REDEFINING DETERRENCE: WARFARE IN THE TECHNOLOGICAL ERA

Colonel Dr. Tiberius TOMOIAGĂ, BEng

Scientific Deputy, Military Equipment and Technologies Research Agency,
Associated Member of Romanian Scientist Academy

DOI: 10.55535/RMT.2025.3.16

The foundational principles of deterrence, largely forged in the crucible of the Cold War's nuclear standoff, are facing an unprecedented stress test in the 21st century. The rapid proliferation of disruptive technologies is fundamentally reshaping the character of warfare, creating new domains of conflict and challenging the efficacy of traditional deterrence models. This paper examines the impact of emerging technologies – including cyberspace operations, artificial intelligence (AI) and autonomous systems, space-based assets and hypersonic weapons – on modern deterrence strategy. It argues that the speed, ambiguity, and asymmetry introduced by these technologies erode the stability of deterrence by punishment and demand a paradigm shift toward a more comprehensive framework. This new framework must integrate deterrence by denial, enhance resilience and leverage all instruments of national power. Through an analysis of recent conflicts and technological trends, this paper provides a series of recommendations for military and policy decision-makers to adapt their strategies to the complex realities of the technological era.

Keywords: deterrence; warfare; emerging technologies; cyberspace; autonomy; space;

INTRODUCTION

The 2022 Russian invasion of Ukraine has served as a stark and brutal reminder that the specter of great power conflict has not been relegated to the annals of history. The war has been a crucible for new technologies and operational concepts, demonstrating the profound impact of unmanned aerial vehicles, sophisticated cyber operations, and the pervasive influence of commercial space technologies on the modern battlefield (CSIS, 2025). The conflict has also exposed the limitations of traditional deterrence strategies. Despite clear and repeated warnings from the United States and its NATO allies, Russia proceeded with its invasion, suggesting a failure of deterrence by punishment. This failure underscores a critical challenge for military and policy decision-makers: the established verities of deterrence, honed during the bipolar nuclear standoff of the Cold War, are proving inadequate in the face of a new technological era.

For decades, deterrence theory rested on a relatively stable foundation. The concept of *Mutually Assured Destruction* (MAD) created a grim but predictable logic that prevented direct conflict between the United States and the Soviet Union. Deterrence was primarily understood as deterrence by punishment – the threat of a devastating retaliatory strike that would inflict unacceptable costs on an aggressor (Freedman, 2020, pp. 1-10). This model, however, is being systematically eroded by a wave of technological innovation. The emergence of new warfighting domains, such as cyberspace and outer space, coupled with the development of artificial intelligence (AI), autonomous systems, and hypersonic weapons, has introduced a level of complexity and ambiguity that traditional deterrence models are not capable to handle.

The central problem is that these new technologies lower the barrier to entry for aggression, create significant attribution challenges and compress decision-making timelines to the point where human cognitive capacity is overwhelmed. A cyberattack can cripple critical infrastructure without a single shot being fired, and its perpetrator can remain shrouded in anonymity (CSIS, 2023). An AI-powered drone swarm could execute a devastating strike in seconds, potentially without direct human intervention (Horowitz, 2021, pp. 764-788). A hypersonic missile, traveling at more than five times the speed of sound, could decapitate a nation’s leadership before it has time to react (Finabel, 2021). These are not science fiction scenarios; they are the emerging realities of 21st-century warfare.

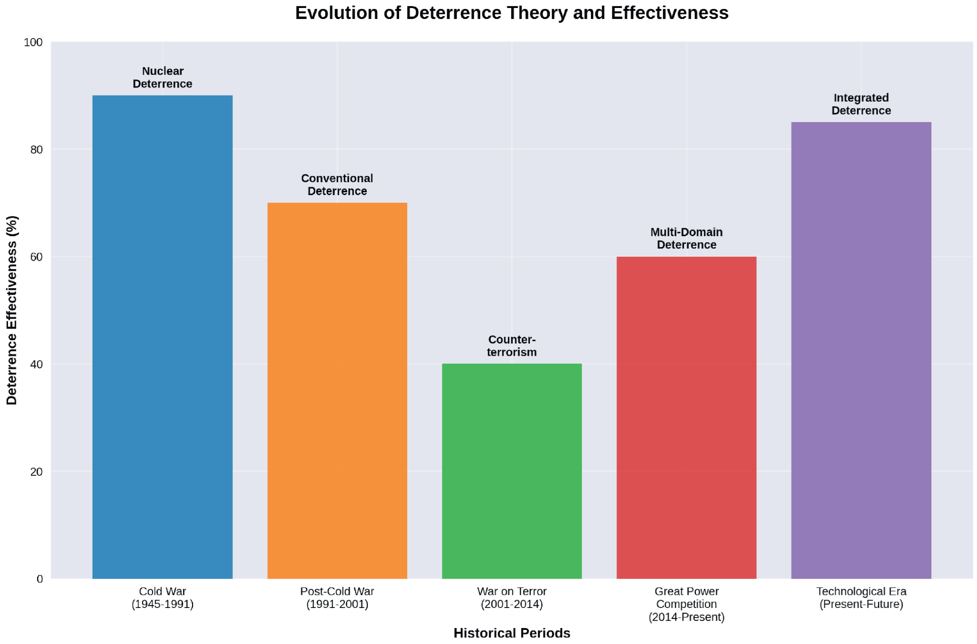

Figure 1: Evolution of deterrence theory and effectiveness across historical periods[1]

This paper argues that the NATO and EU member states must fundamentally redefine their approach to deterrence to meet the challenges of the technological era. A strategy predicated solely on the threat of punishment is no longer sufficient. Instead, a more comprehensive framework is required, one that integrates deterrence by denial, enhances national resilience, and leverages all instruments of national power in a coordinated and synchronised manner. This concept, often referred to as *"integrated deterrence"* is not merely a buzzword; it is a strategic imperative.

To advance this argument, this paper will proceed in five parts. First, it will examine the impact of key emerging technologies on the new domains of warfare, including cyberspace, AI and autonomous systems, space, and hypersonic weapons. Second, it will analyse the phenomenon of hybrid warfare and the *"gray zone"*, demonstrating how adversaries are using a combination of conventional and unconventional tactics to achieve their objectives below the threshold of armed conflict. Third, it will draw on case studies from recent conflicts, including the war in Ukraine and the use of AI in Gaza, to illustrate the practical implications

[1] Author's note: the images were created using AI, based on the text. The data are drawn from the bibliography presented at the end of the article.

of these new technologies for deterrence. Fourth, it will outline a series of policy recommendations for military and policy decision-makers to adapt their strategies to this new reality. Finally, the paper will offer a concluding assessment of the future of warfare and the enduring importance of a credible and effective deterrent.

THE NEW DOMAINS OF WARFARE

The traditional domains of warfare – land, sea, and air have been augmented by new, man-made domains that are increasingly central to military operations and national security.

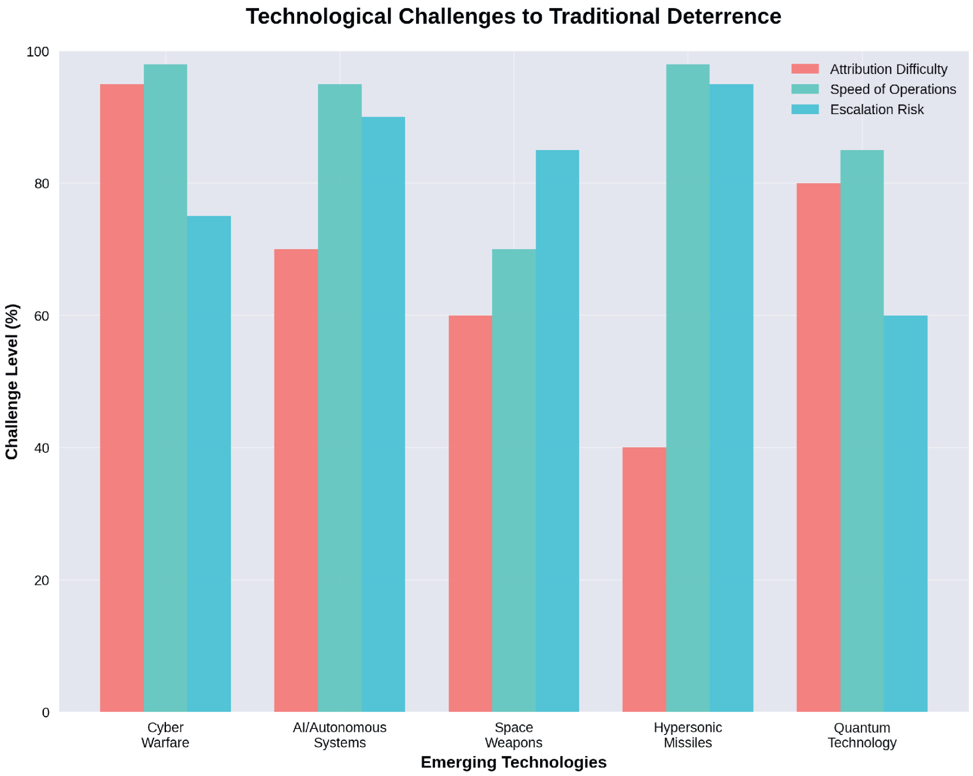

Figure 2: Technological Challenges to Traditional Deterrence Models

Cyberspace and outer space, once considered enabling domains, have become contested warfighting domains in their own right. The proliferation of advanced technologies has created a new reality for military planners and policymakers, one in which the clear distinctions between war and peace are eroding and the potential for rapid, unforeseen escalation is growing.

Cyber Warfare and Deterrence

Cyberspace has emerged as a domain of constant, low-level conflict. State and non-state actors conduct espionage, steal intellectual property, and disrupt critical infrastructure with a degree of anonymity that is unprecedented in the history of warfare. This has profound implications for deterrence. The traditional model of deterrence by punishment, which relies on the ability to credibly threaten retaliation against an aggressor, is difficult to apply in a domain where attribution is often slow, uncertain, and politically fraught (Nye Jr., 2010, pp. 3-14). As the U.S. Congressional Research Service notes, *"cyberspace deterrence strategies seek to influence an adversary's behaviour, discouraging them from engaging in unwanted activities"* (Congressional Research Service, 2022). However, the very nature of cyberspace makes this a challenging proposition.

The attribution problem is perhaps the most significant challenge to cyber deterrence. It can take weeks or even months to trace a sophisticated cyberattack back to its source, and even then, the evidence may be circumstantial. This ambiguity provides cover for aggressors, allowing them to deny responsibility and avoid retaliation. The use of proxies and non-state actors further complicates the attribution problem, creating a layer of deniability that can be difficult to penetrate (Buchanan, 2016, pp.141-157).

Furthermore, the speed of cyber operations creates a significant challenge for decision- makers. A cyberattack can unfold in milliseconds, leaving little time for deliberation or response. This compressed timeline, coupled with the potential for cascading effects across interconnected systems, creates a risk of rapid, uncontrolled escalation. The concept of *"integrated deterrence"*, as articulated by the U.S. Department of Defense, seeks to address this challenge by leveraging all instruments of national power to deter aggression in cyberspace (NDU Press, May 2023).

This includes not only the threat of a military response but also the use of economic sanctions, diplomatic pressure, and law enforcement actions.

AI and Autonomous Systems

The integration of artificial intelligence (AI) and autonomous systems into military operations represents a paradigm shift in the character of warfare. AI-powered systems can process vast amounts of data, identify targets, and execute attacks at speeds that far exceed human capabilities. This has the potential to create a significant military advantage, but it also introduces a host of new risks and challenges for deterrence and strategic stability.

Figure 3: Autonomous Weapons Systems and AI Integration in Military Operations

One of the most significant concerns is the potential for accidental escalation. As AI systems become more autonomous, there is a risk that they could make decisions that lead to unintended conflict. A 2017 report by the Chatham House noted that *"both military and commercial robots will in the future incorporate 'artificial intelligence' (AI) that could make them capable of undertaking tasks and missions on their own"* (Cummings, 2017). This raises the specter of *"flash wars"*, in which autonomous systems engage in a rapid, escalating conflict without meaningful human control. The speed of algorithmic warfare could leave little time for de- escalation or diplomacy, creating a dangerous and unstable dynamic.

The development of lethal autonomous weapons systems (LAWS), or *"killer robots"*, is another area of significant concern. These are weapons that can independently search for, identify, and kill human targets without direct human control. The prospect of ceding life-and-death decisions to a machine raises profound ethical and legal questions (Human Rights Watch, 2012, pp.6-13). It also has significant implications for deterrence. The use of LAWS could lower the threshold for the use of force, as it would remove the risk to human soldiers. This could make it more tempting for states to engage in aggression, undermining the very foundations of deterrence.

Moreover, the proliferation of AI and autonomous systems could lead to a new arms race, as states compete to develop more sophisticated and capable systems. This could create a dangerous and unstable security environment, in which the risk of miscalculation and conflict is high. As a 2024 CSIS report on algorithmic stability notes, *"Information about AI/ML capabilities will influence how states manage* *escalation. Escalation risks will continue to emerge from how warfighting...”* (CSIS, 2024).

Space as a Contested Domain

Outer space, once the exclusive domain of a few superpowers, has become increasingly congested, contested, and competitive. The growing reliance on space-based assets for communication, navigation, intelligence, and military operations has made them attractive targets for adversaries. The development of anti-satellite (ASAT) weapons, including co- orbital *“killer satellites”*, directed energy weapons, and ground-based missiles, has created a new and dangerous dimension of warfare (Bingen, 2023, pp.1-33).

Figure 4: Space-Based Assets and Anti-Satellite Warfare Capabilities

The vulnerability of space assets poses a significant challenge to deterrence. A successful attack on a nation’s satellites could cripple its military and economic infrastructure, leaving it blind, deaf, and unable to respond effectively to an attack. This creates a powerful incentive for a preemptive strike, as the first mover could gain a decisive advantage. The 2023 RAND Corporation report, *“A Framework of Deterrence in Space Operations”*, emphasises that an effective space deterrence strategy must be tailored to the specific adversary and the phase of the conflict (RAND Corporation, 2023).

The challenges of deterrence in space are compounded by the unique characteristics of the domain. The vastness of space and the high speed of objects in orbit make it difficult to track and attribute hostile actions. The problem of space debris, which can be created by the destruction of a satellite, poses a threat to all space-faring nations, including the one that created it. This creates a shared interest in avoiding conflict in space, but it also creates a risk of miscalculation and unintended escalation.

The concept of *"space denial"* has emerged as a potential deterrence strategy. This involves developing the capability to deny an adversary the use of its own space assets in a conflict. This could be achieved through a variety of means, including jamming satellite signals, dazzling sensors with lasers, or using cyberattacks to disrupt ground stations. The goal of space denial is not to destroy an adversary's satellites, but rather to temporarily disrupt their ability to use them. This approach, as outlined in a 2023 NDU Press article, is seen as a less escalatory option than the use of destructive ASAT weapons (NDU Press, October 2023).

Hypersonic Weapons and Strategic Stability

The development of hypersonic weapons, which can travel at speeds in excess of Mach 5, represents another significant challenge to strategic stability. These weapons combine the speed of ballistic missiles with the manoeuvrability of cruise missiles, making them extremely difficult to detect, track, and intercept. This has led some analysts to warn of a new era of vulnerability, in which the traditional pillars of deterrence are undermined (Global Security Review, 2025).

The primary concern is that hypersonic weapons could be used to conduct a disarming first strike against a nation's nuclear arsenal or leadership. The speed and manoeuvrability of these weapons would make it difficult for a targeted nation to respond in time, potentially leading to a *"use-it-or-lose-it"* dilemma. This could create a dangerous and unstable dynamic, in which both sides are incentivised to strike first in a crisis. A 2021 report by Finabel noted that *"emerging military technologies such as hypersonic weapons challenge the established dynamics of nuclear deterrence and strategic stability"* (Finabel, 2021).

The payload ambiguity of hypersonic weapons further complicates the deterrence calculus. It is difficult to determine whether a hypersonic missile is armed with a conventional or a nuclear warhead until it is too late. This could lead to miscalculation and unintended escalation in a crisis. An adversary might mistake a conventional strike for a nuclear one, leading to a devastating nuclear exchange.

The proliferation of hypersonic weapons could also trigger a new arms race, as states compete to develop their own hypersonic capabilities and defenses.

This could lead to a dangerous and unstable security environment, in which the risk of conflict is high. The Atlantic Council has argued for a clear vision for US hypersonic weapons, emphasising that *"deterrence requires credible, visible capabilities"* (Atlantic Council, 2025). However, the development of these weapons also raises the risk of a destabilizing arms race.

HYBRID WARFARE AND THE GRAY ZONE

The challenges to deterrence are not limited to the emergence of new technologies and warfighting domains. Adversaries are also increasingly operating in the *"gray zone"* between peace and war, using a combination of conventional and unconventional tactics to achieve their objectives without triggering a military response. This phenomenon, often referred to as "*hybrid warfare"* has become a defining feature of 21st-century conflict.

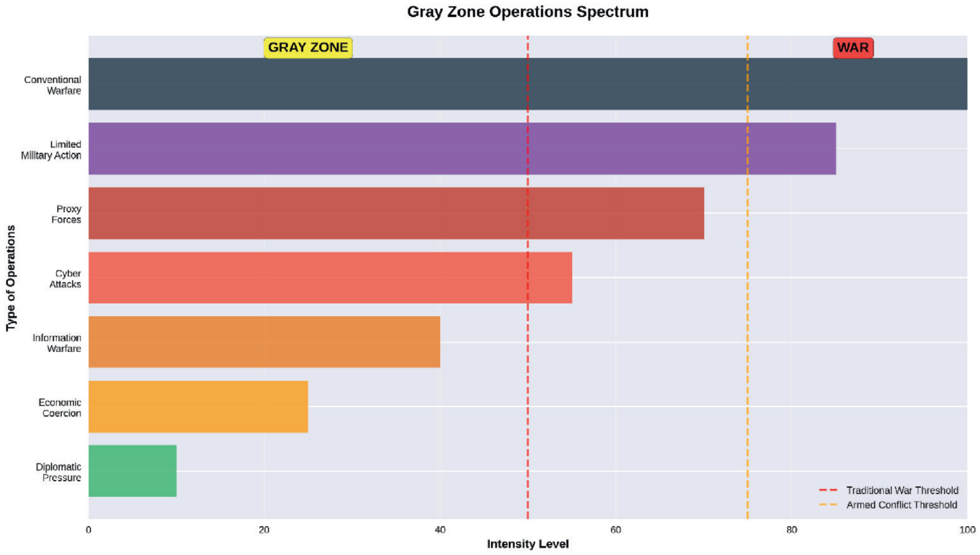

Figure 5: Gray Zone Operations Spectrum – From Peace to War

Hybrid warfare is characterised by the use of a wide range of instruments of power, including disinformation, economic coercion, cyberattacks, and the use of proxies and irregular forces. The goal is to sow confusion, undermine trust in democratic institutions, and create a sense of strategic paralysis. As a 2025 ICRC article notes, terms like *"hybrid threats"* and *"gray zones"* are used to describe *"covert and ambiguous operations, suggesting they blur the lines"* between war and peace (ICRC, 2025).

Russia's actions in Ukraine provide a textbook example of hybrid warfare. Prior to its full- scale invasion in 2022, Russia engaged in a years-long campaign of hybrid warfare, which included the annexation of Crimea, the use of *"little green men"* in the Donbas, and a sustained campaign of disinformation and cyberattacks. These actions were carefully calibrated to remain below the threshold that would trigger a decisive military response from the West.

China has also been accused of engaging in hybrid warfare in the South China Sea. It has used its coast guard and maritime militia to harass and intimidate other claimants, while at the same time engaging in a massive island-building campaign to create a series of unsinkable aircraft carriers. These actions have allowed China to gradually expand its control over the South China Sea without firing a shot.

The challenge of deterring hybrid warfare is that it is often difficult to identify a clear aggressor or a specific act of aggression. The use of proxies and deniable assets makes it difficult to attribute attacks, and the incremental nature of many hybrid warfare campaigns makes it difficult to justify a military response. This creates a significant challenge for policymakers, who must find a way to deter aggression without escalating to a full-blown conflict. A 2025 Small Wars Journal article highlights the need for a framework to measure hybrid warfare, noting that it *"lacks clear definitions"* (Small Wars Journal, 2025).

POLICY IMPLICATIONS AND RECOMMENDATIONS

The profound shifts in the character of warfare demand a commensurate shift in how the United States and its allies approach deterrence. A reliance on Cold War-era models is a recipe for strategic failure. To effectively deter aggression in the 21st century, policymakers and military leaders must embrace a new framework for deterrence, one that is more comprehensive, integrated, and agile. This section outlines a series of policy recommendations designed to achieve that goal.

Redefining Deterrence: From Punishment to a Comprehensive Approach

The cornerstone of a modern deterrence strategy must be a move away from an over- reliance on deterrence by punishment. While the threat of retaliation remains a critical component of deterrence, it is no longer sufficient on its own. A more comprehensive approach is needed, one that also incorporates deterrence by denial, resilience, and cost imposition.

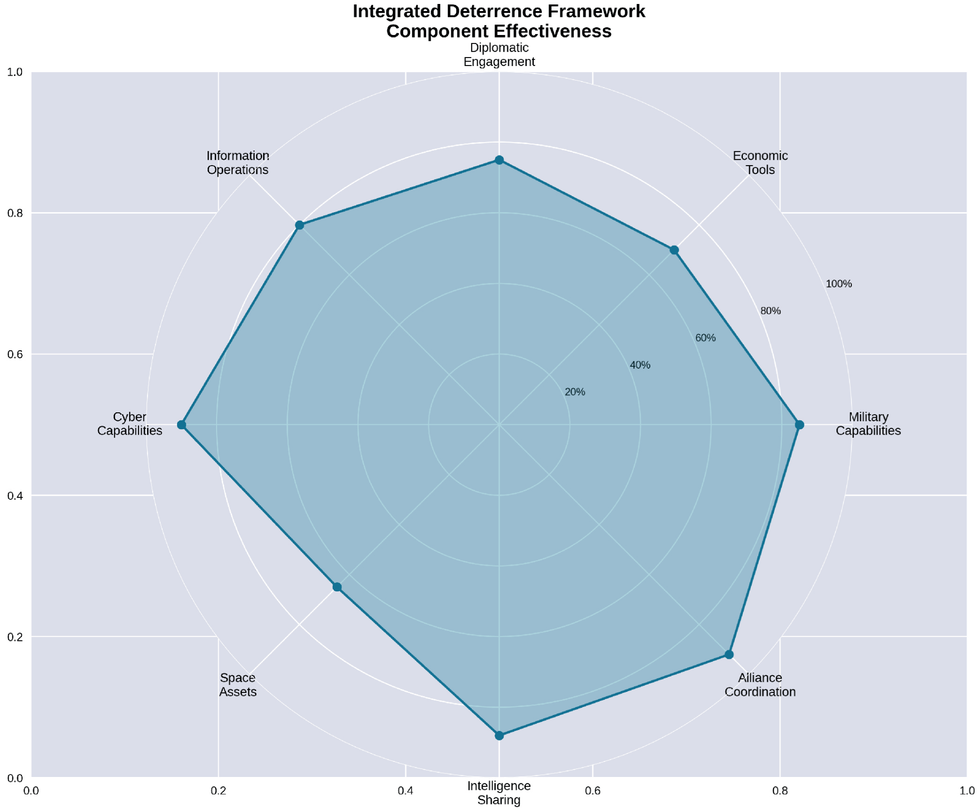

Figure 6: Integrated Deterrence Framework - Multi-Domain Approach

- **Deterrence by Denial:** This involves convincing an adversary that they will not be able to achieve their objectives on the battlefield. This can be achieved through a variety of means, including the development of advanced military capabilities, the hardening of critical infrastructure, and the use of new operational concepts. The goal is to create a credible defence that will deny an aggressor the prospect of a quick and easy victory.
- **Resilience:** In an era of persistent, low-level conflict, it is no longer possible to prevent all attacks. Therefore, it is essential to build a resilient society that can withstand and recover from an attack. This includes everything from hardening critical infrastructure against cyberattacks to developing a robust civil defence program.
- **Cost Imposition:** This involves imposing costs on an adversary for their aggressive behaviour, even if it falls below the threshold of armed conflict. This can be achieved through a variety of means, including economic

sanctions, diplomatic isolation, and law enforcement actions. The goal is to make it clear that there will be consequences for aggression, even if it does not trigger a military response.

Integrated Deterrence: A Whole-of-Government Approach

The concept of integrated deterrence, as articulated in the 2022 US National Defense Strategy, is a critical component of a modern deterrence strategy. It recognises that military power is only one instrument of national power, and that a truly effective deterrent requires the integration of all instruments of power, including diplomatic, economic, and informational.

This requires a whole-of-government approach to deterrence, in which all agencies and departments are working together to achieve a common set of objectives. It also requires close coordination with allies and partners, who are essential to building a broad coalition to deter aggression.

Technological Superiority: The Race for the High Ground

In an era of rapid technological change, maintaining a technological edge is more important than ever. The NATO and EU member states must continue to invest in research and development to ensure that they have the most advanced military capabilities in the world. This includes everything from developing new AI-powered systems to building more resilient space assets.

However, technological superiority is not just about having the best hardware. It is also about having the best people. The NATO and EU member states must invest in the education and training of their military personnel to ensure that they have the skills and knowledge to operate in a complex and rapidly changing security environment.

Arms Control and Norms: Building Guardrails for a New Era

The development of new and disruptive technologies has created a pressing need for new arms control agreements and international norms. The existing arms control framework, which was designed for the Cold War, is ill-equipped to deal with the challenges of the 21st century. New agreements are needed to govern the development and use of AI, autonomous systems, and hypersonic weapons.

In addition to formal arms control agreements, there is also a need to develop new international norms of behaviour. This includes everything from establishing rules of the road for cyberspace to developing a code of conduct for military operations in outer space. The goal is to create a more stable and predictable security environment, in which the risk of miscalculation and conflict is reduced.

Professional Military Education: Preparing Leaders for the Future of War

Finally, it is essential to reform professional military education to prepare leaders for the challenges of the 21st century. Military leaders must have a deep understanding of the implications of new technologies for warfare and deterrence. They must also be able to think critically and creatively about how to solve complex security problems.

This will require a new approach to professional military education, one that emphasizes interdisciplinary learning, critical thinking, and a deep understanding of the changing character of warfare. It will also require a greater emphasis on wargaming and simulation, to give leaders the opportunity to test new concepts and ideas in a realistic and challenging environment.

CONCLUSIONS

The technological tsunami of the 21st century has washed away the familiar landmarks of the Cold War deterrence landscape. The emergence of cyberspace and outer space as warfighting domains, coupled with the development of artificial intelligence, autonomous systems, and hypersonic weapons, has created a new and dangerous security environment. The old verities of deterrence, which were based on the threat of a devastating nuclear exchange, are no longer sufficient to deter aggression in an era of hybrid warfare and gray zone conflict.

This paper has argued that the NATO and EU member states must fundamentally redefine their approach to deterrence to meet the challenges of the technological era. A strategy predicated solely on the threat of punishment is a recipe for strategic failure. Instead, a more comprehensive framework is required, one that integrates deterrence by denial, enhances national resilience, and leverages all instruments of national power in a coordinated and synchronised manner.

The policy recommendations outlined in this paper provide a roadmap for how to achieve this goal. They include a call for a new, more comprehensive approach to deterrence; a greater emphasis on integrated deterrence; a sustained investment in technological superiority; a renewed focus on arms control and international norms; and a reform of professional military education. These recommendations are not a panacea, but they do provide a starting point for a much-needed debate about the future of deterrence in the 21st century.

Ultimately, the challenge of redefining deterrence is a challenge of imagination. It requires policymakers and military leaders to think creatively about how to deter aggression in a world where the lines between peace and war are increasingly

Technology Domain	Key Challenges	Deterrence Impact	Policy Response
Cyber Warfare	Attribution difficulty Speed of operations Non-state actors	High - Undermines retaliation credibility	Integrated cyber deterrence Active defense International norms
AI/Autonomous Systems	Flash wars Ethical concerns Accidental escalation	Very High - Removes human control	Human-in-the-loop requirements AI arms control Ethical guidelines
Space Domain	Debris creation Dual-use technology Attribution challenges	High - Critical infrastructure vulnerability	Space denial strategies International agreements Resilience building
Hypersonic Weapons	Payload ambiguity Compressed timelines Defense penetration	Very High - First-strike advantage	Early warning systems Defensive capabilities Arms control
Hybrid/Gray Zone	Below-war threshold Deniability Incremental nature	Medium - Gradual erosion of deterrence	Whole-of-government response Cost imposition Resilience measures

Table 1: Summary of Technological Challenges to Deterrence and Policy Responses

blurred. It requires a willingness to question old assumptions and to embrace new ideas. And it requires a recognition that the future of warfare will be determined not only by the technologies we develop, but also by the strategies we devise to use them.

BIBLIOGRAPHY:

1. Atlantic Council (19 August 2025). *A Vision for US Hypersonic Weapons,* https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-vision-for-us-hypersonic-weapons/, retrieved on 2 September 2025.
2. Bingen, K.A., Johnson, K., Young, M. (2023). *Space Threat Assessment 2023*, Center for Strategic and International Studies/CSIS, pp.1-33.
3. Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford University Press.
4. Congressional Research Service (18 January 2022). *Cybersecurity: Deterrence Policy*, https://www.congress.gov/crs- product/R47011/, retrieved on 26 August 2025.
5. Center for Strategic and International Studies/CSIS (15 November 2023), *Deterrence and Cyber Strategy*, https://www.csis.org/analysis/deterrence-and-cyber-strategy/, retrieved on 12 August 2025.
6. Center for Strategic and International Studies/CSIS (10 June 2024). *Algorithmic Stability: How AI Could Shape the Future of Deterrence*, https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence/, retrieved on 2 September 2025.
7. Center for Strategic and International Studies/CSIS (2 May 2025). *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience*, https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy- information-and-resilience/, retrieved on 12 August 2025.
8. Cummings, M. (26 January 2017). *Artificial Intelligence and the Future of Warfare,* Chatham House, https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf, retrieved on 29 August 2025.
9. Finabel (9 February 2021). *The Strategic Implications of Hypersonic Weapons,* https://finabel.org/the-strategic-implications-of-hypersonic-weapons/, retrieved on 20 August 2025.
10. Freedman, L. (2020). *The Evolution of Deterrence Strategy and Research*, in NL ARMS Netherlands Annual Review of Military Studies, DOI:10.1007/978-94-6265-419-8_1, pp.1-10.
11. Global Security Review (5 May 2025). *Hypersonic Weapons: Are We Entering a New Era of Vulnerability?,* https://globalsecurityreview.com/hypersonic- weapons-are-we-entering-a-new-era-of-vulnerability/, retrieved on 10 September 2025.
12. Horowitz, M.C. (2021). *When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability*, in *Emerging Technologies and International Stability*, ed. Michael Krepon, Taylor&Francis, pp.764-788.
13. Human Rights Watch (19 November 2012). *Losing Humanity: The Case against Killer Robots*, ISBN: 1-56432-964-X, pp.6-13.

14. ICRC (16 January 2025). *'Hybrid Threats', 'Grey Zones', 'Competition', and 'Proxies': When Is It Actually War?*, https://blogs.icrc.org/law-and-policy/2025/01/16/hybrid-threats-grey-zones-competition-and-proxies-when-is-it-actually-war/, retrieved on 5 September 2025.
15. NDU Press (4 May 2023). *Cyber Deterrence Is Dead! Long Live 'Integrated Deterrence'!,* https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3379791/cyber-deterrence-is-dead-long-live-integrated-deterrence/, retrieved on 26 August 2025.
16. NDU Press (30 October 2023). *Space Denial: A Deterrence Strategy,* https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3569640/space-denial-a- deterrence-strategy/, retrieved on 27 August 2025.
17. Nye Jr., J.S. (May 2010). *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School.
18. RAND Corporation (31 August 2023). *A Framework of Deterrence in Space Operations*, https://www.rand.org/pubs/research_reports/RRA820-1.html, retrieved on 2 September 2025.
19. Small Wars Journal (17 June 2025). *Quantifying the Gray Zone: A Framework for Measuring Hybrid Warfare*, https://smallwarsjournal.com/2025/06/17/framework-for-hybrid-warfare/, retrieved on 10 September 2025.