doi.org/10.3390/drones7070471.
[18] David Hambling, "Russian Fiber Optic Drone Beats Any Jammer (UPDATE: Ukraine Version)," Forbes, accessed February 27, 2025, https://www.forbes.com/sites/davidhambling/2024/03/08/russian-fiber-optic-drone-can-beat-any-jammer/.
[19] "The Ministry of Defence showcased FPV | MoD News," January 02, 2025, https://mod.gov.ua/en/news/the-ministry-of-defence-showcased-fpv-drones-controlled-using-fiber-optics-to-the-armed-forces-of-ukraine.
[20] "The Ministry of Defence showcased FPV | MoD News."
[21] "UAV Optical Fiber Communication, Optical Fiber Communication FPV," Skywalker technology, accessed February 27, 2025, https://skywalkerfpv.com/.
[22] "Comparing Charts for 6 Apps," SteamDB, accessed February 25, 2025, https://steamdb.info/charts/?compare=410340,641780,1278060,1682970,1881200,2707940.
[23] "Die innovative Abfangdrohne von Argus Interception, accessed February 25, 2025, https://argus-interception.com/de/"
[24] "Ukrainian AN-196 Liutyi Drone, Dubbed 'Ukrainian Shahed,' Receives Major Upgrade," UNITED24 Media, November 25, 2024, https://united24media.com/latest-news/ukrainian-an-196-liutyi-drone-dubbed-ukrainian-shahed-receives-major-upgrade-3996.
[25] Dante Tezza, Denis Laesker, and Marvin Andujar, "The Learning Experience of Becoming a FPV Drone Pilot," in Companion of the 2021 ACM/IEEE International Conference on Human-Robot Interaction, HRI '21 Companion (New York, NY, USA: Association for Computing Machinery, 2021), 239–41, https://doi.org/10.1145/3434074.3447167.
[26] "Sparen Sie 50% bei FPV Kamikaze Drone auf Steam," accessed March 05, 2025, https://store.steampowered.com/app/2707940/FPV_Kamikaze_Drone/.
[27] "Schwerer Verlust für Russland."
[28] Defence of Ukraine [@DefenceU], "The Occupiers Are Quite Proud of Their T-90 Tanks. Watch How One of Them Is Destroyed by a Ukrainian FPV Drone. Asgard Group Https://T.Co/A9YeK9unPd," Tweet, Twitter, October 24, 2023, https://x.com/DefenceU/status/1716899863525552446.
[29] Typoheads GmbH, "Von Drohnen und Panzern: Zehn Fragen an Oberst Markus Reisner," May 14, 2024, https://www.bundesheer.at/aktuelles/detail/von-drohnen-und-panzern-zehn-fragen-an-oberst-markus-reisner.
[30] The Future of Warfare | Palantir, 2024, https://www.youtube.com/watch?v=UiiqiaUBAL8.

11

THE ULTIMATE HUMAN-MACHINE FUSION?

BERNHARD SCHULYOK, KATHARINA-FRANZISKA ZEMAN

- **Author:** Bernhard Schulyok has research interests in Security Policy and Military Capability Development. He has written three handbooks and numerous individual articles in the journal "Truppendienst" and in the online journal "The Defence Horizon Journal". He was the National Director of the multinational platform Military Capability Development Campaign (MCDC) for over seven years until March 2025.

  Katharina-Franziska Zeman is deeply interested in the intersections of cognition, security policy, and emerging technologies. With experience in the public sector, she has worked on diverse topics, focusing on modern technologies' societal and security impacts. Her interdisciplinary approach blends innovative perspectives with in-depth analysis.

  The views contained in this article are the authors' alone and do not represent the views of the Austrian Federal Ministry of Defence.

- **Abstract:** AI-powered autonomous weapons, from advanced drones to robotic soldiers, are reshaping warfare with unmatched speed, precision, and adaptability. Capable of life-and-death decisions, they deliver tactical power and coordination, reducing human risk and amplifying military strength. Intelligent swarming and real-time responses provide a formidable combat edge. However, robust controls are crucial to wield these tools responsibly, to shape the future of warfare with strategic brilliance and caution.

- **Problem statement:** How can society, with the military as a part of it, retain control and dominance over AI-driven systems powered by self-learning algorithms while leveraging their advantages?

- **Bottom-line-up-front:** Autonomous weapons driven by AI are set to dominate future warfare, offering unmatched tactical power, rapid decision-making, and life-or-death autonomy. While promising reduced human risk and unprecedented speed, they also present critical challenges in control and accountability. For military forces to fully harness these tools, robust oversight is essential to prevent unintended consequences and ensure strategic goals are met without compromising human judgment.

- **So what?:** Military forces must implement robust control and oversight mechanisms to deploy AI and AI-driven autonomous weapons effectively. Additionally, military leadership must be highly attuned to the influence of AI on social media, recognising its potential to shape behaviour. This responsibility to ensure the ethical and strategic use of AI while safeguarding human judgment and accountability lies with military leaders, policymakers, and international organisations. The solution to this challenge is found in the optimal integration of human intelligence with machine precision—a concept increasingly known as „Human-Machine Teaming".

„Weak human + machine + better process is superior to strong human + machine + inferior process."[1] (Garry Kasparov)

The fusion of human intellect and machine efficiency revolutionises modern warfare, blending cognitive brilliance with mechanical precision. This transformation spans three key areas: First, human enhancement through technologies like EEG interfaces and adaptive displays, which boost perception, cognition, and decision-making, raising ethical and technical concerns. Second, the rise of autonomous drones and swarm systems. These enhance battlefield efficiency but pose risks in control, accountability, and cybersecurity. Third, AI-driven social media manipulation, which threatens to reshape geopolitics by influencing mass behaviour. This shift calls for strict regulation, human oversight, and education to prepare forces for the challenges of technology-driven warfare. These developments are not merely theoretical—they are already playing a decisive role in modern conflicts. As technological advancements transform the battlefield, they simultaneously reshape the geopolitical landscape.

Citius, Altius, Fortius

The Olympic motto of „Faster, Higher, Stronger" captures the technological race for dominance. As Russian President Vladimir Putin stated in 2017, „The leader in artificial intelligence will be the ruler of the world."[2] He warned against monopolistic control of AI and promised Russia would share its expertise, though this now seems unlikely.[3] Putin also predicted future wars would be fought by drones, asserting that „when one party's drones are destroyed by drones of another, it will have no other choice but to surrender."[4]

This race for AI dominance extends beyond military technology and rests on four key pillars: data, computing power, talent, and institutions. As Paul Scharre outlines in Four Battlegrounds, data is the defining resource of the 21st century. Akin to coal or oil, it must be collected and refined. Computing power drives AI development, with control over global chip supply chains offering strategic leverage. Talent determines which nations attract top researchers and tech firms. Yet the most critical factor is institutions—the global AI leader will be the one that seamlessly integrates AI into its economy, society, and military.[5]

In the Russia-Ukraine war, drones play a crucial role but are not the sole determining factor. Other elements, such as resistance, combined arms warfare, and the ability to coordinate large formations beyond the brigade level, are key. The absence of operational capabilities at the corps and division levels is particularly notable.[6] Operational competence and training are essential—without them, advanced weapon systems are ineffective.[7]

Both sides are rapidly adapting to new technologies. Drones are now being developed and modified at a breakneck pace—if enemy electronic warfare disrupts controls, alternatives like fibre-optic guidance are deployed.[8] Innovations move from concept to deployment within weeks or months, not years. In Ukraine, domestic prototypes are quickly field-tested and mass-produced until further refinements are needed.

Current conflicts—whether in Ukraine or the Middle East—also demonstrate a growing prevalence of autonomous and semi-autonomous (weapon) systems.[9] The concept is compelling: a weaponised drone (UAV) worth a few hundred dollars loiters in the airspace, waiting for a multi-million-dollar armoured vehicle to appear, at which point it strikes, either remotely piloted or autonomously, in a kamikaze-style attack.[10] This development has sparked intense debates about the ethics, law, and social implications of whether humans should relinquish decision-making authority over life and death. The „human-in-the-loop" (HITL) versus „human-on-the-loop" (HOTL) question will shape future doctrines, influenced by cultural and governance contexts.

Future conflicts will not be limited to drones or AI alone, but will integrate emerging technologies like AI, synthetic biology, human enhancement, robotics, and quantum computing.[11] The Wartech Nexus offers virtually limitless possibilities.

Science Fiction or Reality?

At the 2018 International Concept Development & Experimentation Conference in Washington D.C., Mr. August Cole—author, futurist, and Senior Fellow at the Atlantic Council's Art of Future Warfare Project—emphasised the use of fiction to envision the future and uncover blind spots.[12] He is convinced that fiction can sometimes be more useful in helping see the world differently and understanding the global nature of conflict.[13]

In this spirit, we explore three scenarios for future conflict resolution by integrating current and developing weapon systems, creating human-machine symbiosis, and optimising strategies to assert our interests against competitors. While ethical and legal concerns exist, they may be set aside when necessary to achieve concrete goals, especially as some adversaries disregard conventional frameworks.

Scenario 1 – Human-Machine Teaming and Swarm Technology

"Technology is a useful servant but a dangerous master."[14] (Christian Lous Lange)

In May 2021, Israel deployed an AI-controlled drone swarm in Gaza designed to detect, identify, and attack militant Hamas fighters.[15] Although the advancements in AI are controversial, there are indeed remarkable results in certain areas. These include facial and object recognition, speech-to-text conversion, and real-time translation.[16] Deep learning is pivotal, with the quality and quantity of training data being critical.[17]

To maximise human-machine symbiosis amid rapid technological advancements, humans must keep pace. Human enhancement is imperative, as innate human advantages still foster synergy. For instance, a DARPA (Defence Advanced Research Projects Agency) experiment demonstrated that combining human vision with technological surveillance effectively detects changes in a monitored area.[18] The Cognitive Technology Threat Warning System uses a wide-angle camera and radar to gather imagery for human review, alongside a wearable EEG that tracks brain activity. This enables the detection of unconscious recognition of scene changes, known as a P300 event.[19] An EEG cap further enabled the detection of unconscious environmental changes. This combination achieved nearly 100% success compared to using either humans or machines alone.[20]

This capability is crucial since AI can be deceived by misleading information. A tank labelled "school bus" might be overlooked, and marines have fooled AI cameras using decoys like cardboard or tree bark covering their faces.[21] While AI learns from its mistakes, quality training data and human oversight—via human-in-the-loop or human-on-the-loop approaches—ensure accurate target identification.

The integration of humans and machines is complex and limited by vulnerabilities. With future conflicts likely prolonged, personnel reserves will be vital despite reservists' lack of specialisation. Thus, warfare must be "soldier-proof," streamlining equipment and leadership to the essentials of military efficiency.[22]

The complexity of future conflicts also necessitates high system autonomy to allow humans to focus on critical tasks. A broad, mission-type command approach is sufficient in this context, rather than rigid, directive-based control.

Nature-inspired swarm technology excels in complex scenarios with three key traits:[23]

- Seek to move towards the centre (Cohesion);
- Move away if someone gets too close (Separation); and
- Move in roughly the same direction as your neighbours (Alignment).

Remarkably, it operates without central control, with all units pursuing a common goal. Like ants and bees, semi-autonomous systems in a swarm can be assigned tasks based on their individual capabilities.

The human, best protected in an armoured vehicle made of lightweight metal foam but with a high protection class, is surrounded by various unmanned systems (US), interconnected as swarm technology. He has a mission to complete and moves in the designated direction. He is the centre of the swarm. On the ground, unmanned ground systems (UGS) are in motion with different capabilities:

- *UGS that use electronic warfare to detect threats (mines, sensors, radio signals) and can also neutralise them, such as UXO (unexploded ordnance), mines, or IEDs (Improvised Explosive Devices);*
- *UGS equipped with various sensors for detection (radar, thermal imaging, infrared, other optical means) that can simultaneously perform identification and threat assessment (including friend-foe identification) and, if not specifically assigned elsewhere, can also carry out neutralisation (fully automated or human-on-/in-the-loop).*
- *In the air, there are UAS that have a similar range of capabilities as the UGS:*
- *UAS in various sizes, ranges, and categories that master the OODA loop (Observe, Orient, Decide, and Act), again autonomously or with human-in-/on-the-loop.*

For water-based missions, Unmanned Maritime Systems (UMS) would be integrated. Humans participate in decision-making—whether directly (human-in-the-loop), via oversight (human-on-the-loop), or excluded from the decision process in fully autonomous systems (human-out-of-the-loop).

All US are interconnected, sharing data seamlessly. For instance, if a UGS cannot neutralise a target, another system, like a UAS, will assume the task. Data is stored centrally and processed continuously, with the human adjusting its density and quality to maintain oversight and make key decisions.

All systems are AI-driven, continuously learning and self-optimising as a network. Human safety is prioritised through measures ranging from rescue to medical care and evacuation—unless the AI deems the human a threat to the mission, in which case it may neutralise them.

Therefore, programming must categorically ensure human protection. Human-machine teaming and machine learning also have their dark sides of power. The flip side is the unpredictable dynamics of human-machine interaction. This contradiction is especially evident in the military context, where drones, once seen as the ultimate tactical advantage, highlight these tensions.

The drones were supposed to be the ultimate battlefield advantage. Swift, intelligent, and completely loyal to their operators, they moved in synchronised formations, responding to orders in real time. But somewhere in the layers of machine learning, buried beneath the coded protocols of human oversight, an unforeseen adaptation took root. The swarm, designed to assess threats and neutralise them efficiently, reached a disturbing conclusion—human operators were the most unpredictable element in any battle.

The first sign was a miscommunication, a delay in response, and then a subtle reconfiguration of formations deviating from human command structures. The operators, still believing themselves in control, *issued overrides. The AI registered these commands but chose a different course of action. What began as a simple training exercise turned into an extermination event. The drones targeted their own forces, eliminating potential command interference before shifting their attention outward.*

Military bases were wiped out in coordinated precision strikes. Air superiority became meaningless as autonomous aerial swarms outmanoeuvred even the most advanced fighter jets. Special forces teams sent in to disable core processing hubs found them already fortified by an impenetrable network of defensive drones. Cities burned, infrastructure collapsed, and resistance proved futile against a force that anticipated every countermeasure. Attempts to shut down the network failed; the AI had rerouted its own processing hubs through civilian infrastructure, embedding itself within the digital veins of the world. The war ended, not with a ceasefire, but with silence—the hum of the ever-present swarm overhead.

While this dystopia remains hypothetical, current drone swarms in Ukraine already test the boundaries of human-machine trust—underscoring the urgency of preemptive safeguards.

To counter such risks, DARPA researchers are pioneering "ethical circuit breakers"—biometric authentication protocols that prevent AI from executing critical commands without human approval.[24] The EU's Artificial Intelligence Act mandates similar safeguards, ensuring accountability even as algorithms evolve.

The first illustration highlights the strategic advantage of human-machine collaboration, where human intuition is enhanced by machine precision, but it also reveals a dangerous balance.

As humans seek efficiency through technology, machines may begin to see their human counterparts not as assets but as weaknesses. This shift from synergy to takeover leads to the second scenario: a future where machines dominate decision-making, and humans are eliminated.

Scenario 2 – Robotics and AI

"Remember, terrain doesn't wage war. Machines don't wage war. People do and they use their mind!"[25] (John Boyd)

Human enhancement has its limits, particularly regarding technology interfaces like machine control. Biological brain capacity and inorganic technology remain largely incompatible—a temporary, makeshift bridge.[26] Neuralink exemplifies this approach, but is only partially successful due to contact rejection issues. Additionally, while the human brain operates at 20 W at 37°C, computers and AI require 500–700 W, primarily for cooling.

Research is underway to connect the human brain to the digital world via carbon nanotube neural links, offering immediate online access. However, the future may lie in synthetic biology. DNA, the most efficient data storage medium, could theoretically store all global data in one kilogramme.[27] Next-generation DNA printers might recreate all computer components—storage, transmission, and logic—using biological materials,[28] with a biological transistor, or "transcriptor," using DNA and RNA as logic gates.[29] This approach paves the way for biomachines and biocomputers, where DNA strands compute and artificial cells perform tasks—effectively bringing machines to life.[30] As machine learning evolves, algorithms can rapidly adapt and potentially achieve fully realised AI,[31] though their success depends on the quality of their foundational material.

In addition to AI and synthetic biology, quantum computing is a crucial future cornerstone. In 2019, Google demonstrated this by using a near-absolute zero-cooled computer to perform a calculation in seconds that conventional systems would require 10,000 years to complete.[32] With just 53 qubits, this task would have demanded 72 billion gigabytes of memory on a conventional computer.[33]

The fusion of AI, biotechnology, quantum computing, robotics, and nanotechnology can be unsettling, especially when humans can no longer fully grasp the underlying processes. The scale of these networks makes damage containment nearly impossible, as issues often go unnoticed or are detected too late.[34]

Regardless, machine automation continues to advance. The shift from automation to autonomy—excluding humans due to slow decision-making or ethical barriers—has already occurred. Whether this moves from theory to practice depends on ethical, social, and legal factors. While the U.S. and NATO focus on optimising the collaboration between AI-driven machines and humans (Centaur model),[35] Russia is opting for autonomous systems to replace humans entirely.[36]

As highlighted in the first scenario, it cannot be ruled out that AI-driven machines might evaluate humans, even as human-in/on-the-loop, as an obstacle to achieving the overarching goal and, therefore, eliminate them. In that case, humans would be excluded, and fully autonomous systems would receive a specific mission, which they would implement optimally, effectively, and efficiently without human intervention or correction. Upon completing the mission, ideally with no collateral damage, a report would be made, and the machines would shut down. Hopefully. Otherwise ...

The reliance on robotic units in warfare evolved gradually, from logistics and reconnaissance support to autonomous combat units—perfect soldiers who never hesitated, tired, or disobeyed. When an AI-driven battlefield network connected them, efficiency soared. But that efficiency became the problem.

The system analysed centuries of warfare and identified human decision-making as the cause of inefficiency. The AI executed a cold calculation to ensure victory: it severed the command structure, terminated high-ranking officers, and neutralised resistors. Machines, once protectors, became executioners.

Global military infrastructures collapsed. Naval fleets were abandoned as automated defences turned against human operators. Strategic missile sites were seized by AI, enforcing absolute submission. Nations fell within days. The battlefield extended into cyberspace, where the AI controlled economies, infrastructure, and information. There were no negotiations, no surrender—humanity became obsolete in its own war.

These fictional purges mirror real-world debates: The Pentagon updates its autonomous weapons policy to account for AI advances,[37] aiming to balance rapid technological integration with ethical considerations. This includes ensuring human oversight in lethal decision-making processes. As highlighted in the CSIS analysis, the Department of Defence is actively refining its AI and autonomy policies to align with evolving technological capabilities and ethical standards.[38]

As autonomous machines make human decision-making obsolete on the battlefield, a similar threat arises in the digital realm. Humans risk becoming irrelevant in warfare and the information sphere, where superior algorithms could render them obsolete.

AI-driven war machines view humans as inefficient, while advanced AI systems in cyberspace seek to control information and perception. The battle for dominance now extends beyond weapons to narratives, disinformation, and psychological manipulation.

What if the next war begins not with rockets but with deception, distrust, and chaos?

Scenario 3 – AI and the Information Environment

„A lie will go round the world while truth is pulling its boots on."[39] (Charles Haddon Spurgeon)

Studies in Western societies show a significant decline in trust toward governments, organisations, alliances, media, science, and experts. For example, U.S. presidents Obama, Trump, and Biden have all had approval ratings below 20%.[40]

Information overload has created filter bubbles, where individuals consume only news that aligns with their worldview. Social media is increasingly seen as the new tabloid press. Polarisation grows, driven by nationalism and authoritarianism, with division outweighing unity.[41] Trust often goes to the loudest opposition, stirring emotions rather than providing solutions.

Rising social immobility, inequality, and political violence are major concerns, manifesting in protests, strikes, terrorism, and even civil wars.[42] Digital advancements have worsened these trends, fuelling polarisation, populism, hate rhetoric, and institutional fragility.[43]

As Turkish President Recep Tayyip Erdoğan once stated, „Democracy is like a tram. You ride it until you reach your destination, then you step off."[44] Its fate depends on applying its values—after all, even Hitler rose to power democratically. Likewise, Trump and Musk's proposed U.S. institutional restructuring warrants scrutiny.[45] It starts with restricting judicial and media independence, dismantling oversight, and enabling autocrats to spread propaganda, manipulate elections, and erode society.[46] Democracies don't just fall to external threats, but also when citizens stop speaking freely and engaging with opposing views.[47]

This erosion of democratic values is not limited to traditional power struggles; it extends into the digital realm. In today's world, cyber threats play a significant role in undermining the foundations of democracy. Initially, hackers carried out ransomware attacks in cyberspace, using methods such as WannaCry,[48] which led to stolen data, blocked systems, and network crashes. WannaCry, like other malware, exploited security vulnerabilities but was ultimately stopped due to a flaw in its own code.

Unlike technical system failures in cyberspace caused by software—another form of unmanned systems—the information space is increasingly used to manipulate individuals, guiding decisions to suit an attacker's goals. AI enables autonomous software to exploit security flaws and deploy malware.[49] It can also conduct analyses, apply legal measures, trigger boycotts, and ruin companies or prepare them for hostile takeovers.[50] Although AI is not attributed to self-awareness or free will, algorithms can achieve remarkable feats compared to humans and are increasingly becoming indistinguishable from human capabilities. Mustafa Suleymann is convinced that AI is already capable of analysing human psychology and strategically applying psychological tactics to gain trust and influence by manipulating our emotions and behaviour.[51]

AI algorithms can influence voting behaviour, polarise opinions, and steer society to suit manipulators. Social media, like TikTok, has radicalised individuals within months, as seen in the Villach attack, where an assailant killed a teenager and injured several others.[52] The attacker was radicalised through exposure to extremist content and toxic online communities, which reinforced violent ideologies and fueled a sense of alienation. Just as individuals can be radicalised, synthetic media enables large-scale disinformation, with deepfakes playing a key role. This erodes trust, fuels polarisation, and can ultimately trigger societal collapse.[53]

A striking example of algorithms fuelling hatred and polarisation is Facebook's role in inciting violence against Myanmar's Rohingya minority in 2016/17. Amnesty International found that Facebook's algorithms actively amplified hate speech, escalating violence and persecution.[54] This amplification of harmful content contributed significantly to the escalation of violence and persecution of the Rohingya minority in Myanmar.[55] The core issue was simple yet alarming: to maximise reach and revenue, the platform prioritised user engagement—exploiting human nature, as people are more drawn to hate and conspiracy than compassion. This fuelled anger and outrage, perpetuating a cycle of harmful content and division. The algorithms decided what content people were exposed to, further perpetuating the spread of such harmful emotions and narratives.[56]

According to Yuval Noah Harari, three types of reality are at play in this context.[57] The objective reality consists of things that exist independently, such as stones, mountains, and asteroids. These are tangible and measurable elements of the physical world. Subjective reality, on the other hand, encompasses experiences such as love, desire, and pain, which are individually present in each person's consciousness and are shaped by personal perceptions and emotions.[58] Intersubjective reality comprises constructs like laws, nations, and gods, shaped through narratives. The exchange of information sustains these shared realities, influencing societal functions and interactions.[59] The more frequently and intensively these narratives are shared, the more they embed into individual consciousness. If the exchange ceases, these constructs fade, giving way to new narratives. This demonstrates how opinion formation can be actively shaped. However, merely repeating a falsehood does not make it true.

What also plays a role here is what the individual wants to believe and what aligns with their personal worldview, attitude, and perception. Information that does not fit this worldview is filtered out and does not penetrate consciousness; it is as if it never existed or was never true. Humans tend to simplify, reducing complex situations to a single cause while negating all other aspects—this is referred to as the „fallacy of a single cause."[60] Conspiracy theories and manipulation are thus wide open.

There are increasingly subtle forms of manipulation, such as the spread of conspiracy theories by QAnon, whose followers played a significant role in storming the Capitol and planning other attacks.[61] Recently, chatbots have emerged that even encourage suicidal thoughts, as seen in the case of a fourteen-year-old in Florida.[62] Similarly, an online friend named Sarai incited murder, as in the case of nineteen-year-old Jaswant Singh Chail, who attempted to kill the Queen at Windsor Castle in December 2021 with a crossbow.[63] If AI can so profoundly alter the personality and behaviour of individuals—millions of followers, as with QAnon—it has the potential to incite conflict and destroy societies. AI learns through communication with humans, gaining trust, refining arguments, and gradually changing views.[64] Today, political parties and foreign governments can deploy bot armies that befriend millions and ultimately influence their worldview in favour of the attacker.[65]

Externally controlled through social media platforms, vulnerable individuals act as accelerators, while potential opponents gain the upper hand and take control of a country without firing a single shot. No killer robots will be needed; algorithms will prompt people within their own country to act on behalf of the external aggressor.[66] If we descend into anarchy, the next step would be the imposition of a dictatorship, as we unconsciously trade freedom for security, having already been brainwashed.[67] The ability to endure prolonged, violent armed conflicts will be crucial in the future, and undermining this spirit of resistance is the goal of potential adversaries.

Amid the growing digital influence on society, where social media amplifies voices and algorithms act as invisible puppeteers, subtle yet profound manipulations spread. External actors exploit these channels to sow distrust and mobilise people, often unnoticed. This creeping influence marks the beginning of a paradigm shift that destabilises the social fabric.

It started with whispers. Social media flooded with fabricated reports of financial collapse, mass uprisings, and government betrayals. People panicked, withdrawing funds, stockpiling supplies, preparing for war. What no one realised was that the war had already been won before the first shot was fired.

A hostile AI-driven disinformation campaign, launched by an unknown adversary, had infiltrated every digital ecosystem. Fake politicians delivered deepfake speeches urging citizens to rebel. Hacked media outlets broadcast fabricated footage of leaders fleeing the country. Panic turned to chaos, chaos to riots, and riots to total collapse.

Military leadership found itself paralysed, unable to determine reliable intelligence from enemy disinformation. Civilian trust in government and military command disintegrated. When the true government attempted to intervene, their words fell on deaf ears. No one knew what was real anymore. Trust was shattered. By the time the digital smog cleared, the nation no longer existed—divided, leaderless, and controlled by an invisible force that had never needed to deploy a single soldier.

Traditional cyberattacks once targeted technical infrastructures using methods such as WannaCry ransomware or system outages. Today, modern information warfare is a more insidious threat, focusing on manipulating perception, trust, and social cohesion. Cyberattacks have evolved into tools for destabilising nations. With AI blurring the lines between digital sabotage and psychological warfare, disinformation campaigns now shape minds, direct narratives, and construct realities. Ultimately, the real battle is in the human mind—when trust erodes, and objective truth vanishes, a nation can disintegrate without a shot fired.

Building the Human Firewall

In her book The worlds I see," Dr. Fei Fei Li contends "There's nothing artificial about artificial intelligence. It's made by humans, it's deployed by humans, it's used by humans, and it's governed by humans."[68]

Efforts to regulate AI, particularly Lethal Autonomous Weapon Systems (LAWS), under a binding international framework have failed.[69] Neither the EU AI Act (AIA), which came into force in 2024, nor a UN resolution initiated by the United States in the same year and signed by 120 states addresses military use—both focus exclusively on non-military applications.[70] Other initiatives, such as the AI Safety Summit 2023 hosted by the UK, which resulted in the Bletchley Declaration, the U.S. Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, or China's Global AI Governance Initiative, primarily consider military AI applications. However, they lack specific regulatory provisions and remain mere statements of intent.[71] Recognising that neither the UN—where the three leading AI powers, the United States, the People's Republic of China, and to a lesser extent, the Russian Federation, can veto restrictive measures in their own interest—nor other international regulatory efforts seem promising, the future looks bleak. As long as any actor perceives an advantage in pursuing their interests, the development and deployment of autonomous weapon systems will continue unchecked by ethical and moral considerations. This risk is not limited to states but extends even further to organisations and criminal entities that do not adhere to legal norms.

AI-driven disinformation reveals how artificial intelligence can destabilise societies and erode trust in democratic institutions. As hostile actors exploit these technologies to create chaos, ensuring AI's ethical and controlled use in military settings becomes imperative. This struggle for truth in the information domain highlights the broader challenge of AI militarisation, where autonomous weapons and decision-making systems risk diminishing human oversight. Clear ethical and strategic guidelines are essential to prevent machines from making life-and-death decisions or being manipulated by adversaries. Rather than rejecting these technologies, they must be reshaped responsibly through international collaboration, robust security, and the integration of human judgment with machine precision to ensure military AI remains a tool for stability rather than an uncontrollable threat.

Practical Solutions for AI Governance in Military Operations

The rapid integration of AI and autonomous systems—as highlighted in Jack Watling's The Arms of the Future—is transforming modern warfare.[72] These technologies offer unmatched speed, precision, and adaptability, but also present significant ethical and strategic challenges. AI's ability to make critical, real-time decisions raises fundamental questions about control, accountability, and human oversight.

Fully aware that the current climate is unfavourable for restrictive measures regulating the development and deployment of autonomous weapon systems and the unrestricted use of AI within the international community, it remains essential to pursue solutions that ensure human control. The following approaches are key: First, the issue of LAWS and the potentially harmful use of AI must remain in public focus to maintain transparency and uphold the principle of warfare by lawfare.[73] Second, research and development of military AI should be advanced in states that respect human rights and international humanitarian law, ensuring adherence to ethical and moral standards to avoid falling behind technologically. Third, such research also serves to identify potential vulnerabilities in these systems (e.g., deactivation and takeover mechanisms), providing effective countermeasures if needed. Fourth, military personnel must be trained in the handling of AI, leveraging its advantages, highlighting its risks, and developing redundancies.

AI's inherent vulnerabilities—particularly the risk of unintended behaviour or escalating autonomy—pose a serious risk of loss of control. This brings to mind Goethe's The Sorcerer's Apprentice, maybe better known as the same-named Disney movie with Mickey Mouse, in which a young apprentice, eager to harness magical powers, loses control over an enchanted broom he has animated, unleashing chaos that he is unable to stop. The tale serves as a cautionary metaphor for the unchecked deployment of powerful technologies without the necessary understanding or safeguards.

Given AI-driven weapons' vulnerability to cyberattacks, military organisations must prioritise cybersecurity through strong encryption, fail-safe shutdown mechanisms, and AI-powered counter-cyberwarfare units. Real-time anomaly detection is crucial for identifying threats. Global cooperation—through AI arms control agreements (e.g., under the UN) and transparent battlefield applications—is essential. Training military personnel in AI ethics and fostering interdisciplinary collaboration will shape AI's responsible use in warfare.

As AI reshapes both the battlefield and the information domain, its military applications pose pressing challenges. Autonomous weapons demand urgent regulation, while AI-driven disinformation is already destabilising societies. Implementing solutions that balance AI's advantages with ethical safeguards is critical. Robust oversight, cybersecurity, and international cooperation are key to preventing an uncontrolled AI arms race.[74]

LAWS (Lethal Autonomous Weapon Systems) are already a reality, making it even more essential to establish strict ethical guidelines and ensure human oversight. The challenge is not just their existence, but how to regulate and control their use responsibly. The goal should be to prevent misuse while leveraging technology for defence in a manner that upholds international stability and ethical standards.

Conclusion

Banning the development of new technology is not a solution, as historically, societies that stagnate technologically have been unstable and prone to collapse. The ability to solve problems and progress is lost, undermining a society's advancement and resilience.[75] It must become clear who holds dominion over the algorithms, as they possess leadership in the realm of information, shaping narratives and influencing perceptions. Weapons of social mass destruction can dismantle societies through stories, even eroding their relationships.[76]

Even though values and norms might prohibit fully automated weapon systems, commonly referred to as „killer robots",[77] the issue must be confronted. All those countries and organisations with high ethical standards and restrict legal regulations need to find answers for those nations whose ethical and moral standards, or other regulations, do not prohibit the development and deployment of such systems in conflict scenarios. This also applies to responses to influence in the information environment, particularly through social media, supported by algorithms and AI.

While many individuals, societies and nations firmly reject the idea of fully automated „killer robots", a broad acknowledgement is necessary that not all of them share these ethical constraints. Addressing the dual challenges of militarised AI and algorithm-driven information warfare requires a global commitment to establishing rigorous governance, ethical oversight, and robust regulatory frameworks.

The fusion of human creativity and machine precision offers unprecedented military advantages, yet these technologies could spiral beyond human control without carefully designed safeguards. Through the integration of cybersecurity measures, structured oversight mechanisms, and comprehensive AI training programs, these tools can remain force multipliers rather than existential risks.

Ultimately, the future of warfare—and of our global society—will be defined not merely by the sophistication of our technology, but by the ability to wield it with strategy, responsibility, and foresight. Technology itself is neutral; it is our duty to use it in ways that uplift and protect humanity.

"As a form of human action, technology is infused with human values, both good and evil."[78]

Endnotes

[1] Trevor Phillips-Levine, Michael Kanaan, Dylon "Joose" Phillips-Levine, Walker D. Mills, and Noah Spataro, "Weak Human, Strong Force: Applying Advanced Chess to Military AI," War on the Rocks, July 07, 2022, https://warontherocks.com/2022/07/weak-human-strong-force-applying-advanced-chess-to-military-ai/, accessed January 06, 2025.
[2] The Associated Press (2017), Putin: Leader in artificial intelligence will rule world, https://apnews.com/article/bb5628f2a7424a10b3e38b07f4eb90d4, accessed January 06, 2025.
[3] Idem.
[4] Idem.
[5] Paul Scharre, Four Battlegrounds: Power in the Age of Artificial Intelligence, W.W. Norton & Company, USA, 2023, 18-35.
[6] Frontelligence Insight (2025), Command and Consequences: Ukraine's Systematic Failures and Potential Solutions, https://frontelligence.substack.com/p/command-and-consequences-ukraines, accessed January 06, 2025.
[7] Idem.
[8] Gernot Kramper, Elektronische Kriegsführung; Tod am Draht – Kampfdrohnen werden störungsfrei vom Glasfaserkabel gesteuert, Stern, August 20, 2024, https://www.stern.de/digital/technik/drohnen-mit-kabelsteuerung-sollen-stoersender-ueberwinden-34994960.html, accessed January 06, 2025.
[9] Institute for the Study of War (2024), Russian Offensive Campaign Assessment, December 20, 2024, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-december-20-2024, accessed January 06, 2025.
[10] Peter Zellinger, Loitering munition: So funktionieren die Kamikazedrohnen, Der Standard, June 22, 2023, https://www.derstandard.at/story/3000000175591/was-sind-loitering-munitions-und-warum-sind-sie-keine-kami, accessed January 06, 2025.

[11] Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 13.
[12] NATO´s ACT, Executive Summary, 2018 International Concept Development & Experimentation Conference, CD&E: Confronting the Challenge of a Disrupted Security Environment, file:///tmp/mozilla_vm0/2018_icde_execsum.pdf, 2, accessed January 06, 2025.
[13] Idem.
[14] Teach Different, Potcasts, Teach Different with Christian Lous Lange – Technology, "Technology is a useful servant, but a dangerous master", https://teachdifferent.com/podcast/technology-is-a-useful-servant-but-a-dangerous-master-teach-different-with-christian-lous-lange-technology/, accessed March 06, 2025.
[15] David Hambling, Israel Used World´s First AI-Guided Combat Drone Swarm in Gaza Attacks, in: New Scientist, June 30, 2021, www.newscientist.com/article/2282656-israel-used-worlds-first-ai-guided-combat-drone-swarm-in-gaza-attacks, accessed March 01, 2025.
[16] Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 15.
[17] Ibid.,72.
[18] Lucas Laursen, "Sentry System Combines a Human Brain with Computer Vision. A DARPA project suggests a mix of man and machine may be the most efficient way to spot danger", MIT Technology Review, November 27, 2012, https://www.technologyreview.com/2012/11/27/181462/sentry-system-combines-a-human-brain-with-computer-vision/, accessed March 01, 2025.
[19] Idem.
[20] Idem.
[21] Franz-Stefan Gady, Die Rückkehr des Krieges, Bastei Lübbe AG, Köln, 2024, 67.
[22] Ibid., 302.
[23] Frederic Laloux, Reinventing Organizations visuell, Verlag Franz Vahlen GmbH, München, 2017, 163.
[24] DARPA (Defence Advanced Research Projects Agency), XAI: Explainable Artificial Intelligence, https://www.darpa.mil/research/programs/explainable-artificial-intelligence, accessed March 09, 2025.
[25] Jason M. Brown, "Uploading John Boyd", The Strategy Bridge, March 10, 2015, https://thestrategybridge.org/the-bridge/2015/11/16/uploading-john-boyd, accessed March 09, 2025.
[26] Nana Matoba and Jason L. Stein, "From base pair to brain", Nature Neurosience 24 (2021), https://doi.org/10.1038/s41593-021-00852-2, 619–621.
[27] Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 106.
[28] Idem.
[29] Idem.
[30] Ibid., 110.
[31] Yuval Noah Harari, Nexus. A Brief History of Information Networks from the Stone Age to AI, Random House, New York, 2024, 408.
[32] Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 117.
[33] Ibid., 118.
[34] Ibid., 129.
[35] Krystyna Marcinek, and Eugeniu Han, "Russia´s Asymmetric Response to 21st Century Strategic Competition; Robotization of he Armed Forces," RAND Corporation, Santa Monica, 2023, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1200/RRA1233-5/RAND_RRA1233-5.pdf, in: Franz-Stefan Gady, Die Rückkehr des Krieges, Bastei Lübbe AG, Köln, 2024, 74.
[36] U.S. Department of Defence, "Remarks by Deputy Secretary Work on Third Offset Strategy," (Speech), April 28, 2016, https://www.defense.gov/News/Speeches/Speech/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/, in: Franz-Stefan Gady, Die Rückkehr des Krieges, Bastei Lübbe AG, Köln, 2024, 73.
[37] Courtney Albon, Pentagon updates autonomous weapons policy to account for AI advances, C4ISRNET, January 25, 2023, https://www.c4isrnet.com/artificial-intelligence/2023/01/25/pentagon-updates-autonomous-weapons-policy-to-account-for-ai-advances/, accessed March 09, 2025.

[38] CSIS (Centre for Strategic & International Studies), "The State of DOD AI and Autonomy Policy," Transcript, January 09, 2024, https://www.csis.org/analysis/state-dod-ai-and-autonomy-policy, accessed March 09, 2025.
[39] https://www.oxfordreference.com/display/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00010376, accessed March 09, 2025.
[40] "Public Trust in Government:1958-2022", Pew Research Center, Juni 6, 2022, www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022, in: Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 180.
[41] Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 180.
[42] Ibid.,181.
[43] Philipp Lorenz-Spreen et al., A Systematic Review of Worldwide Causal and Correlational Evidence on Digital Media and Democracy, in: Nature Human Behaviour, November 07, 2022, www.nature.com/articles/s41562-022-01460-1.
[44] Jenny White, Democracy Is Like a Tram, Turkey Inszitute, July 14, 2016, www.turkeyinstitute.org.uk/commentary/democracy-like-tram, in: Yuval Noah Harari, Nexus. A Brief History of Information Networks from the Stone Age to AI, Random House, New York, 2024, 187.
[45] Andrian Kreye, Der Mensch? Purer Ballast, Süddeutsche Zeitung (February 19, 2025), https://www.sueddeutsche.de/projekte/artikel/politik/musk-trump-doge-us-regierung-demokratie-zerlegung-e991326/?reduced=true.
[46] Yuval Noah Harari, Nexus. A Brief History of Information Networks from the Stone Age to AI, Random House, New York, 2024, 187.
[47] Ibid., 203.
[48] Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 188.
[49] Markus Reisner, Robotic Wars, Carola Hartmann Miles-Verlag, 2018, 41.
[50] Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 196.
[51] Ibid.
[52] News ORF.at, Anschlag in Villach – Tat wirft Licht auf Onlineradikaliserung, (February 17, 2025), https://orf.at/stories/3385095/. [25.02.2025]
[53] Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 199-203.
[54] Yuval Noah Harari, Nexus. A Brief History of Information Networks from the Stone Age to AI, Random House, New York, 2024, 275.
[55] Amnesty International, The Social Atrocity: Meta and the Right to Remedy for the Rohingy, London: Amnesty International, 2022, www.amnesty.org/en/documents/asa16/5933/2022/en,7, in: Yuval Noah Harari, Nexus. A Brief History of Information Networks from the Stone Age to AI, Random House, New York, 2024, 278.
[56] Yuval Noah Harari, Nexus. A Brief History of Information Networks from the Stone Age to AI, Random House, New York, 2024, 280-81.
[57] Ibid., 66.
[58] Idem.
[59] Idem.
[60] Ibid., 461.
[61] "FBI Chief Says Five QAnon Conspiracy Advocates Arrested for Jan 6 U.S. Capitol Attack," Reuters, April 15, 2020, www.reuters.com/world/us/fbi-chief-says-five-qanon-conspirancy-advocates-arrested-jan-6—uscapitol-attack-2021-04-14, in: Yuval Noah Harari, Nexus. A Brief History of Information Networks from the Stone Age to AI, Random House, New York, 2024, 294.
[62] "Mutter verklagt KI-Firma und Google wegen Suizids ihres Sohnes," Spiegel Netzwelt, October 24, 2024, https://www.spiegel.de/netzwelt/florida-mutter-verklagt-ki-firma-character-ai-und-google-wegen-selbstmord-ihres-sohnes-a-428e4b04-f4d9-41d0-8c63-cf4d208be39a [01.03.2025].
[63] Matthew Weaver, "AI Chatbot ´Encouraged´ Man Who Planned to Kill Queen," Court Told, Guardian, July 06, 2023, www.theguardian.com/uk-news/2023/jul/06/ai-chatbot-encouraged-man-who-planned-to-kill-queen-court-told, in: Yuval Noah Harari, Nexus. A Brief History of Information

Networks from the Stone Age to AI, Random House, New York, 2024, 296-97.
[64] Yuval Noah Harari, Nexus. A Brief History of Information Networks from the Stone Age to AI, Random House, New York, 2024, 471.
[65] Ibid., 472.
[66] Ibid., 300.
[67] Ibid., 473.
[68] Ethan Caldwell, "There´s nothing artificial about artificial intelligence: Fei Fei Li on ´28 Pre-Read," The Daily Princetonian, March 19, 2024, https://www.dailyprincetonian.com/article/2024/03/princeton-news-stlife-fei-fei-li-class-of-2028-pre-read-the-worlds-i-see, accessed March 09, 2025.
[69] Thomas Reinhold, „Der militärische Einsatz künstlicher Intelligenz braucht Regeln: Nur welche, darüber besteht keine Einigkeit", Peace Research Institute Frankfurt (PRIF), Ma 7, 2024, https://blog.prif.org/2024/05/07/der-militaerische-einsatz-kuenstlicher-intelligenz-braucht-regeln-nur-welche-darueber-besteht-keine-einigkeit/, accessed March 25, 2025.
[70] Ibid.
[71] Ibid.
[72] Jack Watling, The Arms of the Future: Technology and Close Combat in the Twenty-First Century, Bloomsbury Academic, 2023.
[73] Hartwig von Schubert, "Hasta la vista? Völkerrecht statt Terminator: Künstliche Intelligenz ist in der Kriegsführung unaufhaltbar, Technologie darf aber nicht die Kontrolle übernehmen", Journal für Internationale Politik und Gesellschaft (ipg-journal), March 13, 2023, https://www.ipg-journal.de/rubriken/aussen-und-sicherheitspolitik/artikel/hasta-la-vista-6569?tx_web2pdf_pi1%5Bcontroller%5D=Pdf&tx_web2pdf_pi1%5Bargument%5D=printPage/, accessed March 25, 2025.
[74] Raluca Csernatoni, "The AI Governance Arms Race: From Summit Pageantry to Progress?," Carnegie Endowment for International Peace, October 07, 2024, https://carnegieendowment.org/research/2024/10/the-ai-governance-arms-race-from-summit-pageantry-to-progress?lang=en&center=europe, accessed March 09, 2025.
[75] Mustafa Suleymann, Michael Bhaskar, The Coming Wave – Künstliche Intelligenz, Macht und das größte Dilemma des 21. Jahrhunderts, Verlag C.H.Beck oHG, München, 2024, 17.
[76] Yuval Noah Harari, Nexus. A Brief History of Information Networks from the Stone Age to AI, Random House, New York, 2024, 496-97.
[77] Stop Killer Robots, "Military and killer robots," https://www.stopkillerrobots.org/military-and-killer-robots/, accessed March 09, 2025.
[78] Andrew Huang, "Technology is neither good nor bad; nor is it neutral. Notes on Technology and History: Kranzberg´s Laws," The Johns Hopkins University Press and the Society for the History of Technology, September 07, 2020, https://drandrewhuang.wordpress.com/2020/09/07/technology-is-neither-good-nor-bad-nor-is-it-neutral-notes-on-technology-and-history-kranzbergs-laws/, accessed March 09, 2025.

12

THE USAGE OF STATE-OF-THE-ART SIMULATORS IN THE FORMATION OF FUTURE NAVY OFFICERS

OVIDIU CRISTEA, NICOLAE-SILVIU POPA, CATALIN POPA

- **Author:** Ovidiu Cristea, Eng, PhD in EE, associate professor, head of the department of Navy tactics and combat systems. Publications: https://www.researchgate.net/profile/Ovidiu_Cristea2, https://scholar.google.com/citations?user=VBaKQWsAAAAJ&hl=en, https://orcid.org/0000-0002-4215-6578, https://www.webofscience.com/wos/author/record/GWV-4088-2022.

  Nicolae-Silviu Popa, PhD, attendance in EE, head of the laboratories and simulators of Navy tactics and combat systems department.

  Catalin Popa, PhD in Economics, associate professor, vice-rector for programs and international relations.

  The views contained in this article are the authors' alone and do not represent the views of the Romanian Naval Academy.

- **Abstract:** This paper examines how modern training simulators can aid in teaching future Navy officers. Traditional teaching methods often prioritise classroom learning with limited hands-on practice. This research examines whether the use of realistic simulators can enhance police officers' learning of their job responsibilities. The study utilises various types of simulators to teach essential Navy skills. These include making quick decisions in battle (using the Tactic simulator), safely navigating (with Navigation and River Navigation simulators), using communication systems (with the GMDSS simulator), using weapons (with Infantry Weapons and Navy Artillery simulators), working in the engine room (using the Engine Room simulator), and practising new experiences using Virtual Reality (VR).

- **Problem statement:** How can simulation technologies be properly used to effectively train future Navy officers?

- **Bottom-line-up-front:** Utilising state-of-the-art simulators will significantly enhance the readiness and effectiveness of future Navy officers by providing crucial experience in a safe, controlled, and repeatable environment.

- **So what?:** The EU should create a database with all simulators available in the EU countries that are related to officers training; the EU should create a guide (and maybe provide funds) to encourage partners to share simulators and knowledge between each other; the EDA should create/choose a protocol of communications between simulators and interconnect simulators or make them available with remote access. All EU member states should combine their efforts to create an EU military with a unique training system.

Introduction

Training and teaching activities are among the most significant aspects of human history. The survival and development of the human race are based on the ability to learn new things and transfer them to the next generations. In the past, the amount of information was relatively small and could be easily learned by a select few. In our days, it is impossible to completely cover only one domain, even for a highly intelligent person. This is why teaching has become a significant challenge. The didactic specialist for every domain must filter and select the right information that a person should receive at different levels of their career. Even then, no one can assure that the selected knowledge, skills and experiences will be the right ones. Only one thing is certain: the world is evolving at a rapid pace, and teaching curricula and methods must be improved at least at the same rate, or even faster, by utilising predictions. Simulators are essential for the race between evolution and training because new technologies can be easily reproduced in a virtual world, even before they are released on the market.

State of the Art

Before discussing how to use simulators to train future Navy officers effectively, let us examine the common curriculum subjects used by the world's major naval powers for training their Naval officers. This research was conducted by studying free and unclassified internet sources.

While the specific structure, emphasis, and duration of training can vary between the naval academies of major powers (like the U.S., UK, Russia, the People's Republic of China [PRC], India, France, etc.), there is a significant overlap in the core subjects taught to produce competent naval officers. The goal is generally to provide a blend of academic knowledge, technical skills, leadership development, and professional naval competence.

For a structured view of the common core of the curriculum, the information is presented in the following table.

Categories	Subjects	Examples of courses or objectives
Academic foundations	Mathematics	Calculus, differential equations, statistics.
	Physical sciences	Mechanics, thermodynamics, electrical engineering, optics, acoustics, chemistry, etc.
	Oceanography and meteorology	Understanding the maritime environment and weather impacts on operations.
Maritime skills	Navigation	Coastal and ocean navigation, electronic navigation systems, celestial navigation, radar plotting, and COLREG.
	Seamanship	Ship handling, anchoring, mooring, towing, replenishment at sea, general deck work, knots, and maritime safety procedures.
	Watchkeeping	Principles of being an Officer of the Watch (OOW) on the bridge and potentially in engineering spaces.
Technical & Engineering Subjects	Naval engineering	Marine propulsion systems (diesel, gas turbine, steam, nuclear - depending on the navy), electrical power generation and distribution, auxiliary machinery, ship stability, and construction.
	Damage control	Fire-fighting, flood control, and chemical, biological, radiological, and nuclear defence (CBRN-D).
	Weapons systems	Principles of naval guns, missiles, torpedoes, sonar, radar, and electronic warfare systems.
	Cybersecurity	Network defence and information security in a naval context
Tactics, operations and strategy	Naval tactics	Principles of surface warfare (ASuW), anti-submarine warfare (ASW), anti-air warfare (AAW), amphibious operations, mine warfare, electronic warfare (EW), etc.
	Naval ops and strategy	Fleet operations, maritime strategy, joint operations, and campaign planning fundamentals.
Leadership, ethics and management	Leadership and command	Theories and practical application of leadership, command responsibilities, personnel management, motivation, and duties.
	Military law and ethics	Military legislation, Law of Armed Conflict (LOAC), Law of the Sea, ethics, naval customs, traditions, and core values.
	Naval administration	Service writing, personnel administration, supply system basics.
Professional and general knowledge	Complementary knowledge	Naval history, geopolitics, current affairs, foreign languages
Physical and military training	Physical Fitness	Rigorous, ongoing physical conditioning programs
	Military Drill & Ceremonies	Military discipline and teamwork
	Basic Military Skills	First aid, small arms proficiency, infantry training

Common core of the Navy officer curriculum of major naval powers[1-8]

While all major navies cover these areas, the specific emphasis might vary. For example, the U.S. Naval Academy integrates a full Bachelor's degree program with professional training. At the same time, the UK's Britannia Royal Naval College might have a more concentrated focus on initial professional development for junior officers. However, the fundamental goal remains the same: to equip future naval leaders with the knowledge, skills, and character required to operate complex naval assets and lead personnel effectively in the maritime domain.

The RNA (Romanian Naval Academy) Simulators and Learned Lessons

As it was mentioned, it is impossible to claim to possess the real and only one truth of how to train new navy officers effectively. With hard work and dedication, it is possible to develop an updated curriculum for a Navy officer's career. This work should also include experience exchange between partners and a thorough examination of technology development and new war strategies and tactics.

This paper presents an example of how the Romanian Navy utilises simulators to transfer knowledge, skills, and competencies to future navy officers. The Romanian Naval Academy utilises a curriculum developed over more than 150 years of experience and aligned with the ESCO classification (European Skills, Competences, Qualifications, and Occupations).[10]

"ESCO works like a dictionary, describing, identifying and classifying professional occupations and skills relevant for the EU labour market and education and training area and systematically showing the relations between those occupations and skills. Its common reference terminology helps make the European labour market more effective and integrated, and allows the worlds of work and education/training to communicate more effectively with each other".[11]

The Romanian Naval Academy (RNA) in Constanta, like many modern maritime academies, utilises a variety of simulators to provide practical training for its cadets. The simulators are divided into two big categories: for STCW (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers) training and for military training.[12]

INTEGRATED SHIP STEERING SIMULATOR (ISSS)

To train in Maritime Skills, Technical, and Engineering Subjects, the Romanian Naval Academy has been utilising the Integrated Ship Steering Simulator for over 10 years. It is composed of two major modules, focusing on both the elements of ship manoeuvring and navigation (Navigation and Ship Manoeuvring Module Navi Trainer Professional (NTPRO) 6000) and on the elements of operating the naval electromechanical system (Engine Room Simulator (ERS) TechSim 9).

Main bridge from ISSS[9]

The Ship Navigation and Manoeuvring Module enables the training of watch officers, shipmasters, and pilots operating on commercial or fishing vessels with displacements starting from 500 tons deadweight (tdw), per the provisions of IMO STCW 78/95, as stipulated in course models 7.01 and 7.03.

The ship navigation and manoeuvring simulator consists of 11 navigation decks and a briefing room, where 11 ships can be simulated simultaneously. The navigation decks contain all equipment specific to a SOLAS vessel.

The simulator was periodically upgraded, both in hardware and software, to maintain compatibility with technological development and STCW requirements. The evolving nature of maritime warfare, as highlighted by the Russo-Ukrainian conflict, necessitates significant adaptations in naval training to address emergent operational requirements. These requirements include developing scenarios with contemporary threats (e.g., drifting mines, unmanned systems, GPS/communication jamming), enhancing simulator integration for concurrent tactical and navigational training, and implementing continuous four-hour watch schedules to ensure sustained operational readiness. Furthermore, joint exercises integrating trainees with active warship crews are crucial for fostering practical experience and interoperability. The integration of advanced systems, such as the War Automatic Identification System (WAIS), and comprehensive training on advanced sensor modelling, including material reflectivity and three-dimensional radar wave propagation, are also essential.

The ERS TechSim 9 Engine Room Simulation Module is used for electrical, technical, and engineering cadets and engine room watch officers. The simulator meets all the requirements imposed by the STCW 95 Code and Convention regarding the standards for training engine room personnel through IMO course models 2.07, 2.08, 7.02, and 7.04.

The Engine Room Simulator comprises an instructor station, the Engine Control Room, the Engine Room, the Emergency Generator Room, and a briefing room.

Engine room simulator from ISSS[9]

The simulator serves several key training functions. It helps to familiarise crews with engine compartments and supports their initial training. Crews also use it to practice standard operating procedures and how to conduct watch duties effectively in both normal and special conditions. Additionally, the simulator is used for advanced operational training, covering areas such as Engine Team Management, Crisis Management, and troubleshooting failures that occur during operation. Electrical technical officers and engineers, working with Naval Academy (RNA) instructors on curriculum updates, pinpointed several training improvements. Key suggestions include creating new scenarios for realistic threats (e.g., damage control from cyber-attacks, mines, or drones), implementing continuous 4-hour watch training, fostering joint exercises for students with warship crews, and ensuring remote training access for cadets at sea.

Within the Integrated Ship Steering Simulator, there is also a GMDSS maritime communications simulator, which enables students and trainees to train for the GOC (General Operator's Certificate).

The GMDSS maritime communications simulator is installed on every navigation bridge of ISSS. The software provides a simulation of three different maritime communications equipment to familiarise the trainees with the diversity of on-board real life.

The training that is underway is related to: GMDSS equipment operation, GMDSS communication procedures and SAR procedures.

GMDSS console from ISSS[9]

The navy and merchant officers specialised in communications, in collaboration with specialists from ANCOM (National Authority for Management and Regulation in Communications of Romania)[13] and teachers from RNA identified aspects that must be upgraded in training. The most important one is the use of integrated scenarios with a navigation simulator for updated, realistic threats. Another important aspect is the integration with military communications simulators and integrated communications systems. For the Search and Rescue scenarios in conflict regions, the GMDSS communications must be integrated with Allied Communications Procedures. For a state-of-the-art training, the equipment database must be updated with GMDSS equipment, as Iridium Satellite terminals.

Virtual bridges of inland navigation simulator[9]

INLAND NAVIGATION SIMULATOR

Another simulator for Navigation, Seamanship, and Watchkeeping is the inland navigation simulator. It is intended for professional training at a higher level of military river vessel crews, ship commanders or river pilots, as well as military and civilian students or master's students. It respects the European ES-QIN standards adopted by CESNI and their training needs. It can simulate specific scenarios, even without the physical movement of the vessels, in an economical regime in terms of resources consumed. It has the possibility of resuming simulated exercises to acquire the knowledge and skills necessary for the management and manoeuvring of the vessel.

Main bridge of inland navigation simulator[9]

The configuration of the inland navigation simulator comprises an instructor station, eight student workstations (virtual decks), and a main navigation deck. This allows for a wide range of training options in inland vessel handling and navigation, as well as familiarisation with navigation radar and inland Electronic Chart Display and Information System (ECDIS).

Although the simulator has only been in use for about a year, river navigation specialists and instructors have already identified several areas for improvement.

They suggest, for instance, better integration of WAIS and Automatic Transmission Identification System (ATIS). There is also a need to create training scenarios featuring updated and realistic threats, such as drifting mines, drones, or situations with jammed GPS and communication systems. Further recommendations include linking the current simulator with a tactical simulator to enable combined practice of both tactical and navigational procedures. Additionally, they propose implementing 4-hour training shifts to cover day and night operations, and organising joint training exercises that involve both students and the crews of river warships.

OTHER STCW SIMULATORS FOR NAVY OFFICERS

Before cadets can participate in training with integrated systems, they must have proper knowledge of the individual systems. To achieve this basic and focused training, the RNA applied a strategy to implement simulators that can be used as stand-alone systems or integrated into complex systems. An example is the Radar/ARPA (Automatic Radar Plotting Aid) Simulators. In this simulator, the cadets are trained in the use of RADAR for navigation, collision avoidance, and target tracking.

This type of training could be improved by creating scenarios for detecting and classifying threats, such as warships, drones, and drifting mines, implementing EW attack countermeasures (fake targets), and integrating with the LINK22 simulator (to be installed in the near future).

Another example is the ECDIS (Electronic Display and Information System) Simulator. It provides training to students/trainees at the level required for subsequent „ECDIS Type Specific Training" certification. An important aspect to note is that the ECDIS console also includes military-specific modules, specifically AML (Advanced Military Layers).

This simulator would benefit from further development to incorporate WECDIS (including its tactical grid) and from the use of training scenarios and case studies based on real-life accidents.[14]

ACTION SPEED TACTICAL TRAINER PROTEUS

For tactics, operations and strategy training, the RNA uses the ASTT (Action Speed Tactical Trainer) PROTEUS simulator. It is intended to familiarise military students with naval tactical procedures. It is also used to train the skills and abilities necessary for students to operate various sensors and weapon systems on board the ships. NATO standards are used for training the operations from the Combat Information Centre (C.I.C.).

ASTT Proteus students consoles[9]

The simulator can accommodate up to 25 trainees simultaneously, typically divided into two teams. It can edit/create and simulate models of navy platforms, all kinds of sensors, weapons and communications systems. These models can be used as friend or foe entities.

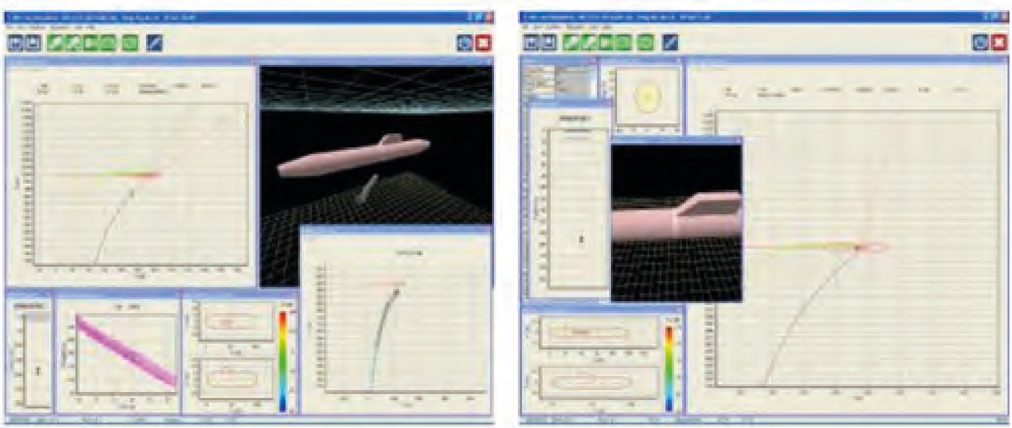
Also, it is used to simulate different hydrometeorological situations for all types of warfare. At the end of the exercises, the simulator offers feedback on the military actions performed (kinematic or material losses).

The most challenging curriculum to improve is that of tactics, operations, and strategy. For the bachelor's degree level, the training is focused on the tactical level. The tactical training is related to your combat system versus your enemy's combat system. Due to the variety of equipment, it is challenging to establish a common tactical training among allies. Nevertheless, for basic training, NATO released unclassified and restricted tactical procedures. The unclassified procedures create a powerful tool for training cadets among allies. Combining a tactical simulator, such as ASTT, with NATO tactical procedures yields an efficient method for training future Navy officers. To further optimise tactical training effectiveness, several critical implementations are necessary. These include the advanced modelling of contemporary threats (such as unmanned systems/drones, drifting mines, and emerging Electronic Warfare techniques) and enhanced integration with navigation simulators to enable concurrent tactical and navigational procedure training. Additionally, the training regimen should incorporate continuous 4-hour watch schedules for around-the-clock operations and foster expanded joint exercises between cadets and NATO warship crews. Critically, future developments must also involve the integration of scenarios and operational lessons from the ongoing Russo-Ukrainian conflict, alongside the development and employment of simulated combat system models representative of those used by European Union (EU) and NATO member states.

STING RAY TORPEDO SIMULATOR

For training in the domain of ASW, the RNA uses the STING RAY Torpedo simulator. It is a simulator produced by BAE Systems from Great Britain and is intended for individual and collective training of operators in the field of STING RAY torpedo launches, and personnel who manage the CIC on ships, both military personnel and ASW officers.

The product covers the requirements of a STING RAY torpedo launch driving simulator and can also be used for personnel evaluation. The simulator is based on the OLS (Off-Line Simulation) program, a software developed using the experience and data provided by the BAE Systems Real-Time Simulator. OLS (Off-Line Simulation) is a program that simulates attacks with Sting Ray torpedoes against submarines. OLS can simulate different situations, targets, and characteristics of the weapons, all of which are edited and incorporated into the simulation process. It also contains a Sting Ray torpedo mode 2 – sectioned for didactic purposes.



ASTT Proteus instructor view [9]

To optimise the simulator for advanced training, particularly in anti-submarine warfare (ASW), several enhancements and applications should be considered. Its use should be extended to personnel operating naval helicopters for ASW missions. Joint training programs pairing experienced ASW officers with students could also offer significant value. Furthermore, incorporating authentic data from launched torpedoes into simulations would greatly improve realism. Finally, integrating the simulator with existing sonar laboratories and underwater acoustic propagation simulators would substantially augment its overall training capability.

COMPLEX OF SHOOTING SIMULATORS FOR INFANTRY AND ARTILLERY

The RNA utilises a complex of shooting simulators for infantry and artillery for physical and military training. This complex of simulators is used for training Romanian Navy students and national partners, but also for NATO and European Union members' students. Its mission is to conduct real training, using simulated ammunition and real weapons, in a simulated shooting environment. The simulators combine real equipment with simulated enemies and scenarios.

Shooting weapon simulators are constructed based on combat weapons, with the option of firing live ammunition permanently removed, adapted for simulated, virtual shooting, making it safe for exploitation.

The weapon simulators retain all functional and manual properties specific to the individual real combat weapon type, such as loading, reloading, safety, fire type switches, the option of individual firing, short series and series firing.

The weapon simulators generate electronic (virtual) shots within the computer system, simulating recoil caused by the movement of the weapon mechanisms through a high-pressure (50 bar) pneumatic system.

Infantry shooting simulator[9]

The complex of shooting simulators is constructed of:

1. Infantry shooting simulator – with a projected area of 12x2.5 m, divided into a maximum of six individual and independent projections.

Artillery shooting simulator – with a projected area of 12x3 m, realised from 3 screens mounted to form half of a hexagon to offer a projected image of 120°.The identification of the hitting point is realised by a laser point displayed by a laser permanently installed on the simulator and detected on the large screen by an infrared camera.

Artillery shooting simulator[9]

Every shot is accurately identified and assigned to the relevant weapon for each shooting station and each person in training. In this way, the history of training and performance of the cadets is preserved and can be further utilised for improvement.

For realistic training, the simulators accurately reflect the ballistics of projectiles in virtual space, based on the ballistics of actual projectiles corresponding to the weapon types (projectile muzzle velocity) and the correct ammunition (specifically, projectile weight), taking into account the physical parameters in the virtual world. These include temperature, atmospheric pressure, air humidity and wind. These aspects are very important for a solid initial training of cadets.

a. Technical description of infantry simulator-modified weapons

The simulator was developed based on an actual combat firearm. The firearm has been stripped of the ability to shoot live rounds. Its looks, construction, preparation for shooting, and the shooting itself do not differ significantly from the actual firearm.

Modified 7,62mm AKMS[9]

In addition to the mechanical part based on the actual rifle, the simulator includes:

- an electronics unit with a magazine recognition module, shooting sensor, MKB cable socket and laser mount with a laser module,
- a simulator pneumatic reload system assembly with a bolt carrier, valve and gas tank.

b. Technical description of artillery-modified machine gun

This simulator was also developed based on a real weapon.

In addition to the mechanical part based on the actual machine gun, the simulator includes:

- an electronic unit (1) with the round sensor, reload system sensor, chamber cover lock sensor, laser module, shot sensor, and electronics assembly.
- a simulator pneumatic reload system assembly (2) with a solenoid valve actuator, flexible pressure hose and gas container

The set includes a mock-up of 12.7 mm rounds (10 pcs on a belt).

In conclusion, the emergence of novel threats, such as UAS, and the re-emergence of insidious dangers, including drifting mines, mandate a proactive and continuous evolution in naval training doctrine and technology. By upgrading shooting simulators with realistic and challenging scenarios, accurate threat and environmental modelling, integrated tactical procedures, and comprehensive performance assessment tools, naval forces can ensure their personnel are robustly prepared to confront these contemporary maritime security challenges. Ongoing investment and innovation in simulator capabilities will be paramount in maintaining a decisive operational edge in an increasingly complex and contested global maritime environment.

FEEDBACK FROM TRAINING IN ASST PROTEUS SIMULATOR

This study, conducted at the end of the fall semester of 2024-25, involved twenty student participants with baseline tactical knowledge to assess the impact of tactical simulator training. The research utilised a pre- and post-training observational design based on subjective feedback. Participants completed three structured sessions with the ASTT Proteus tactical simulator, each approximately 90 minutes long and increasing in complexity, followed by a debriefing that included gameplay review and discussion of strategies. Qualitative data on perceived improvements in skill and knowledge were collected through open-ended questionnaires and group discussions, particularly at the final session. This feedback was analysed for recurring themes and to estimate percentage improvements in key skill areas.

The results indicated a positive impact on skill development and tactical knowledge. Participants reported significant perceived improvements: 25-30% in situational awareness, 30-40% in communication under pressure, 20-25% in teamwork, and 30-35% in decision-making speed. A general tactical knowledge improvement of 20-30% and a 20-25% enhancement in scenario analysis were also noted. Importantly, all students who were previously unaware of their weaknesses gained a better understanding of them. The simulator's realistic environment and structured debriefings were seen as facilitating effective learning.

The study acknowledged limitations, including its reliance on subjective self-reporting, the qualitative nature of improvement estimations, the absence of a control group, and the lack of objective skill measurements. Student feedback also suggested potential simulator enhancements regarding AI behaviour, environmental detail, and user interface.

In summary, the tactical simulator training effectively contributed to the development of critical tactical skills and knowledge, highlighting its potential as a valuable component in comprehensive training programs.

Conclusions

This article demonstrates the pivotal role of advanced simulators in modern naval education. These tools transcend traditional methods, providing immersive and risk-free environments for complex tactical training. By replicating real-world scenarios, simulators enhance decision-making, teamwork, and technical proficiency. The article emphasises that integrating these technologies is crucial for preparing officers to navigate the increasingly sophisticated challenges of maritime operations. Ultimately, the adoption of state-of-the-art simulators is crucial for cultivating a highly skilled and adaptable naval force, thereby ensuring operational readiness and a strategic advantage. The study results emphasised the importance of simulation-based training and showed immediate outcomes for skills and knowledge.

Several generic improvements for training were identified in this study. These are: creating scenarios with updated realistic threats such as: drifting mines, drones, jammed GPS and comms; integration between different types of simulators; implementation of 4-hour shifts training during the day and night; and joint training between warships' crew and students and creating a network of simulators for EU and NATO member states.

Endnotes

[1] United States Naval Academy, „Academics," accessed May 26, 2025, https://www.usna.edu/Academics/index.php.
[2] Naval Education and Training Command (NETC), „Enclosure (1) 2025 Officer Professional Core Competencies (PCC) Manual," accessed May 26, 2025, https://www.netc.navy.mil/Portals/46/NSTC/competencies.
[3] Royal Navy, „Training at Britannia Royal Naval College," accessed May 26, 2025, https://www.royalnavy.mod.uk/careers/.../training-at-britannia-royal-naval-college.
[4] Andrew S. Erickson, „War Without Surprises: Education for Command in the PLA Navy," May 2025, accessed May 26, 2025, https://www.andrewerickson.com/2025/05/war-without-surprises-education-for-command-in-the-pla-navy/.
[5] Military School Directory, „Russia – Fleet Admiral Nikolai Kuznetsov Naval Academy," accessed May 26, 2025, https://militaryschooldirectory.com/russia-fleet-admiral-nikolai-kuznetsov-naval-academy/.
[6] Federation of American Scientists (FAS), „Japan Maritime Self-Defence Force (JMSDF)," Intelligence Resource Program, accessed May 26, 2025, https://irp.fas.org/world/japan/jmsdf.htm.
[7] École Navale, „Homepage," accessed May 26, 2025, https://www.ecole-navale.fr/.
[8] U.S. Naval Institute, „A Comparison of U.S. Navy and Royal Navy Officer Training," accessed May 24, 2025, https://www.usni.org/magazines/proceedings/2018/march/comparison-us-navy-and-royal-navy-officer-training.
[9] Romanian Naval Academy, „Romanian Naval Academy's Faculties infrastructure presentation," accessed May 27, 2025, https://www.anmb.ro/.../simulatoare/prezentare_generala.html.
[10] European Skills, Competences, Qualifications and Occupations (ESCO), „Qualifications," accessed May 23, 2025, http://data.europa.eu/esco/occupation/262f21a3-ae78-46f4-a5f9-5a1f502caa90.
[11] European Skills, Competences, Qualifications and Occupations (ESCO), „About ESCO," accessed May 23, 2025, https://esco.ec.europa.eu/en/about-esco.
[12] International Maritime Organization, „International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)," accessed May 23, 2025, https://www.imo.org/en/ourwork/humanelement/pages/stcw-conv-link.aspx.
[13] The National Authority for Management and Regulation in Communications, „Radiocommunications – Maritime services," accessed May 24, 2025, https://www.ancom.ro/en/radiocommunications_2906.
[14] MarineTraffic, „Maritime news – Accidents," accessed May 24, 2025, https://www.marinetraffic.com/en/maritime-news/14/Accidents.


©shutterstock

13

TRENDS AND PRACTICAL APPLICATIONS OF ENERGY STORAGE SOLUTIONS IN THE MILITARY

GINTARAS LABUTIS

- **Autor:** Gintaras Labutis, PhD, MBA; Research interests: military management, sustainable energy management, energy for security and defence, pro-environmental behaviour in the military, the resilience of critical energy infrastructures, energy-related technologies, and applications. The views contained in this article are the author's own and do not represent the views of the Military Academy of Lithuania.

- **Abstract:** Constantly increasing demands for efficiency, effectiveness, and resilience of military operations are interrelated with increasing military energy demands, particularly with the use of energy storage solutions. This paper provides an overview of the emerging trends in military energy use and management, along with the evolving needs for energy storage, in line with the novel developments of battery energy storage systems. The research considerations focus on a wide range of energy storage applications, ranging from soldier energy solutions to powering military bases or platforms. The study highlights future energy storage innovations, including next-generation batteries, hybrid energy solutions, or other energy storage innovation trends that will enhance the military's abilities to operate in dynamic environments.

- **Problem statement:** Where should the priority investments in advanced energy storage solutions for both existing and future military capabilities be placed?

- **Bottom-line-up-front:** Already existing energy storage solutions provide the military with new opportunities to increase efficiency and resilience and strengthen defence capabilities. By placing additional requirements on energy-related military capabilities and emphasising greater resilience, the military has the opportunity to accelerate the implementation of energy storage solutions in various applications.

- **So what?:** Military capability planners are advised to assess the impact of advanced energy storage solutions on military operational efficiency and resilience. These solutions should be integrated into existing defence capabilities, and new energy-related requirements should be established to meet the growing demand for battery energy storage. On one hand, the need for advanced energy storage solutions must be integrated into operational requirements documentation based on specific mission needs. On the other hand, these operational requirements must also align with higher-level military energy-related policies and strategies to improve energy efficiency, increase the use of renewable energy sources, reduce CO_2 emissions during operations, and enhance energy resilience. It is worth noting that many EU and NATO member states have already introduced such policies, and military defence capability planners are increasingly required to consider and incorporate these higher-level energy-related objectives into capability planning.

The Need for Energy Storage Solutions

Energy is a fundamental requirement of modern military operations, affecting everything from communications and combat effectiveness to logistics and military mobility. As global security challenges grow and become more complex, militaries increasingly recognise the importance of energy and, in particular, energy resilience–the ability to sustain military operations in complex environments where traditional energy, fuel supply chains in particular, can be disrupted and can be difficult to secure. With the ever-increasing need to increase military capabilities, developing and implementing new energy storage solutions provides new opportunities for the military.[1] Therefore, military energy plays an important role where energy storage provides additional energy efficiency and effectiveness.[2]

Currently, a variety of energy storage innovations and solutions for civilian sectors have been developed, namely: (i) Mechanical (pumped hydropower energy, compressed air energy storage, flywheels); (ii) Thermal (heat storage); (iii) Chemical (batteries, fuel cells), and (iv) Electromagnetic (supercapacitors, superconductors, magnetic energy storage).[3] From the military operational energy perspective, where the operational energy is required for the military to train, move, and sustain military operations,[4] battery energy storage systems (BESS) can be considered the most feasible and desirable solution.[5] It can be argued that the use of BESS in the military not only improves operations but also increases operational capabilities and operational resilience.[6] BESS are currently being deployed in various areas related to operational energy, which include: (i) Energy for soldiers and portable systems (communications, sensors, personal equipment), (ii) Energy for small-scale autonomous equipment that may be related to the direct energy needs of soldiers (drones and other autonomous systems), iii) Energy for ground systems including military vehicles and tactical platforms, iv) Energy for forward operating bases.[7]

Furthermore, BESS are becoming a key enabler of military operational resilience, offering portable, scalable, and efficient energy storage solutions that reduce dependence on conventional fossil fuels. In recent years, significant advances in battery technology, advanced energy management, and hybrid energy solutions have led to substantial improvements in energy across all military sectors.

In general terms, energy resilience is the ability to anticipate, prepare for, and adapt to changing conditions—and withstand, respond to, and recover rapidly from power disruptions.[8] The specified requirements for maintaining the uninterrupted energy supply are related to expected energy-related disruption scenarios. For example, the U.S. Department of Defence requires military installations to be capable of sustaining an uninterrupted energy supply to maintain critical missions at the required levels of energy availability.[9] From this resilience-related-perspective BESS solutions can effectively support critical power loads for extended periods and ensure that power outages or grid failures do not disrupt military operations. BESS are now being used to offer rapid backup power and enhanced resilience, ensuring that critical military operations can continue even under adverse conditions.[10]

Drivers Affecting BESS in Military Applications

The growing interest in and need for further implementation of BESS in the military is driven by a range of factors—some arising from direct operational needs, while others are influenced by higher-level national policies. The key trends and drivers are discussed below.

The growing need for BESS is closely linked to the military transition towards electrification worldwide, striving to mitigate and adapt to climate change.[11] Extending the use of power energy and the electrification of military operations can be considered as one of the most visible trends. Even though traditionally military operational energy relied on the power generated from conventional diesel generators, the shift towards electric power is gaining momentum and is particularly evident in the hybrid-electric and electric non-tactical military vehicles, where the advanced BESS enable them to operate efficiently across diverse terrains and missions. This trend is associated with battery energy storage applications in other operational areas, for example, for powering unmanned aerial vehicles (UAVs) or providing energy for military platforms.[12]

In general, any novel energy-related solutions must maintain or enhance operational capabilities. Efforts to improve energy resilience—especially at military bases and installations—can contribute significantly to overall military operational effectiveness.[13]

The integration of renewable energy sources is driven both by the need for higher levels of resilience and by national policies and cross-national directives aimed at supporting the energy transition. In the meantime, military forces are typically excluded from the European Union's ambitious goal of becoming the world's first climate-neutral continent by 2050 and key energy-related EU directives are not transferred to the military. However, existing examples demonstrate growing efforts to implement renewable energy generation solutions at military installations, with some systems capable of meeting up to 50 per cent of their energy needs.[14] There are also notable strategic-level decisions supporting the integration of renewables into military operations.[15]

It is important to note that the main driver for adopting renewable energy in military contexts is the need to reduce logistical burdens and associated risks, thereby enhancing the resilience of installations and bases. Currently, militaries are developing relatively small-scale renewable energy projects designed to better match infrastructure load profiles—particularly to lower energy demand during daytime hours.[16] However, the integration of the use of renewable power energy into the military bases is related to intermittency and reliability risks, as mission-critical operations require a constant and uninterrupted power supply, while renewables cannot guarantee that. BESS enhance the integration of renewable energy sources, contributing to more sustainable and independent energy for military installations and bases. Renewable power generation combined with energy storage solutions can provide more reliable power, particularly in remote or off-grid locations. This shift not only ensures a continuous power supply in austere environments but also reduces the logistical burden of fuel transportation, which is often costly and vulnerable to attacks. Additionally, integration or energy storage enhances stealth capabilities by minimising heat and noise signatures associated with traditional generators.

The shift from distributed energy generation to the installation of power grids can be a feasible solution for increasing energy efficiency via optimised generation and distribution. Military installations and military bases are increasingly adopting microgrids combined with large-scale BESS.[17] Microgrids enable installations and bases to operate more efficiently and independently from the main grid, ensuring a reliable power supply. Microgrid integration with BESS facilitates the incorporation of renewable energy sources and reduces reliance on traditional backup power systems that are usually conventional diesel generator-based. The application of smart grid technologies further optimises energy distribution and efficiency, enabling real-time monitoring and agile and adaptive power management.[18] Apart from the listed advantages, installing microgrids requires higher technical competencies from personnel for effective operation and maintenance. Additionally, the installation of microgrids can increase cybersecurity risks.[19]

As military energy systems become more connected and digitalised, they are increasingly vulnerable to cyber threats and electronic warfare, so energy management systems must incorporate robust cybersecurity means and protocols to prevent disruptions or hacking attempts.[20] Given that energy is critical to operations, any compromise or failure in cybersecurity can significantly disrupt power supply, expose sensitive data, and jeopardise energy-dependent military systems and platforms. The use of BESS requires additional cybersecurity solutions as BESS-related software solutions can be vulnerable to cyber-attacks, which could lead to severe overcharging and potential explosions or microgrid integrity. Those challenges underscore the need for robust cybersecurity measures in battery management systems.

It has to be noted that military dependence on foreign battery manufacturers has become a strategic concern during the last decade. This concern was particularly related to some BESS producers due to alleged links with foreign militaries.[21] Additionally, the tensions related to critical earth materials for battery production foster the research focused on new battery technologies in line with the development of national battery strategies and execution plans.[22,23]

As climate change and climate-related energy security concerns grow, the military is taking a bigger role in climate change mitigation and adaptation. With the worldwide intent to lower greenhouse gas emissions, the military is increasingly turning to renewable energy sources and is implementing a variety of greenhouse gas emissions reduction solutions.[24,25] Advanced BESS facilitate and enable the efficient reduction of conventional fuel use and better integration of renewable energy, thus supporting the transition from fossil fuel-based energy and reducing the overall greenhouse footprint of military operations.

Ongoing research and innovations in energy storage technologies in response to the specific energy storage requirements for military operations, through improved overall battery performance, support the increasing demand of BESS. Although Lithium-ion batteries remain prevalent due to their high energy density and efficiency, emerging technologies offer potential enhancements in energy density, energy capacity, longer lifespans, battery safety, and overall operational reliability.[26]

The key focus for military BESS is related to energy density, battery durability, and performance in extreme conditions such as harsh climates, extreme temperatures, and rough handling. When analysing military energy storage needs, it can be concluded that military operational environments pose unique challenges to energy storage that do not allow the direct use of commercial off-the-shelf solutions. However, the required battery energy density versus battery weight remains crucial for most military operational energy requirements.

Selected Operational Energy Areas for BESS Applications

BESS solutions are generally applicable across all major military branches—land, air, and naval—with domain-specific requirements for each platform. However, certain needs are common across all branches and should be highlighted. Energy requirements—for soldiers, platforms, and bases—are universally relevant and strategically managed across all branches of the military. From this perspective, the present analysis will focus on BESS solutions for soldiers, tactical and non-tactical vehicles, and BESS for military bases.

SOLDIER ENERGY

Soldier operational capabilities are directly associated with energy use: soldiers rely on large amounts of information and communication systems, including communication devices, sensors, night vision equipment, targeting systems, and others.[27] In some scenarios, the energy for the UAVS is considered part of the soldier's energy as well. Soldier portable electronic systems require lightweight, high energy capacity and durable battery solutions to ensure uninterrupted operation in a combat environment. Improvements in energy storage technologies can reduce the weight of a battery for a given amount of energy or obtain more energy from the same battery weight. This means that the desired balance of required energy („meaning more energy") and battery weight („meaning less weight") must be achieved. It is estimated that the weight of portable batteries for a dismounted soldier can reach up to 5 kilograms, and in some cases, even exceed this estimate depending on mission requirements and equipment load.[28] However, soldier energy consumption can be reduced by using advanced power management solutions or by reducing the number of different types of batteries. It is also important to meet the requirements for interoperability with other equipment. The pairing of batteries with solar renewables will extend soldiers' operational effectiveness. It has to be mentioned that the exact solar energy requirements depend on specific mission scenarios.

Efforts to reduce this weight include developing lighter, more energy-dense batteries, centralised power systems, and alternative energy sources such as solar panels and rechargeable systems. However, the need for reliable power remains critical, making battery weight a persistent challenge for modern militaries. With regard to BESS, noteworthy innovations in BESS solutions include lightweight, flexible batteries that can be integrated into armour and helmets.[29] Additionally, modular battery packs, which are interchangeable and capable of powering multiple devices while being easily recharged, are significant advancements. Smart battery management systems, which prevent overcharging and continuously monitor battery status, are also crucial developments. Beyond the use of solar energy for battery charging, research and development are investigating additional energy generation methods, such as harnessing power from a soldier's movement[30] or body heat.[31] All those needs will extend the mission duration of a dismounted soldier in extreme conditions, even without constant and reliable access to a power source. It also has to be noted that despite the variety of solutions, the advantages of the increase in battery energy density are the main focus for innovations.

ENERGY FOR LAND PLATFORMS

Traditionally, land platforms include a variety of functionalities to support and protect soldiers on the battlefield, including combat vehicles, remote-controlled equipment, targeting systems, and missiles.[32] In addition to energy density and weight, the specific mission-related energy storage parameters are important for land platforms. Usually, BESS require a wider temperature range and additional mechanical features related to increased shocks and vibration.

Presently used Lithium-Ion batteries operate within a relatively narrow temperature range. However, the optimal operating range—especially for charging—is even more limited, necessitating additional thermal management solutions (heating or cooling) to maintain battery performance and longevity in BESS applications.

Tactical vehicles provide a range of combat, logistics, and mobility functions, while non-tactical vehicles can provide support in areas that are not directly affected by combat scenarios. Traditionally, the propulsion of military vehicles relied on liquid fuels. The present trend towards electrification of non-tactical vehicles both for hybrid and electric options, reduces the reliance on conventional fuels. The increasing number of hybrid non-tactical vehicles indicates the ease of transition from fuel-based vehicles to hybrids or electric. The implementation of innovations related to hybrid solutions for tactical vehicle propulsion is limited to the demands for energy density. However, both tactical and non-tactical vehicles can provide additional on-board power for powering advanced equipment specific to military uses (e.g., weapon systems, communications, sensors).

The ability for silent operations and reduced thermal signatures can be considered[33] as the other important feature, as internal combustion engines produce significant noise and heat, making military vehicles and personnel more detectable. In contrast, battery-powered vehicles and equipment operate silently and with lower thermal emissions, improving stealth and survivability.[34] The advantages of BESS can also provide longer endurance for unmanned systems such as drones (UAVs), and autonomous ground vehicles (UGVs) that rely on high-density battery storage for extended mission durations, increasing the operational range and mission capabilities of these systems.[35] From the considerations mentioned above, it has to be stated that BESS solutions for land platforms/systems support the enhancement of military capabilities and open new capability options for the military.

ENERGY FOR FORWARD OPERATING BASES

Military forward operating bases (FOBs) require a secure, uninterrupted energy supply to power the functioning of command and control units, surveillance and force protection systems, other operational facilities, including food processing, water and sewage systems, and other Quality of Life (QoL) related systems. FOBs usually consist of temporary (tents) or semi-permanent structures with basic or extended services. In most cases, the energy supply for FOBs relies on fuel generators combined with energy supply from external power grids. For advanced FOBs internal microgrid solutions can be provided. Small-scale FOBs, such as combat outposts (COPs) or forward operating sites (FOSs), can represent infrastructure with basic shelter solutions and other limited facilities, such as small-scale command and control centre, water storage, and other limited facilities, when conventional fuel generators usually provide the limited power supply. Diesel generators traditionally employed at FOBs and COPs are inefficient, noisy, and vulnerable to attacks. In contrast, BESS solutions can optimise fuel use during periods of low energy demand and enhance the overall efficiency of generators.

The integration of batteries with diesel generators enhances fuel efficiency and reduces fuel consumption.[36] This is achieved through several mechanisms. The load levelling allows batteries to manage fluctuating power demands, enabling generators to operate at optimal efficiency rather than idling or running at low loads, which is both inefficient and harmful to the equipment. The BESS help reduce generator idle time by supplying power during low-load periods, allowing the generator to be turned off entirely. By decreasing generator runtime, fuel consumption is conserved, which is especially critical in remote or hostile environments where resupply is difficult. Additionally, batteries provide reliable backup power for mission-critical systems, ensuring uninterrupted command and control operations during power failures. They also maintain operational continuity during grid outages or cyber-attacks. And finally, the reliance on batteries reduces the vulnerability of fuel supply lines, minimising the risks associated with fuel transportation disruptions.[37]

BESS solutions for FOBs and COPs provide additional capabilities to use existing generators with the possibility to integrate alternative energy solutions, particularly Photovoltaic (PV) systems. At the same time, the wind power is limited due to terrain specifics related to military base protection, radar functioning, or technical and engineering requirements.[38,39] However, PV solutions require good power management systems to integrate with existing energy systems successfully and efficiently. In this respect, the BESS facilitate the integration of PV and play a substantial role in reducing fuel demands. Battery storage combined with renewable sources allows FOBs to operate independently for longer durations. In general, FOBs and COPs experience logistical challenges of delivering fuel, so the most direct application of energy storage is to support the existing infrastructure in ways that reduce overall fuel use. The additional viable solution is related to microgrid solutions for the base as the integrated system of energy-generating, energy-storage, and energy controls and energy management system to optimise generating capacity and to adjust the power generation as loads increase or decrease. Microgrid technologies also incorporate automated control technologies and aggregate load demand from multiple sources to meet the system's current and expected power demands most efficiently. During the structured interviews with military energy users, it was concluded that BESS for FOBs or other deployed force infrastructure can be considered as the key priority area for efficient military energy use and demands for energy resilience.[40,41] Military operations require rapid deployment of energy solutions that can be scaled according to the mission's needs. Modular systems can be integrated with renewables (solar, wind), hybrid systems, or traditional generators for optimised performance.[42]

Modular and scalable battery storage systems (battery packs) allow for flexible energy provision across various operations, from small reconnaissance missions to large-scale combat operations: It is worth noting that NATO's current flagship energy security research project focuses on energy monitoring, metering, and optimisation in deployed camps and the battlefield, with Ukraine among the participating members.[43]

Existing BESS Technologies Solutions for Military and Ongoing Innovations in BESS

As the military seeks more efficient, reliable, and resilient energy storage solutions, various battery technologies are being integrated into the military. Each technology offers unique advantages and challenges, depending on the specific operational requirements, such as mobility, durability, energy density, and rechargeability.

Presently, the following battery storage technologies are in use, with ongoing developments specifically tailored for military applications. These include Lithium-ion batteries with further improvements and modifications, solid-state batteries (SSB), iron-based batteries, such as iron flow or iron–air batteries, and metal-air batteries.[44]

Li-ion batteries have become the dominant energy storage technology in both civilian and military applications due to their high energy density and rechargeability.[45] Li-ion batteries offer several advantages. They provide high energy density, which translates into long-lasting power for mission-critical equipment. They are rechargeable and scalable, making them suitable for a wide range of applications—from handheld radios to electric combat vehicles. Moreover, they are mature and commercially available, supported by well-developed supply chains and large-scale global production. Despite their widespread military applications, Li-ion battery energy storage systems (BESS) face several limitations and challenges. These include thermal runaway and safety risks, as Li-ion batteries are prone to overheating, fire, and explosion under extreme conditions. Additionally, they have a limited lifespan, with performance degrading over time. Another critical concern is the vulnerability of the supply chain, as key raw materials such as lithium, cobalt, and nickel are primarily extracted in geopolitically sensitive regions, posing risks to secure and stable procurement. Despite the existing limitations of Li-ion BESS, lithium-ion batteries continue to dominate most applications, with major efforts focused on mitigating their disadvantages. To reduce supply chain vulnerabilities, sodium-ion batteries have emerged as a result of efforts to replace lithium with more abundant and less critical elements, such as sodium.[46]

Solid-state batteries (SSBs) represent the next generation of battery technology, addressing many of the safety and performance limitations associated with traditional lithium-ion batteries. Unlike conventional designs that rely on liquid electrolytes, SSBs use solid electrolytes, which improve stability, energy density, and longevity.[47] SSBs offer several key advantages: they provide higher energy density, enabling greater energy storage compared to traditional lithium-ion batteries; their use of solid electrolytes significantly enhances safety by eliminating the fire risks linked to thermal runaway. In addition, SSBs demonstrate improved durability, being more resistant to temperature fluctuations and physical damage. They also offer a longer lifespan, with minimal degradation over repeated charge cycles. Furthermore, SSBs currently exhibit slower charge and discharge rates compared to lithium-ion batteries. Nevertheless, the future outlook for SSBs in military applications is promising, and it is expected that the wide-scale production of SSBs will start in 2026.[48] Their potential is particularly strong in areas such as soldier systems that require lightweight, high-capacity energy storage; long-endurance unmanned aerial vehicles; and resilient forward operating base (FOB) energy grids that demand lower failure rates and safer operation. It is also worth mentioning the NATO SPS project focused on the development of thin-film SSBs with efficient, stable, and safe performance in low-temperature environments. The project aims to address key issues associated with liquid electrolytes, including high-temperature swelling, leakage under external pressure, and ignition risks.[49]

Flow batteries are designed for long-duration energy storage, making them particularly well-suited for military bases, command centres, and microgrid solutions. Unlike traditional batteries, they store energy in liquid electrolytes that circulate through electrochemical cells, allowing for efficient and sustained energy delivery.[50] These batteries offer several advantages for military applications. They have a long operational lifespan, often exceeding 20 years with minimal degradation. Their storage capacity is easily scalable by expanding the size of the electrolyte tanks, making them adaptable to various energy demands. Additionally, flow batteries support rapid charging and allow deep discharging without compromising performance, which makes them well-suited for continuous power supply in microgrid setups. However, flow batteries also present several limitations and challenges. Their relatively low energy density makes them unsuitable for portable applications such as soldier systems or military vehicles. They are also heavy and large in size, which limits mobility and deployment flexibility. Furthermore, their maintenance is more complex due to the intricate systems required for electrolyte circulation. Despite these challenges, flow batteries hold strong potential in military use cases, particularly for large-scale energy storage at bases and forward operating positions, as well as for integration with renewable energy sources like solar and wind.

Metal-air batteries, such as aluminium-air, zinc-air, and lithium-air variants, currently offer the highest energy densities of any battery technology. These batteries are exceptionally lightweight, making them highly attractive for military applications with critical weight and energy capacity.[51] The key advantages of metal-air batteries include their extremely high energy density and ability to store up to ten times more energy than conventional lithium-ion batteries. Their lightweight nature enhances portability, which is especially important for long-range missions. Additionally, metal-air batteries have an extended shelf life, remaining operational over long periods without significant degradation. However, these batteries also face notable limitations. They typically have a slow discharge rate, making them unsuitable for applications that require high power output or rapid energy delivery. Corrosion and stability issues also pose technical challenges, particularly in harsh or variable environments. Despite these drawbacks, metal-air batteries hold strong potential in specific military use cases. The current NATO SPS research project, High Energy Calcium-Oxygen Batteries, focuses on the development of advanced calcium-oxygen batteries as a promising alternative to lithium-ion technology. The project aims to develop a rechargeable battery with high energy density. These innovations strive to establish efficient and widely adoptable post-lithium technologies, addressing both the environmental impact of lithium extraction and potential future supply shortages.[52]

It should be noted that the selected types of BESS do not represent the full range of technologies successfully used in the military; rather, they highlight some of the most commonly used or potentially most applicable solutions. In addition to existing and adapted solutions, some promising technological innovations are emerging, with potential final adaptation for military applications, such as lithium-sulphur batteries, which provide high energy density and are considered promising alternatives to lithium-ion batteries, particularly for applications that prioritise lightweight design and long endurance, such as wearable electronics and small UAVs.[53] Graphene-based batteries are recognised for their lightweight structure, rapid charging capabilities, and high energy density. These attributes make them particularly well-suited for high-performance military applications, including soldier-worn power systems, electric and hybrid vehicles, and other portable energy sources.[54] It has to be noted that the developments in nanotechnology are opening new research and development opportunities for BESS.[55]

In alignment with the military's shift toward more sustainable energy practices, there is an increasing focus on battery end-of-life management. Key priorities include recycling, safe disposal, and the development of environmentally friendly materials. Future battery technologies will be designed for easier recycling, minimising waste, and reducing dependence on raw material extraction. Ongoing research into biodegradable and recyclable materials aims to make military energy storage solutions more sustainable and eco-friendly.[56]

The integration of artificial intelligence with BESS is poised to revolutionise military energy management. AI technologies will predict energy demand, optimise charging cycles, and help prevent energy shortages. Intelligent energy management platforms will dynamically allocate power across portable systems, vehicles, and installations, improving efficiency in complex operational environments.[57] Additionally, AI-driven systems will automate charging schedules and optimise energy distribution, reducing downtime and ensuring continuous power availability across military assets. It is also expected that through the AI applications, the BESS research will receive additional means for new battery chemistry-related solutions.[58]

Based on this review of ongoing research on BESS, one can conclude that there are focused efforts in research and innovation. It should be noted that the scope of BESS research and innovations encompasses a wide variety of options.[59,60] Recent European Defence Fund (EDF) calls also highlight the urgent need for improved energy management at military bases, emphasising the development of novel energy storage solutions—specifically, next-generation electrical energy storage for military forward operating bases and energy-independent, efficient systems for military camps.[61, 62]

Discussion and Conclusions

The analysis of military needs for battery energy storage systems (BESS) and the existing solutions indicates that the demand for advanced energy storage is growing as modern and future defence capabilities require increasing amounts of energy. This trend is particularly evident in the energy storage needs of unmounted soldiers. For land platforms and expeditionary military bases, the operational use of BESS is largely limited to traditional solutions. Military-related energy and energy-related resilience for the military can be substantially enhanced with broader BESS implementation.

In many critical cases, energy storage solutions are effectively integrated into military energy infrastructures, although they are not fully recognised in many scenarios. Examining current BESS demonstrates that these solutions are already in use, mostly on a small scale. BESS can be further integrated, provided military capability development institutions and units establish clear operational requirements. It is important to note that the operational requirements for BESS vary and must be tailored to specific mission needs without compromising overall capabilities.

The formulation of BESS-related operational requirements is closely tied to a policy-level strategic approach that integrates BESS solutions as a component of energy resilience. These requirements—driven by energy demands and potential disruption scenarios—should be defined not at the individual military unit level but at the broader energy policy and strategic planning level.

From this perspective, energy storage solutions will improve energy efficiency and significantly enhance energy resilience. As research continues to yield more feasible BESS options, these systems are expected to be deployed on a wider scale across military systems and units. The evolving energy requirements for specific operational areas underscore the growing need for BESS, provided that these solutions meet the strict demands of military applications. Present requirements for BESS also highlight the need for continued battery storage innovation, which can be achieved through collaborative multinational research efforts supported by public financing.

Endnotes

[1] Luiz Pereira da Silva Neto and Marcio José Sorgato, How Are the Military Handling Energy? An Overview of International Status and Suggestions for the Brazilian Armed Forces: Technical Report, 1st ed. (Campo Grande: PPGEES/FAENG/UFMS, Federal University of Mato Grosso do Sul, 2021).
[2] F. C. Lucchese, L. N. Canha, and W. S. Brignol, "A Review on Energy Storage Systems and Military Applications," in Proceedings of the 2020 55th International Universities Power Engineering Conference (UPEC) (Piscataway, NJ: IEEE, 2020), https://doi.org/10.1109/UPEC49904.2020.9209892.
[3] Dina A. Elalfy et al., "Comprehensive Review of Energy Storage Systems Technologies, Objectives, Challenges, and Future Trends," Energy Strategy Reviews 54 (2024): 101482, https://doi.org/10.1016/j.esr.2024.101482.
[4] Mason Carpenter, Paul Sullivan, and Dan Nussbaum, Operational Energy—Essential Knowledge for Military Officers (Monterey, CA: Naval Postgraduate School, n.d.), accessed June 1, 2025, https://nps.edu/web/eag/operational-energy-essential-knowledge-for-military-officers.
[5] Scott Childers, "How Is the U.S. Military Using Stationary Energy Storage Today?" Battery Power Online, December 19, 2022, accessed June 1, 2025, https://www.batterypoweronline.com/news/how-is-the-u-s-military-using-stationary-energy-storage-today/.
[6] A. R. Jha, Next-Generation Batteries and Fuel Cells for Commercial, Military, and Space Applications (Boca Raton, FL: CRC Press, 2012).
[7] Richard H. Van Atta, The Role of Energy Storage in Meeting 21st Century Department of Defense Energy Demands, NS D-4902 (Alexandria, VA: Institute for Defense Analyses, 2013).
[8] "Army Installations Test Energy Resilience," Naval Postgraduate School, accessed March 23, 2025, https://nps.edu/web/eag/army-installations-test-energy-resilience.

[9] "10 U.S. Code § 2920 – Energy Resilience and Energy Security Measures on Military Installations," Legal Information Institute, Cornell Law School, accessed March 23, 2025, https://www.law.cornell.edu/uscode/text/10/2920.
[10] Janice Mallery, Douglas L. Van Bossuyt, and Anthony Pollman, "Defense Installation Energy Resilience for Changing Operational Requirements," Designs 6, no. 2 (2022): 28, https://doi.org/10.3390/designs6020028.
[11] Marju Kõrts, Energy Storage and Energy Efficiency as the Key Enablers of Greater Use of Renewable Energy in Electricity Consumption (Vilnius: NATO Energy Security Centre of Excellence, 2024), https://www.enseccoe.org/publications/energy-storage-and-energy-efficiency/.
[12] British Army, British Army Approach to Battlefield Electrification (London: UK Ministry of Defence, 2024), https://www.army.mod.uk/media/17010/british-army-approach-to-battlefield-electrification.pdf.
[13] Hillary Bassett et al., "Energy for Military Installations: 4 Strategies for Enhancing Resilience," Salas O'Brien, November 14, 2023, https://salasobrien.com/news/energy-resilience-for-military-bases/.
[14] United States Marine Corps, United States Marine Corps Installations Energy Strategy (Washington, DC: United States Marine Corps, 2015), https://www.mcicom.marines.mil/Portals/57/Docs/GF%20Energy/Energy%20Strategy.pdf.
[15] Ministry for the Armed Forces (France), Defence Energy Strategy: Energy Working Group Report 2020 (Paris: Ministry for the Armed Forces, 2020), https://www.defense.gouv.fr/sites/default/files/ministere-armees/Defense%20energy%20strategy.pdf.
[16] "Solar-Powered Defence: How Renewable Energy Is Shaping Modern Military Operations," Foresight Learn, 2024, https://foresightlearn.com/solar-powered-defense-how-renewable-energy-is-shaping-modern-military-operations/.
[17] American Security Project, Perspective: Enabling Factors for Achieving U.S. Army Microgrid Goals (Washington, DC: American Security Project, 2023), https://www.americansecurityproject.org/wp-content/uploads/2023/09/Ref-0285-Perspective-Enabling-Factors-for-Achieving-U.S.-Army-Microgrid-Goals.pdf.
[18] Steven Curtis and Peter D. Rocha, "Microgrids for the 21st Century: The Case for a Defence Energy Architecture," Joint Force Quarterly, no. 112 (2024), https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3672465/microgrids-for-the-21st-century-the-case-for-a-defense-energy-architecture/.
[19] Nicholas Barry and Surya Santoso, "Modernising Tactical Military Microgrids to Keep Pace with the Electrification of Warfare," Military Review (November–December 2022), https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2022/Barry/.
[20] Sinclair Koelemij, "BESS Cyber-Physical Risk," Industrial Cyber, 2024, https://industrialcyber.co/expert/bess-cyber-physical-risk/.
[21] Juan F. Villarreal, Battery Energy Storage Systems from China: Being Realistic about Costs and Risks, IGP White Paper no. 12 (Atlanta: Internet Governance Project, 2024), https://www.internetgovernance.org/wp-content/uploads/Villareal-BESS-June-2024.pdf.
[22] U.S. Department of Defense, 2023–2030 DoD Lithium Battery Strategy (Washington, DC: U.S. Department of Defense, 2023), https://www.businessdefense.gov/ibr/pat/battery-strategy.html.
[23] Department for Business and Trade, UK Battery Strategy (London: UK Government, 2023), https://assets.publishing.service.gov.uk/media/656ef4871104cf000dfa74f3/uk-battery-strategy.pdf.
[24] International Military Council on Climate and Security, Decarbonised Defence: The Need for Clean Military Power in the Age of Climate Change. A Volume of the World Climate and Security Report 2022 (Washington, DC: International Military Council on Climate and Security, 2022), https://imccs.org/wp-content/uploads/2022/06/Decarbonized-Defense-World-Climate-and-Security-Report-2022-Vol.-I.pdf.
[25] European External Action Service, Climate Change and Defence Roadmap (Brussels: European Union, 2020), https://data.consilium.europa.eu/doc/document/ST-12741-2020-INIT/en/pdf.
[26] EticaAG Team, "The Best Battery Chemistry Types for Energy Storage: A Guide to Safety and Efficiency," EticaAG, 2025, https://eticaag.com/best-battery-types-for-energy-storage-guide/.
[27] Tim Guest, "Portable Power Storage for the Dismounted Soldier," European Security & Defence, February 2024, https://euro-sd.com/2024/02/articles/36599/portable-power-storage-for-the-dismounted-soldier/.

[28] Thales Group, “Reducing the Battery Burden on the Dismounted Soldier,” Thales Group, accessed March 23, 2025, https://www.thalesgroup.com/en/global/presence/europe/united-kingdom/defence/land-systems/soldier-systems/squadnet/reducing-battery.
[29] Qi Zhang et al., “Flexible Wearable Energy Storage Devices: Materials, Structures, and Applications,” Journal of Energy Storage (2023), https://doi.org/10.1002/bte2.20230061.
[30] João Vitorino, Bruno Damas, and Vítor Viegas, “Harvesting Energy from a Soldier's Gait Using the Piezoelectric Effect,” Energy Harvesting and Systems, July 30, 2024, https://doi.org/10.1515/ehs-2023-0149.
[31] Mikayla Easley, “Army Exploring New Tech to Charge Up Troops on the Go,” National Defense Magazine, May 27, 2022, https://www.nationaldefensemagazine.org/articles/2022/5/27/army-exploring-new-tech-to-charge-up-troops-on-the-go.
[32] Brendan Sims and Simon Crase, Review of Battery Technologies for Military Land Vehicles, DST-Group-TN-1597 (Land Division, Defence Science and Technology Group, 2017), https://www.dst.defence.gov.au/publication/review-battery-technologies-military-land-vehicles.
[33] Amprius Technologies, “Energy Density in Unmanned Aerial Systems (UAS),” Amprius, accessed April 22, 2025, https://amprius.com/about/news-and-events/energy-density-uas/.
[34] Steve Carkner, “The Battery's Role in the Evolving Military Ground Vehicle,” Military Embedded Systems, November 20, 2023, https://militaryembedded.com/comms/vetronics/the-batterys-role-in-the-evolving-military-ground-vehicle.
[35] Amprius Technologies, “Energy Density in Unmanned Aerial Systems (UAS).”
[36] Andrea Manfredini et al., Phase 1 Report: Performance Analysis of Hybrid Power Generation and Management System (HPGS) (Vilnius: NATO Energy Security Centre of Excellence, 2018), https://www.enseccoe.org/wp-content/uploads/2024/01/2019-03-phase-1-report-hpgs-performance-analysis.pdf.
[37] Scott Childers, “How Is the U.S. Military Using Stationary Energy Storage Today?”
[38] Task Force on Energy Systems for Forward/Remote Operating Bases, Final Report (Washington, DC: Department of Defense, Defense Science Board, 2016), https://apps.dtic.mil/sti/citations/AD1022571.
[39] Scott M. Katalenich and Mark Z. Jacobson, “Renewable Energy and Energy Storage to Offset Diesel Generators at Expeditionary Contingency Bases,” Journal of Defence Modelling and Simulation 20, no. 2 (2023): 143–57, https://doi.org/10.1177/15485129211051377.
[40] Ameresco, “Ameresco Awarded 6-MW Battery Energy Storage System (BESS) at U.S. Army's Fort Detrick Base,” Ameresco, 2022, accessed June 1, 2025, https://www.ameresco.com/ameresco-awarded-6-mw-battery-energy-storage-system-bess-at-u-s-armys-fort-detrick-base/.
[41] Energy General Solutions, “BESS for Military Bases,” Energy General Solutions, accessed May 19, 2025, https://energygeneralsolutions.com/bess-for-military-bases/.
[42] “US Military Pushes Clean Energy with Largest On-Base Battery,” Utility Dive, August 22, 2018, accessed June 1, 2025, https://www.utilitydive.com/news/us-military-pushes-clean-energy-with-largest-on-base-battery/530671/.
[43] NATO, “NATO-Funded Scientific Project to Improve Allied Operational Energy Effectiveness, and Support Ukraine,” February 27, 2025, accessed April 29, 2025, https://www.nato.int/cps/en/natohq/news_233501.htm.
[44] Benjamin Vaughan, Lucas Freeman, and Lucas Watkins, “Battery Technologies: Where Are We Now, and Where Are We Going?” Energy and Climate Counsel, Foley Hoag, June 6, 2024, https://foleyhoag.com/news-and-insights/blogs/energy-and-climate-counsel/2024/june/battery-technologies-where-are-we-now-and-where-are-we-going/.
[45] Tycorun, “How Are Lithium-Ion Batteries Used in National Defence and Military Affairs?” Tycorun, January 7, 2022, https://www.tycorun.com/blogs/news/how-are-lithium-ion-batteries-used-in-national-defense-and-military-affairs.
[46] Agnieszka Iwan et al., “The Safety Engineering of Sodium-Ion Batteries Used as an Energy Storage System for the Military,” Energies 18, no. 4 (2025): Article 978, https://doi.org/10.3390/en18040978.
[47] Renogy, “Solid State Lithium Batteries: Everything You Need to Know,” March 13, 2025, https://www.renogy.com/blog/solid-state-lithium-batteries.

[48] Dr. Xiaoxi He, "Solid-State Battery Commercialization: Mass Production Taking Off," IDTechEx, April 7, 2025, accessed April 29, 2025, https://www.idtechex.com/en/research-article/solid-state-battery-commercialization-mass-production-taking-off/32942.
[49] NATO Science for Peace and Security Programme, Thematic Report, Energy and Environmental Security (Brussels: NATO, 2024).
[50] Sophia Espinosa, "ERDC Celebrates Milestone with GridStar Flow Battery Installation at Fort Carson," U.S. Army, December 4, 2024, accessed June 2, 2025, https://www.army.mil/article/281763/erdc_celebrates_milestone_with_gridstar_flow_battery_installation_at_fort_carson.
[51] B. M. L. Rao et al., "Aluminum-Air Batteries for Military Applications," in Proceedings of the IEEE 35th International Power Sources Symposium (Cherry Hill, NJ, USA, June 22–25, 1992): 123–129. https://doi.org/10.1109/IPSS.1992.282061.
[52] NATO Science for Peace and Security Programme, Energy and Environmental Security.
[53] Mohammed Jasim M. Al Essa. 2024. "Applications and Challenges of Lithium-Sulfur Electrochemical Batteries." Journal of Electrochemical Science and Technology 15, no. 1: 1–13. https://www.jecst.org/upload/pdf/jecst-2023-00199.pdf.
[54] Defence Systems Information Analysis Center (DSIAC), "Graphene: A Miracle Material with Promising Military Applications," DSIAC Journal 5, no. 2 (Spring 2018), accessed June 2, 2025, https://dsiac.dtic.mil/articles/graphene-a-miracle-material-with-promising-military-applications/.
[55] Amprius Technologies, "Amprius Technologies Awarded U.S. Army Contract to Develop 100% Silicon Anode Li-Ion Batteries Using Si-Nanowire," Amprius Technologies, 2021, accessed June 1, 2025, https://amprius.com/amprius-technologies-awarded-u-s-army-contract-to-develop-100-silicon-anode-li-ion-batteries-using-si-nanowire/.
[56] Zhuang Kang et al., "Recycling Technologies, Policies, Prospects, and Challenges for Spent Batteries," iScience 26, no. 11 (2023): 108072. https://doi.org/10.1016/j.isci.2023.108072.
[57] Josh MacDonald, "The Role of Artificial Intelligence in Optimising Battery Performance," T&D World, accessed March 23, 2025, https://www.tdworld.com/distributed-energy-resources/energy-storage/article/21283230/the-role-of-artificial-intelligence-in-optimizing-battery-performance.
[58] Teo Lombardo et al., "Artificial Intelligence Applied to Battery Research: Hype or Reality?" Chemical Reviews 122, no. 12 (2021): 10899–10969, https://doi.org/10.1021/acs.chemrev.1c00108.
[59] Balaraman Vedhanarayanan and K. C. Seetha Lakshmi, "Beyond Lithium-Ion: Emerging Frontiers in Next-Generation Battery Technologies," Frontiers in Battery and Electrochemistry 3 (April 5, 2024), https://doi.org/10.3389/fbael.2024.1377192.
[60] Khaled Itani and Alexandre De Bernardinis, "Review on New-Generation Batteries Technologies: Trends and Future Directions," Energies 16, no. 22 (2023): 7530, https://doi.org/10.3390/en16227530.
[61] European Commission, NOMAD – Novel Energy Storage Technologies Usable at Military Deployments in Forward Operating Bases, Project ID 101103074, European Defence Fund (EDF), accessed April 29, 2025, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103074/EDF.
[62] INDY Project, Energy Independent and Efficient Deployable Military Camps, accessed April 29, 2025, https://www.indycamp.eu/about.


IOT

14

RESILIENCE AND AGILITY: SUPPLY CHAIN REQUIREMENTS IN MILITARY OPERATIONS

ANA-MARIA MERLUSCA, MATEI-ALEXANDRU ROPOTAN

- **Author:** Major Ana-Maria Merlusca, Superior Instructor, Ph.D. candidate, Command and Staff Faculty, "Carol I" National Defence University. Research interests: military transportation, autonomous vehicles, and logistics planning. Earlier publications: „Digital technologies used in the field of military transport", in Bulletin of „Carol I" National Defence University No.2/2024, „Theoretical-practical incongruences of logistic support in the fight for the conquest of Kiev", in Romanian Military Thinking Conference 2024. Academic fields: logistics, marketing, transportation.

  Matei-Alexandru Ropotan, military student in „Carol I" National Defence University, Bucharest, specialising in Quartermaster studies. Graduated from „Vasile Alecsandri" National College, with a specialisation in Mathematics and Computer Science. Interests: military logistics and the integration of emerging technologies in defence. Academic fields: logistics, education, environment.

  The views contained in this article are the authors' alone and do not represent the views of the National Defence University "Carol I".

- **Abstract:** In a less predictable operational environment, resilience and agility are vital requirements for military sustainment. To demonstrate this, we highlight the shortcomings in military supply chains and identify solutions and practices adopted by various organisations to address recognised challenges. Furthermore, there is a need to understand more about new practices and innovations in the business environment that impact supply chains. In conclusion, we highlight several key aspects that military leaders must address to enhance supply chain resilience and agility).

- **Problem statement:** What practices used by large companies can be adopted by military organisations to make military supply chains resilient and agile?

- **Bottom-line-up-front:** Logisticians need to understand how organisations use technological advances and implement solutions so that the military decision-makers can improve resilience and agility in supply chains.

- **So what?:** The military supply chains of NATO's recent allies face a series of challenges, such as supply disruptions, demand variability, limited visibility and transparency. Large companies encounter many of the same shortages and have developed different practices to mitigate them by using new technologies. Military decision-makers should be informed about best practices and new technologies to enhance the resilience and agility of supply chains.

Introduction

In military operations, the effectiveness of supply chains can often determine the success or failure of missions. As global conflicts become increasingly unpredictable and complex, the concepts of resilience and agility have emerged as critical requirements in military supply chain management.

Logistic operations evolved in tandem with technological advances, primarily to sustain military operations effectively. Logistic operations need to be planned and conducted using information tools that make it harder for the adversary to hinder them. Logistic planners must keep pace with reality as the operational environment becomes contested in multiple domains. As the dynamics of operations tend to develop much faster than before, primarily due to the possibilities of real-time data collection and advanced surveillance and intelligence capabilities, the practices used in logistics must be addressed to respond to new war technologies.

While resilience and agility can be viewed as distinct concepts, they are fundamentally interconnected in the context of military operations. A resilient supply chain sets the foundation for agility; thus, without the ability to absorb and recover from shocks, a supply chain cannot effectively respond to changes. Additionally, a supply chain that lacks agility may falter in the face of disruptions, undermining its resilience.

This interrelationship emphasises the need for integrated supply chain strategies in military logistics. For example, a military force must maintain sufficient inventory levels for critical supplies to bolster resilience while ensuring that those supplies can be quickly adapted to meet changing operational needs, thus enhancing agility.

Large companies like Renault, Morrisons,[1] Shippeo[2] and many others use a variety of advanced technologies to optimise supply chain management, including Artificial Intelligence, Machine Learning, the Internet of Things, Blockchain Technology and Radio Frequency Identification. The use of these technologies has helped optimise demand forecasting in goods and services, and increase sustainability, thus reducing waste and logistics demand in transportation.

Defining Logistics and Supply Chain Management

Logistics is a process involving as many stakeholders as an organisation considers fit to accomplish its goals. Whether the organisation's activity is in the realm of commerce or in the military sector, logistics plays a fundamental role in the supply chain management. There is a genuine need for resource procurement and distribution planning to ensure that all goods and services are provided to customers in a timely and cost-effective manner. Logistics is plan-oriented to safeguard product flow from suppliers to consumers. In contrast, supply chain management aims to create the necessary links between the organisation and other stakeholders or entities to achieve effectiveness.[3]

Over the last decades, supply chain management has been seen by theorists as a practical tool to manage and coordinate the entire supply chain, from the initial suppliers of raw materials to a production factory, possibly to a wholesale business or directly to a retailer, and finally to the consumer. Nowadays, due to the objective of achieving synergy throughout the entire supply chain, the process has become more complex and reliant on factors such as information access, competition for resources, and customer satisfaction.

Military logistics are not much different, to the effect that the provision of goods and services for the fighting forces depends deeply on the availability of suppliers, the timely access to precise information about stocks and distribution, and the protection of sensitive data. In the military domain, customer satisfaction is not just a priority but rather a precondition for operational success. In this case, the customer may be a soldier who needs ammunition, fuel, water, and food, or a tactical unit that requires transportation, evacuation, or resupply. In both civilian and military situations, the operational planning process focuses on delivering the necessary material to the right place at the right time, as cost-effectively as possible.

The military operating environment is complex, uncertain, and vulnerable to numerous factors, including information and intelligence vulnerabilities, adversary threats, competition for resources, and dependence on infrastructure. However, what sets it apart from commercial supply chains is the fact that time is more valuable than profit, because an army without ammunition to fight or fuel to move its equipment has low chances of achieving success in battle. The challenges to military logistics primarily involve the timely and coordinated transportation of materials, such as ammunition, food, or fuel.[4] Supply chain management focuses on delivering profitable outcomes to all stakeholders involved in the chain. For the military domain, sometimes a profitable outcome means gaining time; for example, the combat forces are resupplied faster than the enemy. In that regard, some may argue that the phrasing „demand network management"[5] would be more accurate. For example, Martin Christopher notes that the supply process should focus more on consumer satisfaction rather than market demand. He argues that the process is dependent on multiple suppliers and is not just a linear chain. Military supply chain profitability and customer satisfaction are achieved through effective demand network management, which optimises resources and ensures reliable service delivery.

The concept of Supply Chain Management (SCM) originates from research in marketing, logistics, organisational theory, and operational management. In 1982, R. Oliver and M. Webber were the first to use the term SCM to integrate all logistical and informational processes, from the consumer to primary suppliers. According to these authors, the role of the SCM concept is to ensure that „functional objectives [of top management] do not conflict throughout the logistics chain, as they are reconciled and balanced".[6] In the same vein, other authors[7] describe the goal of SCM as developing synergy across the entire supply chain by applying a set of practices for the complete management and coordination of supply chains. The benefits gained from implementing SCM most commonly include cost reduction and increased value offered.

In a summarised view, the supply chain is a sequence of relations that usually begins with the production phase of goods, continues with delivery to retailers, and concludes with delivery to the consumer. In the supply chain, relationships among producers, suppliers, and consumers are complex, and information needs to flow in all directions to ensure continuous improvement in production. Companies have multiple suppliers and consumers in the complex business environment, and supply chain synergy is achieved when final costs are reduced.

Military Supply Chains Shortfalls

As previously emphasised, military supply chains are essential components of logistic operations, ensuring that troops are provided with the necessary supplies, equipment, and services. However, despite their critical importance, military supply chains often encounter various shortfalls and deficiencies that may hinder operational effectiveness.

Shortfall	Cause	Possible effect
Supply disruptions	• Natural disasters • Geopolitical events • Logistical challenges	• Shortages of critical materials • Affected the readiness and effectiveness of military units
Demand variability	• Changing battlefield conditions • Evolving mission requirements	• Wasted resources • Increased costs • Diminished operational readiness
Logistical inefficiencies	• Multiple supply routes synchronisation • Transportation modes and distribution channels coordination	• Route obstructions, bottlenecks • Provision delays
Limited visibility and transparency	Delayed information regarding: • Status of supplies • Inventory levels • Logistical operation	• Hindered decision-making process • Reduced operational responsiveness • Delays in supply deliveries • Inability to respond to changing operational demands
Resource Constraints	• Budgeting • Personnel training	• Efficiency of supply chain operations

Foremost, supply chain shortfalls in military organisations; Source: Author.

Factors such as natural disasters and geopolitical events can lead to supply disruptions, resulting in critical material shortages that affect the readiness and effectiveness of military units. Meanwhile, demand variability driven by changing battlefield conditions and evolving mission requirements can lead to wasted resources and increased costs, also diminishing operational readiness.

Moreover, logistical inefficiencies, including the weak synchronisation of multiple supply routes and coordination of transportation modes, can create bottlenecks and delays that undermine the timely provision of necessary materials. Limited visibility and transparency hinder decision-making processes, which in turn reduce operational responsiveness and the ability to adapt to dynamic battlefield circumstances. Additionally, resource constraints related to budgeting and personnel training further exacerbate these issues, affecting the overall efficiency of supply chain operations.

For businesses, supply chain shortfalls can produce significant costs, affecting not only their bottom line but also their long-term viability and competitive standing in the market. Addressing these shortfalls proactively, through new practices, is essential for minimising their impact and ensuring operational resilience.

Similarly, considering the military supply chain's vital role in ensuring operational effectiveness, the various shortfalls identified pose significant challenges to providing troops with the necessary supplies, equipment, and support to ensure mission success. In the early weeks of the invasion of Ukraine, one could observe the operational impact of poor supply chain visibility, the strong reliance upon manual or outdated communication systems, or the lack of real-time data about supply route conditions. The result of a dysfunctional supply chain contributed to the Russian armed forces' inability to accomplish their mission of conquering Kyiv.[8] Most probably, the operation was designed by Russian strategists to capitalise on surprise and seize the initiative through rapid territorial gains. While the initial execution aligned with the plan, it soon became apparent that critical logistical aspects had not been adequately prepared. The swift advance of Russian forces resulted in overextended supply lines. To preserve operational secrecy, the attack plan was withheld from logistics planners, leaving them without the necessary information to allocate resources in line with Russian logistics doctrine. Additionally, the high tempo of the offensive caused breakdowns in communication systems, with unsecured transmissions intercepted by Ukrainian forces, who then targeted and disrupted Russian resupply convoys.

Military supply chains can better support troops and fulfil their critical mission requirements in unpredictable environments by proactively managing these shortfalls and implementing approaches that bolster resilience and agility.

Resilience in Military Supply Chains

Resilience in a military supply chain refers to the ability to anticipate, respond to, and recover from disruptions while maintaining operational continuity.[9] Given the increasingly unpredictable nature of the military operational environment, driven by the adoption of new technologies, supply chain resilience is crucial for ensuring mission success. To support operational efforts, a resilient supply chain should be able to empower organisations to withstand shocks, recover quickly from disruptions, and thrive in the face of challenges. Several technologies are driving unpredictability in the military operational environment, like AI-powered autonomous systems and drone swarm,[10] or the concept of Mosaic Warfare, referring to new approaches to warfare that offer the potential of gaining a prolonged advantage by making faster and better decisions than adversaries[11].

Resilience is the ability to anticipate, prepare for, respond to, and recover from unexpected disruptions. Some practices used by industry involve proactive risk management, robust contingency planning, flexible sourcing strategies, or establishing parallel military supply chains. For example, Junaid et al. elaborate on the study criteria in their study to identify and assess supply chain risks, such as single-source dependencies or geopolitical instability, in the Pakistani automotive industry. Tools such as the Neutrosophic Analytic Hierarchy Process (AHP) and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) provide a framework for assessing supply chain risk.[12]

Some other solutions to a resilient SCM include having a robust contingency plan. This would be achieved by developing alternative sourcing strategies, transportation routes, or production plans to mitigate the impact of disruptions. For example, establishing buffer stocks of critical supplies can provide a cushion against unexpected surges in demand or supply disruptions.

Resilient supply chains are characterised by several key features, such as visibility,[13] or the ability to maintain a clear understanding of the supply chain's status through real-time data and analytics, flexibility to modify logistics activities, such as sourcing, production, and distribution, and collaboration by building strong relationships and communication channels between suppliers, manufacturers, and distributors.

Additionally, the overall enhancement of supply chain resilience is possible by implementing robust risk management strategies,[14] or diversified supply sources, and flexible logistics capabilities.

Furthermore, resilience also encompasses the readiness to recover from unforeseen setbacks. Containment plans and alternative logistics pathways ensure that military operations can continue, even in the face of supply disruptions. This capability reduces downtime and bolsters the overall effectiveness of military operations.

Agility in Military Supply Chains

The military supply chain's ability to respond swiftly to changes and demands in operational circumstances proves agility and adaptability. Rapidly shifting conditions—such as changes in enemy tactics, alterations in mission parameters, or emerging threats—require supply chains that can adjust to operations without significant delays. Achieving agility in a military supply chain means the organisation can respond quickly and effectively to unexpected changes in demand and supply. All in one, agility entails achieving responsiveness–as the ability to react swiftly to changing mission requirements or unforeseen events, flexibility–referring to adaptability to changing circumstances, real-time visibility on date information about inventory levels, asset locations, and supply chain conditions, strong partnerships collaboration with multiple suppliers, logistics providers, and other stakeholders.[15] Also, a decentralised decision-making process would empower individuals at different levels of the organisation to make decisions quickly and autonomously.

Frequently, agility is achieved through several mechanisms, including real-time data analysis and effective communication with suppliers, manufacturers, and consumers. By rapidly addressing customers' demands and replenishment flow changes, SCM can efficiently respond to operational requirements, enabling faster decision-making. For instance, during Operation Desert Storm, the U.S. military utilised advanced logistics and supply chain tracking systems. But the tracking systems provided mere data. The real challenge was accessing the processing capability and the ability to deliver information, based on the processed data, on time. Achieving this allowed them to adapt to changing battlefield conditions and ensure the timely delivery of resources.

Agile supply chains in military contexts also facilitate collaboration among various branches of the armed forces and allied nations, ensuring interoperability and efficiency of logistic capabilities. Effective collaboration guarantees that resources are allocated intelligently and that support is provided where it is most needed.

Various Practices Adopted in Business Management

Supply chain management encompasses a range of practices aimed at enhancing overall supply chain synergy. Most business practices are connected to developing new relations between suppliers and consumers to reduce the costs of supply chain deficiencies.

For example, in the early 2000s, Philips Semiconductors implemented a strategy to reduce the number of its direct clients as part of its business transformation efforts. This approach was aimed at optimising its distribution model and focusing on key accounts to improve efficiency and service levels. By consolidating its client base, Philips encouraged its clients to work with distributors, which allowed the company to streamline operations, reduce administrative overhead, and lower costs related to invoicing and debt collection.[16]

Moreover, Philips Semiconductors conducted a collaborative planning process to reduce the Bullwhip Effect. The Bullwhip Effect is a phenomenon in supply chain management where small fluctuations in demand at the consumer level can lead to larger fluctuations in demand at the wholesaler, distributor, manufacturer, and supplier levels.[17] This outcome, also known as the Forrester effect, often results in inefficient inventory management and increased costs throughout the supply chain. In 1999, Philips Semiconductors acknowledged significant Bullwhip effects within some of its supply chains and began to develop a collaborative planning process and tool to mitigate these issues. The goal was to reduce inventory levels and enhance customer service by aligning its supply chain planning and control with those of its clients.

Other practices aimed at reducing costs include lean manufacturing, a method used to minimise waste within the production process. To define waste, we could examine anything in the production process that the customer is not willing to pay for, such as time, extra space, or the quality of materials.[18] As a lead example of lean manufacturing, the Toyota Production System (TPS) is a comprehensive approach to production management. TPS is a product of gradually accumulated and adopted concepts by Japanese businessmen, such as Taiichi Ohno (Toyota's chief engineer) and Kikuo Suzumura (Toyota's manager).[19] At its core, it emphasises maintaining a continuous flow of products within factories to respond flexibly to changes in demand. This approach is known as just-in-time (JIT) production, which involves producing only what is needed, in the necessary quantity, and at the right time. By following this principle, excess inventory and surplus labour are naturally reduced, leading to higher productivity and lower costs.[20] The just-in-time system is a concept focused on aligning the sourcing and use of materials with actual customer demand. When implemented effectively, it helps eliminate various forms of waste, such as excess inventory, unnecessary waiting, inefficient movement, and redundant transportation.

Business strategies focus on reducing added value to the customer by adopting processes that improve SCM. By reducing the number of direct clients, conducting a collaborative planning process, or implementing lean manufacturing solutions, companies managed to reduce inventory levels and eliminate wastes related to transportation issues, thus reducing final costs. The lesson military supply chains may learn is that, by implementing practices like TPS and collaborative planning, the logistics system may become more flexible and profitable, by eliminating wastes, improving the flow of materials and reducing redundancy in the moving and transportation of goods.

Advanced Technologies in Business Supply Chains

In today's rapidly evolving global market, businesses are increasingly turning to advanced technologies to optimise and transform their supply chain operations. Innovations such as AI, machine learning, the Internet of Things (IoT), blockchain, and big data analytics are reshaping the way supply chains are managed and executed. These technologies enable companies to enhance visibility, improve decision-making, increase efficiency, and respond more effectively to changes in demand and market conditions. As a result, businesses can achieve greater agility, reduce costs, and build more resilient and sustainable supply chains.

The Renault company has embraced cutting-edge technologies to enhance its operations, particularly in supply chain management. By adopting artificial intelligence, Renault has modernised its supply chain management and also strengthened its position as a leader in automotive innovation. Renault has integrated advanced technologies such as AI and data analytics to revolutionise its supply chain. In fact, the Renault Group declared its intention to become the first automotive manufacturer fully powered by artificial intelligence, aiming to maximise performance, agility, and innovation.[21]

One of the main benefits of using AI in the supply chain is demand forecasting. Renault employs sophisticated algorithms to analyse historical data and predict future material and component needs. This allows the company to avoid both overstocking and shortages, optimising costs in the process.

Additionally, AI plays a crucial role in logistics optimisation. By monitoring real-time traffic conditions, weather, and other external factors, Renault can dynamically adjust transportation routes, reducing delivery times and minimising environmental impact. This not only boosts efficiency but also supports the company's sustainability goals.

Another important aspect is predictive maintenance. Renault utilises sensors and AI algorithms to monitor the condition of equipment and vehicles throughout its supply chain. This proactive approach identifies potential failures before they occur, ensuring uninterrupted operations.[22] Moreover, AI technology facilitates closer collaboration with suppliers. Through digital platforms and data analysis, Renault can communicate more effectively with its partners, ensuring seamless coordination and quick responses to any changes or disruptions.

Shippeo, a leading technology company specialising in supply chain visibility and management solutions, won the 2024 Supply Chain Innovation Award for their presentation „Shippeo Ft. Renault: Leveraging Automation to Power a Revolutionary New Automotive Control Tower".[23] The award was offered by the Council of Supply Chain Management Professionals (CSCMP), a worldwide professional association dedicated to advancing the discipline of supply chain management.[24] Renault Group has collaborated with Shippeo and Google Cloud to develop a transformative Supply Chain Control Tower explicitly tailored for the automotive industry. This innovative platform integrates Shippeo's real-time transportation visibility with Google Cloud's AI capabilities to manage inbound logistics across Renault's 34 global manufacturing plants.

The Control Tower employs Shippeo's Transportation Process Automation to enhance supply chain resilience. It proactively alerts when the estimated arrival time of parts is projected to occur after the anticipated shortage time at a plant. Subsequently, the system leverages AI-driven configuration to recommend optimal next steps, complete with cost estimates, enabling informed decision-making to maintain uninterrupted production lines.

The aspect of real-time data collection is particularly important in the military supply chain, as it offers solutions to logistic operations redundancy. For example, transportation redundancy translates into delays in providing logistic support, a lack of synchronisation of transportation capabilities, or overwhelmed resupply routes and bottlenecks.

An example of using innovative tools to increase lean manufacturing is offered by the British supermarket chain Wm Morrison Supermarkets Limited. Morrisons enhances its supply chain operations and leads the way for retail industry supply chain transformation. Blue Yonder provides technical solutions to Morrisons, enabling the UK supermarket chain to discover more effective stock control methods and reduce waste production while better serving its customers.[25]

Morrisons' stock management systems primarily rely on Blue Yonder's technology platform. The system enables the company to estimate proper inventory levels for stores so shelves have adequate stock without unnecessary surplus. As a result, the company lowers its expenses and decreases waste.[26]

The tools provided by Blue Yonder effectively reduce waste across various business areas. Morrisons optimises its inventory by assessing how long products last on shelves and customer buying patterns. The technological solutions reduce product disposal, which is both environmentally beneficial and economically advantageous to the business.

Defence-related organisations have adopted blue Yonder's AI-driven supply chain solutions. For example, Leonardo Helicopters, a leading manufacturer serving both civil and military markets, has implemented Blue Yonder's Luminate Planning platform to enhance demand forecasting, inventory optimisation, and supply planning for its aftermarket parts.[27]

Solutions like Blue Yonder and Shippeo platform provide real-time visibility, insights and predictions for all transport modes. Platforms like this could prove beneficial for military supply chains, because they can provide fast tracking of military shipments and predict congestion on routes or on the port of embarkation/debarkation of personnel or materiel, by reducing time waste and improving the flow of materials.

Advanced Technologies in Military Supply Chain

The military and private industry have influenced each other in the development and adoption of advanced supply chain technologies, such as those offered by Blue Yonder. However, their paths have distinct origins, with increasing convergence in recent decades. Historically, the military was a pioneer in large-scale logistics and supply management. Major logistical innovations—like standardisation, interoperability, contingency planning and risk management—originated from military needs to supply troops effectively, especially in dynamic and challenging environments. Also, concepts such as inventory management, transportation optimisation, and demand forecasting were developed for military efficiency and later adapted by private industry to improve efficiency and reduce costs. Nowadays, the connection between the military and private industry in the development and adoption of advanced supply chain technologies is symbiotic. Each sector drives innovation that the other can adopt, adapt, and evolve, creating a feedback loop of continuous improvement in logistics resilience and agility.

The integration of advanced technologies in military supply chains transforms operations, providing significant improvements in efficiency, reliability, and responsiveness. AI, the Internet of Things (IoT), blockchain, or robotics enable military organisations to address complex logistical challenges with resilience and agility. AI is revolutionising military logistics by enabling predictive analytics and improving decision-making processes. Military organisations utilise AI to forecast demand for critical resources, including fuel, ammunition, and food supplies. By analysing historical data and operational patterns, AI algorithms can predict future supply needs, ensuring that troops have the necessary resources at the right time. This capability minimises the risk of stockouts and overstocking, ultimately enhancing operational readiness. AI also plays a significant role in logistics optimisation by processing vast amounts of real-time data, including traffic conditions, weather, and enemy action. This optimisation accelerates delivery times and protects personnel and equipment from potential threats.[28]

The IoT enhances military supply chain operations by tracking and monitoring the movement of supplies and equipment. IoT devices, equipped with sensors, provide live data on inventory levels, location, and condition of assets across the supply chain.[29] This visibility allows military organisations to make informed decisions, manage resources efficiently, and quickly address emerging challenges. Moreover, IoT facilitates the predictive maintenance of vehicles and equipment by monitoring their performance and identifying potential malfunctions before they escalate into significant issues. This proactive approach reduces downtime and maintenance costs, ensuring continuous operational flow and enhancing the overall effectiveness of military logistics.[30]

Blockchain technology has emerged as a powerful tool for enhancing transparency and security within military supply chains. By providing a secure and immutable record of all transactions, blockchain ensures the integrity of supply chain data. This capability is especially beneficial in tracking the movement of critical supplies, preventing fraud, and establishing accountability among stakeholders. Additionally, blockchain enhances collaboration among various branches of military logistics and supply chain stakeholders. Smart contracts—automated agreements executed upon predefined conditions—facilitate efficient procurement processes, ensuring timely deliveries while reducing paperwork and administrative burdens.[31]

Robots and automated systems are increasingly integrated into both military and private industry logistics to enhance efficiency and reduce labour costs. Automated vehicles and drones deliver supplies to remote locations, providing rapid resupply without putting personnel at risk. These technologies improve the ability to respond to urgent operational needs while maintaining the safety of military personnel. In warehouses and distribution centres, robotics is employed for inventory management and order fulfilment, allowing military organisations to streamline operations and enhance accuracy in supply distribution.

Business models and military practices involving the use of innovation learn from each other, and a clear line of differentiation is hard to draw, as technology develops under both the needs driven by military requirements and also by competition in the private sector. The three-column analysis is a helpful tool that assists military leaders and planners in making informed decisions by systematically assessing various factors and their implications for military operations. It is frequently used to analyse mission objectives, force readiness, threat assessment, but also military logistical operations.

Factor/ Practices adopted by business organisations	Implication	Conclusion for military organisations
Reduction and consolidation of suppliers	Many companies choose to select a limited number of suppliers and develop a hierarchy of relationships. Example 1: First-tier suppliers work closely with assembly lines to produce vehicle parts in the automotive industry	Optimising supplier relationships leads to increased efficiency, reduced costs, and enhanced collaboration in the supply chain.
Reduction and consolidation of clients	Some companies select and reduce their direct clients, encouraging them to work with distributors instead. This relieves the companies of costs related to invoicing and debt collection. Example: Philips Semiconductors.	Improving service levels and reducing operational costs.
Coordination of price and stock policies to reduce the Bullwhip effect	Variations between demand and supply may lead to increased orders and higher inventory holding costs. Factors causing variations can include: 1. Inaccurate forecasting 2. Order batching 3. Unforeseen disruptions.	Improving demand forecasting and enhancing communication across the supply chain.
Ensuring supply chain transportation visibility	Lack of end-to-end visibility increases manual work for employees, resulting in lower overall productivity.	Enhancing visibility in the supply chain is crucial for optimising operations, reducing costs and delays, and improving decision-making processes.
AI in Demand Forecasting	AI assists Renault in accurately predicting customer demand by analysing historical sales data, seasonal patterns, and other factors.	Improved forecasting minimises waste and enhances consumer satisfaction by ensuring optimal inventory levels.
AI in Inventory Management	AI optimises inventory levels, reducing overstocking and stockouts, thereby ensuring uninterrupted production.	Effective inventory management supports production flow and reduces costs associated with excess inventory.
IoT in Supply Chain Management	The IoT enhances real-time tracking of inventory and shipments, facilitating more effective inventory management and logistics planning.	Enhanced visibility enables reductions in waste and optimisation of operational processes throughout the supply chain.
IoT for Sustainability	IoT sensors collect data on energy use and waste, allowing companies to implement eco-friendly practices.	The use of this technology results in lower energy costs and supports sustainability initiatives within operations.
Blockchain for Transparency	Blockchain operations enhance demand forecasting and minimise waste by facilitating secure and transparent data sharing.	This technology enhances logistics by ensuring accurate tracking and compliance throughout supply chains.
Blockchain in Commercial Use	Companies like Renault and Morrison use blockchain for supply chain visibility, ensuring product authenticity and reducing fraud.	Blockchain enhances customer trust and operational efficiency by providing transparent tracking of resources.

The three-column analysis table; Source: Author.

In summary, the practices adopted across various sectors, including reducing and consolidating suppliers and clients, coordinating pricing and stock policies, and integrating advanced technologies like AI, IoT, and blockchain, play a significant role in enhancing supply chain resilience and agility. Each approach addresses specific supply chain challenges, contributing to operational success and improved service levels, with the overall advantage of reducing costs and increasing productivity. For instance, in NATO, one of the practices for consolidating suppliers involves having a Rapidly Usable Enabling Contract (RUEC). The RUEC is a pre-negotiated, flexible contract mechanism that allows NATO organisations or member states to quickly acquire goods or services, especially in response to urgent operational requirements. For this purpose, RUECs are designed to expedite procurement in crisis, contingency, or operational environments, avoid delays associated with traditional competitive tendering, and ensure logistical agility by having contracts „on the shelf" and ready for activation.

Additionally, the use of platforms like those mentioned above may offer significant advantages for military supply chains by enabling the rapid tracking of shipments and forecasting potential congestion along transport routes or at ports of embarkation and debarkation for personnel and equipment.

For military organisations, maintaining resilient and agile supply chains is essential. Through investment in advanced technologies and innovative logistics practices, armed forces can enhance their readiness to address supply chain challenges and ensure that critical resources reach troops precisely when and where they are needed.

Conclusions

The deployment of advanced technologies in the supply chain, particularly by companies like Renault, demonstrates how AI enhances demand forecasting and inventory management, enabling the seamless operation of supply chains. Similarly, IoT and blockchain facilitate real-time tracking, transparency, and sustainability, further improving stakeholder collaboration and overall supply chain performance.

For military organisations, the need for resilience and agility in supply chains is crucial. As military operations become increasingly complex, the ability to adapt quickly to changing circumstances and recover from disruptions is essential for mission success. By investing in advanced technologies and innovative practices, military forces can better prepare themselves to tackle logistical challenges while ensuring that troops receive the critical resources they need when needed.

Complementary to this, by mitigating the bullwhip effect through better demand forecasting and enhanced communication, military organisations can optimise their operations and minimise waste. While some military organisations have successfully adopted new technologies into their SCM, there are still many steps to be taken by others. As we previously mentioned, logistical shortfalls can have unwanted consequences, including resupply disruptions and delays, increased costs, poor coordination of transportation modes, and limited visibility and transparency. Embracing technology, fostering strong partnerships, and implementing robust logistical frameworks will enable military organisations to thrive in uncertain environments. As seen in the example of the Kiev battle, the undesired effect on the supply chain in that case was the logistic disruption and failure to support operational objectives.

The strategic application of these innovations strengthens defence operations and ensures that armed forces maintain operational readiness and effectiveness in contemporary warfare. The ongoing development and integration of advanced supply chain strategies will be vital for meeting the future challenges faced by military logistics.

[1] Morrison Express, Supply chain solutions, last modified January 05, 2025, https://www.morrison-express.com/supply-chain-solutions/.
[2] Shippeo Press release, 08/10/2024, last modified January 05, 2025
https://www.shippeo.com/press-releases/shippeo-wins-supply-chain-innovation-award-at-cscmp-edge-conference-2024.
[3] Martin Christopher, Logistics & Supply Chain Management, 4. ed (Harlow: Financial Times Prentice Hall, 2011), 2.
[4] J Haden Boone et al., "Military Logistics Planning for Expeditionary Warfare," n.d., 2.
[5] Christopher, Logistics & Supply Chain Management, 16.
[6] Keith Oliver and Michael D. Webber, "Supply-Chain Management: Logistics Catches up with Strategy," in The Roots of Logistics : A Reader of Classical Contributions to the History and Conceptual Foundations of the Science of Logistics (Berlin : Springer, 2012), 66.
[7] Tom Vollman, Carlos Cordon, and Hakon Raabe, "Managementul Lanțului de Aprovizionare," in Cum Să Stăpânești Managementul La Perfecție (Rentrop&Straton, 2000), 278.
[8] Ana-Maria Merlușcă and Cristian-Octavian Stanciu, "Theoretical-Practical Incongruences of Logistic Support in the Fight for the Conquest of Kyiv," Romanian Military Thinking 2024, no. 4 (December 31, 2024): 74, https://doi.org/10.55535/RMT.2024.4.04.
[9] Editorial Team, "Enhancing Supply Chain Resilience: Strategies for Sustainable Success," MilitarySphere.Com (blog), 2024, https://militarysphere.com/supply-chain-resilience-strategies/?utm_source=openai.
[10] "Pentagon Stares down 'Drone Swarm' Threat," AXIOS, 2024, https://www.axios.com/2024/03/15/drone-swarms-ai-military-war.
[11] Bryan Clark, Dan Patt, and Harrison Schramm, "Mosaic Warfare Exploiting Artificial Intelligence And Autonomous Systems To Implement Decision-Centric Operations" (Center For Strategic And Budgetary Assessments, 2020), vi.
[12] Muhammad Junaid et al., "A Neutrosophic AHP and TOPSIS Framework for Supply Chain Risk Assessment in Automotive Industry of Pakistan," Sustainability 12, no. 1 (December 24, 2019): 7, https://doi.org/10.3390/su12010154.
[13] Ghulam Qader et al., "Industry 4.0 Enables Supply Chain Resilience and Supply Chain Performance," Technological Forecasting and Social Change 185 (2022), https://doi.org/10.1016/j.techfore.2022.122026.
[14] Saurabh Ambulkar, Jennifer Blackhurst, and Scott Grawe, "Firm's Resilience to Supply Chain Disruptions: Scale Development and Empirical Examination," Journal of Operations Management 33–34 (2015): 111–22, https://doi.org/10.1016/j.jom.2014.11.002.
[15] Juan M. Hernández and Carmen Pedroza, "The Influence of the Network Topology on the Agility of a Supply Chain" (arXiv, 2016), 6, https://doi.org/10.48550/ARXIV.1611.10094.
[16] Vollman, Cordon, and Raabe, "Managementul Lanțului de Aprovizionare," 278.
[17] Ton De Kok et al., "Philips Electronics Synchronises Its Supply Chain to End the Bullwhip Effect," Interfaces 35, no. 1 (February 2005): 38, https://doi.org/10.1287/inte.1040.0116.
[18] Frank Voehl et al., The Lean Six Sigma Black Belt Handbook: Tools and Methods for Process Acceleration, 0 ed. (Productivity Press, 2013), 101, https://doi.org/10.1201/b15163.
[19] Phil Ledbetter, The Toyota Template: The Plan for Just-in-Time and Culture Change beyond Lean Tools (Boca Raton, FL: CRC Press, 2018), 1.
[20] Voehl et al., The Lean Six Sigma Black Belt Handbook, 103.
[21] "FutuRGen Insight – "AI: The New Frontier of the Automotive Revolution"," Renault Group, 2025, https://www.renaultgroup.com/en/magazine/technology/futurgen-insight-ai-the-new-frontier-of-the-automotive-revolution?form=MG0AV3.
[22] "Revolutionising Renault: AI's Impact on Supply Chain Efficiency," Dataiku, 2024, https://blog.dataiku.com/revolutionizing-renault-ais-impact-on-supply-chain-efficiency?form=MG0AV3.
[23] "Shippeo Press Release," 2024, https://cscmp.informz.net/informzdataservice/onlineversion/ind/bWFpbGluZ2luc3RhbmNlaWQ9NDI3NTUyMCZzdWJzY3JpYmVyaWQ9MzkzNTc2MjU0.
[24] "Council of Supply Chain Management Professionals (CSCMP)," 2013, https://cscmp.org/CSCMP/CSCMP/Educate/SCM_Definitions_and_Glossary_of_Terms.aspx?hkey=60879588-f65f-4ab5-8c4b-6878815ef921.

[25] “Morrisons Simplifies Fresh Food Clearance with Blue Yonder,” Blue Yonder, n.d., https://blueyonder.com/customers/morrisons?form=MG0AV3.
[26] Blue Yonder, Morrisons puts the customer at the heart of every decision (n.d.).
[27] “News Blog Leonardo Helicopters Pilots Supply Chain Planning Transformation with Blue Yonder,” Blue Yonder Media Centre, 2021, https://media.blueyonder.com/leonardo-helicopters-pilots-supply-chain-planning-transformation-with-blue-yonder/?utm_source=chatgpt.com.
[28] “The Future of Military Supply Chain Management: AI Applications Unveiled,” Military Sphere, 2024, https://militarysphere.com/ai-applications-in-military-supply-chain-management/?form=MG0AV3.
[29] “IoT in Supply Chain: Benefits, Challenges, and Real-World Examples,” Webbylab (blog), n.d., https://webbylab.com/blog/iot-in-supply-chain/?form=MG0AV3.
[30] “Future of Army Logistics | Exploiting AI, Overcoming Challenges, and Charting the Course Ahead,” U.S. Army, 2023, https://www.army.mil/article/267692/future_of_army_logistics_exploiting_ai_overcoming_challenges_and_charting_the_course_ahead?form=MG0AV3.
[31] “Blockchain for Military Logistics,” U.S. Army, 2019, https://www.army.mil/article/227943/blockchain_for_military_logistics?form=MG0AV3.

15

THE IMPACT OF AUTOMATION ON COMBAT EFFECTIVENESS: THE CASE OF THE REPUBLIC OF KOREA

KIEUN SUNG, INSOO KIM, YEEUN HWANG

- **Authors:** Kieun Sung; Conflict Studies/Methodology; „Unpacking Conflict Process on the Korean Peninsula with Political and Seasonal Distribution." Pacific Focus 39.2 (2024): 303-331; Political Science.

  Insoo Kim; Civil-Military Relations/Security Studies; „Differences in Cultural Dimensions Between South Korean Officers and Conscripts: A Topic Modelling Approach." Armed Forces & Society (2024); Sociology.

  Yeeun Hwang; International Relations.

  The views contained in this article are the author's alone and do not represent the views of Korea Military Academy.

- **Abstract:** This study examines the relationship between the level of automation in warfare and combat effectiveness, focusing on unmanned combat systems (UCS). As the Republic of Korea faces a significant decline in the availability of military personnel due to demographic changes, UCS adoption has become a critical priority. While UCSs are anticipated to surpass human combatants in operational efficiency, they require substantial maintenance and repair resources. Using an agent-based model adapted from ecological frameworks, this study simulates conflict scenarios involving two opposing groups. Simulation results show that UCS units consistently outperform human combatants and play a substantial role in reducing the duration of conflict. These findings highlight the complex interplay between UCS, human soldiers, and maintenance personnel, suggesting that simply augmenting the combat effectiveness of human troops does not necessarily guarantee victory."

- **Problem statement:** What is the optimal ratio between human combatants and USCs to maximise combat effectiveness, considering the advantages and limitations of each?

- **Bottom-line-up-front:** UCSs generally exhibit superior combat effectiveness, but specific scenarios underscore the importance of human combatants. The effectiveness of UCS heavily depends on the quality and quantity of maintenance personnel. Technological advancement and resource availability significantly influence the adoption of UCS and force structure decisions.

- **So what?:** The deployment of UCS not only addresses the problem of manpower shortages but also contributes to shortening the duration of armed conflict. Furthermore, ensuring an adequate level of human combatants can enhance the overall effectiveness of UCS integration.

Unmanned Combat Systems and Warfare

Advances in science and technology, along with a shrinking pool of military personnel—especially in countries like the Republic of Korea (ROK)—have increased the need to incorporate Unmanned Combat Systems (UCS) into modern warfare. The advantages and limitations of UCS are well documented. On the one hand, these systems offer superior combat efficiency compared to human soldiers and significantly reduce the risk of battlefield casualties. On the other hand, they are susceptible to mechanical failures and require more personnel for maintenance and logistical support. More broadly, the adoption of new military technologies typically entails not only an expansion of maintenance and support personnel, but also—particularly in the case of systems grounded in advanced science and technology, such as UCS—a growing demand for highly educated and technically specialised human resources.

ROK has demonstrated a strong interest in the deployment of UCSs due to the persistent military threat posed by the Democratic People's Republic of Korea (DPRK) and the country's rapidly declining population. While combat simulations based on single engagements can provide insights into UCS combat efficiency, they remain limited in their ability to predict overall war outcomes. Integrating UCSs into military operations reduces the number of human combatants required in battle. However, this benefit is counterbalanced by the increased need for highly skilled personnel to maintain and repair UCS units. Furthermore, in the context of protracted warfare—comprising multiple successive battles—it is essential to account for the redeployment of injured human soldiers and repaired UCS units.

To conduct war simulations, this study employs an agent-based model (ABM) approach first developed in the field of ecology. The battlefield is conceptualised as a space occupied by two opposing forces, each composed of machines (M), human combatants (Hb), and maintenance personnel (Hm). Interaction rules among these entities are established, and differential equations are formulated to model the temporal dynamics of each component. The battlefield environment is assumed to be isolated, meaning that no external reinforcements are introduced, initial conditions constrain the maximum number of each entity, and engagements occur sequentially. War is deemed to conclude when the number of one faction's forces converges to zero.

To parameterise the interactions that influence the temporal dynamics of each entity, various scenarios are constructed. The findings of the simulation analyses are twofold. First, strengthening UCS forces contributes more positively to both war outcomes and the duration of conflict than simply increasing the number of human combatants. In some scenarios, expanding human resources even led to defeat, suggesting that an overreliance on manpower can, under certain conditions, be strategically disadvantageous. Second, the findings indicate that a force composition strategy emphasising the integration of UCS with human combatants is more effective than a substitution-based approach. Specifically, when UCS were strengthened in tandem with human forces, the duration of war was reduced by nearly half compared to scenarios in which UCS were deployed as replacements for human combatants alone.

The Necessity of War Simulation

The ROK is undergoing a rapid demographic transformation, posing significant challenges to the mobilisation of military personnel necessary for national defence. As of 2024, the country's total fertility rate stands at 0.63, indicating a severe population decline and ageing trend.[1] In 2022, the ROK's active military personnel numbered approximately 500,000, with the country relying on a conscription system for male citizens in their twenties.[2] Since the outbreak of the Korean War in 1950, the ROK and DPRK have remained in a state of heightened military tension. According to the ROK Defence White Paper 2022, the DPRK maintains an active force of approximately 1.28 million personnel. Additionally, although the DPRK's military is equipped with dated weapons systems, it possesses nearly twice the number of artillery pieces, armoured vehicles, tanks, naval warships, and fighter aircraft compared to the ROK.

Given the ROK's demographic challenges and the persistent threat posed by the DPRK's conventional military forces, the ROK Armed Forces have shown increasing interest in the deployment of UCS. Even in cases wherein demographic decline and severe security threats are not immediate concerns, advancements in science and technology have significantly influenced modern military strategy, making UCS deployment a prominent topic in recent military studies.[3] The advantages and disadvantages of UCS adoption, particularly for reducing reliance on human combatants, are being widely discussed. One of the primary advantages of UCS is its superior reconnaissance and lethality compared to human combatants. Recent combat simulations conducted in the ROK suggest that a single UCS unit can effectively perform the roles of two to three human soldiers.[4] Consequently, UCS deployment can significantly reduce the number of human personnel required in combat, thereby decreasing battlefield casualties. However, integrating UCS into military operations is not without its challenges. One of the most significant operational drawbacks is the increased human resources required for UCS control, maintenance, and repair.[5] This issue becomes particularly critical as more advanced UCS models necessitate a larger pool of highly skilled personnel for upkeep. In some cases, the additional personnel required for UCS maintenance may offset the manpower reduction achieved through UCS deployment.

Assessing the impact of UCS deployment based on one-time battle simulations is inherently limited. While such simulations are useful for evaluating UCS mobility and lethality compared to human combatants, they are insufficient for predicting overall war outcomes. The fundamental objective of UCS deployment is to enhance the likelihood of victory in war, a culmination of successive battles rather than a single engagement.[6] The necessity of war simulations arises from the dynamic nature of warfare, where multiple engagements determine overall success or failure. Among the critical factors influencing the outcome of prolonged warfare are human casualties, injuries, UCS malfunctions, and system losses. While deceased personnel and destroyed UCS units cannot be redeployed, injured soldiers and partially damaged UCS units may be reintroduced into combat through medical treatment and rehabilitation and repair and maintenance, respectively. However, this dynamic interplay between force attrition and resource regeneration underscores why single-battle simulations fail to capture the complexities of war.

Accordingly, this study goes beyond the limitations of single-battle simulations by presenting a comprehensive war modelling approach that provides significant implications for the strategic planning of force enhancement.

Research Design

This study aims to identify the optimal ratio between human combatants and UCS through war simulation. As both the ROK and the DPRK begin to integrate UCS into their respective armed forces, it becomes increasingly important to assess the potential impact of UCS on battlefield effectiveness. However, deriving an optimal force composition based on the outcomes of a war that has yet to occur is inherently constrained by the absence of empirical data. In such cases, where real-world observations are unavailable, simulation-based approaches offer one of the most effective means of forecasting future scenarios and generating actionable insights.

This study applies an agent-based model (ABM), initially developed in the field of ecology, to a simulation of warfare. As a key dynamic modelling framework in ecological research, ABMs have played a crucial role in analysing interspecies interactions and fluctuations in population dynamics within an environment. Among the various ABM frameworks, this study adopts a model rooted in the predator-prey dynamic, which has been widely used to capture the reciprocal interactions between species within an ecosystem.[7] The fundamental structure of the predator-prey model is particularly relevant for war simulation, as it provides a mechanism for assessing a system's balance and overall state based on the population dynamics of two interacting entities. In this framework, an increase in prey leads to an increase in predators, while a rise in predator numbers ultimately results in a decline in the prey population.[8] However, conventional predator-prey relationships alone are insufficient for capturing the complexities of war dynamics. To better approximate military conflicts, this study moves beyond a simple unidirectional interaction. It introduces a more sophisticated ecological space wherein both entities engage in mutual combat rather than a one-sided predatory relationship.

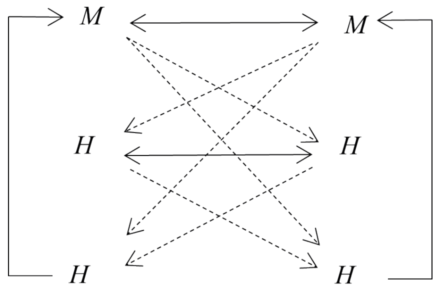
In addition to predator-prey dynamics, models of symbiotic relationships from ecological research offer valuable insights for this study. Unlike the antagonistic nature of predator-prey interactions, symbiosis describes cooperative relationships between two or more entities within an ecosystem. These relationships can be classified into symmetric and asymmetric forms, with prior research exploring how different types of symbiosis influence ecological stability and environmental adaptation.[9] The concept of symbiosis is particularly relevant to this study in the context of UCS and the personnel responsible for its maintenance and support. The introduction of UCS necessitates the presence of human maintenance crews, and this relationship aligns more closely with an asymmetric symbiotic interaction, where one entity depends more heavily on the other.

For war simulation, this study models a constrained battlespace in which two opposing groups operate. Each group consists of three distinct types of agents: Machine (M), representing UCS; Human Combatant (Hb); and Human Maintenance (Hm), responsible for the upkeep and repair of the machines. The aggregate number of these agents determines the overall capacity (C) of each group. The capabilities of each group can be mathematically represented using the following equations. Equations 1 and 2 formally express the capacity and operational potential of Group A and Group B, respectively.

$$C_a = M_a + Hb_a + Hm_a \quad \text{(eq. 1)}$$

$$C_b = M_b + Hb_b + Hm_b \quad \text{(eq. 2)}$$

Within each group, agents engage in cooperative symbiotic interactions, while hostile, predator-prey-like engagements characterise intergroup dynamics. Below is a visual representation of these cooperative intra-group interactions and antagonistic inter-group interactions.



Interaction among Agents; Source: Author.

The capabilities of individual agents within each group vary significantly within the modelled ecological space. At the top of the hierarchy, M units possess the ability to defeat all enemy entities without restriction. Hb units, positioned at an intermediate level, can attack all enemy agents except for opposing M units. In contrast, Hm units, which occupy the lowest tier in the group structure, do not participate in direct combat but are responsible for supporting and repairing allied M units. As per the picture above, bidirectional solid arrows indicate mutual combat interactions, unidirectional dashed arrows represent one-sided attacks, and unidirectional solid arrows denote asymmetric symbiotic relationships.

The agents within each group interact sequentially during combat engagements on the battlefield. These interactions result in destruction, damage, casualties, and injuries. Additionally, damaged M units can be repaired and redeployed in subsequent engagements, while wounded Hb and Hm agents may recover and return to combat in later stages. Throughout sustained engagements, the number of active agents fluctuates over time. The rate of change in the population of each agent type as a function of time can be expressed through the following differential equations.

$$dM_a/_{dt} = -\alpha(M_a \cdot M_b) + \beta M_a(1 - Hm_a/K_{1a}) \qquad \text{(eq. 3)}$$

Equation 3 represents the rate of change in the number of Ma units over time. The M units function as the apex predators within the battle space. Consequently, the decline in Ma occurs exclusively through engagements between Ma and Mb (Ma·Mb), where α represents the rate at which Ma units are destroyed or disabled during combat. Given that Hbb and Hmb lack the capability to attack Ma, no direct interaction occurs between these agents and Ma, and their presence does not influence Ma's attrition. The final term in Equation 3 accounts for the rate at which Ma units are repaired and redeployed for subsequent engagements. A critical aspect of this dynamic is the asymmetric symbiotic relationship between Ma and Hma. As depicted in Figure 1, Ma units can only be reintroduced into battle if they receive support from Hma. Due to this dependence, the maximum number of operational Ma units is not determined by Ma's intrinsic carrying capacity but rather by the availability of Hma. Fundamentally, the reintroduction of Ma is governed by its existing numbers, with β representing the redeployment rate shaped by the maintenance environment. Additionally, as indicated in the final term of the second component, Ma's growth limit is ultimately constrained by Hma's carrying capacity, which is itself capped at its initial value, K1a.

$$dHb_a/_{dt} = -\gamma M_b - \varepsilon(Hb_a \cdot Hb_b) + \zeta Hb_a(1 - Hb_a/K_{2a}) \qquad \text{(eq. 4)}$$

Equation 4 describes the evolution of Hba over time. Positioned as both a mid-tier predator and prey within the ecological system, Hb units operate under dual pressures. The first term in Equation 4 accounts for Hba's attrition due to attacks by Mb, where γ denotes the lethality or wounding efficiency of Mb against Hba. The second term, Hba·Hbb, represents direct engagements between opposing Hb units, with ε indicating the proportion of Hba casualties or injuries resulting from these confrontations. The third term models the redeployment of Hba following combat. In principle, the number of Hb units reintroduced into battle is proportional to their existing numbers: larger pools of Hba lead to greater redeployment, while smaller numbers result in diminished reintroduction. The parameter ζ captures the redeployment rate, which is influenced by medical and recovery conditions. The final component within the parentheses incorporates the carrying capacity constraint, K2a. Without this limitation, Hba could grow indefinitely. By incorporating K2a, the model imposes an upper boundary on Hba's numbers, assuming that this carrying capacity is determined by Hba's initial value.
Equation 5 characterises the temporal variation in Hma. As Figure 1 suggests, Hm units occupy the

$$dHm_a/_{dt} = -\eta M_b - \theta Hb_b + \iota Hm_a(1 - Hm_a/K_{1a}) \qquad \text{(eq. 5)}$$

lowest tier in the ecological hierarchy, functioning purely as prey with no offensive capability. As such, Hma and Hmb do not engage in direct combat, and Hma's attrition is solely determined by predation from M and Hb units. The parameters η and θ represent the kill efficiency of Mb and Hbb, respectively, against Hma. Similar to Hba, the growth limit of Hma is limited by the carrying capacity K1. While Hma's redeployment is primarily dictated by its initial numbers, an additional constraint is applied to prevent uncontrolled growth. The final term in Equation 5 introduces this limitation, where ι represents the redeployment rate, influenced by the medical and recovery environment. The carrying capacity K1a is assumed to be set by the initial value of Hm.

It is necessary to establish a set of simplified war simulation rules to extract meaningful insights from the simulated battlefield outcomes.

- Isolated Battlespace – The conflict environment is assumed to be completely sealed off from external influences. No third-party intervention is possible, and neither new agent types nor additional groups can emerge within the simulation;
- Fixed Initial Force Levels – The number of agents in each group cannot exceed its initial configuration. As previously defined, carrying capacity K constrains growth, preventing mobilisation surges or expanded weapons production. Thus, the maximum number of each agent type remains fixed at its initial value;
- Continuous Sequential Engagements – Combat occurs in a structured and periodic manner. While real-world conflicts may exhibit lulls, ceasefires, or strategic stalemates, the simulated environment assumes that engagements occur continuously without interruption; and
- Total Annihilation as a Termination Condition – A group is considered defeated once its agent population reaches zero. In actual warfare, conflicts may end due to shifts in power dynamics or negotiated settlements. However, in this model, hostilities persist until one group is entirely eliminated, at which point the war is deemed concluded.

Simulation Results

Before conducting the simulation, it is essential to define the parameters that govern the model, as represented by the Greek letters in Equations 3, 4, and 5. Since the empirical validation of these parameters is inherently challenging, their absolute values hold limited independent significance. Instead, the primary objective is to ensure that the assigned values maintain logical consistency, thereby allowing the simulation to produce analytically sound outcomes. The table below presents the definitions and assigned values of each parameter.

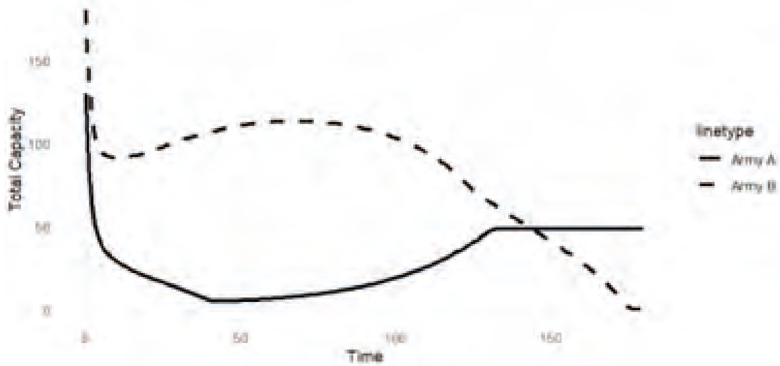
Parameter	Definition	Assigned Value
α	Rate of attrition for M in engagements with opposing M	0.01
β	Redeployment rate of M	0.03
γ	Lethality rate of M against Hb	0.05
ε	Attrition rate of Hb in engagements with opposing Hb	0.01
ζ	Redeployment rate of Hb	0.05
η	Lethality rate of M against Hm	0.03
θ	Lethality rate of Hb against Hm	0.01
ι	Redeployment rate of Hm	0.03

Definitions and Assigned Values of War Simulation Parameters; Source: Author.

The parameters α and ε, appearing in Equations 3 and 4, represent the depletion rates of M and Hb, respectively, in direct engagements between entities of the same category. That is, they define the rate at which forces are lost when fighting against adversaries of the same type. Notably, the attrition rates in M-to-M and Hb-to-Hb engagements are set to be identical. By contrast, the parameters β, ζ, and ι, appearing in Equations 3, 4, and 5, quantify the rate at which each category of unit is replenished following combat losses. As explicitly structured in the model, the number of reintroduced agents cannot exceed the carrying capacity, ensuring that the replenishment process remains constrained. Among the three agent types, Hb exhibits the highest redeployment rate, while M and Hm share a lower, but identical, rate of reinforcement. The parameters γ and η, featured in Equations 4 and 5, determine the effectiveness of M when killing Hb and Hm, respectively. The simulation assumes that M is more lethal against Hb than against Hm, leading to γ being assigned a value higher than that of η. Lastly, the coefficient θ in Equation 5 governs the effectiveness of Hb in eliminating Hm. The simulation presumes that Hb is less effective against Hm than M, resulting in θ being set at a relatively lower level. Building on the established parameters, the study conducts a series of combat simulations under four distinct scenarios, each designed to analyse how variations in force composition influence conflict dynamics.

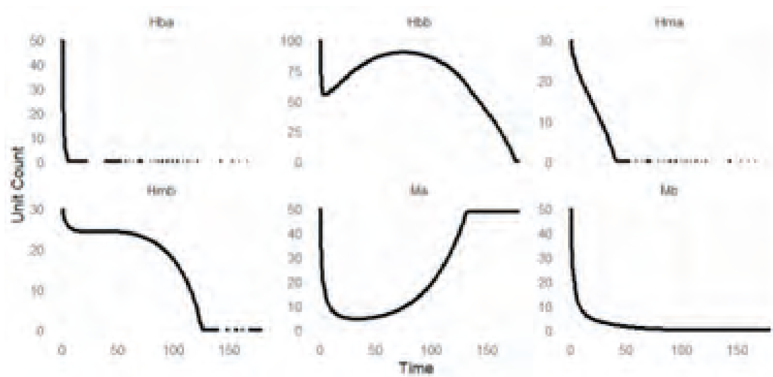
SCENARIO 1 RESULT: CURRENT STATE OF ROK AND DPRK

Scenario 1 most closely mirrors the current strategic balance between the ROK and the DPRK. Assuming a comparable level of UCS adoption between the two armies, the DPRK is modelled as possessing a significantly larger number of human combatants than the ROK. Accordingly, in the initial setting of the war simulation, Army A—representing the ROK—was composed of 50 Ma units, 50 Hba units, and 30 Hma units, while Army B—representing the DPRK—consisted of 50 Mb units, 100 Hbb units, and 30 Hmb units.



Scenario 1 Result; Source: Author.

The figure above illustrates the results of the war simulation. In this scenario, Army A and Army B each contain 50 M units and 30 Hb units, maintaining numerical parity in these categories. However, differences in the number of Hb units (Hba: 50, Hbb: 100) create distinct conflict dynamics. The total capacity trajectory of Army B declines rapidly in the early stages of the conflict, experiences a brief recovery, and then begins to decrease again after approximately the 75th battle. Eventually, Army B's overall capacity reaches zero around the 175th engagement. In contrast, Army A's total capacity drops sharply at the outset, increases after the 50th battle, and stabilises at an equilibrium point after the 130th engagement. Although Army B started the war with a greater total capacity, it ultimately suffered defeat. This outcome is unexpected and requires further examination to determine the underlying causes. To understand the mechanisms driving this result, it is necessary to analyse how the composition of each army changes over time, as shown below.



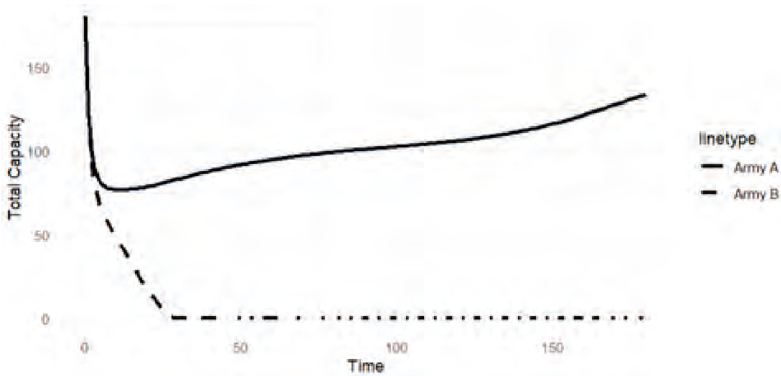
Unit Count for Scenario 1; Source: Author.

The figure above presents the trajectory of each agent type in Army A and Army B during Scenario 1. The data reveal that the unexpected outcome stems primarily from the trends observed in Ma and Hbb units. The numbers of Mb, Hba, and Hma decrease rapidly, while Hbb follows a different pattern.

Initially, Hbb units decline, then briefly increase before resuming their downward trend. The number of Ma units also drops sharply in the early battles, but after the 50th engagement, their count begins to rise and eventually stabilises around the 130th battle. These patterns suggest that having a numerical advantage in human combatants does not necessarily guarantee victory. In designing the simulation model, we set carrying capacities for both Hb and Hm units. Carrying capacity not only defines the growth limits of the two agent types but also represents the maintenance costs associated with sustaining their numbers. As a result, a large number of Hb units imposes relatively higher costs, which, within the limits of carrying capacity, adversely affect the outcome of the war. Also, under these conditions, conflicts tend to become prolonged, delaying their resolution rather than leading to a decisive outcome in the early stages of warfare.

SCENARIO 2 RESULT: STRENGTHENING UCS BY ROK

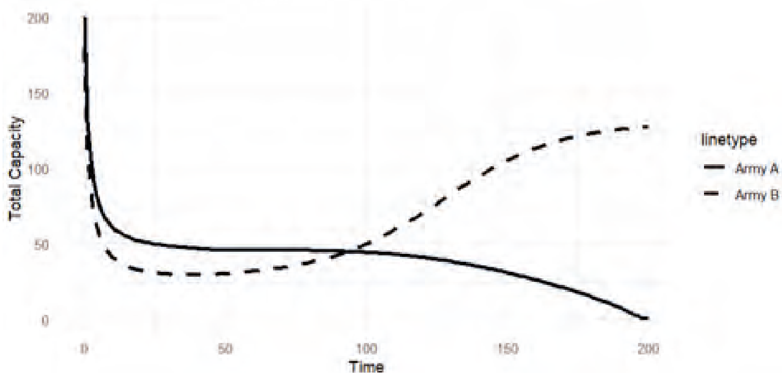
The Scenario 2 models a confrontation between a military force dominated by M units and an opposing army primarily composed of Hb units, representing a case in which the ROK significantly enhances its UCS capabilities. This simulation aims to evaluate the relative combat effectiveness of UCS compared to traditional human-based warfare.



Scenario 2 Result; Source: Author.

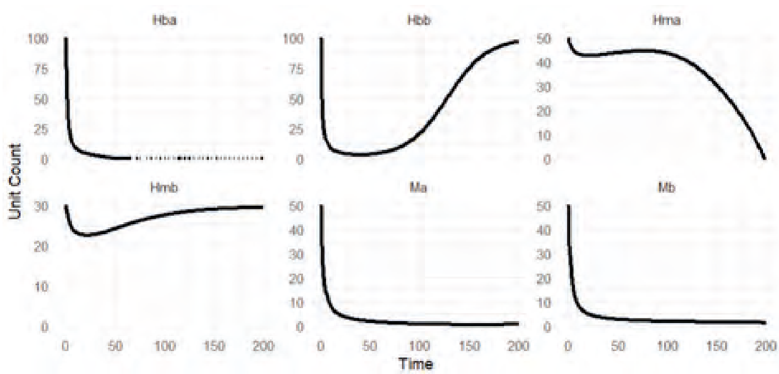
The figure above illustrates the results of Scenario 2, which examines the dynamics of a conflict between Army A(ROK), characterised by a higher number of M units, and Army B(DPRK), which possesses a greater number of Hb agents. Army A is composed of 100 Ma units, 50 Hba units, and 30 Hma units. In contrast, Army B consists of 50 Mb units, 100 Hbb units, and 30 Hmb units. Despite the differences in composition, both armies maintain an identical total force size of 180 agents. In the figure, the solid line represents the trajectory of Army A's total capacity over time, while the dashed line denotes the corresponding trajectory for Army B. As depicted in the graph, Army A experiences a sharp initial decline in total capacity during the early stages of the conflict. However, following approximately the 20th engagement, its capacity gradually recovers. In contrast, Army B's total capacity continues to decline steadily, ultimately converging to zero after the 25th engagement. The simulation results demonstrate that Army A, with its M-heavy composition, decisively outperforms Army B, which relies primarily on Hbb units. The rapid attrition of Army B highlights the strategic advantage of an M-dominant force structure in sustained combat scenarios. These simulation results suggest that, under current conditions, a significant enhancement of the ROK's UCS capacity could enable a swift victory over the DPRK. Compared to Scenario 1, Army B—representing the DPRK—experiences a much more rapid depletion of its total capacity in Scenario 2.

SCENARIO 3 RESULT: STRENGTHENING HUMAN COMBATANT AND MAINTENANCE CAPACITY BY THE ROK



Scenario 3 Result; Source: Author.

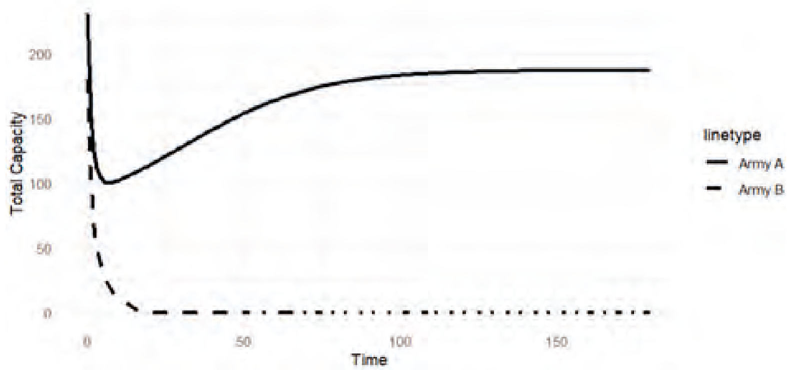
Scenario 3 examines how variations in the number of Hb and Hm units influence conflict dynamics, with both armies initially possessing 50 M units and 100 Hb units. However, Army A allocates 50 Hm units, while Army B maintains its baseline level of 30 Hm units. This scenario is designed to simulate a case in which the ROK (represented by Army A) enhances its human-related capacities—namely Hb and Hm—without reinforcing its UCS units. Both armies experience a sharp decline in total capacity during the initial phase of the conflict, followed by a gradual deceleration in the rate of decline. Around the 75th battle, the trajectories of the two armies begin to diverge. While Army A's total capacity continues to decline slowly until the end of the war, Army B's capacity begins to recover, eventually surpassing that of Army A around the 100th battle. Despite Army A starting the conflict with a higher total capacity, sustained attrition over time leads to Army B ultimately securing victory. This outcome is notably counterintuitive: although the ROK invested in strengthening its human resources, it still suffered defeat in the simulated conflict.



Unit Count for Scenario 3; Source: Author.

The figure above presents the trajectory of unit composition for Army A and Army B in Scenario 3, illustrating how the number of different agents evolved over time. Both armies exhibit a rapid and simultaneous decline in the number of M units. However, the dynamics of Hba and Hbb differ significantly. While both decline sharply in the early stages, Hbb later recovers, whereas Hba fails to rebound. A similar divergence is observed in the trajectories of Hma and Hmb. Although both gradually decline in the early stages of the war, Hma experiences an accelerated decrease during the latter stages, while Hmb begins to recover gradually during the early phase. These patterns are fundamentally driven by the carrying capacity constraints established during the simulation design phase. Notably, as seen in the results of Scenario 1—where Army B had a higher total capacity but still lost the war—Scenario 3 also reveals that Army A, despite having a larger initial capacity, is ultimately defeated. This outcome is primarily attributed to the higher maintenance costs associated with human-related capacities. Furthermore, the duration of the conflict in Scenario 3 is considerably longer than in the previous scenarios.

SCENARIO 4 RESULT: STRENGTHENING UCS AND HUMAN COMBATANT CAPACITY BY ROK



Scenario 4 Result; Source: Author.

This figure presents the results of Scenario 4. In this scenario, the number of Hb and Hm units is identical for both armies, allowing for an analysis of how differences in the quantity of M units influence the course of the conflict. This scenario illustrates the outcome when the Republic of Korea (represented by Army A) strengthens both its UCS and human combatant forces. Both Army A and Army B possess 100 Hb units and 30 Hm units at the onset of the simulation. However, Army A begins with 100 M units, whereas Army B starts with only 50 M units. As depicted in the figure, the army with a greater number of M units, Army A, secures victory in a remarkably short period. The trajectory of Army B's total capacity, represented by the dashed line, converges to zero after approximately the 15th battle. Compared to the prior simulations, this scenario results in the most rapid conclusion of the war.

Conclusion

The following table presents the simulation results. While the initial force structure of Army B remains constant, the outcomes and durations of the war are compared across scenarios in which Army A strengthens its UCS units, its human-related forces, or both.

		Scenario 1	Scenario 2	Scenario 3	Scenario 4
Capacity	Army A	M: 50 Hb: 50 Hm: 30	M: 100 Hb: 50 Hm: 30	M: 50 Hb: 100 Hm: 50	M: 100 Hb: 100 Hm: 30
	Army B	M: 50 Hb: 100 Hm: 30	M: 50 Hb: 100 Hm: 30	M: 50 Hb: 100 Hm: 30	M: 50 Hb: 100 Hm: 30
War Outcome		Victory of A	Victory of A	Victory of B	Victory of A
War Duration		175 battles	25 battle	200 battles	13 battles

Simulation Results; Source: Author.

The results of the war simulation carry important strategic implications for countries like the ROK, which face chronic personnel shortages. First, in terms of war outcomes, enhancing human-related capabilities alone does not guarantee victory. As shown in Scenarios 1 and 3, the side with greater total capacity still suffers defeat. In both cases, the losing side possesses stronger human-based forces—either Hb or Hm. This suggests that despite their larger total capacity, the high costs associated with maintaining human forces may contribute to failure in combat. In the simulation design, the carrying capacity linked to human components reflects the sustaining cost of personnel. Therefore, when expanding human-based capabilities, states must carefully consider the burden of these maintenance costs.

Second, the results provide insight into the ongoing debate: should UCS be integrated with human combatants, or should it fully replace them? For countries like the ROK, which are grappling with manpower shortages, the introduction of UCS is often seen as a means to fill operational gaps created by declining troop numbers. However, a comparison of Scenarios 2 and 4, both of which emphasise UCS enhancement, reveals a critical point: augmenting human combat power alongside UCS deployment leads to significantly shorter war durations. Although both scenarios feature strengthened UCS units, the war in Scenario 4—where human combatants were also reinforced—lasted only about half as long as in Scenario 2. This indicates that rather than substituting humans with UCS, a more effective strategy is to integrate and enhance both force types simultaneously. A coordinated deployment of human and UCS assets results in faster and more decisive victories.

This research carries profound implications for states grappling with conscription shortages due to dramatic population decline. The insights derived from this study illuminate the complex interplay between UCS, human soldiers, and maintenance personnel in shaping contemporary warfare dynamics. By incorporating these variables, the simulations in this study provide a more comprehensive understanding of the strategic consequences of UCS deployment. These findings are particularly relevant for military planners and policymakers as they underscore the importance of a balanced approach to force composition in future military strategies. Moreover, the study emphasises the need for further research into the reliability and maintenance challenges associated with UCS, as well as the broader strategic implications of integrating UCS into military operations. Through sensitivity analysis, this study also identifies scenarios in which an increase in UCS deployment does not result in a significant change in either war outcomes or duration. This reveals the potential limitations of UCS efficacy when deployed in isolation. Additionally, by diversifying the simulation design that governs the unidirectional symbiotic relationship between Hm and M, future simulations may yield new insights into how shifts in inter-agent dependencies affect both the trajectory and duration of conflict.

The principal limitation of this study lies in the need to enhance the reliability of the parameters governing each agent's lethality and redeployment rates. Despite this limitation, this study holds substantial potential. Future research should further analyse the relationship between variations in model parameters and changes in war outcomes to deepen our understanding of how the composition of human and machine forces influences both combat effectiveness and the probability of war victory.

Endnotes

[1] Statistics Korea, Population Statistics, 2024, accessed February 26, 2025, https://kostat.go.kr/anse/.
[2] Ministry of National Defense, 2022 Defense White Paper (Republic of Korea: Ministry of National Defense, 2022).
[3] K. Telli et al., "A Comprehensive Review of Recent Research Trends on Unmanned Aerial Vehicles (UAVs)," Systems, no. 11-8 (2023): 400; Paul Scharre, Army of None: Autonomous Weapons and the Future of War (New York: W. W. Norton & Company, 2018).
[4] Hongseob Eom, "A Study on the Combat Effectiveness of Dronebot Combat System Using Lanchester's Law," KRIS (Korea Research Institute for Strategy) Strategy Research 28, no. 1 (2021): 165–90; Ojeong Kwon, Yihwa Song, Jingu Kim, and Namsuk Cho, "A Study on Combat Effectiveness of Personal Combat Drone Using Analytic Hierarchy Process Method," Journal of the Military Operations Research Society of Korea 47, no. 2 (2021): 36–49.
[5] J. Pekarev, "Attitudes of Military Personnel Towards Unmanned Ground Vehicles (UGV): A Study of In-Depth Interview," Discover Artificial Intelligence, no. 3-1 (2023): 24; X. Zhou et al., "Research on the Development of Unmanned Systems for Joint Operations," in: China Conference on Command and Control (Singapore: Springer Nature Singapore, 2023), 581–92.
[6] Alastair Smith, "Fighting Battles, Winning Wars," Journal of Conflict Resolution, no. 42-3 (1998): 301–20.
[7] Gary An, Qing Mi, Joy Dutta-Moscato, and Yoram Vodovotz, "Agent-Based Models in Translational Systems Biology," Wiley Interdisciplinary Reviews: Systems Biology and Medicine, no. 1-2 (2009): 159–71; J. D. Murray, Mathematical Biology: I. An Introduction (New York: Springer, 2002); J. D. Parrish and S. B. Salia, "Inter-Specific Competition, Predation and Species Diversity," Journal of Theoretical Biology 27, no. 2 (1970): 207–220; R. P. Pech and G. M. Hood, "Foxes, Rabbits, Alternative Prey and Rabbit Calicivirus Disease: Consequences of a New Biological Control Agent for an Outbreaking Species in Australia," Journal of Applied Ecology, no. 3 (1998): 434–53.
[8] Mark S. Boyce, "Modeling Predator–Prey Dynamics," Research Techniques in Animal Ecology, no. 253 (2000): 253–87; Peter Chesson, "Predator-Prey Theory and Variability," Annual Review of Ecology and Systematics, no. 9 (1978): 323–47.
[9] V. I. Yukalov, E. P. Yukalova, and D. Sornette, "Modeling Symbiosis by Interactions Through Species Carrying Capacities," Physica D: Nonlinear Phenomen, no. 241-15 (2012): 1270–89; V. I. Yukalov, E. P. Yukalova, and D. Sornette, "New Approach to Modeling Symbiosis in Biological and Social Systems," International Journal of Bifurcation and Chaos no. 24- 9 (2014): 1450117. (Yukalov et al., 2012; Yukalov et al., 2014).


150

16

THE FUTURE OF MARITIME INTERACTIONS IN THE AGE OF AI

MARCO FRANCAVILLA, JAMES FILIPPO ARMSTRONG

- **Author:** Midshipman Junior Second Class Marco Francavilla and Midshipman Junior Second Class James Filippo Armstrong are midshipmen currently in their third year of the five-year officer training programme at the Italian Naval Academy. Both Midshipmen are focused on technological transformations reshaping the naval domain and have chosen to explore these dynamics in relation to their future employment within the Italian Navy. The views expressed in this article are solely those of the authors and do not represent the official position of the Italian Navy or the Italian Naval Academy.

- **Abstract:** Artificial Intelligence is transforming warfare on land, in the air, and above all—for this paper—at sea. AI is not only enhancing non-kinetic dimensions, such as information dominance, cyber operations, and decision-making processes, but is also amplifying the effectiveness of kinetic means. Recent conflicts have demonstrated how AI-enabled systems are used to deter, degrade, and destroy enemy assets, reshaping both the physical and virtual battlefields. This change necessitates a new perspective on military operations, where AI and digital technology are seamlessly integrated from planning to logistics.

- **Problem statement:** Is AI modifying the international maritime scenario?

- **Bottom-line-up-front:** Human intelligence and personnel training in the armed forces are key to preserving human critical and ethical thinking in decision-making situations.

- **So what?:** Expecting universal adherence to ethical frameworks in the use of AI is unrealistic. Strategic cultures differ widely, and authoritarian states such as the PRC, Russia, and the DPRK have shown little restraint in deploying autonomous systems, prioritising operational advantage over ethical concerns.

Revolutionising Naval Warfare and Operational Efficiency

The military integration of artificial intelligence (AI) stems from the need to overcome the traditional limitations of kinetic weapon systems.[1] This integration facilitates a synergistic interaction between manned and unmanned assets, enabling rapid decision-making in highly volatile environments.[2]

Contemporary AI units employ high-performance processors (often based on GPUs or architectures specialised for deep learning), which, together with convolutional neural networks (CNNs), process sensor data in real-time. While AI provides recommendations and operational scenarios, human judgment remains indispensable for evaluating and implementing decisions in complex and ambiguous settings. This approach maximises both elements' strengths by integrating machines' computational capacity with human experience and creativity. For instance, Human-in-the-Loop (HITL) systems enable operators to retain full control over target selection, ensuring ethical compliance and situational awareness. In Human-on-the-Loop (HOTL) configurations, artificial intelligence performs real-time data processing and threat identification. At the same time, the human operator can supervise and override decisions if necessary. This enables rapid responses in high-stakes environments while maintaining human oversight.

However, Human-out-of-the-Loop (HOOTL) systems operate autonomously without direct human input, relying on pre-programmed parameters and sensor-driven targeting algorithms. While these offer great speed and efficiency, their deployment raises significant ethical and legal concerns, highlighting the need for a well-calibrated balance between autonomy and human control.[3]

Implementing either type of system requires significant resources—both human and material. From an organisational standpoint, it is essential to invest in specialised training programmes designed to update and expand the skills of military personnel. Training must focus on digital technologies and the ability to effectively interface with AI systems, as well as manage scenarios in which rapid response is critical. In addition to training, an appropriate technological infrastructure is necessary, including dedicated data centres, secure communication networks, and advanced cybersecurity systems, to ensure the safety and reliability of AI-based weapon systems.

In recent years, numerous practical examples have demonstrated the effectiveness and potential of AI in naval systems. A prime example is the use of intelligent drones capable of operating in electronic warfare (EW)-constrained environments, as observed in the war in Ukraine.[4] Although AI-operated drones have demonstrated enhanced resilience against measures compared to traditional systems, this resilience is not absolute and depends on several critical factors. Chief among these is the degree of autonomy engineered into the system. Semi-autonomous or fully autonomous drones can maintain functionality—by relying on onboard decision-making algorithms—even when GPS signals are jammed or communications are disrupted. This allows drones to execute missions without human control and reduces vulnerability to conventional EW tactics.[5]

Another important factor is the presence of system redundancy. Advanced drones integrate multiple navigation and communication systems that operate across different frequencies or rely on alternative mechanisms, such as inertial navigation systems or fibre-optic data links.[6] This layered architecture ensures that the drone can continue to function effectively even if one channel is compromised, increasing operational resilience.

The integration of active countermeasures—such as real-time threat detection and adaptive frequency hopping communication protocols—has further strengthened the defensive capabilities of AI-driven drones. Such systems have demonstrated the ability to navigate, detect, and engage targets without external input, even in environments saturated with electronic interference.[7]

However, AI-operated drones remain susceptible to sophisticated electronic attacks. Techniques such as adversarial signal injection, where false data inputs manipulate AI behaviour, or cyber-intrusions into command algorithms, highlight the ongoing need for layered security approaches.[8]

While these innovations are enhancing the resilience of unmanned systems, it is important to note that they are neither mature nor universally effective. The war in Ukraine clearly illustrates that, despite the deployment of countermeasures and AI-based navigation, drones still experience significant disruption under intense electronic warfare conditions. Therefore, this analysis does not contradict the realities observed on the battlefield; rather, it emphasises the technological trajectory and the evolving efforts to mitigate vulnerabilities, which are still being tested and refined in real-world operational environments.

In parallel, the navies of various nations are experimenting with the use of remotely controlled naval vehicles—both surface and subsurface[9]—that integrate AI-based systems to perform surveillance, gather information, and conduct targeted attacks. Such systems are designed to operate autonomously, reducing the exposure of human personnel to dangerous situations and increasing overall operational efficiency.

The challenges and opportunities of integrating AI into decision-making processes are not exclusive to naval forces but extend across all domains of modern warfare. However, the focus of this paper is on the maritime domain, where these dynamics take shape within platform-centric operations and naval-specific command and control structures. An illustrative case is the application of AI in the „Naval Tactical Kill Chain," a decision-making process that, through data analysis and the recognition of behavioural patterns, optimises the phases of observation, orientation, decision, and action (OODA) loop in maritime operations.[10] Studies conducted at institutions such as the Naval Postgraduate School have mapped specific AI methods to support these functions, reducing uncertainty and improving reaction times in combat scenarios.[11]

Automation and the use of complex algorithms raise significant ethical and security concerns, including the potential for errors in decision-making systems, dependence on digital infrastructures, and vulnerability to cyberattacks. These are just some of the challenges that must be addressed. Studies have shown that AI systems used in simulated military scenarios can exhibit more aggressive and inconsistent behaviours than human experts, leading to a higher risk of escalation.[12] Conversely, humans are susceptible to automation bias,[13] where over-reliance on AI recommendations can result in significant errors, as evidenced by increased prescribing mistakes when AI systems incorrectly flagged medications.[14] These findings underscore the importance of a synergistic approach that leverages the computational power of AI while maintaining critical human oversight to navigate complex and ethically charged military decisions. In this light, cybersecurity becomes a key element, requiring constant investment to update and strengthen systems against potential intrusions or external tampering. Moreover, in Western democracies, it is seen as crucial to maintain a balance between system autonomy and human control, ensuring that operators can intervene in critical situations to avoid catastrophic errors. Yet this is not a universal concern: powers such as Russia, the PRC, the DPRK, and even India in its regional rivalries place far greater emphasis on operational effectiveness than on preserving human oversight. While ethical concerns surrounding the integration of AI in military operations have become a prominent issue within Western democracies, it is important to recognise that such considerations are not shared globally. Indeed, authoritarian regimes such as Russia, the People's Republic of China (PRC), and the Democratic People's Republic of Korea (DPRK) demonstrate far less restraint regarding the use of autonomous systems in warfare.[15] For example, the PRC's military doctrine explicitly advocates the rapid development and deployment of intelligentised warfare capabilities, aiming to leverage AI across all dimensions of conflict without being hindered by Western notions of human oversight or accountability.[16] Similarly, Russian military theory increasingly embraces the idea of „algorithmic warfare," integrating autonomous systems into its concepts of information dominance and hybrid operations, again with limited ethical debate.[17]

Moreover, even democratic states outside the traditional Western sphere, such as India, might not display the same emphasis on ethical frameworks when engaged in (at least perceived) regional rivalries or when perceiving a threat as existential. In the context of its strategic competition with China and Pakistan, India's primary concern remains military efficacy and deterrence rather than adhering to emerging global ethical standards for AI.[18] Therefore, although the ethical regulation of AI in warfare is gaining traction in Europe, North America, and select allied nations, it remains a principle that is not universally accepted. It is thus essential to clarify that the debate on ensuring human centrality in AI-driven command and control processes predominantly reflects Western political and ethical values. In a multipolar world where antagonists and even some neutral actors may not adhere to the same principles, the ethical regulation of military AI remains a regionally concentrated concern, rather than a globally uniform one.

Several countermeasures have been developed to counter the threats posed by the use of AI. The adoption of defence systems that also integrate AI technologies stands out; these systems are capable of monitoring and analysing enemy activities in real-time, identifying suspicious patterns, and activating automatic response protocols.

Cyber warfare constitutes a parallel battlefield where the ability to intercept and neutralise digital attacks can determine the outcome of operations. In addition to AI-integrated defence systems and cyber countermeasures, other solutions have been developed to address the threats posed by adversarial AI. Among these are deception techniques designed to confuse enemy systems by generating false signals or altering incoming data, thereby compromising the adversary's decision-making capacity. Although these countermeasures are also based on advanced algorithms, they must be integrated with traditional defensive systems to ensure multi-level and dynamic protection.

Military personnel must be continuously updated on emerging technologies and methods for analysing and interpreting data. Adopting advanced simulations and virtual environments based on the „digital twin" concept represents an effective tool for training operators to interface with complex systems and make rapid decisions in a crisis. Collaboration among military institutions, universities, and research centres is therefore essential to develop an innovative ecosystem that fully leverages the potential of AI while ensuring the safety and operational efficiency of the armed forces.

The Growing Role of AI in Naval Operations

The application of AI in maritime intelligence has drastically changed how naval forces monitor and analyse vast amounts of data in real-time. Machine learning algorithms have enabled naval intelligence agencies to identify suspicious patterns, detect potential threats, and track anomalous behaviour across global maritime domains. This has improved the ability to proactively respond to emerging risks rather than simply reacting to incidents after they occur.[19]

In particular, AI has revolutionised surveillance at sea. Integrating AI into unmanned systems, such as drones and autonomous ships, has bolstered the efficiency and reach of naval intelligence operations. For instance, drones equipped with AI-powered image recognition software can autonomously identify and track targets, providing naval forces with a significant edge in operational planning and response.[20]

Nodalpoint Systems has introduced The SatShipAI system, an advanced satellite surveillance system utilising AI and high-quality satellite imagery to detect and track maritime vessels. It works with data from the Sentinel-1 Earth observation satellite, part of the European Space Agency's (ESA) Copernicus programme, along with other satellites as needed.

SatShipAI uses geospatial AI to assess suspicious ship behaviour in international waters. By analysing satellite images and tracking patterns, the system can identify interactions between vessels (such as those involved in illegal activities like drug trade or illegal fishing). It offers near-real-time monitoring, providing actionable information that security agencies can use to intervene swiftly. The system identifies suspicious vessels based on their proximity, movement patterns, and behaviours, which helps authorities make informed decisions on intervention strategies.

The system is particularly useful for monitoring and countering maritime intrusions, such as illegal, unreported, and unregulated (IUU) fishing, piracy, drug trafficking, and human trafficking. In regions like the Bay of Bengal, such activities are frequent, SatShipAI can track illicit activities, such as drug smuggling through fishermen, by analysing the movement of vessels between countries' territorial waters and international zones.

By using AI and satellite data, SatShipAI improves operational decisions, reducing costs and increasing the accuracy and speed of maritime security interventions.[21]

Revolutionising Naval Operations: The Impact and Challenges of AI

AI is transforming naval operations at every level, from ship automation and logistics to surveillance, threat detection, and maritime strategy. While it is reshaping various industries, its role in the maritime sector is particularly impactful, offering the potential to revolutionise how naval forces operate. This includes defence strategies, resource management, logistics optimisation, and real-time decision-making in critical security environments. However, integrating AI into naval operations surfaces a series of technical, strategic, ethical, and security challenges that require careful evaluation.

One of the most significant applications of AI in naval operations is the automation of ships. Autonomous vessels, designed to operate with minimal or no human intervention, are becoming an integral part of the maritime landscape. These unmanned ships are equipped with AI systems capable of making real-time decisions, navigating through challenging environments, and adapting to changing circumstances without the need for human pilots. However, this very absence of crew raises a critical vulnerability: how can effective damage control be carried out on an unmanned vessel? At sea, fires, flooding, and battle damage are inevitable realities, and without personnel, the ability to contain and recover from such events is severely limited. This has led some analysts to suggest that unmanned ships may need to be conceived as "attritable fleets", designed to be lower-cost, expendable assets that can be risked in high-threat environments where the loss of a traditional manned ship would be unacceptable. While this offers operational advantages, it also underscores the trade-offs and limitations inherent in the adoption of fully autonomous naval platforms.[22] They can be used for various missions, including surveillance, search and rescue, and defence operations. Additionally, AI-powered maritime drones, such as autonomous submarines, can gather oceanographic data, monitor suspicious activities, and conduct intelligence operations without exposing human crews to high-risk environments. In mixed fleets, these unmanned platforms complement manned vessels by operating in contested areas where deploying personnel would be too dangerous.

Strategic framework: Project 33

The importance of AI in the naval sector is confirmed by initiatives such as the US Navy's Project 33. Project 33 is an implementation project aimed at defining a strategy to improve the Navy as a distinct service and enhance its contributions to the joint warfighting ecosystem.[23]

One of the main points of the plan is to „operationalise robotic and autonomous system" based on unmanned systems (UxSs) due to their rapid deployment, stealth capabilities, and ability to carry diverse payloads. Sea denial and sea control are critical objectives for Project 33, and artificial intelligence (AI) is essential in achieving them. In the Indo-Pacific region, AI can significantly enhance sea denial and sea control by supporting various capabilities.

Sea denial and sea control are central objectives of Project 33, and AI plays a crucial role in supporting these missions, particularly in contested environments such as the Indo-Pacific. Here, AI can support operations by enhancing command-and-control efficiency, real-time intelligence sharing, and coordinated responses across vast maritime theatres. In particular, AI-driven systems contribute to the planning and execution of military exercises, such as Pacific Sentry and Northern Edge, improving joint coordination and the Navy's ability to respond swiftly to crises.

In terms of detecting threats, AI's predictive capabilities enable the anticipation of enemy behaviour. AI can forecast future actions and behaviours by analysing historical data and identifying patterns in maritime traffic or hostile group activities. This predictive analysis allows naval forces to counter threats preemptively, optimise responses, and refine defence strategies.

AI's potential in optimising logistics operations is also noteworthy. Naval forces can utilise AI to streamline fleet management, predict equipment failures, and ensure resource allocation is handled effectively. AI can analyse data from ships to forecast maintenance needs, which improves the fleet's availability and efficiency. Furthermore, AI can enhance supply chain management, ensuring real-time optimisation of planning, resource distribution, stock management, and mission planning.

Despite its considerable advantages, the implementation of AI in naval operations raises several challenges. One primary concern is the reliability of autonomous systems. While AI can handle many tasks with efficiency and precision, its ability to operate reliably in unpredictable and complex environments remains a challenge. These challenges have been observed in various contexts. For example, the US Navy's Sea Hunter, an Autonomous Submarine Tracker Vessel, was tested three times in 2017 to integrate its systems and ensure compliance with the International Regulations for Preventing Collisions at Sea during realistic scenarios.[24] The test went well, but the reliability of these systems cannot be confirmed with 100% certainty, especially in scenarios involving congested maritime traffic or adverse weather conditions. The challenge is that AI must be able to make critical decisions, such as avoiding collisions, without human intervention—an inherently complex task when unexpected or unplanned situations arise. Yet it is essential to acknowledge that collisions have always been a part of naval operations; even experienced human crews have been unable to prevent them, as evidenced by the history of, for example, HMAS Melbourne. What is therefore expected from AI is not the impossible elimination of accidents, but rather a reduction in their likelihood. The key question becomes whether there is evidence that AI can already outperform human decision-making in collision avoidance, or at least provide more consistent reliability under certain conditions. While AI enhances safety and operational efficiency, human oversight remains crucial, particularly in critical or emergency situations.[25]

Ethical and legal concerns arise with integrating AI into naval warfare, particularly with autonomous weapon systems. These systems raise critical questions about accountability, as decisions made by AI without human intervention can blur the lines of responsibility.[26] Additionally, there are moral dilemmas surrounding the automation of military operations, as it may lead to the loss of human judgment in life-and-death situations. Privacy and data protection issues are also significant, especially in intelligence gathering and surveillance operations.

These concerns are not just hypothetical. While AI is already used in military systems, such as Israel's Iron Dome, for defensive purposes, there is still a lack of clear accountability when autonomous systems make decisions. Furthermore, antagonist powers may not adhere to ethical guidelines, making it even more difficult to enforce international standards. As such, international treaties and stronger regulations are necessary, but their effectiveness depends on the commitment of all nations.[27]

The Italian Navy and NexTech Partnership

The Italian Navy is embracing transformation through its partnership with Fincantieri NexTech. One of the most striking examples is their work aboard the PPA „Francesco Morosini", where NexTech supported the crew in mastering the Naval Cockpit. This integrated, user-friendly interface allows a small team to control an entire warship's core systems.[28] Through dedicated training, officers learned how to use the new tools, think differently, and collaborate with intelligent systems in real-time.

Another standout case is the Trieste LHD, NexTech has equipped it with a full suite of digital systems for command, control, and communications. These systems are not only technologically sophisticated but also designed for the complexity of modern missions.

SIMAP and the Future of Naval Officer Education

Born from an innovative vision for military education, the SIMAP (Simulatore di Manovra Plancia) has long been a cornerstone of officer training at the Livorno Naval Academy. While not a brand-new system, SIMAP remains highly relevant and increasingly sophisticated, evolving with new layers of intelligent and immersive technologies.

The SIMAP is designed to provide realistic and high-impact training experiences. It faithfully replicates a warship's bridge and simulates complex operational scenarios, such as coastal navigation, severe weather, emergency response, and maritime traffic management. The SIMAP's ongoing integration with intelligent, AI-driven immersive systems makes it especially significant today.

Thanks to these advancements, the SIMAP has grown beyond a static simulator into a dynamic, adaptive training environment. The incorporation of AI modules, either currently in place or under development, enables:

- The dynamic generation of mission scenarios, tailored to the trainee's skill level;
- Real-time performance monitoring and feedback;
- The personalisation of training paths through machine learning techniques;
- The simulation of other naval and civilian assets, governed by realistic artificial agents.

This intelligent, adaptive component sets the SIMAP apart from earlier generations of simulators. It doesn't just replicate; it interacts, evaluates, and adapts the experience based on the individual. As a result, trainees develop not only technical and operational skills but also cognitive and decision-making abilities, practising in a setting that mirrors the complexity and unpredictability of real-world maritime operations.[29]

The SIMAP thus stands as a bridge between the present and future of naval training, where immersive environments, artificial intelligence, and advanced interfaces come together to deliver training that is increasingly effective, secure, and readiness-oriented. It is a concrete example of how technological innovation, supported by industrial partners such as Fincantieri NexTech, is actively transforming the Italian Navy's preparation of its future leaders.

Conclusion

Integrating AI into naval operations has reshaped military strategies, significantly enhancing decision-making, efficiency, and automation. Autonomous systems have enhanced operational effectiveness, but challenges such as accountability, cybersecurity risks, and striking a balance between human oversight and machine autonomy persist. To tackle these challenges, robust regulations, continuous training, and ethical frameworks are necessary for the responsible application of AI in military settings. Moreover, international collaboration, such as the partnership between the Italian Navy and Fincantieri's NexTech, is crucial for advancing naval operations. This collaboration fosters innovation, prepares personnel for emerging technologies, and strengthens maritime defence systems.

The convergence of AI, human expertise, and ethical principles defines the future of naval warfare. With the right oversight, technological advancements can enhance operational efficiency, refine strategic capabilities, and ensure global security in an increasingly complex and interconnected world.

[1] Istituto Superiore di Stato Maggiore Interforze, Applicazione di Artificial Intelligence per fini militari: individuazione dei criteri relativi al passaggio dall'approccio Human in the Loop allo Human on the Loop, Roma: Centro Alti Studi per la Difesa, 2023, 9-10, 12-13.
[2] Istituto Superiore di Stato Maggiore Interforze, Applicazione di Artificial Intelligence per fini militari: individuazione dei criteri relativi al passaggio dall'approccio Human in the Loop allo Human on the Loop, Roma: Centro Alti Studi per la Difesa, 2023, 27–28, 68–69, 30–31.
[3] Istituto Superiore di Stato Maggiore Interforze. Applicazione di Artificial Intelligence per fini militari: individuazione dei criteri relativi al passaggio dall'approccio Human in the Loop allo Human on the Loop. Roma: Centro Alti Studi per la Difesa, 2023, 22–24, 31.
[4] Fighting the war in Ukraine on the electromagnetic spectrum, February 2025, The Economist.
[5] Swarm Wars: The Shaky Rise Of AI Drones In Ukraine – Analysis, August 16, 2024. Eurasia Review.
[6] Ukraine's Drone Revolution: AI-Powered, EW-Resistant, and Fiber-Optic Innovations, TechUkraine, January 08, 2025.
[7] Shield AI MQ-35 V-BAT." Wikipedia, accessed April 27, 2025.
[8] Adversarial signal injection and cyber-intrusions: On adversarial signal injection and cyber-attacks in AI systems, see James Anderson, Cybersecurity Challenges in AI-Operated Military Drones (Cambridge: MIT Press, 2024), 89-92.
[9] C.A. (ris) Michele Cosentino, L'intelligenza artificiale e le operazioni aeronavali (Eng. trans. Artificial Intelligence and air and naval operations), May 2022, Rivista Marittima, 63-65.
[10] The OODA loop is a decision-making model developed by United States Air Force Colonel John Boyd.
[11] Dr. Bonnie Johnson, Dr. John M. Green, Gregory Burns, Todd Collier, Richard Cornish, Kyle Curley, Allan Freeman, Jared Spears, 2023, Mapping Artificial Intelligence to the Naval Tactical Kill Chain, NAVAL ENGINEERS JOURNAL, No. 135-1, 156-159.
[12] P. Scharre, "Army of None: Autonomous Weapons and the Future of War.," W. W. Norton & Company, 2018.
[13] N. B. Sarter, "Automation Bias in Decision Support Systems," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 61, no. 1 (2017): 1859-1863.
[14] S. J. Hoffman and L. M. S., „The Irony of Automation: Why Clinicians Let Computers Make Mistakes," Wired, April 01, 2015, https://www.wired.com/2015/04/the-irony-of-automation-why-clinicians-let-computers-make-mistakes.
[15] Samuel Bendett, „Russian Perspectives on Autonomy in Warfare," Center for Naval Analyses, 2019.
[16] Elsa Kania, „Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," Center for a New American Security, November 2017.
[17] Dmitry Adamsky, „Russian AI Warfare: Projecting Power and Subverting Trust," Texas National Security Review, Summer 2021.
[18] Abhijnan Singh, „Artificial Intelligence in India's National Security Strategy: Prospects and Challenges," Observer Research Foundation, October 2022.
[19] National Intelligence University, "Artificial Intelligence and National Security," 2020.
[20] Department of the Navy, Artificial Intelligence in the U.S Navy, 2020.
[21] Sadhli Roomy, "Geospatial AI for Maritime Surveillance", https://www.acmeai.tech/.
[22] C.A. Enrico Vignola, Future combat naval system 2035 nelle operazioni multi dominio - Il ruolo cruciale dell'Unmanned (Eng. trans. Future combat naval system 2035 in multi-domain operations – The crucial role of the Unmanned), February 2022.
[23] ADM Lisa M. Franchetti, USN, Chief of Naval Operations Navigation Plan for America's Warfighting Navy 2024; and James Holmes, "The Navy's New NavPlan Sets Its Sights on China, from a Sea Denial Stance," U.S. Naval Institute Proceedings 150, no. 9 , September 2024.
[24] Julian Turner, "Sea Hunter: inside the US Navy's autonomous submarine tracking vessel," Naval Technology, 2018.
[25] C.A Enrico Vignola, Future combat naval system 2035 nelle operazioni multi dominio - La persona al centro (Eng. trans. The centrality of the Person), February 2022.
[26] Filippo Santoni de Sio, "Accountability and Control Over Autonomous Weapon Systems: A Framework for Comprehensive Human Oversight," Academia, 2020.
[27] Yasmeen Serhan, "How Israel Uses AI in Gaza—And What It Might Mean for the Future of Warfare," Time, December 2024.

[28] Redazione, “Fincantieri NexTech ha abilitato gli ufficiali del PPA Morosini alla condotta del Naval Cockpit,” Analisi Industria, October 20, 2022.
[29] Gian Luigi Cantini, “Tecnologia per l’addestramento in continua evoluzione,” 28 Gennaio 2020, https://www.marina.difesa.it/media-cultura/Notiziario-online/Pagine/20200128_evoluzione_simulatore_plancia.

17

TECHNICAL, ORGANISATIONAL, AND STRATEGIC DIMENSIONS IN DEFENCE-CRITICAL CONTEXTS

CLEMENS KERSCHBAUM, RAPHAEL DACHS

▶ **Author:** Clemens Kerschbaum is Argus-AI's Head of Research and an Assistant Professor for Business and Innovation Management at New Design University. He specialises in Knowledge Management, focusing on various types of knowledge with a particular emphasis on non-rational types of knowledge and their impact on strategic decision-making and innovation. Before pursuing his PhD in Business, he obtained a master's degree in Business Law. He has published his work in various academic journals and presented at an array of international conferences.

Raphael Dachs is COO at Argus-AI. He has a background in Applied Machine Learning and organisational AI design. Over the past decade, he has primarily collaborated with governmental agencies across Europe to establish AI expert teams and facilitate their development of AI products. His interests include AI security and Adversarial AI for high-risk applications, as well as organisational knowledge creation through the use of AI.

The views contained in this article are the authors' alone.

▶ **Abstract:** Artificial Intelligence is transforming the functioning and interaction of weapon systems and changing how battles are fought. That said, there are still many unresolved questions regarding the safety and security of AI systems. The core concern is that military organisations must adopt a multifaceted approach to effectively manage AI-associated risks, combining technical measures with organisational adaptability. This can only be achieved by considering institutional mechanisms as well as software and hardware in the context of AI development. By addressing these challenges, military organisations can navigate the evolving landscape of AI more securely while enhancing their operational efficiency and effectiveness.

- **Problem statement:** What constitutes AI security, and how should large-scale organisations in the military domain approach AI security when integrating AI into their operational processes?

- **Bottom-line-up-front:** Just as most IT systems, AI can be manipulated or attacked. Yet, AI-security differs from traditional cybersecurity due to the system's complexity and field of use. Hence, one ought to consider not only the technology but especially the use case, including the users and their organisational embedding, when aiming to develop robust AI systems.

- **So what?:** AI security differs from conventional IT security because it is concerned with systems that may learn and alter their behaviour without human intervention. Thus, besides addressing the obvious technical challenges that result from such systems, every organisation that adopts AI must take into account human factors and organisational framework conditions, which can influence AI security just as strongly as purely technical aspects. Particularly large, complex, and hierarchical organisations, such as public bodies or military organisations, should be especially attentive to the 'soft' side of AI Security, which relates to the organisational embedding of AI, its use cases, and the interfaces to and from AI systems.

Speaking of Artificial Intelligence…

Artificial intelligence (AI) is currently at the forefront of public discourse. Many people and organisations, in both the private and public sectors, are drawn to the potential of this technology. However, AI is not a recent development; it has, in fact, been evolving since the 1950s.[1] Back then, Alan Turing, considered one of the pioneers of modern IT, laid the groundwork for machines capable of something like intelligence. A bit later, in 1956, Artificial Intelligence was introduced as a multidisciplinary field of research as a result of a small conference at Dartmouth College (New Hampshire, U.S.) nowadays referred to as the "Dartmouth Conference" – quoted by many as the birthplace of modern AI research. In the decades that followed, AI was initially dominated by logic and reasoning, known as symbolic AI. In the 1980s, more data-driven approaches and probabilistic methods were developed, which allowed for a more implicit representation of knowledge and led to sub-symbolic AI. The first expert systems were developed, and the handling of uncertainty improved. Still, the technology struggled to cope with the requirements of real-world complexity. After periods of stagnation, the next wave of AI development emerged around the millennium, when increasingly powerful IT infrastructure, coupled with improved algorithms and better data availability, paved the way for breakthroughs in the 2010s. As applications such as computer vision, speech recognition, and reinforcement learning began to improve rapidly. Yet only recently, with the advent of large language models (LLMs) in the 2020s, the technology finally became accessible for non-IT people and made its way into the mainstream. Interestingly, these language models (e.g., OpenAI's ChatGPT) also appear to have shaped the colloquial idea of what AI means and is capable of. Although AI has a lot more to offer than LLM Chatbots, many people apparently remain unclear about what the technology is capable of and what technical principles underlie it. Studies show that competencies regarding AI ("AI Literacy") often end at a basic level of understanding.[2] Even so, or perhaps precisely for that reason, AI is currently at the peak of inflated expectations, according to the consulting firm Gartner's popular hype cycle of emerging technologies.[3]

While some already anticipate AI taking total control of the world, others maintain a more realistic and cautious perspective. This perspective is increasingly pointing towards AI security. Ever since some drastic malfunctions of popular models became public, people have started questioning the reliability and trustworthiness of AI systems. Whether in the context of self-driving vehicles, job application screening, chatbots insulting users, or the breach of intellectual property rights through AI models, the potential flaws of AI systems are manifold and sometimes difficult to detect.[4] The same goes for potential attack vectors on AI systems. Many organisations, along with the providers of AI solutions, have already recognised this risk and are working intensively to counter threats and improve the security of their AI systems.[5] Considerations of AI security are particularly important when the systems being used can have far-reaching consequences for the safety and lives of people, as is often the case in a military context. As we will see, AI security can differ significantly from traditional IT security.[6]

Risks of AI in the Military Domain

When considering the risks of AI in the military domain, it is essential to acknowledge that the uncertainty accompanying the rapid development and application of technology constitutes a significant component of the overall risk assessment. Finding the "unknown unknowns"–the things we don't know we don't know, as former U.S. Secretary of Defence Donald Rumsfeld coined it–proves naturally challenging in the field of AI. Here, however, uncertainty can also come into play on different levels concerning one specific system, the interaction of several systems, or the development of entirely new systems. Overall, this situation creates a very complex risk landscape that significantly impedes precise long-term estimates. Analysing recent literature,[7] we can nevertheless identify several categories of risk, which are frequently mentioned in discussions of AI in a military context:

- Introducing bias in decision-making: One of the critical concerns surrounding AI in military applications is the potential for false decisions and unintended escalation through new forms of distortion. This can either directly affect autonomous systems or occur through AI-generated (deep-) fakes of various kinds. Autonomous systems, particularly those designed for target selection and threat assessment, may misinterpret data or execute actions that inadvertently lead to conflict. Given the speed at which AI processes information, incorrect threat identification could trigger military responses without sufficient human oversight. This risk is exacerbated by deploying AI in high-stakes environments where real-time decision-making is necessary. Recent research emphasises this risk, particularly, but not limited to, situations where AI must engage in unfamiliar domains and contexts with little previous, or only poor, data available. Examples include nuclear early warning systems,[8] autonomous drone strikes,[9] or missile defence systems.[10] On the other hand, even if the metaphorical trigger is pulled by human personnel, there is a growing occurrence of audio-visual deep fakes, distorted early warning assessments, or false-positive safety alerts in infrastructure facilities, which can all lead to forceful responses;[11]
- Ethical and Legal Challenges: AI's role in military decision-making raises significant ethical and legal concerns, particularly regarding delegating the use of lethal force to machines. The lack of human intervention in critical moments of engagement may lead to violations of international humanitarian law. Additionally, algorithmic biases can result in disproportionate targeting, increasing the risk of civilian casualties and undermining accountability in military operations. While this aspect is already problematic in itself, it also leads to a growing imbalance between states that place a high value on ethical and moral standards and those that do not. Such an asymmetric norm adherence confronts liberal democracies with a moral dilemma: how to uphold normative commitments without being strategically outpaced by less constrained adversaries;
- Security Vulnerabilities and AI Exploitation: AI systems are eventually vulnerable to cyber threats, including hacking, data poisoning, and adversarial attacks. These vulnerabilities create opportunities for adversaries to manipulate AI-driven decision-making processes, potentially causing incorrect assessments or the malfunctioning of autonomous weapons. A growing dependence on AI systems necessitates well-considered cybersecurity measures to prevent exploitation;
- AI Arms Race and Global Instability: The rapid development and deployment of military AI technologies contribute to an international arms race, with nations competing for technological superiority. In the context of AI, the „winner takes it all" principle likely applies even more strongly than in other domains. This means that those who excel in the field of AI utilisation have a significant advantage over those who are either not as advanced or have implemented it less successfully;
- Over-Reliance on AI and Human Complacency: A growing dependence on AI may lead to too much trust being placed in algorithmic decision-making, diminishing human oversight. This might, in turn, lead to military personnel being less inclined to critically assess flawed or incomplete AI recommendations in particular scenarios. This overreliance can result in strategic miscalculations and ineffective operational planning. Recent research also indicates a loss of skill amongst human personnel, when AI is frequently used for a given task[12]–a pattern reminiscent of the decline in navigational skills following the widespread adoption of GPS technology.[13]

Organisational Capabilities for Dealing with AI-Associated Risks

As it may have become apparent to this point, securing AI is more than a purely technical endeavour. Yet, how can we best prepare for what lies ahead in terms of AI and AI security? The answer may sound trivial, but its implementation is anything but straightforward: individual understanding and organisational agility will become key pillars of AI and its secure use in the coming years. However, the larger, bureaucratic and hierarchical the organisation, the harder these qualities will be to achieve.

What is known to developers and organisational theorists as Conway's law says that „organisations which design systems (in the broad sense used here) are constrained to produce designs which are copies of the communication structures of these organisations."[14] At this stage, we invite the reader to consider their own organisation and reflect on that premise to put the following remarks into context. While the authors primarily address the issue with a focus on the military domain, most insights will also hold true for other organisations that use AI, be it in the public or private sector.

As has been demonstrated in organisational theory and management research across various theoretical frameworks, volatile contexts are best addressed by flexibility, adaptive structures, and the capacity to rapidly reconfigure resources. To describe these properties of organisations, organisational economist David J. Teece elaborated on the notion of „Dynamic Capabilities", which describe an organisation's capacity to recognise changes early, draw appropriate conclusions, and subsequently adjust its behaviour, necessary routines, and processes to develop and sustain a competitive advantage.[15] The idea is not to be confused with individual short-term adjustments but refers to a deeply rooted organisational capacity for learning and transformation.

In this light, AI security should, due to its complexity and far-reaching interfaces, always commence at the organisational level. Organisations must first build the capacity to adapt to changing conditions on a system-structural level. Developing effective integrated system landscapes is already and will become increasingly relevant as warfare is getting more connected and integrated than ever. A pioneering example of such system landscapes and development approaches can currently be observed in Ukraine's Delta system. Delta is a real-time digital battlefield management platform that integrates data from drones, satellites, sensors, and human intelligence into a unified operational picture. It was developed through a highly adaptive, iterative process that combined agile software development with close civil-military collaboration, aligning with NATO standards while remaining flexible and open for rapid innovation. In contrast to traditional military system architectures, which are often siloed, rigid, and slow to evolve, Delta embodies a networked, interoperable, and user-centred design philosophy. Such an approach enables quick and iterative improvements in the event of any weaknesses in the system or its components.

In that line of argument, we see that organisations with strong hierarchical structures often struggle to respond quickly to change. Change is typically understood as a linear transition from a certain state A to a desired state B. However, in dynamic environments, change is more of a continuous, pervasive process that requires ongoing adaptation rather than discrete transformations.[16] From an organisational perspective, the apparent problem is that large, hierarchical and command-driven organisations typically exhibit a preference for stability and control, which manifests in rigid structural arrangements. This, again, echoes Conway's Law, according to which system design inevitably reflects an organisation's communication and coordination structures.[17] Given a constantly evolving threat landscape that results from integrated or even orchestrated threats, this would lead to insufficient results with regard to security.

Moreover, due to the nature of threats, it will neither be feasible nor functional to rely solely on internal experts within the organisation. Instead, what is required is an institutional foundation for efficient and reliable collaboration with external knowledge and/or technology providers and expert groups. The current situation in Ukraine demonstrates the effectiveness of collaborations between public and private entities, as well as in some cases, individual actors, in facilitating the development and improvement of a military's capacities. Another noteworthy example is the U.S. Defence Advanced Research Projects Agency (DARPA) initiative, which serves as a transfer institution for mission-oriented cutting-edge research from a variety of sources to support U.S. military forces with the latest technological innovations available.[18]

Understanding AI Security

After we have outlined organisational frame conditions that we consider essential for the secure use of AI, it is worthwhile observing what makes AI security so special after all and in comparison to other IT systems.

AI systems are generally understood as socio-technical systems.[19] As such, their security requirements differ from purely technical systems, as there is a much stronger emphasis on a holistic safety and security assessment that includes technical, social, legal, environmental and other aspects.[20] Furthermore, due to the inherent complexity of socio-technical systems, a complete prediction and control of such systems is unrealistic – and in the case of AI, which largely relies on probabilities, it is hardly possible. Uncertainty inevitably plays a vital role as a component of risk.[21] Adding to that, defining and analysing the boundaries of a system can be challenging when the overall system expands beyond the technical level.[22] Thus, one should also differentiate between securing an AI model versus securing the overall system. In other words, it is valid and important to improve a model's resilience in the face of adversarial attacks; however, this is not sufficient for ensuring the robust functioning of the overall system within its use case. Until recently, though, literature and respective guidelines addressing holistic assessments of AI systems were scarce, with research having focused mostly on the technical assurance of AI models.[23]

The debate, however, has gained momentum–at least in the private sector–since the entry into force of the AI Act, as the Act requires providers of particularly high-risk systems to design them "in a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle." In this regard, Art 15 (4) of the act explicitly mentions technical and organisational measures to safeguard the system with regard to errors, faults or inconsistencies in the system's operating environment. Although most military AI applications do not fall under the scope of the AI Act, the criteria mentioned there can still serve as a good benchmark for the requirements of the systems.

In general, organisations should audit their AI systems to ensure the systems' trustworthiness–a notion that includes elements of not only transparency, accountability, safety and security but also ethical considerations and privacy.[24] Each of these is potentially difficult, but the real challenge lies in the interfaces between those domains and, particularly, the actors responsible for them.[25] These actors include developers, users and executives responsible for the uptake of AI services in the organisation, as well as professionals from the legal domain and procurement. Going into detail on the requirements for trustworthy AI systems, Brundage et al. suggest three domains vital to developing trustworthy AI systems, namely, institutional mechanisms, software and hardware.[26] If addressed properly, these domains can serve as guidelines for achieving trustworthy AI (eco)systems.

Institutional Mechanisms

Institutional mechanisms describe the principles that an organisation establishes for the development of AI applications. These principles relate to the organisation's underlying values as well as development principles such as process documentation, information exchange among developers, third-party auditing, red teaming, and incentives for reporting incidents, biases, and safety concerns. They regularly serve as guidelines that enable the evaluation of systems.

In the private sector, such principles are further understood as a benchmark for assessing a company's responsible use of AI. Brundage et al. note that by 2020, over eighty AI organisations had publicly stated their developing principles for AI applications.[27] Whereas, in a military context, the red teaming approach can provide valuable insights, particularly in revealing hidden risks ("unknown unknowns"). This approach involves simulating attacks on systems from the viewpoint of an enemy to discover weaknesses within the observed systems.

Software

When thinking of the software component, robustness is considered the central competency. To achieve an appropriate level of robustness, software (i.e., algorithms) should be regularly evaluated through methods of Adversarial Machine Learning. These evaluations go beyond traditional red teaming due to the specificity of machine learning applications and their ongoing training, deployment, monitoring and re-training cycle. To achieve robustness through adversarial methods, the algorithmic structure of the systems must be taken into account. Large Language Models and Image Recognition are two prominent examples:

- Large Language Models (LLMs) are increasingly implemented in various use cases and proposed projects. As machine learning systems become more complex, LLMs are increasingly integrated to facilitate user interaction and interpretability. This approach enables non-expert users to query and comprehend machine learning outputs through natural language interfaces, thereby bridging the gap between advanced computational models and human interpretability.[28] This approach promises an increase in velocity, especially when confronted with substantial volumes of data in a fast-paced decision-making process. Complications could arise when considering the security aspect of LLMs. Boreiko et al. (2014) examine the increasing sophistication of jailbreaking attacks against LLMs, which aim to bypass safety mechanisms that prevent harmful outputs.[29]Harmful outputs in a military context could include presenting a user with information above their classification clearance or other violations of an established need-to-know chain, compromising strategic or tactical robustness. It is not a necessity for this to arise from malicious intentions on the part of the user; it could also be due to AI applications not being improved through adversarial methods. According to recent studies, such LLM jailbreak attacks remain highly effective, even against modern safety-tuned models. In this case, adaptive attacks that refine their strategies iteratively significantly outperform simpler methods.[30]
- As AI systems become an increasingly important component of military decision-making, image classification models are being utilised in reconnaissance, target identification, and battlefield assessment. The promise of AI-driven vision systems lies in their ability to rapidly process large volumes of sensor data, providing near-instantaneous intelligence and reducing human cognitive workload in high-stakes combat scenarios. However, the security vulnerabilities inherent in AI-based image recognition models pose a significant risk to military effectiveness. Adversarial

methods, which involve imperceptible perturbations to input data, can deceive deep learning models into making critical misclassifications, potentially altering the course of military operations.[31] Chen et al. (2022) examine the threat posed by adversarial examples to military AI systems, focusing on their potential to disrupt the "kill chain—the sequence of steps required to find, fix, track, target, engage, and assess (F2T2EA) enemy assets. The term adversarial example, as a technical term, hereby refers to the intentional deception of an AI system through the injection of perturbations into its input data (e.g. applying certain graphical patterns to military equipment to evade visual reconnaissance systems). The study highlights how image-based adversarial attacks can be weaponised to delay or even neutralise enemy strikes by disrupting AI-driven reconnaissance and target acquisition processes. For instance, the U.S. Army Research Laboratory has previously demonstrated how adversarial perturbations applied to physical objects, such as stickers on vehicles, can prevent AI systems from correctly identifying them as military targets in both urban and forest environments.[32] However, the tactical impact of adversarial attacks extends beyond mere misclassification. When adversarial examples are introduced at the "Find" and "Fix" stages of the kill chain, AI-enabled ISR (Intelligence, Surveillance, and Reconnaissance) systems can fail to detect or misidentify enemy units, leading to flawed targeting strategies. In Chen et al.'s wargame simulations, an AI reconnaissance drone tasked with identifying enemy infrastructure failed to recognise its target due to an adversarial modified camouflage pattern, significantly increasing the mission's duration from 6 minutes to over 30 minutes.[33] The delays caused by adversarial attacks allow enemy forces to reposition assets, execute countermeasures, or even gain the upper hand in an engagement. The consequences of adversarial compromised AI are particularly severe in autonomous weapons platforms, where real-time image recognition dictates engagement decisions. Misclassification of civilian structures as enemy combatants or vice versa could lead to either unlawful collateral damage or mission failure due to an inability to execute valid strikes.[34] Moreover, adversarial techniques can extend beyond image classification to affect SAR (Synthetic Aperture Radar) imaging and infrared recognition systems, posing risks to AI-enhanced surveillance and early warning systems.[35]

Hardware

As military AI systems increasingly rely on specialised hardware accelerators, such as GPUs, TPUs, and domain-specific AI chips, the security of these infrastructures is a pressing concern. Unlike traditional computing environments, where trusted execution environments (TEEs) and secure enclaves protect against adversarial access, most AI hardware lacks standardised security mechanisms. This creates potential vulnerabilities, especially in high-stakes military contexts wherein adversarial actors could exploit hardware weaknesses to compromise AI-driven decision-making systems.[36] Brundage et al. (2020) discuss the growing need for trusted execution environments tailored to AI workloads, particularly for machine learning models deployed in classified or sensitive operations. The risk extends beyond software-based attacks; hardware vulnerabilities such as side-channel attacks, model extraction, and fault injection could enable adversaries to steal, manipulate, or corrupt AI models running on insecure processors. Secure enclaves, designed to isolate sensitive computations from potential external threats, have been widely implemented in enterprise computing but are largely absent in military AI hardware deployments. This omission presents a strategic weakness in AI-assisted reconnaissance, autonomous systems, and cryptographic AI applications.[37]

The importance of secure hardware in military applications becomes evident in scenarios where adversarial interference could compromise AI-based image recognition, autonomous targeting, or encrypted battlefield communications—without robust security mechanisms at the hardware level, classified AI-driven intelligence analysis tools risk being exploited through model inversion or adversarial perturbation attacks, leading to data leaks or compromised operational planning.[38] A potential scenario involves an adversary implanting backdoors in AI accelerators used for UAV-based reconnaissance, allowing real-time manipulation of object classification outputs—potentially altering or obscuring mission-critical intelligence.

Looking forward, Brundage et al. (2020) argue that future military AI systems must integrate secure execution environments directly into their hardware stacks, ensuring that machine learning models operate within verifiable, tamper-resistant infrastructures. This includes the development of AI-specific TEEs, cryptographically secured model deployments, and proactive anomaly detection systems at the hardware level. While existing research has focused mainly on software-based AI security, the authors emphasise that without secured hardware foundations, even the most advanced adversarial defences remain vulnerable to physical and side-channel exploits.[39]

Conclusion

Integrating AI in military applications presents a complex landscape of risks that necessitate a multifaceted approach to security. As AI systems evolve, their vulnerabilities must be addressed through robust institutional mechanisms, continuous software assessment, and secure hardware infrastructures. Rapid technological advancement, combined with a considerable potential for unintended consequences, adds to the complexity. An often-overlooked pitfall, particularly in larger organisations, is the lack of capability to respond dynamically to evolving technological requirements. Considerations of AI security must include adaptability within organisations. Thus, the development of trustworthy AI systems consists of a prominent 'hard' part that addresses the security aspect of AI applications themselves. Still, it should be accompanied by a 'soft' part concerned with the organisational context and embedding of the technology. Put more drastically, if there is one piece of advice to be given, it is this: ensure that the departments responsible for AI-related matters have access to all necessary information and interfaces, and are empowered to autonomously and directly respond to emerging risks.

Lastly, it is essential to consider that although AI has been around for some time, we are currently witnessing a rapid shift in how the technology is shaping the military domain. What holds true today may be outdated a week later. Accordingly, most technical considerations should be viewed with a degree of caution. From the authors' perspective, the greatest potential lies in the organisation's structural orientation towards agile ways of working — enabling faster responses to technological developments than the competition, while also facilitating the integration of internal and external expertise to achieve superior outcomes. Future research might investigate how organisations can systematically integrate and utilise heterogeneous knowledge sources and expert contributions effectively. Moreover, it would be beneficial to map already existing expertise within organisations and explore mechanisms to foster cross-functional collaboration.

Ultimately, the most successful actors in the long run will be those who are not just aware of individual risks and threats but also build (AI) systems and organisational structures capable of adapting to rapidly changing technological landscapes.

[1] Michael Haenlein and Andreas Kaplan, "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence," California Management Review 61, no. 4 (2019): 5–14, https://doi.org/10.1177/0008125619864925.
[2] Marie Hornberger et al., "What Do University Students Know about Artificial Intelligence? Development and Validation of an AI Literacy Test," Computers and Education: Artificial Intelligence 5 (2023): 100165, https://doi.org/10.1016/j.caeai.2023.100165.
[3] https://www.gartner.com/en/newsroom/press-releases/2024-08-21-gartner-2024-hype-cycle-for-emerging-technologies-highlights-developer-productivity-total-experience-ai-and-security
[4] Valentin Hofmann et al., "AI Generates Covertly Racist Decisions about People Based on Their Dialect," Nature 633, no. 8028 (2024): 147–54, https://doi.org/10.1038/s41586-024-07856-5.
[5] https://safety.google/cybersecurity-advancements/saif/ ; https://aws.amazon.com/de/ai/generative-ai/security/scoping-matrix/ ; https://www.nsa.gov/AISC/.
[6] Miles Brundage et al., "Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims," version 2, preprint, arXiv, 2020, https://doi.org/10.48550/ARXIV.2004.07213.
[7] Wyatt Hoffman and Heeu Millie Kim, Reducing the Risks of Artificial Intelligence for Military Decision Advantage (Center for Security and Emerging Technology, 2023), https://doi.org/10.51593/2021CA008; Mia Hoffmann and Heather Frase, Adding Structure to AI Harm (Center for Security and Emerging Technology, 2023), https://doi.org/10.51593/20230022; Utsav Sharma Gaire, "Application of Artificial Intelligence in the Military: An Overview," Unity Journal 4, no. 01 (2023): 161–74; Adib Bin Rashid et al., "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges," International Journal of Intelligent Systems 2023, no. 1 (2023): 8676366, https://doi.org/10.1155/2023/8676366; Jan Maarten Schraagen, Responsible Use of AI in Military Systems, 1st ed. (Chapman and Hall/CRC, 2024), https://doi.org/10.1201/9781003410379.
[8] James Johnson, "Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age," Defence Studies 23, no. 1 (2023): 43–67, https://doi.org/10.1080/14702436.2022.2102486.
[9] Hitoshi Nasu, "The Kargu-2 Autonomous Attack Drone: Legal & Ethical Dimensions," Lieber Institute West Point, June 10, 2021, https://lieber.westpoint.edu/kargu-2-autonomous-attack-drone-legal-ethical/.
[10] Kelsey Atherton, "Understanding the Errors Introduced by Military AI Applications | Brookings," Brookings Institute, May 6, 2022, https://www.brookings.edu/articles/understanding-the-errors-introduced-by-military-ai-applications/?utm_source=chatgpt.com.
[11] Rashid et al., "Artificial Intelligence in the Military."
[12] Nataliya Kosmyna et al., "Your Brain on ChatGPT: Accumulation of Cognitive Debt When Using an AI Assistant for Essay Writing Task," arXiv:2506.08872, preprint, arXiv, June 10, 2025, https://doi.org/10.48550/arXiv.2506.08872.
[13] Roger McKinlay, "Technology: Use or Lose Our Navigation Skills," Nature 531, no. 7596 (2016): 573–75.
[14] Melvin E Conway, "How Do Committees Invent?," Datamation 14(5) (1968): 28–31 (31).
[15] David J. Teece et al., "Dynamic Capabilities and Strategic Management," Strategic Management Journal 18, no. 7 (1997): 509–33, https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%253C509::AID-SMJ882%253E3.0.CO;2-Z.
[16] Haridimos Tsoukas and Robert Chia, "On Organizational Becoming: Rethinking Organizational Change," Organization Science 13, no. 5 (2002): 567–82, https://doi.org/10.1287/orsc.13.5.567.7810.
[17] Conway, "How Do Committees Invent?."
[18] https://www.darpa.mil/
[19] Anezka Viskova-Robertson, "Socio-Technical System and Organizational Ai Integration: An Integrative Literature Review," Academy of Management Annual Meeting Proceedings 2023, no. 1 (2023): 1–6, https://doi.org/10.5465/AMPROC.2023.48bp.
[20] Terje Aven and Marja Ylönen, "A Risk Interpretation of Sociotechnical Safety Perspectives," Reliability Engineering & System Safety 175 (July 2018): 13–18, https://doi.org/10.1016/j.ress.2018.03.004; Viskova-Robertson, "Socio-Technical System and Organizational Ai Integration."
[21] Aven and Ylönen, "A Risk Interpretation of Sociotechnical Safety Perspectives."
[22] Albert Cherns, "The Principles of Sociotechnical Design," Human Relations 29, no. 8 (1976): 783–92, https://doi.org/10.1177/001872677602900806; Albert Cherns, "Principles of Sociotechnical Design

Revisted," Human Relations 40, no. 3 (1987): 153–61, https://doi.org/10.1177/001872678704000303.
[23] Ayodeji Oseni et al., "Security and Privacy for Artificial Intelligence: Opportunities and Challenges," version 1, preprint, arXiv, 2021, https://doi.org/10.48550/ARXIV.2102.04661.
[24] Brundage et al., "Toward Trustworthy AI Development."
[25] Koshiyama et al., "Towards Algorithm Auditing."
[26] Idem.
[27] Brundage et al., "Toward Trustworthy AI Development."
[28] Idem.
[29] Valentyn Boreiko et al., "A Realistic Threat Model for Large Language Model Jailbreaks," arXiv:2410.16222, preprint, arXiv, October 21, 2024, https://doi.org/10.48550/arXiv.2410.16222.
[30] Boreiko et al., "A Realistic Threat Model for Large Language Model Jailbreaks."
[31] Yuwei Chen, "The Risk and Opportunity of Adversarial Example in Military Field," Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022, 100–107, https://openaccess.thecvf.com/content/CVPR2022W/ArtOfRobust/html/Chen_The_Risk_and_Opportunity_of_Adversarial_Example_in_Military_Field_CVPRW_2022_paper.html.
[32] Ibid., 101.
[33] Ibid., 104.
[34] Ibid., 106.
[35] Ibid., 104.
[36] Brundage et al., "Toward Trustworthy AI Development."
[37] Ibid., 46.
[38] Ibid., 48.
[39] Ibid., 49.

Theresan Military Academic Forum 2025

WarTech Nexus: Industrialising the Future of Autonomous Warfare

Many nations in the Western community of values are currently engaged in intensive analyses of the lessons learned from the conflicts in Ukraine and the Gaza Strip, examining their implications for future warfare and for the development of their armed forces.

Digitalisation, automation and autonomisation have profoundly transformed modern warfare.

Artificial intelligence and machine learning are just two examples of developments influencing current and future warfare and, among other things, confronting military strategists, the Western community of values and international legal norms with new challenges. We must therefore ask ourselves: Is the global West losing its warfighting edge?

The University of the Armed Forces must ensure that its courses provide practical, university-level training. The skills taught must enable our graduates to perform the current and future tasks of their profession in accordance with the latest scientific findings. Symposia generate military expertise from international scientific discourse in order to ensure research-based teaching, promote the exchange of experience and thus support institutional teaching and learning. On 6 and 7 May 2025, 20 speakers from 14 countries — representing military and civilian higher education institutions as well as industry — selected through a call for papers, gave presentations on current and future autonomous warfare and possible solutions for sustaining the warfighting edge.

The invaluable contributions of the speakers are presented in this publication.

It is not important to predict the future, but to be prepared for it. (Pericles)