The Geopolitics of Technology, Social Media, and New Power Brokers

Edited by:
J.C. Ellis

NATO Allied Command Transformation
University of Cambridge Centre for Geopolitics

Copyright Page

Opinions, conclusions, and recommendations expressed or implied within are solely those of the contributors and do not necessarily represent the views of University of Cambridge, Allied Command Transformation or any other agency of the North Atlantic Treaty Organization.

"The Geopolitics of Technology, Social Media, and New Power Brokers"
Editors: J. C. Ellis
Researchers: Karolina Muti, Ottavia Credi
© 2026 SACT NATO HQ - 7857 Blandy Road, suite 100, Norfolk, Virginia USA
ISBN: 979-8-234-02496-1

Foreword

Vlasta Zekulic

In an age where the boundaries of warfare are increasingly blurred, with cyberattacks, disinformation campaigns, economic coercion, and asymmetric and conventional military tactics converging, states must reconsider how they define and defend against aggression. Understanding the conceptual frameworks that govern such complexity and evolutionary trends has never been more urgent.

For NATO, the challenge lies not only in adopting new technologies at speed and scale but in strategically shaping their employment to enable action. The challenge is essentially twofold:

- How can NATO and Allies harness the power of technology that now underpins military strength, economic competitiveness, and societal resilience while upholding ethical standards and interoperability across members?
- How can NATO win the technological race for dominance in artificial intelligence, quantum computing, and, most importantly, cognitive space, given the decision advantage of our adversaries and competitors?

With this in mind, the Royal United Services Institute (RUSI) hosted NATO Allied Command Transformation (ACT) and the University of Cambridge Centre for Geopolitics for the 2025 NATO Academic Conference. The event gathered a team of experts, academics, and military and industry innovators to discuss the growing impact of technology and what NATO and Allies can do about it.

Harnessing the Power of Technology

Historically, breakthroughs–from industrialization to the digital revolution–have redrawn alliances and altered the balance of power. Today, the pace, scale, and global diffusion of technology far exceed previous eras, creating unprecedented opportunities. As academics discussed the role of foresight, organizational and procedural adaptability, and the need to alter strategic planning to enable NATO's absorption of innovation and retention of its technological edge, a common theme emerged. They emphasized the need for proactive international leadership to both harness the power of new technologies and demonstrate their use by example.

The rising importance of the private technology sector in transforming global power structures creates additional challenges for the Alliance. Tech corporations now hold capabilities once reserved for states, ranging from artificial intelligence and cyber defense to satellite networks and digital communications. Their influence extends into economic systems, political narratives, and national security architectures.

As private ownership of critical digital infrastructure expands, the boundary between public and private power blurs. Corporate decisions increasingly affect global security, creating new interdependencies and tensions. Issues such as data sovereignty, regulatory oversight, and reliance on corporate-controlled technologies are emerging as strategic concerns for NATO.

Consequently, NATO's role increasingly extends beyond defense in the physical domain to safeguarding information integrity, the cognitive domain, and public trust. By building strategic partnerships among governments, civil society, media, and the private sector, there is an opportunity to design a "whole-of-society" defense against manipulation and coercion, while still ensuring that security measures do not compromise fundamental rights such as open discourse and freedom of expression. In this recalibrated relationship, it is important to note that the private sector is not merely a vendor but a strategic partner.

Attacking and Defending the Mind

While technology has fundamental implications for every aspect of human life, as well as for NATO's deterrence and defense, the most resonant challenges during the conference concerned its impact on the human mind.

In the recently developed Cognitive Warfare Concept, designed by Allied Command Transformation, NATO experts note:

> *Cognitive warfare is not the means by which we fight; it is the fight itself. The brain is both the target and the weapon in the fight for cognitive superiority. Cognitive Warfare focuses on attacking and degrading rationality, which can lead to exploitation of vulnerabilities and systemic weakening. However, this becomes increasingly complex as non-military targets are involved.*
>
> *Contesting in this environment comprises deliberate, synchronized military and non-military activities throughout the continuum of competition designed to gain, maintain and protect cognitive advantage.*[1]

The Cognitive Warfare Concept, for the first time within NATO, builds systematic defenses within the cognitive space, focusing on a very niche element of hybrid warfare: the human mind.

Historically, hybrid warfare sat at the crossroads of "politics by other means" and "wars by other means." In the former Soviet Union, these were called "active measures." They aimed to break NATO from within by attacking all its weak points and undermining the mutual confidence of the Allies in each other and in NATO as a whole. While the aims are not new, the tools available to achieve them have changed so profoundly that hybrid warfare now approximates any other

[1] NATO Allied Command Transformation, "Cognitive Warfare," accessed October 27, 2025, https://www.act.nato.int/activities/cognitive-warfare

form of war and can even trigger Article 5 of the North Atlantic Treaty, through which an attack on one is considered an attack on all.[2]

One of the key insights from the 2025 Academic Conference was the recognition of pivotal moments in history when new technologies challenged states' control of information and narratives–from the invention of the printing press to the rise of radio, television, and the internet. More recently, the proliferation of social media represents both a tool of empowerment and a vector of vulnerability. It enhances civic participation and information sharing, yet it also provides a fertile environment for cognitive manipulation, disinformation, and influence operations by state and non-state actors.

This dual nature of digital platforms poses challenges for societal cohesion and democratic resilience. AI-generated content, deepfakes, and malicious manipulation of online narratives can erode trust in institutions, distort society's understanding of truth itself, intensify polarization, and undermine the foundations of governance. Consequently, if Allied populations' will-to-fight is compromised, no number of sophisticated weapons systems will win future wars.

Conclusion

The NATO 2025 Academic Conference highlighted that technology is now both the terrain and the instrument of global competition, as its geopolitical, societal, and corporate dimensions are deeply intertwined. For NATO, sustaining strategic advantage will require anticipating disruption, strengthening societal resilience, and forging principled partnerships with industry - all while preserving democratic integrity and the collective trust that underpins the Alliance itself.

For these reasons, whether you are new to this subject or a seasoned expert, you will find something here that resonates deeply. This compendium is not just informative; it is transformative and gives any reader full appreciation of the complexity, ambiguity, benefits and risks that technological growth offers.

[2] North Atlantic Treaty Organization, "Countering Hybrid Threats," accessed October 27, 2025, https://www.nato.int/cps/en/natohq/topics_156338.htm

Acknowledgements

This publication is the result of the NATO Academic Conference "The Geopolitics of Technology, Social Media, and New Power Brokers" organized by NATO Allied Command Transformation (ACT) and the Center for Geopolitics, the University of Cambridge.
The Conference is the nineth iteration of ACT's Academic Conference series, and it took place at the Royal United Services Institute (RUSI) in London, from the 30th June to 01 July 2025.
The success of the event was due to the joint efforts of the three institutions, with special thanks for their dedication and expertise to ACT's Academic Outreach Team led by Ms Luisa Freutel, Center for Geopolitics team championed by Mrs Suzanne Raine and Mr John Ellis, and our gracious RUSI hosts Mrs Rachel Ellehuus and Mrs Sabrina Downey.

NATO Allied Command Transformation
Center for Geopolitics, University of Cambridge

Table of Contents

Foreword iii
Vlasta Zekulic

Acknowledgements vi

Executive Summary ix

NATO and the Geopolitics of Technology: Past Lessons, Present Questions, and Future Horizons 1
Gorana Grgić

Beyond Disinformation: The Role of Weaponized Identity in Cognitive Warfare 18
Tanna M. Krewson

When the Private Tech Sector Disrupts the Defense Industry: What Is NATO's Strategy? 38
Dominika Kunertova

Between Minds and Machines: The Transformative Power of AI and Its Implications for NATO 55
Sofia Romansky

List of Contributors 71

Executive Summary

The 2025 NATO Academic Conference, jointly convened by NATO Allied Command Transformation (ACT) and the University of Cambridge Centre for Geopolitics, brought together academics, practitioners, industry leaders, and policy experts to examine how accelerating technological change is reshaping global power and the foundations of international security. Under the theme "The Geopolitics of Technology, Social Media, and New Power Brokers," participants assessed the strategic implications of emerging disruptive technologies (EDTs), the rise of influential private-sector actors as geopolitical agents and accelerating contestation over the cognitive domain.

This compendium–and the conference from which it draws its conclusions–highlights how today's security environment is primarily shaped not only by renewed great power competition, but by the rapid diffusion of advanced technologies: from artificial intelligence and commercial space systems to social media and algorithmic information flows. These disruptive technologies sit outside the functional remit of national governments, adding an additional layer to an increasingly convoluted strategic landscape. This compendium illustrates how these forces are redistributing strategic leverage across the various strata of society and are impacting NATO's operating assumptions about deterrence, decision-making, and resilience. This volume and the associated conference served as a touchpoint in the Alliance's broader adaptation agenda, aligning closely with NATO's Rapid Adoption Action Plan, the Warfighting Capstone Concept, and the evolving requirements of multi-domain operations.

Another central theme within this volume is the expanding role of the private technology sector as a new class of geopolitical actor. Companies now own and operate capabilities–cloud infrastructure, satellite constellations, AI models, and digital communication networks–that represent both threats to and opportunities for collective defense. Moreover, corporate decisions now shape operational conditions and have direct consequences on the outcomes of traditional security crises. This volume suggests NATO must view these firms not merely as vendors, but as strategic partners whose market incentives, risk tolerances, and governance practices often diverge from the Alliance's approach to collective defense, resilience, and escalation management. Bridging these conceptual and operational divides between NATO and its partner firms will be a central challenge for the Alliance in the coming years.

This volume also foregrounds increasing contestation in the cognitive domain. Contributors explore the implications of NATO's Cognitive Warfare Concept, noting how adversaries now target identity, belonging, and emotion in ways that transcend traditional "disinformation." Indeed, one key takeaway is that nebulous concepts, such as "disinformation," often obscure the strategic challenges facing the Alliance more than they clarify the problem to policymakers. Contributors aver that identity-based manipulation–upscaled through social media algorithms, and new generative AI tools–pose a systemic threat to the internal political cohesion

undergirding Alliance cooperation. The compendium depicts “disinformation” as merely one tool within a broader array of identity-based manipulation techniques. Defense, therefore, must extend beyond fact-checking and a whack-a-mole approach to false narratives; it requires a whole-of-society posture rooted in psychological resilience, social cohesion, interdisciplinary cooperation, and communication practices that acknowledge how identity and emotion shape human cognition. NATO doctrine can play an important role in clarifying these various categories and facilitating cooperation on appropriate countermeasures.

This volume also describes the fragility of globally distributed supply chains; the dual-use nature of commercial space systems; and the risks of over-reliance on private infrastructure whose disruption could cascade across military, political, and societal domains. Across these areas, the contributors point towards the need for layered resilience, anticipatory governance, and mechanisms that facilitate quicker technological adoption within the Alliance.

Taken together, this compendium and the 2025 conference reaffirm that NATO’s strategic advantage depends on its ability to integrate technological foresight and foster principled partnerships with industry while safeguarding the security and democratic values its member states. These goals remain the Alliance’s raison d’être and cannot be subordinated to the logic of technological accelerationism. This compendium reflects those debates and provides a forward-looking assessment of the geopolitical, cognitive, and technological forces that will shape Euro-Atlantic security in the years ahead.

NATO and the Geopolitics of Technology: Past Lessons, Present Questions, and Future Horizons

Gorana Grgić

In the domain of foreign and security policy, technologies are instruments of political work: they reshape what states see as feasible, alter the speed and opacity of decision cycles, and redistribute leverage among states, firms, and publics. NATO's strategic environment today is defined by three interacting features. First, the resurgence of great power competition has made strategic advantage a central concern once again. Second, frontier technologies–especially artificial intelligence, information platforms, and commercial space services–are diffusing rapidly outside state control, creating many new relevant actors. Third, the economic architectures and supply networks that underpin advanced systems are globally distributed, and therefore potentially fragile. Together, these shifts make traditional measures of military power necessary but insufficient indicators of an alliance's capacity to deter and to act in crisis.

This paper draws on the discussions from workshops convened as part of the NATO 2025 Academic Conference in London. Participants were explicitly invited to move away from the tyranny of presentism and to place contemporary technological dilemmas in a broader historical and institutional context by reflecting on three core prompts: *Historical Insight*–"Think of a moment in history when technology shifted global power or redefined alliances; what lesson does that moment offer NATO today?"; *Foresight*–"Spot a future trend or risk at the intersection of tech and geopolitics; how might this influence NATO's deterrence strategy or cohesion in the years ahead?"; and *Strategic Reflection*–"What is one big question NATO needs to be asking itself today to be ready for tomorrow when it comes to the intersection between geopolitics and technology?"

These guided conversations produced the principal takeaways synthesized below. Namely, historical exemplars such as the nuclear revolution, the space race, mass-media transformations, and the introduction of new weaponry in World War I provide analytic frames. Near and medium-term risks coalesce around AI and information operations, supply chain fragility, space vulnerability, and the diffusion of dual-use technologies. Strategically, NATO should prioritize behavioral analysis and adoption readiness–how quickly and collectively the Alliance can operationalize new capabilities–rather than rely solely on hardware tallies. This paper integrates these workshop outputs with contemporary scholarly and policy debates and develops concrete recommendations that link rules, norms, resilience, and the institutional capacity to adopt innovation under stress.

Historical Insight: Select Cases and Lessons

Historical analogies occupy an uneasy but indispensable place in strategic analysis. Analogies often serve as an easy template for making sense of the present, offering the reassurance that history provides lessons to avoid repeating past mistakes. Yet many scholars and analysts caution that they are frequently applied in overly mechanical ways, leading to shallow or uncritical comparisons that obscure important differences.[1] This is the analytic posture adopted here: not to insist that any single historical case provides a deterministic model for contemporary policy, but to use selected cases as comparative lenses that highlight problems of signalling, institutional adaptability, legitimacy, and dependence that re-emerge whenever novel technologies attain strategic salience. Four historical episodes–nuclear weapons, the Cold War space competition, the rise of mass broadcast media, and the organizational shock of the First World War–serve this purposive function. Each exposes a distinct but intersecting cluster of risks and institutional requirements that are salient for NATO today.

The Nuclear Revolution

The advent of nuclear weapons fundamentally altered strategic logic. Early theorists recognized that thermonuclear arms made traditional notions of victory and defeat inadequate. They concluded that the "chief purpose" of the military must henceforth shift "from winning wars to *averting* them."[2] In this view, the supreme goal became credible deterrence, hinging on political credibility, signalling, and robust crisis management, rather than military conquest. In practice, nuclear deterrence became a problem of political and institutional design: U.S. and allied planners had to build procedures, communications networks, and crisis protocols to make deterrence credible under deep uncertainty. The Cold War experience shows that simply amassing more nukes was not enough; deterrence required that arsenals be backed by clear chains of command, reliable authority structures, and agreed escalation rules.

Translating these lessons to emerging domains means recognizing that cyber, space, and AI are redefining NATO's security landscape in similarly disruptive ways. These technologies can blur attribution and compress timelines. For example, AI-driven cyberattacks "pose new challenges related to attribution," since they may be carried out autonomously by bots "making it difficult to determine the source of an attack."[3] In practice, an AI-enabled campaign could escalate faster than humans can process responsibility or calibrate a response. Thus, NATO faces the task of building an updated political architecture of deterrence: it must develop alliance-wide mechanisms for (near) real-time situational awareness, jointly agreed thresholds for collective

[1] David Patrick Houghton, "Analogical Reasoning and Policymaking: Where and When Is It Used?," *Policy Sciences* 31, no. 3 (1998): 151–176; William Flanik, "Analogies and Metaphors and Foreign Policy Decision Making," in *Oxford Research Encyclopedia of Politics* (2017).
[2] Bernard Brodie, "The Absolute Weapon," in *Strategic Studies* (Routledge, 2008), 193–233.
[3] Silvio Brescia, "Navigating the AI Battlefield: Opportunities and Ethical Frontiers," *NRDC-ITA, NATO Rapid Deployable Corps Italy*, accessed September 2025.

action, and secure communications channels to sustain coordination under profound uncertainty.[4] In short, following the nuclear precedent, it is not enough to field capabilities; NATO must also institutionalize procedures and norms so that these capabilities translate into credible policy in a crisis.

The Space Race

The Cold War competition in space teaches how symbolic programs can evolve into vital dual-use infrastructures. Apollo and Sputnik were, in part, political spectacles, but they laid the groundwork for today's satellite networks. Indeed, modern militaries and economies are deeply reliant on space-based services. Over the past six decades, the United States "has grown more reliant on the information, situational awareness, and connectivity provided by military, civil, and commercial space systems."[5] NATO itself recognizes that its deterrence and defense posture depends on space assets for secure communication, navigation, intelligence and early warning systems.[6] In other words, space is now an integral part of the Alliance's "grammar" of warfighting and crisis response, not a sideshow.

The current era of commercial spaceflight amplifies both the benefits and fragilities of this system. Today, thousands of satellites–including mega-constellations owned by companies such as SpaceX–carry military and civilian traffic in orbit. As of 2025, over 10,000 satellites are active, with the majority privately owned; SpaceX alone operates around 7,000. [7] The explosive growth of commercial space means that key functions now depend on assets outside government control. The surge in private satellites poses challenges to the protection and defense of private sector equities in space. [8] In a contingency, satellites used for both civilian and military purposes could become "legitimate" targets, and loss of space services could have cascading effects on communication, navigation, and intelligence.

The policy implication is a layered resilience strategy. Alliance defense of space cannot rely solely on hardening military satellites. Instead, NATO and partners should combine technical and non-technical measures. This includes building redundancy and distributed architectures to survive attacks, as well as establishing norms and legal frameworks for responsible behavior in orbit. Importantly, it also means integrating commercial actors into contingency planning.

Mass Media

[4] Andrea Gilli, Mauro Gilli, and Gorana Grgić, "NATO, Multi-Domain Operations and the Future of the Atlantic Alliance," *Comparative Strategy* 44, no. 1 (2025): 73–91.
[5] Todd Harrison, Kaitlyn Johnson, Joe Moye, and Makena Young, *Space Threat Assessment 2022* (Center for Strategic and International Studies [CSIS], 2022).
[6] Julia Cournoyer, "Securing the Space-Based Assets of NATO Members from Cyberattacks: The Evolution of the Space Policies of NATO and Its Key Members," *Chatham House*, May 15, 2025.
[7] Clayton Swope, "How Can the U.S. Government Safeguard Commercial Satellites from Threats?," *Center for Strategic and International Studies,* August 25, 2025.
[8] Ibid.

New communication technologies have repeatedly shifted the domestic politics of alliance warfare. Television, for example, made war viscerally real to home audiences and thus altered how democracies wage conflict. The Vietnam War is often called the "first television war."[9] Widespread broadcast of graphic images–from news anchors reporting from the front to uncensored footage of combat–transformed public perceptions. Relatedly, a broader phenomenon of the "CNN effect" has been observed, whereby relentless 24/7 news coverage can have an influence on policymakers.[10]

Today's digital information environment amplifies these dynamics exponentially. Social media platforms use algorithms to micro-target content, and emerging AI-driven tools can generate realistic "deepfakes." Analysts warn that adversaries now have the means to tailor influence operations with unprecedented precision. For example, a study of hostile information campaigns notes that state actors can "tailor their threats to specific population segments and 'influencers'" using AI, and that advances in synthetic audio and video allow them to deliver "coercive messaging in extraordinarily effective ways."[11] In practice, this means fake news or doctored videos can spread rapidly across social networks and reach receptive audiences, blurring truth and propaganda.

The lesson for NATO is not primarily a technical fix but a warning about domestic resilience and cohesion. Alliance solidarity depends on public support at home for bearing security burdens; disinformation and misinformation can erode that support nearly overnight. Therefore, NATO must invest both in technical defenses and societal resilience. On the technical side, this means improving rapid detection and attribution of disinformation (including coordinating with platforms to counter automated bots and AI-generated fakes). On the societal side, it means building media literacy and proactive communications.

World War I

The First World War exemplifies the danger of technological change outpacing institutions. Between 1914 and 1918, armies confronted a perfect storm of new warfare innovations–machine guns, long-range artillery, tanks, and aircraft–that abruptly transformed the battlefield. Three simultaneous "paradigm shifts" which included machine power, air power, and depth of fire rendered prewar doctrine "almost completely obsolete overnight."[12] Commanders had to devise new tactics slowly and painfully by trial and error, at the cost of hundreds of thousands of casualties. Logistic and bureaucratic bottlenecks, from munitions shortages to rigid hierarchies, imposed strategic costs that no amount of bravery could surmount. In short, the war's industrial

[9] Michael Mandelbaum, "Vietnam: The Television War," *Daedalus* (1982): 157–169.
[10] Piers Robinson, "The CNN Effect Reconsidered: Mapping a Research Agenda for the Future," *Media, War & Conflict* 4, no. 1 (2011): 3–11.
[11] Paul N. Stockton, *Defeating Coercive Information Operations in Future Crises*, no. NSADR21002 (2021).
[12] David T. Zabecki, "Military Developments of World War I," *International Encyclopedia of the First World War* 7 (2015).

lethality outstripped the adaptability of armies and staff. As military historians have noted, this organizational lag was itself a principal cause of the staggering human toll.[13]

Today's analogue is the accelerating pace of commercial innovation versus often sluggish defense bureaucracies. Breakthroughs in AI, robotics, biotechnology, and software emerge faster than traditional procurement, training, and legal processes can absorb. For instance, while private tech firms iterate new capabilities in months, acquiring and fielding even mature systems in the military can take years. A recent U.S. Defense Innovation Board report underscored this gap; unlike the Cold War era of "bold risk-taking, rapid research" and "large-scale development," today's defense innovation is hindered by "hesitance, cumbersome processes, [and] misaligned rewards."[14]

The implication is clear: NATO must reform peacetime processes to avoid a World-War-I–style organizational shock. Key measures include streamlining testing and certification and creating flexible pilot programs that fast-track promising technologies. Procurement authorities should empower warfighting units to co-develop and trial new systems under realistic conditions. Legal and ethical oversight can be maintained through modular review processes rather than blanket bans. Crucially, exercises and wargames should explicitly integrate cutting-edge prototypes into coalition scenarios, so that doctrinal lessons are learned in real time. By training alliance staff and troops to use emerging technologies before conflict escalates, NATO can turn the typical institutional lag into a managed transition.

Foresight: Emerging Trends and Strategic Risks

Experts at the workshop identified AI and information operations as the most urgent near-term challenges, while supply chain fragility, space dependence, and the diffusion of dual-use technologies remain deeply consequential. These risks are interconnected: a single vulnerability–such as an exploited logistics network or a degraded satellite link–can cascade into other domains, undercutting coalition situational awareness and readiness. We examine each domain in turn, emphasizing both operational dynamics and political effects.

AI and the Transformed Information Environment

AI is a potent force multiplier for military operations, enabling capabilities that range from advanced sensing to optimized logistics and faster decision loops. For example, machine-learning–driven tools can fuse disparate sensor inputs into higher fidelity battlefield pictures, and predictive-analytics systems can schedule maintenance and manage supply chain demand more efficiently.[15] In doctrine and planning, analysts often frame these gains in terms of compressing

[13] Hew Strachan, *The First World War: Volume I: To Arms* (Oxford: OUP, 2003).
[14] Defense Innovation Board, *Aligning Incentives: Accelerating the Defense Innovation Ecosystem* (Washington, DC: U.S. Department of Defense, July 5, 2024).
[15] Shashank Joshi, "AI on the Battlefield: A Fait Accompli?," *Survival* 67, no. 2 (2025): 115–122.

the traditional observe–orient–decide–act (OODA) cycle, since AI promises to speed routine tasks and free human commanders to focus on strategy.[16] Yet modern AI systems also introduce novel failure modes that complicate reliance on them under stress. Deep learning models can be fragile: carefully constructed adversarial inputs may induce complete misclassification, and systems often behave unpredictably with out-of-distribution data. Moreover, many powerful architectures are effectively opaque, raising questions about explainability and accountability when lives are at stake. These issues mean that, despite AI's theoretical benefits, commanders may hesitate to trust unverified outputs in real time without robust validation and testing.

In parallel, generative AI is reshaping the political information environment. Large-scale models now can synthesize highly credible images, audio, and text at negligible marginal cost, dramatically lowering barriers to disinformation. Armed actors can orchestrate automated influence campaigns that flood public discourse with tailored narratives, amplifying confusion and eroding trust. When adversaries manipulate public perceptions, they can sap political will for coordinated action: an eroded public trust or engineered division makes it harder for democracies to maintain unified policy, even as allied militaries reliant on shared data streams risk being fed deceptive inputs.

Thus, the AI challenge is not only one of algorithmic robustness but of governing the entire socio-technical ecosystem. Defensive measures must extend beyond technology to include institutional and societal practices. Governments and platforms should enforce rigorous validation of defense-grade AI systems–through adversarial testing, cross-validation on diverse data distributions, and clear explainability standards–to ensure they do not fail catastrophically under attack. At the same time, institutions need real-time fusion centers and platform cooperation for situational awareness, along with public communication strategies to inoculate citizens against rapid narrative onslaughts. The recent EU AI Act (Regulation 2024/1689) is an example of this approach: it creates harmonized rules for high-risk AI uses and requires developers and deployers to implement risk mitigation and transparency measures.[17]

Information Operations and Computational Propaganda

Modern information operations are inherently algorithmic and automated. Adversaries routinely employ networks of bots and fake social-media profiles to disseminate divisive content. Studies of "computational propaganda" have documented how concerted inauthentic behavior and microtargeting can stoke polarization and exploit social cleavages. For example, an analysis of influence campaigns in recent US presidential elections notes that operators assemble "a digital

[16] Myriam Dunn Cavelty and Sarah Wiedemar, *AI Decision Support Systems on the Battlefield*, *CSS Analyzes in Security Policy,* no. 366 (Zürich: Center for Security Studies, ETH Zürich, 2025).
[17] Mauro Fragale and Valentina Grilli, "Deepfake, Deep Trouble: The European AI Act and the Fight Against AI-Generated Misinformation," *Columbia Journal of European Law* (2024).

army of fake personas" and use automated accounts to seed content across platforms.[18] The arrival of generative AI intensifies these dynamics by compressing both time and cost for generating bespoke disinformation. In effect, deepfake videos or bogus documents that once took teams to produce can now be created at scale, making influence operations more continuous and sophisticated.

A key challenge is attribution. Unlike a missile launch, which may leave forensic traces, disinformation flows through layers of opaque intermediaries–anonymous accounts, proxy platforms, and cross-border amplification networks. This ambiguity means that defending governments often hesitate to publicly rebut narratives while attribution is uncertain, giving malicious stories time to spread and shape opinions. Operationally, countering this threat requires a combination of technical tools and policy frameworks. Automated detection systems capable of scanning multi-lingual and multi-format content are essential, as are forensic attribution protocols that let allied intelligence share and vet evidence rapidly. Equally important are narrative control measures: governments should prepare "pre-vetted" responses and convene crisis-mode communication exercises so that leaders can swiftly counter false claims with coherent messaging.

Civil society solutions must complement these technical fixes. Investments in media literacy and robust local journalism can raise the bar against disinformation: an informed public is less easily duped. Similarly, regulatory steps such as platform transparency obligations (which mandate disclosure of advertising sources or algorithmic processes) help illuminate the influence campaigns. In brief, technical countermeasures alone cannot substitute for civic resilience.

Supply Chain Resilience and the Industrial Base

The crisis of global trade in recent years–from COVID-19 disruptions to active warfare in Eastern Europe and the Middle East to export control frictions–has spotlighted NATO's dependence on long, just-in-time supply chains for defense technology. Critical choke points now loom large; for instance, advanced semiconductor fabrication is geographically concentrated, specialized optics for satellites come from a handful of firms, and some rare earth elements essential to weapons are produced almost entirely by a single country. Decades of cost-cutting have made the defense industrial base "optimized for efficiency, not resiliency": reliance on just-in-time inventories and foreign sole-source suppliers (often cheap but potentially adversarial) means that disruptions immediately curtail output.[19] In practice, this fragility has already threatened readiness. During COVID, critical components for both civilian and military

[18] Katerina Sedova, Christine McNeill, Aurora Johnson, Aditi Joshi, and Ido Wulkan, *AI and the Future of Disinformation Campaigns: Part 1: The RICHDATA Framework*, *CSET Policy Brief* (Washington, DC: Center for Security and Emerging Technologies, December 2021).
[19] Christine Michienzi, *Defense Mobilization in the 21st Century* (Center for Strategic and International Studies, March 6, 2025).

systems were delayed, and Russia's war against Ukraine has exposed dependence on Russian and Ukrainian sources of key materials such as titanium, gallium, and neon.[20]

The political ramifications are equally stark. When scarce materiel is in play, allies compete–raising the domestic salience of procurement choices and stoking calls for protectionism. Public pressure can force governments into bidding wars for munitions or locking in bilateral deals that undermine unity. Worse, if adversaries believe that NATO cannot quickly replenish expended arms, the Alliance's deterrence credibility erodes. Thus, NATO policy must treat industrial capacity as part of deterrence: ensuring surge supply is as vital as deploying troops. Strategies include diversifying supplier bases (investing in multiple production hubs for semiconductors or optics), establishing vetted "trusted-supplier" networks, and maintaining buffers (strategic stockpiles of critical inputs).

Allies should negotiate pre-arranged surge contracts and co-finance shared facilities so that production can ramp rapidly. For instance, pooling procurement for munitions (as under the EU's recent ammunition funding act) can create scale, and encouraging ally- and partner-shoring of inputs can build redundancy.[21] NATO should also embed resilience metrics into readiness assessments: exercises and war games ought to simulate prolonged conflict and test whether industrial capacity can keep pace.

In short, sustaining NATO's material advantage requires continuous investment in the defense-tech industrial base. Recommendations include formalizing industrial cooperation forums, aligning procurement planning across Allies, and incentivizing joint projects.[22] Taken together, these steps–diversification, trusted procurement frameworks, and co-investment in production–would help ensure that high-tech superiority endures even under severe stress.

Space Dependence and Vulnerability

Allied militaries and economies are deeply interwoven with space-based services. Satellite positioning, navigation, and timing (PNT) underpin precision munitions and logistics, satellite communications link forces worldwide, and orbiting sensors provide critical intelligence, surveillance, and reconnaissance (ISR) data. This constellation dependence has expanded in recent years as commercial actors launch thousands of small satellites. The flipside is obvious: space assets are now prime targets. In practice, the threat spectrum includes electronic attacks like jamming and spoofing, cyber intrusions of ground stations, co-orbital maneuvers, and even kinetic anti-satellite weapons. For example, Russian forces have employed GPS jammers over

[20] Ibid.; Alexandra Alper, "Exclusive: Russia's Attack on Ukraine Halts Half of World's Neon Output for Chips," *Reuters*, March 11, 2022.
[21] European Commission, "The Commission Allocates €500 Million to Boost Ammunition Production, Part of €2 Billion to Strengthen EU Defense Industry," *Press release,* March 15, 2024.
[22] Jade Guiberteau, Lucas Hellemeier, and Kaija Schilde, "Defense Industrial Policy in a Changing International Order: Rethinking Transatlantic Burden-Sharing," *Defense Studies* 24, no. 1 (2024): 166–173.

Ukraine, directly demonstrating the vulnerability of even terrestrial operations to space-domain interference.[23]

The growing role of private space companies adds another layer of complexity. While commercial constellations (e.g., global satellite broadband networks) reduce costs and spur innovation, they also mean that key capabilities are not under direct government control. In a crisis, it may not be straightforward to secure a privately operated network in the same way as a military asset. Moreover, civilian satellites often have dual-use features, blurring the line between peaceful and military targets. From a governance standpoint, there are still no widely accepted norms of behavior in space: rules governing debris, counterspace tests, or the militarization of orbits remain underdeveloped.[24]

To address these risks, NATO should invest in technical and diplomatic solutions.[25] On the technical side, redundancy is essential: multi-path PNT solutions (e.g., terrestrial alternatives to GPS), hardened satellite links, and dispersed ground stations can mitigate single points of failure. Improved Space Situational Awareness (SSA) and attribution capabilities are also crucial, so the Alliance can quickly distinguish interference from benign anomalies and attribute attacks if they occur. Equally important is the diplomatic track: NATO should engage with partners and industry to build contingency arrangements, such as emergency spectrum agreements, and negotiate codes of conduct for space. By promoting norms–for example, declaring a moratorium on tested kinetic antisatellites (ASATs) or agreeing on responsible space traffic management–the Alliance can help raise the political costs of hostile acts in orbit. In this way, technical resilience and normative deterrence together can preserve the benefits of space while reducing the incentives for adversaries to exploit this vulnerable domain.

Dual-Use Diffusion and Actor Plurality

One of the defining features of the current era is how dual-use technologies have proliferated beyond traditional state arsenals. Commercial AI platforms, microsatellites, additive manufacturing tools and biotechnology now enable a wide array of actors to build potent capabilities. Non-state groups, private firms, and even research labs can acquire or develop systems that ten years ago only militaries fielded. This diffusion complicates traditional controls. Modern dual-use items often emerge from open science and global supply chains, meaning that export-license regimes and government-to-government export controls have limited reach. At the same time, the motivations of private actors differ–companies driven by profit or innovation may not automatically prioritize alliance security, creating coordination gaps.

Policy responses must therefore blend regulation with cooperation and incentives. Rather than relying solely on blunt export bans, allies should develop cooperative frameworks with industry.

[23] Todd Harrison et al., *Space Threat Assessment 2022*.
[24] Clémence Poirier, "Swiss Good Offices in Space," *CSS Policy Perspectives* 13, no. 3 (2025).
[25] Todd Harrison et al., *Space Threat Assessment 2022*.

One approach is to craft voluntary certification schemes or technical standards that encourage secure development practices; for example, by rewarding companies that embed robust security into their R&D. Trusted-supplier lists and procurement preferences can nudge markets toward resilient behaviors, effectively aligning economic incentives with security goals. Public-private partnerships are equally vital–by involving firms early in strategy and planning, governments can integrate security concerns into commercial roadmaps. For instance, NATO's Defense Innovation Accelerator (DIANA) and Innovation Fund exemplify how pooling capital and know-how can shepherd dual-use technology into military use cases.[26]

Capacity-building in partner countries also reduces the risk that proliferated technologies fall into adversarial hands. Training programs, shared standards and interoperability protocols can raise the floor globally and make it harder for malign actors to find uncontested supply sources.[27] In all these efforts, it is important to recognize the limits of state coercion in a market-driven world. Therefore, the Alliance's role is often one of facilitator and convenor: bringing together industry, academia, and governments to develop norms and incentives that preserve security without stifling innovation. By doing so, NATO can harness the creative power of a broader innovation ecosystem while guarding against the asymmetric vulnerabilities that unchecked dual-use diffusion would otherwise entail.

Strategic Reflection: Behavior, Adoption, and Layered Deterrence

The workshops produced three interdependent reframings that move beyond narrow technical prescriptions toward a reconfiguration of NATO's operating logic. First, strategic analysis must broaden its lens to encompass behavior and incentives across a heterogeneous ecosystem of actors. Second, the Alliance should treat "adoption readiness"–the capacity to operationalize innovation rapidly and responsibly–as a core strategic metric. Third, deterrence in novel domains must be reframed as layered and multi-instrumental, combining resilience and governance with attribution and calibrated political consequences.

Behavioral mapping

The traditional, state-centric view of security is increasingly obsolete in high-tech domains. Today, private and quasi-public actors–from cloud providers and chip foundries to social-media platforms–wield strategic influence. Major tech firms such as Alphabet, Amazon, Apple and SpaceX now wield more resources and power than most states.[28] Their choices can decisively

[26] David Julazadeh and Kristen Taylor, "Three Ways NATO Can Shift Defense Industrial Capacity into High Gear," *New Atlanticist*, Atlantic Council, July 11, 2025.
[27] Benedetta Berti, "Enhancing Euro-Atlantic and Indo-Pacific Theater Cooperation: What Is NATO's Role?" *International Information Network Analysis (IINA)*, March 28, 2025.
[28] Audrey Kurth Cronin, "How Private Tech Companies Are Reshaping Great Power Competition," *The Kissinger Center Papers* (Henry A. Kissinger Center for Global Affairs, Johns Hopkins School of Advanced and International Studies, August 2023).

affect conflicts–as famously documented in SpaceX's decisions to supply (or withhold) access to the Starlink network to Ukrainian armed forces. Similarly, platform policies on content moderation or data localization can tip the balance in information warfare. Internet giants' services have become "theaters of conflict," and these firms increasingly act as security actors in their own right.[29]

In response, NATO must shift from narrow threat matrices to a political-economy mapping of incentives across this ecosystem. In practice this means embedding dedicated liaison cells and information-sharing with key firms (be it cloud, semiconductor, or space) under strict safeguards. It also means building metrics of private-sector risk, such as market concentration or supplier choke points, into alliance planning. Indeed, recent scholarship emphasizes that NATO's innovation efforts now include "networking with–and investing in–innovators" to access new technologies.[30] In short, analyzing strategic behavior today requires treating big tech and industry as constitutive actors: their investments, locations, and policies directly shape NATO's crisis response capacity.

Adoption readiness

The adage that "possession is not deployment" understates a core contemporary problem: the strategic value of new technologies derives principally from their convertibility into interoperable, legally and ethically usable capabilities under crisis conditions. NATO's *Rapid Adoption Action Plan* aims to accelerate the adoption of emerging technologies, innovation, and operational capabilities across the Alliance (NATO 2025). Adoption readiness, therefore, must be measured and exercised. Conceptually, adoption readiness is a composite construct: it captures legal and regulatory permissibility (export controls, data protection, rules of engagement), technical validation (adversarial testing, interoperability certification), human capital (trained operators and maintainers), logistical continuity (supply chain assurance), and social legitimacy (ethical review, public acceptability).

Exercises play a pivotal role: adoption readiness cannot be proven in isolation but must be stress-tested in combined wargames that simulate degraded environments, legal ambiguity, and contested information conditions. NATO should therefore design "adoption drills" analogous to live-fire or logistics surge exercises–events that measure the time and friction costs of moving prototypes into coalition use, identify legal and procedural bottlenecks, and create routinized pathways for fast-tracked certification under defined guardrails.[31] NATO already runs live-fire cyber drills that serve this purpose. In the annual *Locked Shields* exercise, teams defend allied networks against realistic scenarios. For instance, the 2024 edition emphasized AI-enabled

[29] Peter Warren Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Eamon Dolan Books, 2018).
[30] Stephen Herzog and Dominika Kunertova, "NATO and Emerging Technologies: The Alliance's Shifting Approach to Military Innovation," *Naval War College Review* 77, no. 2 (2024): 47–70.
[31] Office of the Director of National Intelligence (ODNI), *AI Threat Assessment (ATA) 2024–Unclassified Report* (Washington, DC: ODNI, 2024); NATO, *Secretary General Annual Report 2024* (Brussels: NATO, 2024).

threats, such as deepfake disinformation and synthetic identities, and hybrid attacks.[32] NATO should expand this idea beyond cyber: for any novel domain, allies need "adoption drills" that measure how quickly prototypes can be certified and deployed across the coalition. In sum, adoption readiness is not just a buzzword but a measurable posture–one that combines legal, technical, and human factors.

Layered deterrence

In new domains, deterrence cannot rely on one tool or force-count. Instead, it must be layered and multi-modal, blending resilience, norms, robust attribution, and calibrated responses. "Layered deterrence" strategies have overlapping pillars.[33] One cyber-security framework, for example, splits deterrence into (1) entanglement/norms–building international rules, institutions and responsible-use norms to raise the bar for attacks; (2) denial/resilience–hardening infrastructure so attacks have limited impact; and (3) cost imposition–credible punitive measures (sanctions, counter-operations) to make aggression unattractive.[34] NATO needs all three: for instance, normative governance can shape firm incentives (e.g. AI standards or export controls) to align markets with security needs; resilient architectures (multi-path communications, diverse suppliers, backup systems) can blunt attacks; attribution capabilities (forensic tech, intelligence sharing, legal frameworks) are needed so wrongdoing is exposed quickly; and calibrated consequences–from cyber counterstrikes to diplomatic or economic sanctions–translate attribution into deterrence.

Layered deterrence also demands political and legal coordination. Defense planners must work with allies' diplomats and regulators. For example, civilian regulations such as the EU's AI Act create technical standards and governance regimes; NATO can help translate these civilian standards into military requirements and interoperability protocols.[35] At the same time, decision-makers should develop clear rules of engagement and escalation control for cyber and information conflicts. Many digital "grey zone" attacks currently evade punishment because attribution is hard and allies lack unified policies. Strengthening attribution (e.g. shared digital forensics and warning networks) would tighten this gap.[36] Finally, nuclear-style signalling applies: deterrent credibility comes from signalling a credible second-strike capability across domains.

---

[32] NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), "Locked Shields 2024 Demonstrated the Real Power of Cooperative Defense," *CCDCOE News*, April 26, 2024.
[33] Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report* (March 11, 2020); Brandon Valeriano and Benjamin Jensen, "Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report," in *2021 13th International Conference on Cyber Conflict (CyCon)*, 189–214 (IEEE, 2021).
[34] Brandon Valeriano and Benjamin Jensen, "Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report.".
[35] Ibid.
[36] Silvio Brescia, "Navigating the AI Battlefield: Opportunities and Ethical Frontiers," *NRDC-ITA, NATO Rapid Deployable Corps Italy*, accessed September 2025.

In practice, layered deterrence means moving beyond arms counts to an all-of-society posture. This includes civil–military resilience (backup civilian networks, public awareness of disinformation), industrial security (rapid access to critical components, building surge capacity), and public normative work (international consensus on hostile behavior). By weaving together these layers–prevention and denial at the technical level, plus normative alignment and swift punitive measures at the political level–NATO can make any covert aggression strategically unattractive.

Conclusion

Technological change is not destiny but context; it interacts with institutions, incentives, and political cultures to produce outcomes. The historical record–nuclear deterrence, the space race, media-driven political constraint, and the organizational shocks of industrial warfare–provides frames that remain instructive but not entirely prescriptive. Today, AI and information operations sit at the center of a web of risks that also includes supply chain fragility, space vulnerability, and the diffusion of dual-use technologies.

NATO's strategic challenge is essentially institutional: to translate insights drawn from historical precedent and present foresight into organizational routines that enable the Alliance to recognize, assess, and incorporate technological change in ways that preserve collective action. This does not imply simple replication of past solutions but rather the cultivation of architectures–procedural, legal, and technical–that reduce frictions between national authorities, militaries, and private actors when novel capabilities become operationally relevant. Practical components of that architecture include clearer metrics for how quickly capabilities can be adopted across the Alliance, standing mechanisms for anticipatory horizon scanning and engagement with industry, and mechanisms that map and mitigate dependencies in critical infrastructure and supply chains.

At the same time, the workshop discussions and this analysis highlight important limits and trade-offs. Measures that increase speed of adoption may strain legal and ethical oversight; efforts to harden supply chains may raise economic costs and political sensitivities; and normative instruments intended to shape behavior in new domains may collide with divergent domestic regulatory regimes among Allies. Equally, technical fixes–redundant systems, attribution capabilities, interoperable standards–do not eliminate political contestation about thresholds for collective action. Any institutional reform thus needs to be calibrated to these tensions, combining procedural transparency and legal clarity with routine testing and exercises that reveal practical bottlenecks before crisis.

Viewed from this vantage, the imperative is less a single policy program than a change in posture: from episodic responses to a continuous mode of anticipatory management that treats adoption, governance, and resilience as coequal elements of preparedness. If NATO can embed such practices, it will be better positioned to manage the political and operational effects of

technological change. Whether it chooses to do so will shape not only the Alliance's military effectiveness but also the political durability of transatlantic cooperation in the decades ahead.

References

Alper, Alexandra. "Exclusive: Russia's Attack on Ukraine Halts Half of World's Neon Output for Chips." *Reuters*, March 11, 2022. https://www.reuters.com/technology/exclusive-ukraine-halts-half-worlds-neon-output-chips-clouding-outlook-2022-03-11/.

Benincasa, Eugenio. "Making Cyber Attribution More Transparent." *CSS Policy Perspectives* 11, no. 5 (2023).

Berti, Benedetta. "Enhancing Euro-Atlantic and Indo-Pacific Theater Cooperation: What Is NATO's Role?" *International Information Network Analysis (IINA)*, March 28, 2025. https://www.spf.org/iina/en/articles/benedetta_berti_01.html.

Brescia, Silvio. "Navigating the AI Battlefield: Opportunities and Ethical Frontiers." *NRDC-ITA, NATO Rapid Deployable Corps Italy.* Accessed September 2025. https://nrdc-ita.nato.int/newsroom/insights/navigating-the-ai-battlefield-opportunities--challenges--and-ethical-frontiers-in-modern-warfare.

Brodie, Bernard. "The Absolute Weapon." In *Strategic Studies*, 193–233. Routledge, 2008.

CCDCOE (NATO Cooperative Cyber Defense Centre of Excellence). "Locked Shields 2024 Demonstrated the Real Power of Cooperative Defense." *CCDCOE News*, April 26, 2024. https://ccdcoe.org/news/2024/locked-shields-2024-demonstrated-the-real-power-of-cooperative-defense/.

Cournoyer, Julia. "Securing the Space-Based Assets of NATO Members from Cyberattacks: The Evolution of the Space Policies of NATO and Its Key Members." *Chatham House*, May 15, 2025. https://www.chathamhouse.org/2025/05/securing-space-based-assets-nato-members-cyberattacks/03-evolution-space-policies-nato-and.

Cronin, Audrey Kurth. "How Private Tech Companies Are Reshaping Great Power Competition." *The Kissinger Center Papers.* Henry A. Kissinger Center for Global Affairs, Johns Hopkins School of Advanced and International Studies, August 2023. https://kissinger.sais.jhu.edu/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition/.

Cyberspace Solarium Commission. *Cyberspace Solarium Commission Final Report.* March 11, 2020. https://www.solarium.gov/report.

Defense Innovation Board. *Aligning Incentives: Accelerating the Defense Innovation Ecosystem.* Washington, DC: U.S. Department of Defense, July 5,

2024. https://innovation.defense.gov/Portals/63/20240701%20DIB%20Report_Aligning%20Incentives%20PUBLISHED%20STUDY_1.pdf.

Dunn Cavelty, Myriam, and Sarah Wiedemar. *AI Decision Support Systems on the Battlefield. CSS Analyzes in Security Policy,* no. 366. Zürich: Center for Security Studies, ETH Zürich, 2025.

European Commission. "The Commission Allocates €500 Million to Boost Ammunition Production, Part of €2 Billion to Strengthen EU Defense Industry." *Press release,* March 15, 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1495.

Flanik, William. "Analogies and Metaphors and Foreign Policy Decision Making." In *Oxford Research Encyclopedia of Politics.* 2017.

Fragale, Mauro, and Valentina Grilli. "Deepfake, Deep Trouble: The European AI Act and the Fight Against AI-Generated Misinformation." *Columbia Journal of European Law* (2024).

Gilli, Andrea, Mauro Gilli, and Gorana Grgić. "NATO, Multi-Domain Operations and the Future of the Atlantic Alliance." *Comparative Strategy* 44, no. 1 (2025): 73–91.

Guiberteau, Jade, Lucas Hellemeier, and Kaija Schilde. "Defense Industrial Policy in a Changing International Order: Rethinking Transatlantic Burden-Sharing." *Defense Studies* 24, no. 1 (2024): 166–173.

Harrison, Todd, Kaitlyn Johnson, Joe Moye, and Makena Young. *Space Threat Assessment 2022.* Center for Strategic and International Studies (CSIS), 2022.

Herzog, Stephen, and Dominika Kunertova. "NATO and Emerging Technologies: The Alliance's Shifting Approach to Military Innovation." *Naval War College Review* 77, no. 2 (2024): 47–70.

Houghton, David Patrick. "Analogical Reasoning and Policymaking: Where and When Is It Used?" *Policy Sciences* 31, no. 3 (1998): 151–176.

Joshi, Shashank. "AI on the Battlefield: A Fait Accompli?" *Survival* 67, no. 2 (2025): 115–122.

Julazadeh, David, and Kristen Taylor. "Three Ways NATO Can Shift Defense Industrial Capacity into High Gear." *New Atlanticist,* Atlantic Council, July 11, 2025. https://www.atlanticcouncil.org/blogs/new-atlanticist/three-ways-nato-can-shift-defense-industrial-capacity-into-high-gear/.

Mandelbaum, Michael. "Vietnam: The Television War." *Daedalus* (1982): 157–169.

Michienzi, Christine. *Defense Mobilization in the 21st Century.* Center for Strategic and International Studies, March 6, 2025. https://www.csis.org/analysis/defense-mobilization-21st-century.

NATO. *Secretary General Annual Report 2024.* Brussels: NATO, 2024.

NATO. *NATO's Rapid Adoption Action Plan.* Endorsed by Allied Heads of State and Government, June 25, 2025.

ODNI (Office of the Director of National Intelligence). *AI Threat Assessment (ATA) 2024–Unclassified Report.* Washington, DC: ODNI, 2024.

Poirier, Clémence. "Swiss Good Offices in Space." *CSS Policy Perspectives* 13, no. 3 (2025).

Robinson, Piers. "The CNN Effect Reconsidered: Mapping a Research Agenda for the Future." *Media, War & Conflict* 4, no. 1 (2011): 3–11.

Sedova, Katerina, Christine McNeill, Aurora Johnson, Aditi Joshi, and Ido Wulkan. *AI and the Future of Disinformation Campaigns: Part 1: The RICHDATA Framework. CSET Policy Brief.* Washington, DC: Center for Security and Emerging Technologies, December 2021. https://cset.georgetown.edu/wp-content/uploads/CSET-AI-and-the-Future-of-Disinformation-Campaigns.pdf.

Singer, Peter Warren, and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media.* Eamon Dolan Books, 2018.

Stockton, Paul N. *Defeating Coercive Information Operations in Future Crises.* No. NSADR21002. 2021.

Strachan, Hew. *The First World War: Volume I: To Arms.* Oxford: OUP, 2003.

Swope, Clayton. "How Can the U.S. Government Safeguard Commercial Satellites from Threats?" *Center for Strategic and International Studies,* August 25, 2025. https://www.csis.org/analysis/how-can-us-government-safeguard-commercial-satellites-threats.

Valeriano, Brandon, and Benjamin Jensen. "Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report." In *2021 13th International Conference on Cyber Conflict (CyCon),* 189–214. IEEE, 2021.

Zabecki, David T. "Military Developments of World War I." *International Encyclopedia of the First World War* 7 (2015).

Disinfo

WORLD

Disinfo

fake news
se information

Manipulati
and propag

Disinformation and mani
adipi-scing elit. Proin nib
sed, lacinia in, mi. Cras vel
tellus. Phasellus pharetra nu
at risus. Donec venenatis, t
ligula ultricies purus, sed
congue, pede vitae dapibus a
vel tempus metus leo non est
congue mollis.

Phasellus congue lacus e
vitae consectetuer consequat
mollis pede metus

Beyond Disinformation: The Role of Weaponized Identity in Cognitive Warfare

Tanna M. Krewson

Introduction: Beyond the Disinformation Frame

"Disinformation" has become a catch-all term to categorize turbulence in today's information-saturated world. From election interference and public health emergencies to rising ideological and political polarization, disinformation is cited as the unseen hand driving societies toward a convergence of apathy and volatility. In the context of cognitive warfare,[1] it is often pointed to as the primary tactic employed by adversarial actors below the threshold of armed conflict. Traditional disinformation frameworks maintain a relatively straightforward two-part premise: 1) malign actors seek to spread falsehoods to mislead the public, change attitudes and behavior, and decrease trust in institutions; and 2) a verifiable truth capable of countering these objectives exist. Thus, the remedy for disinformation is straightforward: debunk the lie, correct the record, and restore trust.

The results of this premise are as follows:

Social media companies hire armies of fact-checkers. Governments mobilize counter-disinformation task forces. Organizations hold disinformation-focused conferences and workshops. Policymakers call for information literacy campaigns. However, this fixation on disinformation, while politically convenient, obscures the reality of what is happening. Much of the content driving today's polarization and radicalization does not fit into the factual information/disinformation binary because manipulated information is not always fabricated and does not always make false claims. In fact, disinformation is merely one slice of a larger information pie. According to recent research from the Stanford Internet Observatory,[2] the North Atlantic Treaty Organization (NATO) Strategic Communications (StratCom) Centre of

[1] The NATO Cognitive Warfare Concept defines cognitive warfare as: "Cognitive warfare is the fight for cognitive superiority. Contesting in this environment comprises deliberate, synchronized military and non-military activities throughout the continuum of competition designed to gain, maintain and protect cognitive advantage." In this context, it is important to note that cognitive warfare is not the means by which we fight; it is the fight itself. As such, cognitive warfare should also not be misconstrued as Strategic Communications (StratCom) by another name. Information Operations (InfoOps), Psychological Operations (PsyOps), and Military Public Affairs (MilPA) are only some of the capabilities and functions used in the daily contest for cognitive advantage.

[2] Stanford Internet Observatory, "Elections Integrity Partnership: The Long Fuse: Misinformation and the 2020 Election," Stanford University, 2020.

Excellence (COE),[3] EU DisinfoLab,[4] and the RAND Corporation,[5] only about two to five per cent of the information we receive can be classified as disinformation.

However, the term "disinformation" has been expanded to the point of distortion. It is often invoked as a shorthand for everything creating upheaval in today's information environment, from conspiracy theories and propaganda to political spin and emotionally charged rhetoric. While often politically convenient, this linguistic inflation muddies the reality of what is happening. Treating all manipulation as disinformation obscures two critical distinctions: 1) not all manipulative content is false, and 2) not all falsehoods are influential.

By labelling all manipulated or intentionally targeted information as disinformation, we are committing a false conflation, collapsing the distinction between the delivery mechanism—the false or misleading content—and its effect, which is how the content interacts with identity, emotion, and cognition to produce real-world behaviors. Disinformation is only one visible tactic of cognitive warfare; the greater danger often lies in the identity-based effects used to erode trust, fracture cohesion, and alter how people think and behave. Conflating the two means we end up chasing the smoke while ignoring the fire.

Recognizing this, it begs the question of why we continue to latch onto the idea that disinformation or "fake news" is the core problem. Is the issue disinformation itself, or is it our widespread human susceptibility to it? Moreover, if it is the latter, why are we missing the larger picture? If the truth is that emotional pleas, historical grievances, and appeals to group loyalty and identity play a significantly larger role in our cognitive vulnerability than disinformation, then reactive campaigns based on fact-checking, debunking, and media literacy will have little impact on our risk profile. In today's digitally connected, information-saturated world, we are more than just misinformed—we are manipulated, and the two are not the same.

This article argues that we need to move away from using disinformation as a catch-all term because the real danger of cognitive warfare does not lie solely in disinformation, but in how adversaries weaponize our sense of identity and belonging to tear apart and degrade our societies. First, the paper will demonstrate how the overuse and overstretching of the term "disinformation" obscures the deeper mechanisms of manipulation. Second, it will touch upon the role of narratives, further emphasizing that what truly matters is not necessarily the story itself, but how it taps into identity, emotion, and belonging to shape behavior. Third, it will demonstrate how emerging and disruptive technologies (EDTs)—from social media to generative and agentic AI—serve as accelerants, enabling manipulation at speed and scale. Ultimately, it contends that one of the primary approaches employed in cognitive warfare is identity-based manipulation (IBM)—defined as the deliberate exploitation of identities to fracture societies,

[3] NATO Strategic Communications Centre of Excellence, "Robot Rolling the Red Carpet: The Rise of Social Media Bots," 2019.
[4] EU DisinfoLab, "The Disinformation Landscape across Europe," 2022, https://www.disinfo.eu/.
[5] Todd C. Helmus and Elizabeth Bodine-Baron, "Countering Truth Decay: Fighting Disinformation on COVID-19 and Beyond," RAND Corporation, 2021.

inflame divisions, and erode trust—and that disinformation needs to be resituated and recognized as merely a tactic embedded within the broader concept of cognitive warfare.[6] The article concludes with an assessment of what this means for NATO and Allied Nations as they navigate the ever-evolving threat landscape.

From Disinformation to Manipulation

To understand the effects in the cognitive dimension—rather than the mechanisms or tools used to deliver them—we first need to appreciate identity, which shapes how we perceive ourselves, whom we trust, and how we interpret the world. As humans, we will disrupt, fight, destroy our own lives, and even die to defend our sense of identity, because identity is not just a belief—it defines the reality we see around us.[7] When we perceive that our identities—as parents, citizens, people of faith, immigrants, men, women, or any other attachment—are under threat, we often respond with instinctive emotions. We get angry; we become fearful; we act out our shame, pride, and resentment on others.[8] And because identity anchors how we see ourselves and interpret our lives, the reactions tied to it can override our sense of rationality.

Studies consistently demonstrate that emotional and identity alignment matter more to individuals than objective truth.[9] In fact, a robust body of cognitive science research indicates that humans are predisposed to care more about whether information confirms their preexisting identities and worldviews than its factual accuracy.[10] Put differently, we are far more likely to accept information that reinforces our existing beliefs and reject information that challenges them. This is why we line up in droves for the convenient lie and dismiss the inconvenient truth.

Identity as the Centre of Gravity

Definitions of identity vary depending upon the theoretical approach; however, practitioners have described it as both an internal self-concept and a social construct. For our purposes, identity will be defined as the dynamic organization of beliefs and experiences that shape how

[6] IBM leverages multiple tools—such as narratives, disinformation, propaganda, social media algorithms, AI, etc.—to achieve effects. It sits alongside other approaches, including psychological pressure and intimidation, information environment seeding, and direct neurocognitive manipulation.
[7] Anna Abraham, "How Social Dynamics Shape Our Understanding of Reality," in *Neuroscience in Intercultural Contexts*, 75–88 (New York: Springer, 2015).
[8] Dominic Packer and Jay J. Van Bavel, "The Dynamic Nature of Identity: From the Brain to Behavior," in *Psychology of Change*, 239–59 (Hove: Psychology Press, 2014).
[9] Chris Wang, Michael J. Platow, and Eryn J. Newman, "There Is an 'I' in Truth: How Salient Identities Shape Dynamic Perceptions of Truth," *European Journal of Social Psychology* 53, no. 2 (2023): 383–400.
[10] Dan M. Kahan, "Misconceptions, Misinformation, and the Logic of Identity-Protective Cognition," Yale Law School, Cultural Cognition Project Working Paper No. 164 (2017); Keith M. Bellizzi, "Cognitive Biases and Brain Biology Help Explain Why Facts Don't Change Minds," *The Conversation*, July 18, 2022.

individuals perceive themselves, as well as the meaning derived from group memberships and social recognition.[11]

As a starting point, a significant part of identity is rooted in belonging.[12] Social identity theory and modern neuroscience both suggest that the brain's deep-seated wiring for attachment and group affiliation are central to human survival.[13] Narratives, alongside ritual and shared practices, serve as one of the primary mechanisms for transmitting these attachments, reinforcing who we are and where we feel we belong.[14] Yuval Noah Harari, the author of the book *Sapiens*, argues that "Storytelling is our superpower. We are the only species with the ability to use language—not just to describe things we can see, taste, and touch, but also to invent stories about things that don't exist."[15]

If we break the world's literature, art, music, political propaganda, and advertising into their most basic forms, we will find stories rooted in identity and belonging—the hero's journey to triumph, falling in love, the rebel overthrow of a colonial overlord, fitting in, and finding meaning in our trials and tribulations.

In this context, group identity plays a formidable, primary role in shaping perception and behavior,[16] due to our neurological predisposition to form in-groups and out-groups,[17] rapidly categorize the social world,[18] and fiercely defend our affiliations.[19] However, humans do not process information about social groups primarily through rational evaluation. Instead, these judgments are often emotional and unconscious, shaped by mental shortcuts and predictive processes that favor efficiency over accuracy.[20] This reliance on heuristics and affective cues[21] reinforces stereotypes, biases, and preexisting beliefs, making social group perceptions both

---

[11] Henri Tajfel, "Social Identity and Intergroup Behavior," *Social Science Information* 13, no. 2 (1974): 65–93; Erik H. Erikson, *Identity: Youth and Crisis* (New York: Norton, 1968); Castells, Manuel Castells, *The Power of Identity*, 2nd ed. (Malden, MA: Wiley-Blackwell, 2010).
[12] Roy F. Baumeister and Mark R. Leary, "The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation," *Psychological Bulletin* 117, no. 3 (1995): 497–529, https://doi.org/10.1037/0033-2909.117.3.497.
[13] Matthew D. Lieberman, *Social: Why Our Brains Are Wired to Connect* (New York: Crown, 2013).
[14] Ruth Feldman, "The Neurobiology of Human Attachments," *Trends in Cognitive Sciences* 21, no. 2 (2017): 80–99.
[15] Carmine Gallo, "The Power of Storytellers to Shape Our World," *Forbes*, March 17, 2024.
[16] John C. Turner, Rupert J. Brown, and Henri Tajfel, "Social Comparison and Group Interest in Ingroup Favoritism," *European Journal of Social Psychology* 9, no. 2 (1979): 187–204.
[17] David M. Amodio, Bruce D. Bartholow, and Tiffany A. Ito, "Tracking the Dynamics of the Social Brain: ERP Approaches for Social Cognitive and Affective Neuroscience," *Social Cognitive and Affective Neuroscience* 9, no. 3 (2014): 385–93.
[18] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Macmillan, 2011).
[19] Mina Cikara and Jay J. Van Bavel, "The Neuroscience of Intergroup Relations: An Integrative Review," *Perspectives on Psychological Science* 9, no. 3 (2014): 245–74.
[20] Matthew D. Lieberman, "Social Cognitive Neuroscience: A Review of Core Processes," *Annual Review of Psychology* 58 (2007): 259–89.
[21] Affective cues are the signals—verbal, nonverbal, or contextual—that convey emotion or mood, such as tone of voice, facial expressions, body language, or emotionally charged language—essentially, how affect is communicated and perceived.

robust and resistant to change.[22] It also means that the notion that humans are rational actors is incorrect.

In reality, the core of our vulnerability in the information environment is largely born of what we already believe rather than the mere veracity of the information itself. And while disinformation can subtly—and effectively—impact this by exploiting our cognitive biases, it is most potent when it taps into identity and emotion.

If we accept the above, then it becomes clear that the heart of cognitive warfare[23] is less about disinformation or static narratives and more about identity-based influence (IBI)—the deliberate targeting of identities to shape perceptions and behaviors. When used malignantly, IBI becomes identity-based manipulation (IBM): the fire beneath the smoke of disinformation. Through this lens, myopically classifying all forms of influence and manipulation as disinformation is a fundamental and potentially catastrophic miscalculation. Again, it is akin to seeing smoke but ignoring the fire. Disinformation is the smoke; it is the fake story, distorted video, and misleading meme—alarming and visible, but not the real source of the danger. IBM is the fire; the deep, structural manipulation of social and individual identity capable of burning the foundations of shared trust if left unchecked.

This widespread exploitation of society is one of the most significant challenges facing our democracies, particularly because IBM is designed to keep us in a constant state of emotional activation, leaving little mental or emotional space for reflection. The more addicted we become—to our phones, to the latest TikTok trend, to the high we get from feelings of outrage and indignation—the less mental space we have to reflect on why we are so addicted in the first place. We mindlessly tap the like button, hit share, refresh our feeds, and jump to check our notifications, opting for a digital escape over tangible connections with those closest to us. Rarely do we stop to ask why we feel so angry, so isolated, so restless, and so exhausted—and even more rarely do we confront the possibility that the devices in our hands and the platforms at our fingertips are designed to create these feelings by producing addictive feel-good dopamine surges. The narratives that gain traction in this environment are those that short-circuit deliberation and inflame reaction for a reason. They reinforce the idea that the world is divided into “us” and “them,” that one’s in-group is under existential threat; that action must be immediate and unthinking, particularly if it involves a pre-established out-group.

---

[22] Lisa Feldman Barrett, *How Emotions Are Made: The Secret Life of the Brain* (London: Pan Macmillan, 2017); Raymond S. Nickerson, “Confirmation Bias: A Ubiquitous Phenomenon in Many Guises,” *Review of General Psychology* 2, no. 2 (1998): 175–220; Karl Friston, “The Free-Energy Principle: A Unified Brain Theory?” *Nature Reviews Neuroscience* 11, no. 2 (2010): 127–38.

[23] This article specifically focuses on the human factors aspect of cognitive warfare; however, there is ample research suggesting that the future of cognitive warfare will also include things like brain-computer interfaces (BCIs), direct-to-brain manipulation, and cognitive hijacking. While extremely relevant, touching upon these other aspects of cognitive warfare are beyond the scope of this paper. Suffice it to say that the space is rapidly evolving.

Addressing this threat necessitates a fundamental re-evaluation of how democracies approach information security and the information environment, more broadly. It is no longer sufficient to assume that simply telling the truth or appealing to logic will win out. While provocative to say, the reality is that the truth in and of itself does not matter—not in determining whether people accept information as "true" or "good", and certainly not in motivating them to act. This is one of the critical miscalculations governments continue to make. They assume that by communicating neutral, accurate facts and "truth-telling," populations will automatically feel reassured or persuaded and, critically, be motivated to question, think about, or change their behavior or beliefs. However, facts do not generate meaning on their own. The reality is that influence and action depend on whether information resonates with people's identities, emotions, and sense of belonging.

As a result, the real contest in our information-saturated world is over affect, meaning, and emotional resonance. Societies vulnerable to IBM are not merely those inundated with disinformation; they are those in which individuals already feel unheard, unseen, and under siege. Malicious actors merely exacerbate these preexisting conditions; they do not create them from scratch.

The challenge for democracies is not to abandon facts, but to recognize that they must be conveyed in ways that connect to people's self-interest, something tightly linked to identity. Messages that fail to demonstrate why an issue matters to people's daily lives or their inner sense of self risk falling flat, regardless of their accuracy. The most powerful narratives are those that tell audiences not just what is factual, but why the facts matter to their families, communities, and futures. Achieving this requires far more than simply disseminating neutral data. It demands a deeper understanding of how our brains receive and process information, an appreciation for the structures comprising society, and the humility to look in the mirror to ensure our words and deeds are aligned.

Narratives and Disinformation as Tools and Tactics within IBM

Within the Alliance, aspects of this understanding already exist, as evidenced by the behavior-centric approach outlined in NATO doctrine.[24] As part of this, narratives remain one of the most frequently invoked tools for understanding and countering influence based on the understanding that stories play a crucial role in how individuals perceive the world. Thus, narratives are an effective way to reinforce cohesion or counter adversarial messaging.[25] However, narratives in isolation are insufficient. Without resonance with identity, stories remain just that—stories. Their power comes not from their structure, but from how they activate belonging, meaning, and emotion.

[24] Civil-Military Centre of Excellence, *CIMIC COE Handbook*, n.d.
[25] Dan P. McAdams, "'First We Invented Stories, Then They Changed Us': The Evolution of Narrative Identity," *Evolutionary Studies in Imaginative Culture* 3, no. 1 (2019): 1–18.

For this reason, a growing body of scholarship critiques the narrative-centric lens, warning that it obscures the deeper psychological, emotional, and neurocognitive processes at play. [26] [27] Narrative analysis often privileges *what is being said*—the story itself—over *how influence works*.[28] From a systems theory approach, narratives are not endpoints but mechanisms within a broader ecology of influence.[29] As such, NATO's fixation on narrative risks missing the true driver of vulnerability, which is identity-based manipulation (IBM).

Despite criticism, for NATO and its Allies, discarding the terms "narrative" or "disinformation" outright would be a mistake, because they serve an important role. The purpose of this paper is not to stop us from using them but to push for a more thought-through conception of what they mean. Narratives are not inherently vague or useless, and disinformation remains a serious threat. Yet both operate as tactics within a broader ecosystem of identity-based influence (IBI). And when employed by adversaries to exploit identity divisions, these tactics move into the realm of identity-based manipulation (IBM). This distinction must be better understood if governments hope to be effective.

While there is debate to be had, a narrative becomes dangerous only when it resonates with identity, mobilizing emotional or physical reactions. Similarly, disinformation can be disruptive on its own, but it becomes strategically dangerous when combined with rhetoric provoking targeted emotions and behaviors.[30] Recognizing this distinction is crucial to any productive conversation about cognitive warfare. NATO and Allied nations cannot continue with a futile "whack-a-mole" approach, debunking falsehoods or assuming that counter-narratives are the leading solution. The real challenge is understanding how adversaries combine rhetoric, narratives, and disinformation with EDTs to create identity-based cognitive effects at scale.

Following the June 2023 riots in France, Kremlin-linked social media accounts flooded the information space with footage of the unrest, deliberately framed to fuel anti-immigrant and anti-government sentiment—issues deeply bound to identity. The content itself was genuine; it was not disinformation. Yet its emotional framing and algorithmic amplification manufactured division. Similar dynamics played out during COVID-19 in Africa, when manipulated vaccine information tapped into colonial grievances rooted in the West's historic use of medical

[26] Ibid.; Robert C. Rowland, "On Limitations of the Narrative Paradigm: Three Issues," 85–96; William G. Kirkwood, "Narrative and the Rhetoric of Possibility," *Communication Monographs* 59, no. 1 (1992): 30–47.
[27] William G. Kirkwood, "Narrative and the Rhetoric of Possibility," 30–47.
[28] Cigdem Esin, "Narrative Analysis Approaches," in *Qualitative Research Methods in Psychology: Combining Core Approaches*, 92–117 (2011).
[29] Steven R. Corman, "Understanding the Role of Narrative in Extremist Strategic Communication," in *Countering Violent Extremism: Scientific Methods and Strategies*, 47–65 (Washington, DC: NSI, Inc., 2013).
[30] Marilynn B. Brewer and Wendi Gardner, "Who Is This 'We'? Levels of Collective Identity and Self Representations," *Journal of Personality and Social Psychology* 71, no. 1 (1996): 83–93.

experimentation.[31] Here again, the message resonated not because it was wholly false, but because it connected with identity-based wounds and mistrust.

Moreover, during the 2020 U.S. election, narratives and rhetoric about "voter fraud" gained traction not because of wholly fabricated evidence but because they resonated with deep-rooted anxieties about demographic change, political power, and cultural belonging.[32] Researchers found that much of the information used to support the "stop the steal" narrative came from selectively edited videos, exaggerated accounts, and emotionally charged anecdotes targeting communities already primed for mistrust.[33] In essence, the January 6th attack on the U.S. Capitol was more about identity than it was about disinformation. It was less about choosing between truth and lies and more about people's deep-seated anger at having to question the validity and security of the election in the first place. The existence of doubt was at the heart of the betrayal.

People did not storm the Capitol building wholly because of false narratives; they acted after years of feeling unseen, unheard, and unsupported. The real force behind that day was not whether the election was objectively stolen, but what it meant for people to feel that their country no longer represented their identities and their voices. At the end of the day, the truth of the election was immaterial to how the "stop the steal" narrative made people *feel*. Citizens do not participate in an attempted coup because of disinformation alone—they participate because of the meaning they make of that information and what it says about their nation, their place within it, and their identity as citizens.

Technology as an Accelerator

The above examples underscore the importance that any discussion of IBM must also consider the increasing role played by technology. Our evolving yet ubiquitous digital landscape is certainly not the origin of IBM; however, it has profoundly transformed its reach, resonance, and impact. What once required mass movements, lengthy timelines, and costly propaganda planning can now be achieved at scale with remarkable precision and affordability. Moreover, much of this technology is intentionally layered with algorithms, designed to maximize our attention and engagement by structurally rewarding outrage, grievance, and division. What makes us angry keeps us watching and participating for longer, and with that comes outsized profits.

[31] Lynsey Chutel and Max Fisher, "The Next Challenge to Vaccinating Africa: Overcoming Skepticism," *New York Times*, December 1, 2021.
[32] Tye Rush, Chelsea Jones, Michael Herndon, et al., "Catalysts of Insurrection: How White Racial Antipathy Influenced Beliefs of Voter Fraud and Support for the January 6 Insurrection," *Journal of Race, Ethnicity, and Politics* (2025): 1–21.
[33] Hana Matatov, Mor Naaman, and Ofra Amir, "Stop the [Image] Steal: The Role and Dynamics of Visual Content in the 2020 US Election Misinformation Campaign," *Proceedings of the ACM on Human-Computer Interaction* 6, no. CSCW2 (2022): 1–24.

The sheer scale and timing of our engagement compound this dynamic. On average, people globally spend three hours and 43 minutes on their phones each day,[34] a figure that rises to six hours and 38 minutes when all screens are taken into account.[35] Put differently, nearly a quarter of our waking hours are spent on phones, and over 40 per cent are spent in front of screens.

Knowing this, the big question we need to ask ourselves is, when we are absorbed in technology—in our tablets, phones, and laptops— "Who are we giving our time to?" Do we even know? Moreover, who is on the other end of the information and rhetoric we receive when we are mindlessly scrolling? Who is behind the TikTok videos, the viral memes, the "news" articles? Who is paying the influencers we follow—and what about the influencers our children follow? What benefits do platform providers, corporations, and even malicious actors derive from the algorithms directing us to specific content, news feeds, and products?

The systems supporting this ecosystem are designed to ensure that content provoking identity-based reactions is pushed to the top of our social media and news feeds, creating an environment where manipulative and rhetoric-laden narratives thrive not because they are true, but because they are emotionally charged, making us more likely to give them our time and attention. The genius behind it all is that most of us spend hours on our phones, believing we are thinking for ourselves—not realizing that we are being intentionally fed manipulated content via addictive platforms engineered to direct our behavior. Whose thoughts are we having when we are reading the latest emotionally charged headline or Tweet? Do we even know? More importantly, do we even care?

These questions should not be mistaken for shallow, existential musings—they have real-world geopolitical consequences that create tangible strategic asymmetries within our nations. Adversaries can exploit technology to rapidly fracture democracies at minimal cost. But democracies—bound by their own ethical, legal, and normative constraints—struggle to respond with equal agility and emotional resonance. As a result, the cognitive battlespace does not need to be forced upon us because we happily carry one of its primary weapons in our pockets, open it dozens of times a day, and give away our most precious resource—our attention—without realizing it.

Why We Fail to Recognize the Threat

Many of us understand these ideas at a macro level; however, the challenge is that, writ large, the human brain is not particularly adept at recognizing our individual susceptibility to IBM, particularly when technology is involved. Most people assume they are rational, thinking human beings who base their decisions primarily on logic and intellect: "*They* are vulnerable; I'm not. *I* would recognize if I were being manipulated."

---

[34] Christoph Pieh, Elke Humer, Andreas Hoenigl, et al., "Smartphone Screen Time Reduction Improves Mental Health: A Randomized Controlled Trial," *BMC Medicine* 23, no. 1 (2025): 107.
[35] Simon Kemp, "2024 Global Overview Report," Data Reportal, 2024.

But this could not be farther from the truth.

Neuroscientist Lisa Feldman Barrett explains in *How Emotions are Made* that "people are not rational actors."[36] We like to believe we make decisions by "weighing pros and cons before deciding how to act, but the structure of your cortex makes this an implausible fiction."[37] Rational analysis is energy-intensive, while responding emotionally is faster and "cheaper". As a result, we often default to emotions without realising it. Barrett argues that "you feel what your brain believes", meaning no decision is ever entirely free of emotion.

Our brains also work through prediction, using past experiences to dictate how we feel—and often act—in the present. This is why identity and belonging are so powerful: they are innately tied to emotional patterns that can be easily triggered. A single image or message that evokes pride, grievance, or fear can set off physical reactions—an elevated heartbeat, tightness in the chest, restlessness—that feel tangible and urgent, even if the trigger is manufactured.[38]

For communities with histories of war, trauma, poverty, or real or perceived exclusion from mainstream society,[39] these patterns are even stronger. Information that taps into such lived or inherited experiences will provoke bigger emotions because the brain is primed to expect them.[40] This is the essence of how manipulation works: it exploits not just what we think, but how our bodies and brains predict we will *feel*[41] about certain emotions, spurring us to behave responsively—running from shame, burying pain, numbing regret, or seeking to make feelings of *schadenfreude* or genuine joy last a little longer.

Case Studies: Manipulation in Practice

One of the key challenges in this area is effectively demonstrating how scientific principles and theories can be applied in practical settings. It is one thing to debate the role of narratives, rhetoric, and identity in the abstract; it is another to observe how they are deliberately fused with technology to produce real-world effects.

---

[36] Lisa Feldman Barrett, *How Emotions Are Made: The Secret Life of the Brain*.
[37] Ibid.
[38] Ibid.
[39] This is an important point. Social psychologists (Baumeister & Leary, 1995; Eisenberger, Lieberman, & Williams, 2003) have demonstrated that humans possess a fundamental need to belong, such that exclusion activates the same neural pathways as physical pain. Even when the rejection is only perceived, it heightens sensitivity to group belonging cues, making individuals more vulnerable to manipulation and identity-based appeals.
[40] While this paper does not touch upon the impact of generational trauma on the brain's predisposition to predict based on past behavior, a robust body of science (Kellermann, 2001; Yehuda, 2016 Williams & Friston, 2021) points to the ability of generational trauma to embed heightened sensitivity to threats and vulnerability to manipulation in both biological and cultural memory—thereby, impacting how individuals react to stimuli in the present.
[41] How we feel about having specific emotions can be linked to affect, which may involve uncomfortable physiological bodily sensations (i.e. increased heart rate, elevated cortisol levels, upset stomach) that we seek to quell through positive or negative behavior adjustments (i.e. meditation to decrease heartrate, deep breathing to drop cortisol, etc.).

According to Jon Roozenbeek, between 2014 and 2017, the Kremlin used "Novorossiya"—meaning "New Russia"—narratives in Ukraine to "conjure up feelings of a restored Russian empire and righting the historical 'wrong' of assigning Russian lands under Ukrainian jurisdiction."[42] This approach was designed to foster a sense of cultural belonging that resonated with Ukrainians in the Donbas region, priming the ground for physical invasion. Analyzing over 85,000 articles from local and regional media outlets, Roozenbeek found that more than a third of the content was devoted not to reporting events, but to shaping identity by invoking post–World War II grievances and portraying the Ukrainian government as an out-group of "neo-Nazis."[43] Although the campaign ultimately fell short, the Kremlin's broader approach to influence and manipulation is not ad hoc; it is codified in its New Generation Warfare (Война нового поколения) concept and embedded throughout its strategic documents, including the 2014 Military Doctrine, the 2021 Information Security Doctrine, and the 2021 National Security Strategy.[44] Across these texts, the Kremlin emphasizes "information confrontation" (информационное противоборство)[45] as a strategic instrument designed to weaken cohesion, erode trust, and sap the will of societies to resist.

The Chinese Communist Party's (CCP) push for "informationization" and "intelligentization" reflects a similarly systematic approach.[46] According to the country's 2020 Science of Military Strategy and the "Three Warfares" doctrine, China's People's Liberation Army (PLA) envisions a battlespace in which influence can be personalized at scale, tailoring messages to reshape adversary perceptions in real time by integrating AI; psychological warfare; and command and control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).[47] Unlike earlier influence operations that broadcast one-size-fits-all propaganda, this model utilizes data-driven precision to engage individuals based on their unique identities, vulnerabilities, and worldviews.

While Russia and China represent state-level approaches, violent extremist organizations (VEOs) demonstrate the same blending of identity and technology at a smaller scale. For example, the

---

[42] Jon Roozenbeek, "The Failure of Russian Propaganda," University of Cambridge, 2021.
[43] Jon Roozenbeek, "Media and Identity in Wartime Donbas, 2014–2017" (PhD diss., University of Cambridge, 2019).
[44] Çağatay Mehmet Güler and Anna Shakirova, "Deciphering Russia's 2021 National Security Strategy Document," SETA, 2021; Julian Cooper, "Russia's Updated National Security Strategy," NATO Defense College, 2021; European Parliament, "Russia's National Security Strategy and Military Doctrine and Their Implications for the EU," Directorate-General for External Policies, 2017.
[45] The 2016 Doctrine of Information Security of the Russian Federation: "«Информационное противоборство в условиях межгосударственных конфликтов может осуществляться в целях оказания давления на противника, дестабилизации обстановки внутри государства, а также подрыва его суверенитета и территориальной целостности." Translates to: *"Information confrontation in the context of interstate conflicts may be conducted in order to exert pressure on an adversary, destabilize the internal situation in the state, and undermine its sovereignty and territorial integrity.*
[46] Josh Baughman, "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield," *Cyber Defense Review* 9 (2024): 29–36.
[47] Shannon Vaugh, "AI Dependence and Political Blind Spots Undermine Beijing's War Strategy," FPRI, March 2025.

Islamic State of Iraq and the Levant (ISIL) spread more than ideology—they offered belonging, heroism, and purpose to isolated and disaffected youth.[48] On social media and in gaming environments, ISIL's messaging frequently emphasized inclusion and brotherhood, ideas designed to surpass rational arguments by leaning on emotional and identity-based influence.[49] As a result, ISIL's success was not simply based on its ability to spread ideology but its ability to offer identity and an "in-group" community to individuals who, in many cases, felt excluded elsewhere.

The Core Lesson for NATO

NATO is undergoing its most significant transformation since the end of the Cold War. The NATO Warfighting Capstone Concept (NWCC) and Allied Command Transformation's (ACT) work on cognitive warfare and multi-domain operations (MDO) underscore the Alliance's need to adapt to emerging disruptive technologies (EDTs) and adversaries who contest the cognitive dimension with the same intensity as the physical domain. This transformation is designed to ensure NATO remains prepared to deter and, if necessary, fight and win in an increasingly complex and unpredictable security environment.

Meeting this challenge requires NATO to recalibrate its approach to the cognitive dimension by developing a deeper understanding of how cognitive warfare functions. If the Alliance accepts that cognitive warfare is the fight, and the cognitive dimension is contested by adversaries deliberately targeting societal foundations, then identity-based manipulation (IBM) must be recognized as a primary approach. Doctrinally, NATO must view IBM as a cross-cutting threat, aligning StratCom tools, training, and resources to counter it—and, when consistent with NATO's legal and ethical principles, generate effects against adversarial audiences.

Recent examples reveal a consistent dynamic: narratives and disinformation are not threats in themselves; they are accelerants. The fuel is identity. Until NATO recognizes IBM as the true center of gravity, efforts will remain reactive and incomplete.

This recognition demands a shift in posture across three levels:

1. **Analytically -** NATO must treat narratives and disinformation as tactical elements within IBM, not as standalone problems.

[48] Jonathan Landay and Ted Hesson, "Investigators Seek Clues to New Orleans Attacker's Path to Radicalization," *Reuters*, January 3, 2025; Juan Zarate, "The Future of Counterterrorism Strategy," *Hampton Roads International Security Quarterly* (2017): 32–43.
[49] Khalil Sardarnia and Rasoul Safizadeh, "The Internet and Its Potentials for Networking and Identity Seeking: A Study on ISIS," *Terrorism and Political Violence* 31, no. 6 (2019): 1266–83.

2. **Operationally -** NATO must build the capacity to analyze how adversaries combine these tactics with rhetoric, algorithms, and emerging technologies to generate cognitive effects.
3. **Strategically -** NATO must prioritize resilience by addressing vulnerabilities in identity, belonging, and trust since these are the primary levers adversaries exploit.

To accomplish this shift, NATO should consider the following:

1. **Establish a Taxonomy for Cognitive Warfare:** NATO urgently needs to develop a formal taxonomy for cognitive warfare that clarifies the distinctions between the fight, the approaches employed by adversaries, the tactics through which they operate, the tools enabling execution, and the corresponding layered effects. Currently, Allied discussions often conflate these categories, treating disinformation as the fight itself rather than a tactic embedded within broader approaches. This lack of conceptual precision risks misdirecting resources and leaving gaps in training, doctrine, and operational design, and makes coordination across nations difficult.
2. **Adapt Exercises, Wargames, and Training to Simulate the Dynamics of IBM:** Once conceptual clarity is established, NATO must translate this clarity into practice. It is not enough to test responses to cyberattacks or conventional deception; NATO must prepare to counter adversaries who combine behavioral science, identity manipulation, and technological disruption without crossing national borders. To stress-test resilience under cognitive pressure, NATO should incorporate identity-based scenarios into exercises and training—using relevant, fit-for-purpose technology—ensuring commanders, planners, and operators are as prepared to counter attacks on human affect, belonging, and grievance as they are to contest terrain, logistics, or air superiority.
3. **Expand Counter-Disinformation Strategies into a Broader Agenda of Countering IBM:** NATO's counter-disinformation efforts, while important, remain insufficient. Fact-checking, media literacy, and counter-messaging cannot match adversaries using technology-fuelled IBM to shape attitudes, perceptions, and behaviors across national borders.[50] Adopting a broader agenda means moving beyond "debunking lies" and instead contesting IBM directly. This requires investment in public-private partnerships (PPPs) with technology providers, enhancing collaboration with academia and civil society, and building interdisciplinary expertise that captures both human factors and technical skills.

[50] This paper distinguishes between IBI and IBM, noting that IBM is typically employed against NATO and Allied nations by malign actors. However, it does not assess whether NATO's own activities in the cognitive dimension fall under either category. Clarifying this should be part of the proposed taxonomy and further developed through efforts to ensure that NATO and member-state ethical frameworks explicitly account for the central role of identity in the cognitive dimension.

4. **Strengthen Societal Resilience Against Identity-Based Manipulation:** Resilience cannot be defined only in terms of infrastructure, logistics, and continuity of government because a society cannot be truly resilient if its people are psychologically vulnerable to manipulation. IBM explicitly targets the foundations of societal resilience, which rests on the ability of populations to withstand, adapt to and recover from shocks and manipulation while maintaining social cohesion and trust.

   As a result, NATO's resilience pillar must expand to include societal resilience to cognitive warfare, requiring increased investment in education, civic engagement, and national narratives that, in their most basic form, remind people of the reasons why they need each other. Military Public Affairs (MilPA) has a key role to play here, not simply by delivering facts but by framing communication in ways that align with how the human brain processes information. Communication is never neutral. The task is to ensure that communicators recognize this reality and are equipped to engage society in ways that acknowledge the influence of emotions, identity, cognitive biases, and heuristics on human behavior. Without such a psychological foundation, resilience will remain elusive, and no amount of fact-checking, "truth-telling," or debunking will suffice.

5. **Maintain a Focus on Human Factors and Ethical Safeguards:** At the core of these efforts lies the human mind, which is both the target and the weapon of cognitive warfare. IBM exploits cognition by delivering tailored information designed to elicit predictable responses and sow unrest. Once influenced, individuals do not remain passive; they become active carriers of manipulation, amplifying and transmitting the influence on others. Therefore, ensuring humans remain in the loop—both offensively and defensively—is not just a safeguard for effectiveness but a safeguard for legitimacy. The solution cannot just be another digital or AI-based tool. We must ensure that our fascination with the evolving technology landscape does not overshadow our understanding that the human brain is the battlespace.

Conclusion: Building Resilience in the Cognitive Dimension

Responding to cognitive warfare demands more than technical solutions or content moderation because our humanness is at the core of our susceptibility to influence and manipulation. This requires building societies that understand that the problem is bigger than just disinformation; we must teach individuals to recognize when information is false and how to discern when their emotions are being manipulated or their identities are being exploited. We need to ensure that people understand how IBM feels in the moment, underscoring why it is such an effective method of influence in the first place. Solely focusing on countering disinformation or fostering information literacy is not enough. Our approach must be far more holistic.

To do this, we need to ask ourselves intentional questions, designed to prompt reflection on how our identities and past experiences shape our responses to daily information:

"What does it feel like when the values my nation claims to uphold no longer reflect my personal values?"

"Is the anger I feel at specific headlines or topics truly my own, or have I been taught to feel it?"

"Do I find satisfaction in outrage?"

"Have I lost connection with those closest to me?"

"Why am I so enraged by certain groups of people?"

"Do I believe I have the power to shape my society, or have I surrendered that belief to forces beyond my control?"

As anyone who has ever worked in the development or education field will tell you, building societal resilience or fostering social norms change is neither quick nor straightforward. It is not unlike the arduous, slow process of personal growth, requiring time, repetition, and a sustained commitment to self-awareness. In a world focused on quick rewards, it is decidedly unsexy.

And while truth, honesty, and factual information still matter, understanding how our identities can be rapidly and systematically manipulated—whether by factual or false information—matters even more.

Until individuals and governments shift their focus from the "smoke" of disinformation to recognizing IBM as the fire growing within our societies, their capacity to build the capabilities to deter, respond to, and recover from malign manipulation will remain limited. True information literacy requires more than fact-checking or truth-telling; it demands an internal reckoning with the truth of why we are so vulnerable in the first place. Simply acknowledging that malign actors are using information to manipulate our identities is insufficient. We must also confront the uncomfortable reality that sometimes, manipulated information serves as a reassuring salve for the bumps and bruises of our lives, born of heartache and historical anger or simply the realisation that the world is not as we believe it should be—or perhaps that *we* are not as we should be. When we feel indignant and stimulated by outrage, a part of us feels seen, and feeling seen often matters more to us than truth. After all, as humans, we are nothing if not slightly superficial and fallible. It is not surprising that the same can be said of the systems, leaders, and governments we create.

If we are looking for a solution to the scourge of IBM, the reality—for better or worse—is that we often need to look no further than ourselves. That is the real work.

Thankfully, mirrors are never too far away—if only we were strong enough to look into them from time to time.

References

Abraham, Anna. 2015. “How Social Dynamics Shape Our Understanding of Reality.” In *Neuroscience in Intercultural Contexts*, 75–88. New York: Springer.

Ahmed, Sara. 2004. *The Cultural Politics of Emotion*. Edinburgh: Edinburgh University Press.

Amodio, David M., Bruce D. Bartholow, and Tiffany A. Ito. 2014. “Tracking the Dynamics of the Social Brain: ERP Approaches for Social Cognitive and Affective Neuroscience.” *Social Cognitive and Affective Neuroscience* 9 (3): 385–93.

Barnes, Julian. 2025. “Documents Examined by Researchers Show How One Company in China Has Collected Data on Members of Congress and Other Influential Americans.” *The New York Times*, January 28, 2025.

Barrett, Lisa Feldman. 2017. *How Emotions Are Made: The Secret Life of the Brain*. London: Pan Macmillan.

Bar-Tal, Daniel. 2013. *Intractable Conflicts: Socio-Psychological Foundations and Dynamics*. Cambridge: Cambridge University Press.

Baughman, Josh. 2024. “The Path to China’s Intelligentized Warfare: Converging on the Metaverse Battlefield.” *The Cyber Defense Review* 9: 29–36.

Baumeister, Roy F., and Mark R. Leary. 1995. “The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation.” *Psychological Bulletin* 117 (3): 497–529. https://doi.org/10.1037/0033-2909.117.3.497.

Bellizzi, Keith M. 2022. “Cognitive Biases and Brain Biology Help Explain Why Facts Don’t Change Minds.” *The Conversation*, July 18, 2022.

Brewer, Marilynn B., and Wendi Gardner. 1996. “Who Is This ‘We’? Levels of Collective Identity and Self Representations.” *Journal of Personality and Social Psychology* 71 (1): 83–93.

Castells, Manuel. 2010. *The Power of Identity*. 2nd ed. Malden, MA: Wiley-Blackwell.

Chutel, Lynsey, and Max Fisher. 2021. “The Next Challenge to Vaccinating Africa: Overcoming Skepticism.” *The New York Times*, December 1, 2021. https://www.nytimes.com/2021/12/01/world/africa/coranavirus-vaccine-hesitancy-africa.html.

Cikara, Mina, and Jay J. Van Bavel. 2014. “The Neuroscience of Intergroup Relations: An Integrative Review.” *Perspectives on Psychological Science* 9 (3): 245–74.

Civil-Military Centre of Excellence. n.d. *CIMIC COE Handbook*.

Cooper, Julian. 2021. “Russia’s Updated National Security Strategy.” NATO Defense College. https://www.ndc.nato.int/russias-updated-national-security-strategy/.

Corman, Steven R. 2013. “Understanding the Role of Narrative in Extremist Strategic Communication.” In *Countering Violent Extremism: Scientific Methods and Strategies*, 47–65. Washington, DC: NSI, Inc.

Erikson, Erik H. 1968. *Identity: Youth and Crisis*. New York: Norton.

Esin, Cigdem. 2011. “Narrative Analysis Approaches.” In *Qualitative Research Methods in Psychology: Combining Core Approaches*, 92–117.

EU DisinfoLab. 2022. “The Disinformation Landscape across Europe.” https://www.disinfo.eu/.

European Parliament. 2017. “Russia’s National Security Strategy and Military Doctrine and Their Implications for the EU.” Directorate-General for External Policies. https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA%282017%29578016_EN.pdf.

Feldman, Ruth. 2017. “The Neurobiology of Human Attachments.” *Trends in Cognitive Sciences* 21 (2): 80–99.

Friston, Karl. 2010. “The Free-Energy Principle: A Unified Brain Theory?” *Nature Reviews Neuroscience* 11 (2): 127–38.

Gallo, Carmine. 2024. “The Power of Storytellers to Shape Our World.” *Forbes*, March 17, 2024. https://www.forbes.com/sites/carminegallo/2024/03/17/the-power-of-storytellers-to-shape-our-world/.

Güler, Çağatay Mehmet, and Anna Shakirova. 2021. “Deciphering Russia’s 2021 National Security Strategy Document.” SETA. https://www.setav.org/en/perspective-deciphering-russias-2021-national-security-strategy-document.

Helmus, Todd C., and Elizabeth Bodine-Baron. 2021. “Countering Truth Decay: Fighting Disinformation on COVID-19 and Beyond.” RAND Corporation. https://www.rand.org/pubs/perspectives/PEA1143-1.html.

Kahan, Dan M. 2017. “Misconceptions, Misinformation, and the Logic of Identity-Protective Cognition.” Yale Law School, Cultural Cognition Project Working Paper Series No. 164.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. New York: Macmillan.

Kemp, Simon. 2024. “2024 Global Overview Report.” Data Reportal. https://datareportal.com/reports/digital-2024-global-overview-report.

Kirkwood, William G. 1992. “Narrative and the Rhetoric of Possibility.” *Communication Monographs* 59 (1): 30–47. https://doi.org/10.1080/03637759209376245.

Landay, Jonathan, and Ted Hesson. 2025. “Investigators Seek Clues to New Orleans Attacker’s Path to Radicalization.” *Reuters*, January 3, 2025. https://www.reuters.com/world/us/investigators-seek-clues-new-orleans-attackers-path-radicalization-2025-01-03/.

Lieberman, Matthew D. 2007. “Social Cognitive Neuroscience: A Review of Core Processes.” *Annual Review of Psychology* 58 (1): 259–89.

Lieberman, Matthew D. 2013. *Social: Why Our Brains Are Wired to Connect*. New York: Crown.

Matatov, Hana, Mor Naaman, and Ofra Amir. 2022. “Stop the [Image] Steal: The Role and Dynamics of Visual Content in the 2020 U.S. Election Misinformation Campaign.” *Proceedings of the ACM on Human-Computer Interaction* 6 (CSCW2): 1–24.

McAdams, Dan P. 2019. “First we invented stories, then they changed us”: The evolution of narrative identity. *Evolutionary Studies in Imaginative Culture*, *3*(1), pp.1-18.

NATO Strategic Communications Centre of Excellence. 2019. “Robot Rolling the Red Carpet: The Rise of Social Media Bots.” https://stratcomcoe.org/publications/robot-rolling-the-red-carpet-the-rise-of-social-media-bots/71.

Nickerson, Raymond S. 1998. “Confirmation Bias: A Ubiquitous Phenomenon in Many Guises.” *Review of General Psychology* 2 (2): 175–220.

Packer, Dominic, and Jay J. Van Bavel. 2014. “The Dynamic Nature of Identity: From the Brain to Behavior.” In *Psychology of Change*, 239–59. Hove: Psychology Press.

Pieh, Christoph, Elke Humer, Andreas Hoenigl, et al. 2025. “Smartphone Screen Time Reduction Improves Mental Health: A Randomized Controlled Trial.” *BMC Medicine* 23 (1): 107.

Porter, Catherine. 2023. “A Fatal Shooting and a Hijab Ban: Two Faces of France’s Racial Divisions.” *The New York Times*, July 2, 2023. https://www.nytimes.com/2023/07/02/france-nahel-soccer-hijab.html.

Roozenbeek, Jon. 2019. “Media and Identity in Wartime Donbas, 2014–2017.” PhD diss., University of Cambridge.

Roozenbeek, Jon. 2021. “The Failure of Russian Propaganda.” University of Cambridge. https://www.cam.ac.uk/stories/donbaspropaganda.

Rowland, Robert C. 1989. “On Limitations of the Narrative Paradigm: Three Issues.” *Communication Quarterly* 37 (2): 85–96. https://doi.org/10.1080/01463378909385529.

Rush, Tye, Chelsea Jones, Michael Herndon, et al. 2025. “Catalysts of Insurrection: How White Racial Antipathy Influenced Beliefs of Voter Fraud and Support for the January 6 Insurrection.” *Journal of Race, Ethnicity, and Politics*, 1–21.

Sardarnia, Khalil, and Rasoul Safizadeh. 2019. “The Internet and Its Potentials for Networking and Identity Seeking: A Study on ISIS.” *Terrorism and Political Violence* 31 (6): 1266–83.

Stanford Internet Observatory. 2020. “Elections Integrity Partnership: The Long Fuse: Misinformation and the 2020 Election.” Stanford University. https://cyber.fsi.stanford.edu/io/news/long-fuse.

Tajfel, Henri. 1974. “Social Identity and Intergroup Behavior.” *Social Science Information* 13 (2): 65–93.

Turner, John C., Rupert J. Brown, and Henri Tajfel. 1979. “Social Comparison and Group Interest in Ingroup Favoritism.” *European Journal of Social Psychology* 9 (2): 187–204.

Vaugh, Shannon. 2025. “AI Dependence and Political Blind Spots Undermine Beijing’s War Strategy.” *FPRI*, March 2025. https://www.fpri.org/article/2025/03/ai-dependence-and-political-blind-spots-undermine-beijings-war-strategy/.

Wang, Chris, Michael J. Platow, and Eryn J. Newman. 2023. “There Is an ‘I’ in Truth: How Salient Identities Shape Dynamic Perceptions of Truth.” *European Journal of Social Psychology* 53 (2): 383–400.

Zarate, Juan. 2017. “The Future of Counterterrorism Strategy.” *Hampton Roads International Security Quarterly*: 32–43.

When the Private Tech Sector Disrupts the Defense Industry: What Is NATO's Strategy?

Dominika Kunertova

Introduction

NATO is only as strong as the defense industry's ability to support the Alliance's primary task of deterrence and defense. As allies underscored at the Hague summit in June, Russia's war on Ukraine has exposed the danger of years of post-Cold War reductions in armed forces and defense industrial capacity.[1] NATO Europe's attempts to reverse these trends since Russia's invasion have revealed the high per-unit costs of military equipment, as well as atomized supply chains.

At the same time, a new class of power broker–private tech companies–has disrupted the traditional military-industrial complex in the United States and become the main driver for defense innovation in the military.[2] Thanks to their private ownership of transnational communication and data control infrastructures, tech companies will see their geopolitical influence only grow.[3] These rapidly evolving power dynamics on the defense market and the changing balance of influence between governments and tech companies have important consequences for NATO's ability to maintain its technological competitiveness.

The combined pressure to innovate and simultaneously grow armed forces in size compelled NATO to launch several initiatives in the past few years to intensify defense industrial collaboration among its member countries. NATO's current efforts highlight the importance of both increasing defense production and maintaining technological edge. These two distinct objectives are not always necessarily aligned and require different toolkits. Given the ongoing structural changes in the defense sector, is NATO equipped to successfully navigate this twin challenge?

Towards the Alliance's Defense Industrial Strategy

A coordinated approach to defense industry is important for reasons that go beyond efficiency gains from reducing duplication costs.[4] Looking inward, such an alliance defense industrial

[1] U.S. Department of Defense, *State of Competition within the Defense Industrial Base* (Washington, DC: Office of the Under Secretary of Defense for Acquisition and Sustainment, February 2022).
[2] Audrey Kurth Cronin, "How Private Tech Companies Are Reshaping Great Power Competition" (Washington, DC: The Kissinger Center for Global Affairs, August 2023).
[3] Joscha Abels, "Private Infrastructure in Geopolitical Conflicts: The Case of Starlink and the War in Ukraine," *European Journal of International Relations* 30, no. 4 (2024): 842–66.
[4] Keith Hartley, "Defense Industrial Policy in a Military Alliance," *Journal of Peace Research* 43, no. 4 (2006): 473–89.

strategy contributes to forging a common threat picture and a shared appreciation of security risks among the Allies. Socializing national political and military leadership into new technologies, as well as new tech industry representatives into defense affairs, can help steer defense innovation in line with NATO's values and norms. The resulting greater level of mutual trust then enhances alliance cohesion.[5]

Looking outward, NATO's systematic work to gain strategic advantages from new technologies, signals resolve to maintain its technological edge. The Alliance's efforts to improve collective competency in new technologies, as well as increasing the production capacity in turn contributes to deterring external aggression and improving the defense posture. Laying the groundwork for principles of responsible innovation and use of new technologies allows NATO to shape emerging global technology governance.[6]

Despite the desirability of coordinated industrial activities, NATO does not have an official defense industrial *policy*.[7] This is because defense industrial policy–the ability to shape the industrial base and stimulate production–remains a national prerogative.[8] Although NATO leaders acknowledged the need for defense industrial cooperation for the first time at the NATO Chicago Summit in 2012, the resulting guideline document explicitly stated that NATO did not aim to develop defense industrial policy nor regulate national industrial production.[9] However, NATO does coordinate, guide, inform, and harmonize largely because of the Alliance's two strengths: strategic defense planning and standards development.[10]

The alliance membership indeed creates structural incentives for the Allies to integrate their defense industry into NATO networks. They can do so by reorienting exports, investments, and manufacturing, as well as implementing NATO standards to produce interoperable equipment.[11] In turn, NATO membership gives the countries access to know-how, procurement assistance, and current best practices.[12] Overall, thanks to being a member of NATO, national markets are regarded as safe for foreign investment opportunities.[13]

---

[5] Dominika Kunertova and Olivier Schmitt, "Assessing NATO's Cohesion: Methods and Implications," *International Politics* (published online November 2024).
[6] NATO, "Emerging and Disruptive Technologies," last updated June 25, 2025.
[7] NATO, "Summit Declaration on Defense Capabilities: Toward NATO Forces 2020," Press Release, May 20, 2012.
[8] Organization for Economic Co-operation and Development, "Industrial Policy," Policy Issue (accessed September 22, 2025).
[9] NATO, "Framework for NATO Industry Engagement," October 1, 2013, para. 5.
[10] Zoe Stanley-Lockman and Lena Trabucco, "'NATO's Role in Responsible AI Governance in Military Affairs,'" in *The Oxford Handbook of AI Governance*, ed. Justin B. Bullock et al., online ed. (Oxford: Oxford University Press, 2022).
[11] Lucie Béraud-Sudreau and Olivier Schmitt, "Alliance Politics and National Arms Industries: Creating Incentives for Small States?" *European Security* 33, no. 4 (2024): 711–31.
[12] Dominika Kunertova, "Europe's Military Drone Problem," in *De Gruyter Handbook on Drone Warfare*, ed. James Patton Rogers (Berlin and Boston: De Gruyter, 2024), 299–312
[13] Keith Rockwell, "Criticism of NATO Ignores Its Economic Benefit to the US," Wilson Center, March 29, 2024.

Since the 1960s, NATO has institutionalized long-standing relations with the traditional armaments industry through the Conference of National Armaments Directors (CNAD) and NATO Industrial Advisory Group (NIAG), as well as assisted with procurement contracts and defense logistics in the NATO Support and Procurement Agency (NSPA). NATO International Staff also helps the Allies identify opportunities for multinational capability development and follows them through High Visibility Projects.[14] NATO's more recent organizational addition, the Defense Industrial Production Board, makes recommendations on defense industrial planning and procurement to National Armaments Directors.[15]

The confluence of geopolitical competition and new technological advances highlights technological primacy as a condition for battlefield success. The 2022 NATO Strategic Concept committed its member countries to innovating and investing in new emerging and disruptive technologies.[16] Soon afterwards, NATO leaders set up the Defense Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund to build a transatlantic innovation ecosystem of defense tech companies, investors, and end-users. National leaders acknowledged that the difference in the timescale of innovation cycles between the commercial sector (months) and the military (years) can prevent the military from harnessing new technology and even create security liabilities. However, these two initiatives lacked a clear connection to procurement and integration challenges.[17]

NATO's three recent documents–Defense Production Action Plan (2023), NATO Industrial Capacity Expansion Pledge (2024), and Rapid Adoption Action Plan (2025)–are meant to correct that.[18] While the first two documents match industry with aggregated demand from across NATO countries, the Rapid Adoption Action Plan aims to accelerate the pace at which NATO and NATO member countries procure and integrate new technology products. NATO sets the timeline for their adoption to a maximum ceiling of 24 months, in line with priorities set in NATO's Defense Planning Process (NDPP). Together, these initiatives represent a sound alliance defense industrial strategy that helps the Allies to achieve a balanced mix of capabilities. There is just one catch: new power brokers in the defense sector.

Adapting to fast-paced technological changes poses additional challenges for the Alliance.[19] The growing geopolitical influence of private tech companies contrasts with NATO's long-established approach to its relations with defense industry and defense innovation. And in

[14] NATO, "Multinational Capability Cooperation," last updated July 30, 2025.
[15] NATO, "Defense Industrial Production Board (DIPB)," Factsheet, April 2024.
[16] NATO, "NATO 2022 Strategic Concept," June 29, 2022, paras. 5, 8, 13.
[17] Dominika Kunertova, "Embracing Drone Diversity: Five Challenges to Western Military Adaptation in Drone Warfare," Freeman Air and Space Institute, King's College London, Research Paper 29 (2025).
[18] NATO, "NATO's Role in Defense Industry Production," June 26, 2025; NATO, "NATO Industrial Capacity Expansion Pledge," July 10, 2024; NATO, "Summary of NATO's Rapid Adoption Action Plan," June 25, 2025.
[19] Stephen Herzog and Dominika Kunertova, "NATO and Emerging Technologies: The Alliance's Shifting Approach to Military Innovation," *Naval War College Review* 77, no. 2 (2024): 47–69.

contrast to the past, this technology is capability agnostic and privatized.[20] Importantly, while new technologies can address immediate capability shortfalls, they cannot replace some traditional platforms nor they can deliver some desired effects.[21] While NATO focused on specific platforms, capabilities, and partnerships with the traditional military-industrial complex, the current defense power brokers have inverted the innovation pyramid: militaries are importing technology primarily developed for the commercial sector.

New Power Brokers Disrupt the Defense Sector

While the industrialization of war defined the 20th century, the 21st century has witnessed the commercialization of war. In this ongoing quiet revolution, commercial technology is quickly finding its way onto the battlefield and blurring the line between civilian and military spheres. Importantly, the state no longer has a monopoly on military industry or defense innovation. The international context of strategic rivalry and the national context of market competition for frontier technologies have led a new wave of private tech companies to seek business opportunities in the defense sector. The so-called "cultural divide" or "ethical red line" between the Pentagon and Silicon Valley has definitely disappeared.[22]

The traditional military-industrial complex is being replaced with a nascent new private defense tech industry as the Pentagon's primary supplier of new technologies. While in the past, the military-industrial complex tightly controlled the defense procurement market, today the six technology startups dubbed "SHARPE", that is Shield AI, HawkEye 360, Anduril, Rebellion Defense, Palantir, and Epirus, dominate the defense tech sector.[23] Another notable private company SpaceX, in addition to covering nearly 80 percent of all space launches in the United States, also provides its space-based internet service Starlink from private individuals in remote areas to the Ukrainian soldiers fighting the invading Russian troops.[24]

The defense industrial landscape is experiencing fast structural changes. In less than a decade, market valuation of several of these tech companies surpasses that of traditional defense primes, such as Lockheed Martin, Northrop Grumman or General Dynamics.[25] New power brokers have attracted venture capital (VC) investments into the defense sector and open revolving doors

[20] Ibid, p. 9, 12.
[21] Angus Lapsley and Pierre Vandier, "Why NATO's Defense Planning Process Will Transform the Alliance for Decades to Come," Atlantic Council Issue Brief, March 31, 2025.
[22] Roberto Gonzalez, "How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex," Watson Institute for International and Public Affairs, Brown University, April 17, 2024.
[23] Chris Rogers et al., "SHARPE Focus: Emerging Growth Opportunities in Defense Industry," Harris Williams, August 3, 2022.
[24] Mitch Semanik and Patrick Crotty, "U.S. Private Space Launch Industry Is Out of This World," Office of Industry and Competitiveness Analysis, U.S. International Trade Commission, 2023.
[25] Jason Ma, "SpaceX and Palantir Now Have Bigger Valuations than Top Aerospace-Defense Stocks as the Military Eyes Transformation," *Fortune*, December 7, 2024.

between the private commercial and public government spheres.[26] Major VC companies investing in defense tech include Silent Ventures, Marque Ventures, Champion Hill Ventures, Shield Capital, HighVista Strategies, Sequoia Capital, Founders Fund, and influential Andreessen Horowitz.[27]

In Europe, too, VC investments in the defense sector were all-time high in 2024, particularly defense tech start-ups in Germany, the United Kingdom, and France. Their five-fold growth since 2018, reaching 1 billion USD, however, amounts to what U.S. defense tech company Anduril is able to raise for itself in one bidding. Despite this difference in scale, the new and buzzing defense, security, and resilience tech sector has received 10 percent of all VC funding in Europe.[28]

NATO has already set up the structures to engage with new defense industrial stakeholders. In addition to building a network of innovators, accelerators, and test centers through its DIANA organization, NATO invests into bringing new technological products to the desired readiness level. Once mature, NATO Task Force X can proceed with integrating them into the existing capability mix.[29]

Against the backdrop of this systemic approach, NATO has also gained a hands-on experience as an end-user. In just a few months, NATO's Allied Command Operations was able to purchase and integrate Palantir's AI-enabled warfighting platform called "Maven Smart System NATO" (MSS NATO) in the spring of 2025.[30] This acquisition is believed to enhance the alliance's ability to conduct intelligence fusion and targeting, battlespace awareness, and planning.

NATO is expected to adopt other novel warfighting capabilities across the Alliance in the near future. However, leveraging advantages from new technologies runs into several risks related to how these new power brokers operate. Three of them merit further discussion. First, the startup "move fast and break things" culture is an antipode to the institutional "stable and steady" approaches of a multilateral organization. Regardless of their patriotic statements, these private companies are primarily driven by profit and constrained by the dictate of growth cycles.[31] Their CEOs are oftentimes unaware of sociopolitical structures governing societies and their militaries. Privately owned newcomers to the defense sector have both limited public oversight and little operational military experience. Nevertheless, new defense tech companies are very vocal about

[26] Luisa Beltran, "War and Rising Nationalism Is Expected to Spur a Venture Capital Boom in a One-Time Silicon Valley Taboo Sector: Defense Tech," *Fortune*, July 22, 2024.
[27] Aria Alamalhodaei, "5 Investors Have High Hopes for Defense Tech amid Growing Venture Interest," *TechCrunch*, November 20, 2023.
[28] Anna Heim, "Defense and Resilience Tech Reached an All-Time High: 10% of All VC Funding in Europe," *TechCrunch*, February 12, 2025.
[29] NATO, "Summary of NATO's Rapid Adoption Action Plan," June 25, 2025.
[30] SHAPE, "NATO Acquires AI-Enabled Warfighting System," News Release, April 14, 2025.
[31] Elke Schwarz, "Unicorns for Uniforms: On the Problematic Allure of VC Investments in Defense," *Opinio Juris*, September 18, 2024.

their frustration with sometimes decades-long procurement practices and they dislike requirements.

Second, new power brokers in the defense sector create new dependencies. New technology is not public good. The war in Ukraine offers an important cautionary tale about military's dependence on the private tech sector. This is mainly because private companies usually retain control over the use of their assets. The company's executive can decide to restrict the availability of their product in a certain geographical area or make its service available to the other side of the conflict as well. Although thousands of Starlink terminals enabled military communication, including guiding drone strikes, SpaceX did not allow Ukrainians to use Starlink satellites for military purposes over Crimea. Another example includes undersea cables. Only four private companies are responsible for manufacturing and installing some 98 percent of undersea cables across the globe. Importantly, countries may have to rely on high-risk private suppliers for maintenance and repairs of these cables.[32]

And third, by the virtue of market economy, private companies are good at storytelling and creating exaggerated expectations. Defense markets are not immune from such marketing practices. New defense tech companies actively create needs for their customers, the military and the government, so that they can provide them with their tech solutions. They do not shy away from an alarmist language. For instance, to enable the United States to gain strategic AI advantage over China, Palantir's CTO wants to create "an Oppenheimer-like situation", while former Google Chairman and now owner of his own AI startup calls for a Manhattan Project-like program.[33] Such statements can divert limited resources in the national defense budget and distract from other less grandiose but more affordable solutions.

At NATO, any further institutionalization of cooperation with new power brokers needs to avoid these pitfalls. The Alliance can leverage the strength of its 32 member countries to overcome the two most important structural challenges: a lack of public oversight and a vulnerable web of commercial supply chains.[34] While the military has become a net importer of new technologies from the private sector, NATO has the means to build a safe defense innovation ecosystem. However, simultaneously investing into defense industrial production is where it gets complicated.

Innovation-Production Challenge in Five Points

[32] Daniel F. Runde, Erin L. Murphy, and Thomas Bryja, "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition," Center for Strategic and International Studies, August 16, 2024.
[33] Eamon Javers, "How Google's Former CEO Eric Schmidt Helped Write A.I. Laws in Washington without Publicly Disclosing Investments in A.I. Startups," *CNBC*, October 24, 2022.
[34] Jake Steckler and Robert Mayville, "Emerging Tech & American Isolationism: Consequences for AI, Drone, and Space Launch Technologies," Belfer Center for Science and International Affairs, Harvard Kennedy School, 2025.

Improving NATO's defense industrial competency at the pace of technological change can lead to tensions in priority setting.[35] On the one hand, increasing industrial production capacities necessitates coordinated manufacturing of operational warfare equipment. This means speeding up restocking, consolidating supply chains, and aggregating demand for joint procurement. On the other hand, accelerating the adoption of new technologies across allied armed forces requires defense innovation that either enhances existing military capabilities or introduces new systems and kits which are yet to be battle-proven.

This combined pressure to innovate and at the same time to grow armed forces in size creates a complex jigsaw puzzle. For the Alliance to translate its defense industrial strategy into enhanced deterrence and defense, the following five points should deserve more attention from policymakers and defense planners at NATO and in national capitals.

First, AI-enhanced life cycle management. the Alliance's defense industry initiatives highlight the need to improve the speed and economy of scale in production and procurement. However, unlike in wartime economies when defense industrial production follows the dictate of rapid–and mass–attrition, NATO Allies need to maintain their expanded inventories. This is because some equipment is consumable, such as 155mm ammunition shells, or requires system updates, such as most platforms, and eventually needs to be replaced due to low reliability or obsolescence. This is where NATO quietly excels with its continuous work that helps the Allies to keep their military kit in good shape.[36] Given the increasing emphasis on multi-domain systems, it will be important for NATO to efficiently optimize the costs of life cycle management using latest predictive analytics.[37]

Second, innovation awareness. Rapid adoption plans in the context of a multinational organization could sound like an oxymoron. Speaking of such an ambition may create an illusion that the Alliance is able to hack the innovation adoption challenge or mimic the acquisition timelines of a warfighting country. Yet behind major innovations usually lies a years-long research groundwork. For instance, the impressively fast deployment of Baltic Sentry to protect critical undersea infrastructure in the Baltic Sea has not come out of nowhere.[38] NATO Task Force X's mission using maritime drones has leveraged NATO's decade-long efforts in developing standards for communication and command of maritime vessels.[39] This includes the earlier Maritime Unmanned Systems Innovation and Coordination (MUSIC) initiative, which

[35] Daniel Fiott and Antonio Calcara, "Counting on the Cloud? NATO, Digital Modernisation and Cloud Computing," Center for Security, Diplomacy, and Strategy, Paper No. 17, July 2025.,
[36] NATO, "About Life Cycle Management Group," Defense Investment Portal, accessed September 19, 2025.
[37] Manuela Tudosia, "20 Years of NATO Life Cycle Management: Looking Back, Moving Forward, Facing New Challenges," *European Security and Defense*, January 15, 2025.
[38] NATO, "NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security," Press Release, January 14, 2025.
[39] NATO, "NATO Naval Armaments Group," Defense Investment Portal, accessed September 19, 2025; NATO Allied Command Transformation, "NATO's Task Force X: Charting a Course for Autonomous Maritime Dominance," February 26, 2025.

concerned a flexible and interoperable fleet of maritime autonomous systems, and the experience of the U.S. Task Force 59, established in 2021.[40] Shared awareness of the previous programs could improve expectation management and enhance the Alliance's innovation capacity to operationalize advanced technology.

Third, collaboration is a numbers game. In forging collaborative frameworks, it is important to distinguish between capability development and joint procurement. This matters because successful development programs tend to have a leader and involve a maximum of three partners to avoid delays and cost overruns.[41] In contrast, a large number of participants in procurement contracts can bring the cost down.[42] The recent history counsels that developing operational capabilities for purely autonomous reasons can turn out to be prohibitively expensive and lengthy.[43] At times of conflict in an increasingly volatile geopolitical environment, the trade-off among speed, cost, and autonomy tends to favor readily available weapons systems.[44] Indeed, following the Russian full-scale invasion of Ukraine, 78 percent of European defense procurement came from abroad, with 63 percent from the United States.[45]

Fourth, procurement, procurement, procurement. Adopting and integrating new technologies from commercial suppliers requires a qualitatively new approach to ensure their intended military effects. Better coordination or trust building would not suffice. As a rule of thumb, national governments should always include relevant STANAGs (NATO standardization agreements) in the procurement contract to encourage interoperability from the bottom. Yet one of the main pitfalls concerns the procurement process itself. Slow procurement can lead to security liabilities from already obsolete systems by the time they are delivered, while procuring too fast can compromise the safety of armed forces. Procuring too many new gadgets, especially without coordination, can lead to operational challenges within multinational forces and competing logistical tails between legacy systems and new weapons technologies.

Software-centric approach to capability development brings yet another set of challenges. NATO Allies traditionally focused on hardware, while "software [was] largely an afterthought."[46] As software already drives many of the key military platforms, such as fifth-generation fighter jets,

---

[40] NATO, "Maritime Unmanned Systems," Factsheet, November 2020; Xavier Vavasseur, "US Navy Launches New Unmanned Task Group 59.1," *Naval News*, January 25, 2024.
[41] Hannah Aries, Bastian Giegerich, and Tim Lawrenson, "The Guns of Europe: Defense-Industrial Challenges in a Time of War," *Survival* 65, no. 3 (2023): 7–24.
[42] Defense Industry Europe, "NSPA General Manager Highlights the Benefits of Coordinated Procurement," May 23, 2023.
[43] Elisabeth Gosselin-Malo, "Eurodrone Program Bags Fresh Round of EU Subsidies," *Defense News*, March 25, 2024.
[44] Tim Lawrenson and Ester Sabatino, "The Impact of the European Defense Fund on Cooperation with Third-Country Entities," International Institute for Strategic Studies, October 2024.
[45] Sebastian Clapp, "Reinforcing Europe's Defense Industry," European Parliamentary Research Service, PE 749.805, November 2024.
[46] Simona R. Soare, Pavneet Singh, and Meia Nouwens, "Software-Defined Defense: Algorithms at War," International Institute for Strategic Studies, February 2023, p. 1, 3.

third-generation battle tanks, and Patriot missile-defense systems, new weapons systems are increasingly *defined* by their software. New approaches to procurement of technology-supported capabilities experiment with the use of "consumption-based" contracting. For instance, the U.S. Department of Defense launched a new pilot program "Anything-as-a-Service" which highlights that technology is not just a mere product but can take the form of Software-as-a-Service, Data-as-a-Service, and Space-as-a-Service.[47]

However, new software solutions originating from the private tech sector tend to run on commercial–and unprotected–hardware. This reliance on cheap components in commercially outsourced hardware can negatively impact their reliability.[48] To overcome this problem, some tech companies, such as Anduril and Palantir, are selling hardware products tailored for, and already outfitted with, their specific software. Other tech companies partner with traditional defense primes to wrap their software into combat-proven hardware. For instance, German company Helsing has entered into a strategic partnership with Saab to integrate its AI products on board fighter aircraft.[49]

Importantly, in-house experts need to navigate through the commercial marketing noise. This is why initial requirements are so important. Operationalizing new technologies can suffer from incoherence in safety standards and the lack of emphasis on mission-oriented function, ignoring military efficiency measures.[50] Ideally, military end-users should be involved early on in the development of new technology systems in order to build safe software solutions.[51] Military experimental training with such new tech solutions is crucial for identifying the mission for new technology. One potential obstacle to such co-development and procurement of dual-use technologies may be challenged on the grounds of fair market competition.[52]

And **fifth, narratives matter**. NATO burden-sharing parameters need to reflect the evolving role of the defense industry in strengthening NATO's deterrence and defense. The increase of defense spending to 5 percent of annual GDP at the 2025 NATO Summit does not capture this dynamic.[53] While countries are required to spend 3.5 out of these 5 percent to meet the NATO Capability Targets, they are encouraged to invest the remaining 1.5 percent into less tangible goals, such as protection of critical infrastructure, military mobility enablers, innovation, cyber defense, and societal resilience. Defense industrial production and innovation are thus split into two targets.

---

[47] John Harper, "Pentagon Moves to Implement 'Anything-as-a-Service' Pilot Program," *DefenseScoop*, May 6, 2025.
[48] Jakub Jajcay, "I Fought in Ukraine and Here's Why FPV Drones Kind of Suck," *War on the Rocks*, June 26, 2025.
[49] Tim Hepher, "Saab and Helsing Pit AI-Piloted Warplane against Real Fighter Pilot," Reuters, June 11, 2025.
[50] Courtney Crosby, "Operationalizing Artificial Intelligence for Algorithmic Warfare," *Military Review* (July–August 2020): 43–51.
[51] Jeffrey Ding, "Machine Failing: How Systems Acquisition and Software Development Flaws Contribute to Military Accidents," *Texas National Security Review* 8, no. 1 (2024): 9–29.
[52] European Union, *Directive 2009/81/EC on the Coordination of Procedures for the Award of Contracts by Contracting Authorities or Entities in the Fields of Defense and Security* (2009).
[53] NATO, "Defense Expenditures and NATO's 5% Commitment," August 27, 2025.

However, boosting armaments infrastructure enhances the traditional role of NATO in defense planning and coordination. In the language of collective action theory, the alliance defense industrial strategy produces a mix of country-specific private and alliance-wide public goods in terms of closing capability gaps, enhancing interoperability, and encouraging specialization.[54] To tell the story about NATO's robust defense industrial strategy, NATO could revisit its burden-sharing vocabulary and include a fourth "C"–industrial *capacity* to produce and innovate–in addition to the original Three Cs of cash, capabilities, and contributions.[55]

Conclusion

The defense sector is undergoing important structural changes. Privately owned infrastructure and privately financed know-how production are shifting power away from governments and the military, and then concentrating this power into a handful of CEOs. At the same time, NATO faces a twin production-innovation challenge. This paper is intended to bring more clarity to how the Alliance can implement a sound defense industrial strategy that takes into consideration such disruptions.

The paper discussed five main hurdles posed by the emergence of new power brokers coupled with the worsening security environment in Europe. First, more and bigger stockpiles will necessitate better and efficient life cycle management. Second, the pressure to innovate new technological solutions may leave the previous experimental programs unnoticed or uncredited, which may create an illusion of a shortcut to the innovation-adoption challenge. Third, to achieve goals through efficient multilateral defense cooperation, sometimes less can be more. Fourth, procurement reforms in the era of commercialization of war should not contribute to further transfer of power to private defense companies. And fifth, adjusting the burden-sharing narrative can help NATO highlight the importance of defense industrial production and innovation in the context of collective defense efforts.

NATO has the potential to become a leading forum for responsible defense innovation that improves collective competency in critical emerging and disruptive technologies. However, even the soundest alliance defense industrial strategy would make no difference if NATO member countries did not make efforts to implement it. This means stepping up their coordinated engagement with private tech companies based on interoperability requirements; speeding up testing, training, and operationalizing new tech products, and scaling up the production to meet the agreed capability targets. The burden of a successful alliance defense industrial strategy ultimately lies with the individual allies.

---

[54] Dominika Kunertova, "Transatlantic Burden Sharing," in *Routledge Handbook on NATO*, ed. John Andreas Olsen (Abingdon, UK: Routledge, 2024), p. 119–31.
[55] Jonathan Parish, "NATO Experts–What Is the Cost of NATO Membership?" NATO Multimedia TV, October 1, 2019.

If NATO's defense industrial strategy is to strengthen alliance deterrence and defense in the era of new power brokers, it needs to build a resilient network of certified manufacturers with secured supply chains. Such an innovation ecosystem with vetted private companies will ensure that defense innovation aligns with NATO's shared values and security needs, while preventing foreign interference. This is because new power brokers come with a lack of public oversight and profit-driven standard operating procedures. NATO and the Allies thus face the risk of new dependencies on privately owned technology products. Although NATO has traditionally been good at procuring hardware, the pivot to "War-as-Service" is avoidable.

References

Abels, Joscha. "Private Infrastructure in Geopolitical Conflicts: The Case of Starlink and the War in Ukraine." *European Journal of International Relations* 30, no. 4 (2024): 842–66. https://doi.org/10.1177/13540661241260653.

Alamalhodaei, Aria. "5 Investors Have High Hopes for Defense Tech amid Growing Venture Interest." *TechCrunch*, November 20, 2023. https://techcrunch.com/2023/11/20/defense-tech-investor-survey/.

Aries, Hannah, Bastian Giegerich, and Tim Lawrenson. "The Guns of Europe: Defense-Industrial Challenges in a Time of War." *Survival* 65, no. 3 (2023): 7-24. https://doi.org/10.1080/00396338.2023.2218716.

Béraud-Sudreau, Lucie, and Olivier Schmitt. "Alliance Politics and National Arms Industries: Creating Incentives for Small States?" *European Security* 33, no. 4 (2024): 711–31. https://doi.org/10.1080/09662839.2024.2304294.

Beltran, Luisa. "War and Rising Nationalism Is Expected to Spur a Venture Capital Boom in a One-Time Silicon Valley Taboo Sector: Defense Tech." *Fortune*, July 22, 2024. https://fortune.com/2024/07/22/defense-tech-ukraine-israel-war-venture-capital-palantir-spacex-anduril/.

Belfer Center for Science and International Affairs. Steckler, Jake, and Robert Mayville. "Emerging Tech & American Isolationism: Consequences for AI, Drone, and Space Launch Technologies." 2025. https://www.belfercenter.org/sites/default/files/2025-07/DETSP_EmergingTech-AmericanIsolationism_v1-02.pdf.

Britzky, Haley, and Isabelle Khurshudyan. "US Drone Dilemma: Why the Most Advanced Military in the World Is Playing Catch-Up on the Modern Battlefield." *CNN*, September 15, 2025. https://www.cnn.com/2025/09/15/politics/drone-us-military-russia-ukraine.

Center for Strategic and International Studies. Runde, Daniel F., Erin L. Murphy, and Thomas Bryja. "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power

Competition." August 16, 2024. https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

Clapp, Sebastian. "Reinforcing Europe's Defense Industry." European Parliamentary Research Service, PE 749.805, November 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/749805/EPRS_BRI(2023)749805_EN.pdf.

Crosby, Courtney. "Operationalizing Artificial Intelligence for Algorithmic Warfare." *Military Review* (July–August 2020): 43–51. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JA-20/Crosby-Operationalizing-AI-1.pdf.

Cronin, Audrey Kurth. "How Private Tech Companies Are Reshaping Great Power Competition." Washington, DC: The Kissinger Center for Global Affairs, August 2023. https://mediahost.sais-jhu.edu/saismedia/media/web/files/kissinger/how-private-tech-companies-are-reshaping-great-power.pdf.

Defense Industry Europe. "NSPA General Manager Highlights the Benefits of Coordinated Procurement." May 23, 2023. https://defense-industry.eu/nspa-general-manager-highlights-the-benefits-of-coordinated-procurement/.

Ding, Jeffrey. "Machine Failing: How Systems Acquisition and Software Development Flaws Contribute to Military Accidents." *Texas National Security Review* 8, no. 1 (2024): 9–29. https://doi.org/10.26153/tsw/58064.

European Union. *Directive 2009/81/EC on the Coordination of Procedures for the Award of Contracts by Contracting Authorities or Entities in the Fields of Defense and Security*. 2009. https://eur-lex.europa.eu/EN/legal-content/summary/public-procurement-in-the-fields-of-defense-and-security.html.

Fiott, Daniel, and Antonio Calcara. "Counting on the Cloud? NATO, Digital Modernisation and Cloud Computing." Center for Security, Diplomacy, and Strategy, Paper No. 17, July 2025. https://csds.vub.be/publication/counting-on-the-cloud-nato-digital-modernisation-and-cloud-computing/.

Gonzalez, Roberto. "How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex." Watson Institute for International and Public Affairs, Brown University, April 17, 2024. https://watson.brown.edu/costsofwar/papers/2024/SiliconValley.

Gosselin-Malo, Elisabeth. "Eurodrone Program Bags Fresh Round of EU Subsidies." *Defense News*, March 25, 2024. https://www.defensenews.com/global/europe/2024/03/25/eurodrone-program-bags-fresh-round-of-eu-subsidies/.

Harper, John. “Pentagon Moves to Implement ‘Anything-as-a-Service’ Pilot Program.” *DefenseScoop*, May 6, 2025. https://defensescoop.com/2025/05/06/dod-anything-as-a-service-xaas-pilot-program/.

Hartley, Keith. “Defense Industrial Policy in a Military Alliance.” *Journal of Peace Research* 43, no. 4 (2006): 473–89. https://doi.org/10.1177/0022343306064976.

Heim, Anna. “Defense and Resilience Tech Reached an All-Time High: 10% of All VC Funding in Europe.” *TechCrunch*, February 12, 2025. https://techcrunch.com/2025/02/12/defense-and-resilience-tech-reached-an-all-time-high-10-of-all-vc-funding-in-europe/.

Hepher, Tim. “Saab and Helsing Pit AI-Piloted Warplane against Real Fighter Pilot.” Reuters, June 11, 2025. https://www.reuters.com/world/europe/saab-helsing-pit-ai-piloted-warplane-against-real-fighter-pilot-2025-06-11/.

Herzog, Stephen, and Dominika Kunertova. “NATO and Emerging Technologies: The Alliance’s Shifting Approach to Military Innovation.” *Naval War College Review* 77, no. 2 (2024): 47–69. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8417&context=nwc-review.

Jajcay, Jakub. “I Fought in Ukraine and Here’s Why FPV Drones Kind of Suck.” *War on the Rocks*, June 26, 2025. https://warontherocks.com/2025/06/i-fought-in-ukraine-and-heres-why-fpv-drones-kind-of-suck/.

Javers, Eamon. “How Google’s Former CEO Eric Schmidt Helped Write A.I. Laws in Washington without Publicly Disclosing Investments in A.I. Startups.” *CNBC*, October 24, 2022. https://www.cnbc.com/2022/10/24/how-googles-former-ceo-eric-schmidt-helped-write-ai-laws-in-washington-without-publicly-disclosing-investments-in-ai-start-ups.html.

Kunertova, Dominika. “Embracing Drone Diversity: Five Challenges to Western Military Adaptation in Drone Warfare.” Freeman Air and Space Institute, King’s College London, Research Paper 29 (2025).

2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/why-natos-defense-planning-process-will-transform-the-alliance-for-decades-to-come/.

Lawrenson, Tim, and Ester Sabatino. "The Impact of the European Defense Fund on Cooperation with Third-Country Entities." International Institute for Strategic Studies, October 2024. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/10/euro-defense/iiss_the-impact-of-the-european-defense-fund-on-cooperation-with-third-country_24102024.pdf.

Ma, Jason. "SpaceX and Palantir Now Have Bigger Valuations than Top Aerospace-Defense Stocks as the Military Eyes Transformation." *Fortune*, December 7, 2024. https://fortune.com/2024/12/07/spacex-palantir-valuation-market-cap-pentagon-contractor-rtx-lockheed-boeing-northrop/.

NATO. "About Life Cycle Management Group." Defense Investment Portal. Accessed September 19, 2025. https://diweb.hq.nato.int/lcmg/Pages/About.aspx.

———. "Defense Expenditures and NATO's 5% Commitment." August 27, 2025. https://www.nato.int/cps/en/natohq/topics_49198.htm.

———. "Defense Industrial Production Board (DIPB)." Factsheet, April 2024. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/5/pdf/240508-Factsheet-DIPB-en.pdf.

———. "Emerging and Disruptive Technologies." Last updated June 25, 2025. https://www.nato.int/cps/en/natohq/topics_184303.htm.

———. "Framework for NATO Industry Engagement." October 1, 2013. https://diweb.hq.nato.int/indrel/Shared%20Documents/FNIE_Brochure.pdf.

———. "Maritime Unmanned Systems." Factsheet, November 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/11/pdf/2011-factheet-mus.pdf.

———. "Multinational Capability Cooperation." Last updated July 30, 2025. https://www.nato.int/cps/en/natohq/topics_163289.htm.

———. "NATO 2022 Strategic Concept." June 29, 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

———. "NATO Industrial Capacity Expansion Pledge." July 10, 2024. https://www.nato.int/cps/en/natohq/official_texts_227504.htm.

———. "NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security." Press Release, January 14, 2025. https://www.nato.int/cps/en/natohq/news_232122.htm.

———. “NATO Naval Armaments Group.” Defense Investment Portal. Accessed September 19, 2025. https://diweb.hq.nato.int/nnag/Pages/default.aspx.

———. “NATO’s Role in Defense Industry Production.” June 26, 2025. https://www.nato.int/cps/en/natohq/topics_222589.htm#plan.

———. “Summary of NATO’s Rapid Adoption Action Plan.” June 25, 2025. https://www.nato.int/cps/en/natohq/official_texts_236539.htm.

———. “Summit Declaration on Defense Capabilities: Toward NATO Forces 2020.” Press Release, May 20, 2012. https://www.nato.int/cps/en/natohq/official_texts_87594.htm.

NATO Allied Command Transformation. “NATO’s Task Force X: Charting a Course for Autonomous Maritime Dominance.” February 26, 2025. https://www.act.nato.int/article/nato-tfx-maritime-dominance/.

Organization for Economic Co-operation and Development. “Industrial Policy.” Policy Issue. Accessed September 22, 2025. https://www.oecd.org/en/topics/policy-issues/industrial-policy.html.

Parish, Jonathan. “NATO Experts–What Is the Cost of NATO Membership?” NATO Multimedia TV, October 1, 2019. https://www.natomultimedia.tv/app/asset/610729.

Rockwell, Keith. “Criticism of NATO Ignores Its Economic Benefit to the US.” Wilson Center, March 29, 2024. https://www.wilsoncenter.org/article/criticism-nato-ignores-its-economic-benefit-us.

Rogers, Chris, et al. “SHARPE Focus: Emerging Growth Opportunities in Defense Industry.” Harris Williams, August 3, 2022. https://www.harriswilliams.com/our-insights/adg-SHARPE-industry-growth-tech-trends.

Schwarz, Elke. “Unicorns for Uniforms: On the Problematic Allure of VC Investments in Defense.” *Opinio Juris*, September 18, 2024. https://opiniojuris.org/2024/09/18/unicorns-for-uniforms-on-the-problematic-allure-of-vc-investments-in-defense/.

SHAPE. “NATO Acquires AI-Enabled Warfighting System.” News Release, April 14, 2025. https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system-.

Soare, Simona R., Pavneet Singh, and Meia Nouwens. “Software-Defined Defense: Algorithms at War.” International Institute for Strategic Studies, February 2023. https://www.iiss.org/research-paper/2023/02/software-defined-defense.

Stanley-Lockman, Zoe, and Lena Trabucco. “‘NATO’s Role in Responsible AI Governance in Military Affairs.’” In *The Oxford Handbook of AI Governance*, edited by Justin B. Bullock et al. Online ed. Oxford: Oxford University Press, 2022. https://doi.org/10.1093/oxfordhb/9780197579329.013.69.

Tudosia, Manuela. “20 Years of NATO Life Cycle Management: Looking Back, Moving Forward, Facing New Challenges.” *European Security and Defense*, January 15, 2025. https://euro-sd.com/2025/01/articles/42035/20-years-of-nato-life-cycle-management/.

U.S. Department of Defense. *State of Competition within the Defense Industrial Base.* Washington, DC: Office of the Under Secretary of Defense for Acquisition and Sustainment, February 2022. https://media.defense.gov/2022/Feb/15/2002939087/-1/-1/1/STATE-OF-COMPETITION-WITHIN-THE-DEFENSE-INDUSTRIAL-BASE.PDF.

Vavasseur, Xavier. “US Navy Launches New Unmanned Task Group 59.1.” *Naval News*, January 25, 2024. https://www.navalnews.com/naval-news/2024/01/us-navy-launches-new-unmanned-task-group-59-1/.

AI
AI
AI
AI
AI
AI
AI
AI

Between Minds and Machines: The Transformative Power of AI and Its Implications for NATO

Sofia Romansky

Introduction

At this year's Allied Command Transformation (ACT) Academic Conference, an informal exchange in the lunch queue proved to be most memorable. It followed a panel on the growing influence of technology companies in the defense sector, which had focused almost entirely on artificial intelligence (AI). This was hardly surprising: AI promises to deliver unparalleled efficiencies, from helping armed forces maneuver in layered and networked environments to streamlining routine non-operational activities. Private companies have been spearheading innovation across these capabilities at unprecedented speed, fuelled by substantial private investment and sustained military demand alike. Sophisticated multi-modal models and generative AI, as well as claims of companies inching ever closer to artificial general intelligence (AGI), have become omnipresent.[1] Yet, the panel had also prompted caution. The apparent convenience of AI and the hype surrounding it do not mean that its use is straightforward. To maximize the benefits of these systems, significant technical, organizational, and ethical challenges must be addressed.

Echoing this concern, a participant from the private sector asked a pointed question while waiting in line: "If artificial general intelligence is coming, what can my company do to prepare for this reality?" The question was striking–it was relevant but revealed a wider gap in current discussions. Regardless of whether or not AGI emerges, and when, many of the dilemmas it is expected to pose are already evident in the integration of mainstream AI tools: uneven adoption, difficulties embedding systems in existing institutional workflows, and the persistence of cognitive biases.[2] Most importantly, despite growing automation, critical decisions about the deployment and interpretation of AI systems still rest with people; accountability and strategic judgment cannot be delegated to machines. This reply resonated with the interlocutor, who described the difficulties faced when trying to integrate and benefit from even basic generative AI tools in everyday work despite the oft-touted productivity gains.

This is not an isolated sentiment. There is an evident appetite for AI, a recognition of its potential, but a marked gap between enthusiasm and effective use. Crucially, the challenges do not stem solely from the technology itself, but from human interaction with, and perceptions of, these systems. For security organizations such as NATO, which must rapidly adapt to technological change to maintain legitimacy and operational effectiveness, these issues are

[1] Kate Brennan et al., "1.1: The AGI Mythology: The Argument to End All Arguments," *AI Now Institute*, June 3, 2025.
[2] Michael C. Horowitz and Lauren Kahn, "The Cost of the AGI Delusion," *Foreign Affairs*, September 26, 2025.

particularly acute. The human dimension is not a peripheral concern but a central determinant of successful AI integration. And, crucially, organizations and individuals cannot, and should not, wait for AGI to confront these questions.

This compendium contribution aims to identify the complex and interrelated issues at the core of human-AI interaction and offer immediate recommendations for NATO's transformation agenda. It also intends to serve as an introduction for policymakers and practitioners concerned with AI and its implications for institutional design and human agency. The article first scopes the bounds of AI as a transformative category of technologies from the perspectives of geopolitics, the military domain, and security organizations like NATO. It then outlines the challenges that AI creates for human agency and debunks prevalent misconceptions, while stressing that human agency is a non-negotiable element if the benefits of AI are to be realised. The article concludes by providing four recommendations for the transformation agenda:

1. **Return to fundamentals** - Before acquiring, developing, or deploying new AI tools, NATO should clarify the problems these systems are meant to address and determine the role for humans. Clear objectives and boundaries prevent technology-led initiatives from displacing essential human judgment.
2. **Prioritize education on all levels** - Reaping the benefits of AI depends on the ability of personnel, from operators to commanders, to understand a system's capabilities, limitations, and risks. Continuous education and training, from basic digital literacy to human-machine teaming skills, should be embedded across NATO's structures.
3. **Develop human-centered metrics** - Beyond existing technology readiness levels (TRLs), complementary metrics should be developed to assess the quality of human decision-making in AI-enabled contexts, which should impact the ultimate decision to deploy these systems.
4. **Foster change in institutional cultures** - Technological adaptation requires more than procurement. NATO should strive to foster an organizational culture that values reflection, critical thinking, and cross-disciplinary dialogue within institutions and between allies. Creating institutional space for these practices will help ensure that AI enhances rather than erodes collective decision-making.

Together, these measures provide a roadmap for embedding human agency at the heart of AI-enabled elements of security organizations to take maximum advantage of what AI has to offer.

Artificial Intelligence as a Transformative Force

AI is not a single application but a diverse, rapidly evolving category of technologies and capabilities whose development is shaped by geopolitical competition, military demand, and

institutional adoption. Scoping the bounds of AI is crucial for not only understanding its potential benefits, but also the hurdles that must be overcome to achieve them.

The Organization for Economic Co-operation and Development (OECD) defines AI as "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."[3] AI is by no means a new technology, nor is its use new to the defense sector.[4] Yet, key technological and geopolitical factors have launched AI into the spotlight over the last couple of years. While the recent increase in public debate around the use of AI in the military domain can be attributed to the disclosure of Project Maven in 2017, developed by the U.S. Department of Defense (DoD), the release of ChatGPT in 2022 broadened public awareness of and familiarity with AI, specifically its generative modalities.[5] Generative AI is a subset of AI systems "capable of generating seemingly new, meaningful content such as text, images or audio from training data."[6] Touching all aspects of society, transformer-based generative AI models were quickly adopted into the military domain, most notably in the form of AI-enabled decision support systems (AI-DSS). Functionalities of AI-DSS can be categorized into three general types: "(1) description and analysis, which involves collecting, organizing, and presenting data; (2) prediction and extrapolation, which entails identifying patterns and trends in data, including forecasting possible outcomes and their probabilities; and (3) prescription, which focuses on recommending the most effective course(s) of action."[7] Israel's reported use of AI-assisted targeting systems "Lavender" and "Where's Daddy?" in Gaza in early 2024 made it abundantly clear that generative AI is reshaping the character of contemporary warfare by increasing its speed and scale. [8]

The advances in AI models, now capable of processing more diverse datasets with ever-growing numbers of parameters, are shaped by geopolitics and, in turn, contribute to new dynamics. The accessibility of AI technologies has redistributed power among state and non-state actors. Private firms have come to play a decisive role in innovation, altering traditional state-centric dynamics.

---

[3] Organization for Economic Co-operation and Development AI Policy Observatory, "AI Principles Overview," *OECD.AI GPAI.*

[4] "For example, the US and other states developed, use, and export Close-in Weapon Systems, which can autonomously detect and destroy incoming missiles and aircraft mounted on naval vessels. They have been deployed by 40+ states since the 1980s." The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain* (The Hague, 2025), 14; THALES, "Goalkeeper - Close-in Weapon System," *THALES*.

[5] Samuel Gibbs, "Google's AI Is Being Used by US Military Drone Program," *The Guardian*, March 7, 2018.

[6] Stefan Feuerriegel et al., "Generative AI," *Business & Information Systems Engineering* 66, no. 1 (2024): 111–26.

[7] The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*, 19; Anna Nadibaidze et al., *AI in Military Decision Support Systems - A Review of Developments and Debates* (Centre for War Studies, 2024).

[8] Bethan McKernan and Harry Davies, "'The Machine Did It Coldly': Israel Used AI to Identify 37,000 Hamas Targets," *The Guardian*, April 3, 2024.

This extends across supply chains for data, hardware, software, and cloud infrastructure, where control of these inputs creates new vulnerabilities and leverage points. For state defense agencies and alliances, recognizing the importance of cooperation with private industries has become essential to keep pace with AI capabilities progress and guarantee operational advantages. In Ukraine, for example, private-public collaboration and the use of commercial technologies have been key to filling gaps in limited national war-time resources.[9] Simultaneously, AI contributes to new modes of influencing, becoming itself a tool for signalling about power, as well as a direct component of new tactics, including in hybrid threats (information manipulation, cyber operations) for state and non-state actors alike. The use of synthetic video-based disinformation campaigns by Russia against Ukraine and Europe offers a case in point for these concerns.[10]

Access to the most sophisticated AI technologies has become interwoven with perceptions of leadership and power; AI has become a strategic resource, both the subject and object of competition. Governments fear falling behind in AI innovation, creating pressure to secure advantages in supply chains and talent. This has put global governance and shared standard setting into somewhat of a backseat, under the perception that rules would limit the freedom to innovate.[11] Concurrently, AI can offer concrete operational advantages in the military domain, where warfare is the continuation of policy by other means.[12] AI promises enhanced situational awareness through sophisticated, real-time data analysis; more effective intelligence, surveillance, and reconnaissance (ISR) supported autonomous systems; and improved tools for detecting and mitigating threats in the cyber realm.[13] Meanwhile, the integration of AI into command, control, and communications (C3) opens the door for the development of new tactics and concepts, including novel forms of distributed and multi-domain operations that could also ease cooperation within alliances. However, the quest for technological interoperability among NATO allies still has a long way to go,[14] especially when it comes to harmonizing procurement rules and standards, such as the need for an integrated cloud computing system for NATO allies operating in joint missions.[15]

---

[9] Kateryna Bondar, *How Ukraine's War Is Reshaping C4ISR for the Modern Battlefield* (The Hague Centre for Strategic Studies, 2025).
[10] Adam Majchrzak, "Russian Disinformation and the Use of Images Generated by Artificial Intelligence (Deepfake) in the First Year of the Invasion of Ukraine," *Media Business Culture* 2023, no. 1 (14) (2023): 42–55.
[11] Maeve Cullinan, "US and Russia Criticize Plans to Limit AI Weapons," *The Telegraph*, September 26, 2025; Cathy Li, "How to Balance Innovation and Governance in the Age of AI," *World Economic Forum*, November 1, 2024.
[12] The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*, 4.
[13] The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*.
[14] Hans Horan et al., *Securing the Digital Backbone: NATO's Quest for Interoperability in the Age of Emerging Disruptive Technologies* (The Hague Centre for Strategic Studies, 2025).
[15] Antonio Calcara, *NATO's Digital Modernization: The Case of Cloud Computing* (The Hague Centre for Strategic Studies, 2025).

Therefore, it is crucial to recognize that the impact of AI is not confined to operational concepts and combat systems; AI also necessarily impacts the structures, processes, and cultures of the institutions that employ it. From an institutional perspective AI, can offer advantages in non-operational areas such as policy-making, human and legal resources, research development, testing, and evaluation (RDT&E), acquisition and procurement, training, logistics, as well as health and medicine by helping gather, analyze, and leverage increasingly larger sets of data.[16] As AI permeates routine processes, institutional hierarchies and workflows will adapt. Most personnel and stakeholders already encounter AI in everyday civilian life, shaping expectations, behaviors, and skills. As such, AI directly affects the workforce, altering the skills required of personnel at all levels and necessitating corresponding shifts in recruitment, retention, and career structures.[17] AI offers significant opportunities, from enhancing the productivity of existing roles to creating entirely new specialist markets, yet the workforce remains the arena where many of the obstacles to realising these benefits are most evident.[18]

Successful adoption depends on organizational willingness to adapt the status quo, not simply on purchasing new tools.[19] Ultimately, the positive, transformative effects of AI will depend not on the acquisition of new tools alone, but on the institutional foundations that are built; without these, AI risks becoming a superficial add-on to existing processes, generating new obstacles in the process, obscuring the factors that determine whether such technologies succeed or fail.

Human Agency in an AI Era

The same geopolitical, military and institutional trends that make AI a transformative force also place new pressures on human decision-makers, raising fundamental questions about agency in an era of increasing autonomy. Many advantages promised by AI remain aspirational, with practical adoption being constrained by organizational, ethical, and cognitive factors. Crucially, questions of human agency lie at the heart of the challenges posed by AI, but they also provide the foundation for the solutions needed to effectively integrate these technologies into operational and non-operational activities.

---

[16] The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*, 12.

[17] "The Evolving Landscape of Work in the AI Era: Balancing Displacement and Risk-Shifting," in *Innovate to Integrate : A Multidimensional Approach for Managing Business*, by Kh. Anjalee Devi et al. (Empyreal Publishing House, 2024).

[18] Philipp Glock and Sven Von Alemann, "The Paradigm Shift in AI: From Human Labor to Humane Creativity," in *Liquid Legal–Humanization and the Law*, ed. Kai Jacob et al., Law for Professionals (Springer International Publishing, 2022).

[19] Sofia Rizki Aulia and Wen-Shan Lin, "Embracing the Digital Shift: Leveraging AI to Foster Employee Well-Being and Engagement in Remote Workplace Settings in the Asia Pacific Region," *Asia Pacific Management Review* 30, no. 3 (2025): 100339.

The exponential growth of AI technologies and their applications have created a mismatch between the speed of change and the capacity of individuals and institutions to absorb it. This gap arises not only from the unprecedented pace of innovation, with AI computing capabilities reportedly doubling every seven months,[20] but also from the slow rate at which large organizations, bound by set review processes and learning cycles, are able to truly integrate change. The obstacles encountered by NATO during the lengthy processes towards cloud information interoperability among allies, with many countries only starting their transition in 2024, exemplify how outdated practices and differing capabilities can hinder the alliance's capacity to use advanced AI tools.[21] At the same time, the interdisciplinary and multi-stakeholder nature of questions around AI generates information overload around supposed best practices, with multiple debates and narratives unfolding in parallel across technical, legal, and strategic domains. As the emergence of AI at this scale is still relatively nascent, institutions and individuals alike remain in an experimental phase: there are few well-tested guidelines, and one-size-fits-all approaches are neither realistic nor desirable.

In such an environment of rapid change, the questions that become most pressing are not only what AI can do, but how humans can best engage with it. The effectiveness of any system ultimately depends on human understanding and judgment as elements of effective control, making human agency both the area most under pressure and the key to navigating AI's integration. Even the most advanced AI systems cannot determine strategic objects, weigh interrelated consequences, and assume accountability in the same ways as human decision-makers. Yet both the inherent qualities of AI systems and the ways in which they are being integrated into societies and organizations often contribute more to the erosion of human agency than to its reinforcement.

First, opaque AI models, where data parameters and processes to reach outcomes are often inscrutable to developers and users, are inherently difficult for humans to understand without, for example, explainability mechanisms in place. Without additional measures, so-called 'black box' models risk hampering trust and, subsequently, the efficacy of AI systems.[22] Yet, somewhat paradoxically, over-trust in AI systems is also a progressive issue. Without technical knowledge and understanding, users are prone to anthropomorphise AI, misrepresenting the systems as 'knowing' or 'thinking', when they are in fact only performing pattern recognition at scale.[23]

[20] Roland Moore-Colyer, "AI Can Handle Tasks Twice as Complex Every Few Months. What Does This Exponential Growth Mean for How We Use It Live Science, April 27, 2025.
[21] Clara Riedenstein et al., *Defend in the Cloud: Boost NATO Data Resilience* (Center for European Policy Analysis, 2025).
[22] Yasmin Afina and Sarah Grand-Clément, *Bytes and Battles: Inclusion of Data Governance in Responsible Military AI*, no. 308 (Centre for International Governance and Research, 2024).
[23] James Johnson, "Finding AI Faces in the Moon and Armies in the Clouds: Anthropomorphising Artificial Intelligence in Military Human-Machine Interactions," *Global Society* 38, no. 1 (2024): 67–82.

This can lead to misplaced confidence in AI systems, especially when generative AI presents content in incorrect, fabricated, or sycophantic ways.[24]

Second, what is often framed as the 'human challenge' highlights the fact that aspects of technical systems become challenges based on the ways people interact with them, proving more critical than hardware or software-based factors in certain cases. Qualities of human interaction with AI systems risk entrenching existing biases. For example, decision-makers under pressure may over-rely on algorithmic outputs or they may selectively interpret results in ways that confirm preexisting assumptions.[25] At the same time, routine dependence on AI tools can lead to cognitive offloading and skill atrophy: individuals who no longer engage core competencies in pattern recognition and information analysis may lose the ability to operate without machine support.[26] In practice, these tendencies can work against the intended purposes of AI systems, turning tools designed to enhance decision-making into sources of new error and inefficiency.

Clarifying the nature of these pressures requires confronting several common misconceptions about AI adoption and its effects on decision-making:

1. **Ease of use does not remove the need for training.** The apparent intuitiveness and convenience of AI tools can foster complacency while, in fact, emerging trends of human-AI interaction only call for greater vigilance against biases. This risk is heightened by the mistaken assumption that so-called "digital natives", individuals who grew up with digital environments, require no training.[27]

2. **Autonomy does not equal infallibility.** Higher levels of automation do not guarantee better outcomes; errors and misinformation can propagate quickly. Responsibility and accountability remain firmly with human decision-makers.

3. **Unlimited access to knowledge is not a substitute for clear objectives.** The abundance of options generated by AI can overwhelm users, undermining their ability to formulate precise and actionable demands.

4. **Slow adoption reflects insufficient support, not resistance to change.** Barriers to effective use often stem from limited assistance with transition processes and inadequate

[24] The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*, 8; Søren Dinesen Østergaard and Kristoffer Laigaard Nielbo, "False Responses From Artificial Intelligence Models Are Not Hallucinations," *Schizophrenia Bulletin* 49, no. 5 (2023): 1105–7.
[25] Laura Bruun and Marta Bo, *Bias in Military Artificial Intelligence and Compliance with International Humanitarian Law* (Stockholm International Peace Research Institute, 2025), https://doi.org/10.55163/NLWV5347.
[26] Jessica Dorsey, *Proportionality under Pressure: AI-Based Decision Support Systems, the Reasonable Commander Standard and Human(e) Judgment in Targeting*, GC REAIM Expert Policy Note Series (GC REAIM, 2025).
[27] Sharon Greenfield, "Digital Native: The Myth of the Tech-Savvy Youth," in *Digital Media Metaphors*, 1st ed., by Johan Farkas and Marcus Maloney (Routledge, 2024).

understanding of how AI can be applied safely and productively, rather than from human reluctance.

Because these misconceptions are deeply embedded in the public understanding of AI, the technology's considerable potential is often realised in sub-optimal ways. The challenge is compounded by the fact that AI's influence is diffuse, touching multiple domains simultaneously and making it difficult to isolate problems or design targeted solutions. In turn, this contributes to individual and institutional cognitive overload alike: with unprecedented amounts of information and capabilities at their fingertips, many people struggle to make effective use of AI. Rather than improving efficiency, this can reduce productivity and contribute to fatigue. Continuous "innovation" cycles, introduced without adequate time for reflection, risk deepening this strain by generating scepticism and burnout. This is especially dangerous in institutions that rely on knowledge transfer and institutional memory to function, as the erosion of core skills and understanding of institutional mechanisms can weaken long-term resilience and undermine learning, which are essential for transformation.[28]

Within alliances such as NATO, uneven adoption of AI across members already complicates joint decision-making and creates new seams of accountability. Such disparities are not only technical but also institutional, as interoperability and trust ultimately depend on the ability of human decision-makers across the alliance to interpret, oversee, and align the use of AI systems. Therefore, safeguarding human agency is essential: without it, the principles of responsibility and accountability, already embedded in NATO's AI Strategy, risk being undermined.[29] Ensuring human involvement at every stage of the AI system lifecycle is not only a strategic imperative, but also a legal and ethical requirement. For NATO, the stakes are particularly high: public and allied trust depends on visible and proven human oversight of AI-enabled processes, which is fundamental to sustaining the legitimacy of the alliance's policies and operations. These considerations set the stage for practical recommendations on how NATO can embed human agency into its ongoing transformation agenda.

Transformations and Recommendations

The adoption of AI technologies, both in the defense sector and in everyday life, has reached a point of no return; this transformative force is here to stay. To ensure that AI is effectively harnessed for its potential benefits while mitigating its risks, a number of essential steps should be taken. The following recommendations, aligned with emerging expert consensus and directly

[28] Zena Assaad and Adam Hepworth, *A Systems Engineering Lifecycle Approach to Responsible AI*, GC REAIM Expert Policy Note Series (GC REAIM, 2025).
[29] The North Atlantic Treaty Organization, "Summary of the NATO Artificial Intelligence Strategy," NATO, 2021; Tim Sweijs and Sofia Romansky, "International Norms Development and AI in the Military Domain," The Hague Centre for Strategic Studies, 2024.

relevant for NATO's transformation agenda, outline how responsible and effective use of AI can be embedded into operational and institutional practices.

1. *Return to fundamentals*

The first and most essential recommendation may appear obvious yet is often overlooked: a fundamental understanding of AI systems that fit into existing structures and contribute to goals must be the starting point for capability development. Before acquiring, developing, or deploying new AI tools, NATO agencies should clarify the problems these systems are meant to address and determine the appropriate role for human decision-makers in the conceptualisation of capabilities. Establishing clear objectives and boundaries at the outset helps to prevent technology- or industry-driven initiatives from displacing essential human judgment or generating excessive hype for potential solutions that remain insufficiently tested. Key questions that should be addressed at the earliest stages of capability development include: [30]

- What will the AI system, model, or tool actually be used for? What is the intended outcome of use? Is it single or multiple purpose? Who are the intended users?
- What are the existing problems or challenges that could be aided by the AI system, model, or tool? What will human responsibilities and activities be when the AI system, model, or tool is introduced?
- What problems, challenges, and harms can arise from using AI for this purpose? (i.e., does the use of AI lead to skills obsolescence, which may be a detriment to the system's intended purpose?)
- What legal and regulatory boundaries for use exist? What additional boundaries should be imposed? What are the limits of the AI system's functioning without human oversight? What should be the AI system's operating principles and how can they be integrated into its training and design, including the user interface?
- How do we ensure traceable human responsibility through the AI lifecycle? (i.e., what kind of knowledge and training should the individuals who oversee acquisition, development, testing, and deployment of this system have?)
- What broader changes in the current management structure or institution need to occur to ensure efficient and proper use of AI for this purpose?

[30] The short list of questions below is derived from the recommendations found in Sten Allik et al., *White Paper: A Framework for Human Decision-Making through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications*, White Paper (IEEE SA Research Group on Issues of Autonomy and AI in Systems, 2024), 1–63 and The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain.*

Those questions should serve as a reminder to security organizations that the conventional demand-supply relationship still holds. The fact that private companies lead much of today's innovation does not diminish the ability of militaries and alliances to shape the requirements for and influence the outcomes of the technologies which will be used. With sufficient knowledge and understanding, security organizations can direct the development of AI tools to ensure they serve operational needs and uphold strategic priorities, rather than simply adopting what industry happens to produce.

2. *Prioritize education on all levels*

Reaping the benefits of AI depends on the ability of personnel, from operators to commanders, to understand a system's capabilities, limitations, and risks. Continuous education and training should therefore be embedded across NATO's structures and agencies. As generative AI systems increasingly provide accessible, pre-digested information, the ability to critically evaluate, contextualise, and apply that information becomes more important than the ability to simply acquire it. [31] Prioritizing education builds on the fundamentals highlighted in recommendation one, where training should extend beyond an understanding of technical functions to encompass the organization's broader purpose and the individual's role within it–i.e., with what purpose are things done? What is an individual's role and contribution to overall functioning? Basic educational modules should include at a minimum digital literacy training, skill preservation training, and effective interaction with AI tools, including prompt design for operators of AI systems. Modules should additionally address bias awareness and mitigation, countering deskilling, understanding intended use and operational scenarios, assessing reliability, applying system-specific risk assessments, and responding to malfunctions.[32]

3. *Develop human-centered metrics*

Beyond existing technology readiness levels (TRLs), complementary metrics should be developed to assess the quality of human decision-making in AI-enabled contexts, which should impact the ultimate decision to deploy these systems. TRLs, conventionally used in the system development lifecycle, provide a structured framework for assessing the maturity of a technology, but do not necessarily account for the readiness of human operators or institutions to effectively and responsibly use these systems.[33] To address this gap, responsibility by design

---

[31] The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*, 46; Li Qiang, *Key Lessons from Existing Governance Initiatives for the Governance of AI in the Military Domain*, GC REAIM Expert Policy Note Series (GC REAIM & The Hague Centre for Strategic Studies, 2025).
[32] Zena Assaad, "A Risk-Based Trust Framework for Assuring the Humans in Human-Machine Teaming," *Proceedings of the Second International Symposium on Trustworthy Autonomous Systems* (New York, NY, USA), TAS '24, Association for Computing Machinery, September 16, 2024, 1–9, *White Paper: A Framework for Human Decision-Making through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications*.
[33] Fernando Martínez-Plumed et al., "Futures of Artificial Intelligence through Technology Readiness Levels," *Telematics and Informatics* 58 (May 2021): 101525; Ariel Conn et al., *An Approach for Assessing Autonomous and AI-Enabled Capabilities within Weapons Systems*, GC REAIM Expert Policy Note Series (GC REAIM, 2025);

should be embedded into development, ensuring that human obligations are considered from the outset and that clear chains of accountability are preserved, even in legacy systems with new AI-enabled elements that are otherwise capable of operating with minimal human oversight.[34] In practice, this means that both technology and humans must be assessed for whether they have reached adequate readiness levels prior to a technology's deployment: systems should be safe, reliable, and well-integrated into the operational context, while personnel must be trained, equipped with oversight mechanisms, and prepared to respond to malfunctions.[35] Sufficient investment in testing and evaluation is in the interest of security organizations, as it helps ensure that deployed systems are both useful and dependable, and reduces the likelihood of potentially costly flaws emerging only during operations. However, this also does not mean that evaluations should not be continuous. Yet, evaluation cannot be limited to pre-deployment. Given the complex, adaptive, and data-dependent nature of AI, unexpected issues such as emergent behavior, biased outputs, or cascading errors, especially in safety-critical systems, may arise over time. Continuous monitoring and the ability to take systems offline and return them to testing are therefore essential safeguards against harm and disruption of core functions.[36]

4. *Foster change in institutional cultures*

Technological adaptation requires more than procurement; it requires cultural and institutional change. NATO should foster an organizational culture that values reflection, critical thinking, and cross-disciplinary dialogue, both within agencies and between allies, to ensure that AI strengthens rather than erodes collective decision-making. This connects directly to the earlier recommendations: returning to fundamentals clarifies objectives, prioritizing education equips personnel with the skills to meet them, and developing human-centered metrics helps with the efficacy of tools. Yet without embedding these practices into institutional culture, their impact will remain limited. The integration of AI is primarily a change-management challenge, shaped by top-down decisions (i.e., whether to acquire and integrate a certain technology) and bottom-up choices (i.e., the way individuals decide to use or not use these technologies in their everyday practices). Building trust and confidence in the adoption process is therefore critical, with responsibility as the guiding principle. NATO's most recent AI strategy documents highlight six AI principles of responsible use of AI: lawfulness embedded in AI systems, establishment of clear responsibility and accountability structures, traceable and explainable AI decision-making,

---

Herwin Meerveld and Roy Lindelauf, *Context Is Everything: Policy Implications of the Military AI Responsibility Contextualization Framework*, GC REAIM Expert Policy Note Series (GC REAIM, 2025).

[34] Peter Svenmarck et al., "Possibilities and Challenges for Artificial Intelligence in Military Applications," *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists*, 2018.

[35] George Salazar et al., "Understanding Human Readiness Levels," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 64, no. 1 (2020): 1765–69.

[36] More recommendations on how to recenter the human can be found in: The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*; Allik et al., *White Paper: A Framework for Human Decision-Making through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications*.

reliability under expected use and, governability to ensure human control, and bias mitigation efforts.[37] In order to achieve these goals, the above recommendations need to be implemented and appropriate cautions towards the use of AI should be embedded in all relevant aspects of NATO's functioning as a security organization.

Conclusion

The rapid integration of AI into every aspect of human life is not simply a technological development, but a profound philosophical challenge. It forces societies, militaries, and alliances to grapple with fundamental questions about decision-making, responsibility, and the role of human agency in an increasingly automated world. While much of the debate tends to revolve around managing the pace of innovation and the technical capacities of new systems, the more difficult, and often more important, issues lie in understanding the optimal ways in which humans can and should interact with these technologies.

The temptation is often to rush forward, driven either by the ceaseless push of technological development or a fear of being left behind in a perceived global race. Yet, NATO and its member states would be better served by allowing enough time to meaningfully reflect on the challenges and opportunities that AI systems present. Taking such time is not an obstacle to progress, but a prerequisite for successful integration, in ways that support NATO's operational effectiveness, institutional resilience and legitimacy.

In some ways, this is good news. Despite the urgency experienced due to rapid advances in generative models, autonomous systems, and claims of AGI on the horizon, NATO still has time to get this right. The four recommendations, as well as the holistic approach to AI, outlined in this article based on the work of global expert communities, offer an actionable roadmap. They recognize that the human dimension, embedded in training, design, oversight, and institutional culture, will determine whether AI enhances or erodes NATO's ability to act collectively.

Returning to the exchange that inspired these reflections–the conversation started in a lunch queue at the ACT Academic Conference–it also becomes clear how such forums can become an essential part of activities in the era of AI. Conferences provide the space for candid conversations that might otherwise be overlooked in policy documents or technical debates. They allow practitioners, policymakers, and researchers to pause, compare perspectives, and ask the questions that truly need to be asked. These opportunities for collective reflection are themselves part of the transformation process, helping to ensure that decisions about AI are not driven by hype or inevitability, but by understanding.

By placing human agency at the center of its transformation agenda, NATO can ensure that this category of technologies serves to strengthen the principles at the core of the alliance. The

[37] The North Atlantic Treaty Organization, "Summary of the NATO Artificial Intelligence Strategy."

challenge is considerable, but so too is the opportunity, if the time is taken to shape the trajectory of AI with care.

References

Allik, Sten, Rachel Azafrani, David Barnes, et al. *White Paper: A Framework for Human Decision-Making through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications*. White Paper. IEEE SA Research Group on Issues of Autonomy and AI in Defense Systems, 2024. https://ieeexplore.ieee.org/document/10707139.

Antonio Calcara. *NATO's Digital Modernisation: The Case of Cloud Computing*. The Hague Centre For Strategic Studies, 2025. https://hcss.nl/report/natos-digital-modernisation-the-case-of-cloud-computing/.

Assaad, Zena. "A Risk-Based Trust Framework for Assuring the Humans in Human-Machine Teaming." *Proceedings of the Second International Symposium on Trustworthy Autonomous Systems* (New York, NY, USA), TAS '24, Association for Computing Machinery, September 16, 2024, 1–9. https://doi.org/10.1145/3686038.3686045.

Assaad, Zena, and Adam Hepworth. *A Systems Engineering Lifecycle Approach to Responsible AI*. GC REAIM Expert Policy Note Series. GC REAIM, 2025. https://hcss.nl/wp-content/uploads/2025/05/Zena-Assaad-and-Adam-Hepworth.pdf.

Aulia, Sofia Rizki, and Wen-Shan Lin. "Embracing the Digital Shift: Leveraging AI to Foster Employee Well-Being and Engagement in Remote Workplace Settings in the Asia Pacific Region." *Asia Pacific Management Review* 30, no. 3 (2025): 100339. https://doi.org/10.1016/j.apmrv.2024.12.003.

Bruun, Laura, and Marta Bo. *Bias in Military Artificial Intelligence and Compliance with International Humanitarian Law*. Stockholm International Peace Research Institute, 2025. https://doi.org/10.55163/NLWV5347.

Cathy Li. "How to Balance Innovation and Governance in the Age of AI." *World Economic Forum*, November 1, 2024. https://www.weforum.org/stories/2024/11/balancing-innovation-and-governance-in-the-age-of-ai/.

Clara Riedenstein, Lance Landrum, and William Echikson. *Defend in the Cloud: Boost NATO Data Resilience*. Center for European Policy Analysis, 2025. https://cepa.org/comprehensive-reports/defend-in-the-cloud-boost-nato-data-resilience/.

Conn, Ariel, Zena Assaad, and Catherine Tessier. *An Approach for Assessing Autonomous and AI-Enabled Capabilities within Weapons Systems*. GC REAIM Expert Policy Note Series. GC REAIM, 2025. https://hcss.nl/wp-content/uploads/2025/05/Conn-et-al.pdf.

Cullinan, Maeve. “US and Russia Criticise Plans to Limit AI Weapons.” *The Telegraph*, September 26, 2025. https://www.telegraph.co.uk/global-health/terror-and-security/us-russia-artificial-intelligence-weapons-united-nations/.

Dorsey, Jessica. *Proportionality under Pressure: AI-Based Decision Support Systems, the Reasonable Commander Standard and Human(e) Judgment in Targeting*. GC REAIM Expert Policy Note Series. GC REAIM, 2025. https://hcss.nl/wp-content/uploads/2025/05/Dorsey.pdf.

Feuerriegel, Stefan, Jochen Hartmann, Christian Janiesch, and Patrick Zschech. “Generative AI.” *Business & Information Systems Engineering* 66, no. 1 (2024): 111–26. https://doi.org/10.1007/s12599-023-00834-7.

Gibbs, Samuel. “Google’s AI Is Being Used by US Military Drone Program.” Technology. *The Guardian*, March 7, 2018. https://www.theguardian.com/technology/2018/mar/07/google-ai-us-department-of-defense-military-drone-project-maven-tensorflow.

Glock, Philipp, and Sven Von Alemann. “The Paradigm Shift in AI: From Human Labor to Humane Creativity.” In *Liquid Legal–Humanization and the Law*, edited by Kai Jacob, Dierk Schindler, Roger Strathausen, and Bernhard Waltl. Law for Professionals. Springer International Publishing, 2022. https://doi.org/10.1007/978-3-031-14240-6_11.

Greenfield, Sharon. “Digital Native: The Myth of the Tech-Savvy Youth.” In *Digital Media Metaphors*, 1st ed., by Johan Farkas and Marcus Maloney. Routledge, 2024. https://doi.org/10.4324/9781032674612-14.

Hans Horan, Sofia Romansky, and Davis Ellison. *Securing the Digital Backbone: NATO’s Quest for Interoperability in the Age of Emerging Disruptive Technologies*. The Hague Centre For Strategic Studies, 2025. https://hcss.nl/report/securing-the-digital-backbone-natos-quest-for-interoperability-in-the-age-of-emerging-disruptive-technologies/.

Horowitz, Michael C., and Lauren Kahn. “The Cost of the AGI Delusion.” *Foreign Affairs*, September 26, 2025. https://www.foreignaffairs.com/united-states/cost-delusion-artificial-general-intelligence.

Johnson, James. “Finding AI Faces in the Moon and Armies in the Clouds: Anthropomorphising Artificial Intelligence in Military Human-Machine Interactions.” *Global Society* 38, no. 1 (2024): 67–82. https://doi.org/10.1080/13600826.2023.2205444.

Kate Brennan, Amba Kak, and Sarah Myers West. “1.1: The AGI Mythology: The Argument to End All Arguments.” *AI Now Institute*, June 3, 2025. https://ainowinstitute.org/publications/research/1-1-the-agi-mythology-the-argument-to-end-all-arguments.

Kateryna Bondar. *How Ukraine's War Is Reshaping C4ISR for the Modern Battlefield*. The Hague Centre For Strategic Studies, 2025. https://hcss.nl/report/how-ukraines-war-is-reshaping-c4isr-for-the-modern-battlefield/.

Majchrzak, Adam. "Russian Disinformation and the Use of Images Generated by Artificial Intelligence (Deepfake) in the First Year of the Invasion of Ukraine." *Media Business Culture* 2023, no. Issue 1 (14) 2023 (2023): 42–55.

Martínez-Plumed, Fernando, Emilia Gómez, and José Hernández-Orallo. "Futures of Artificial Intelligence through Technology Readiness Levels." *Telematics and Informatics* 58 (May 2021): 101525. https://doi.org/10.1016/j.tele.2020.101525.

McKernan, Bethan, and Harry Davies. "'The Machine Did It Coldly': Israel Used AI to Identify 37,000 Hamas Targets." World News. *The Guardian*, April 3, 2024. https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes.

Meerveld, Herwin, and Roy Lindelauf. *Context Is Everything: Policy Implications of the Military AI Responsibility Contextualization Framework*. GC REAIM Expert Policy Note Series. GC REAIM, 2025. https://hcss.nl/wp-content/uploads/2025/05/Lindelauf-Meerveld-Abu-Dhabi-Housestyle.pdf.

Nadibaidze, Anna, Ingvild Bode, and Qiaochu Zhang. *AI in Military Decision Support Systems - A Review of Developments and Debates*. Center for War Studies, 2024. https://findresearcher.sdu.dk/ws/portalfiles/portal/275893410/AI_DSS_report_WEB.pdf.

Organization for Economic Co-operation and Development AI Policy observatory. "AI Principles Overview." OECD.AI GPAI. https://oecd.ai/en/principles.

Østergaard, Søren Dinesen, and Kristoffer Laigaard Nielbo. "False Responses From Artificial Intelligence Models Are Not Hallucinations." *Schizophrenia Bulletin* 49, no. 5 (2023): 1105–7. https://doi.org/10.1093/schbul/sbad068.

Qiang, Li. *Key Lessons from Existing Governance Initiatives for the Governance of AI in the Military Domain*. GC REAIM Expert Policy Note Series. GC REAIM & The Hague Centre for Strategic Studies, 2025.

Roland Moore-Colyer. "AI Can Handle Tasks Twice as Complex Every Few Months. What Does This Exponential Growth Mean for How We Use It?" Live Science, April 27, 2025. https://www.livescience.com/technology/artificial-intelligence/ai-can-handle-tasks-twice-as-complex-every-few-months-what-does-this-exponential-growth-mean-for-how-we-use-it.

Salazar, George, Judi E. See, Holly A. H. Handley, and Richard Craft. "Understanding Human Readiness Levels." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 64, no. 1 (2020): 1765–69. https://doi.org/10.1177/1071181320641427.

Svenmarck, Peter, Linus Luotsinen, Mattias Nilsson, and Johan Schubert. “Possibilities and Challenges for Artificial Intelligence in Military Applications.” *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists*, 2018. https://www.foi.se/download/18.7fd35d7f166c56ebe0b1005f/1542623791600/Possibilities-and-challenges_FOI-S--5864--SE.pdf.

THALES. “Goalkeeper - Close-in Weapon System.” THALES. https://www.thalesgroup.com/en/goalkeeper-close-weapon-system.

“The Evolving Landscape of Work in the AI Era: Balancing Displacement and Risk-Shifting.” In *Innovate to Integrate : A Multidimensional Approach for Managing Business*, by Kh. Anjalee Devi, Hijam Arnold Singh, Raehaal Yanglem, Ankit Raj Singh, Dr. Ugramohan Jha, and Dr. Manish Kumar. Empyreal Publishing House [EPH], 2024. https://zenodo.org/doi/10.5281/zenodo.10794923.

The Global Commission on Responsible Artificial Intelligence in the Military Domain. *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*. The Hague, 2025. https://hcss.nl/wp-content/uploads/2025/09/GC-REAIM-Strategic-Guidance-Report-Final-WEB.pdf.

The North Atlantic Treaty Organization. “Summary of the NATO Artificial Intelligence Strategy.” NATO, 2021. https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

Tim Sweijs and Sofia Romansky. “International Norms Development and AI in the Military Domain.” The Hague Centre for Strategic Studies, 2024. https://hcss.nl/report/international-norms-development-and-ai-in-the-military-domain/.

Yasmin Afina and Sarah Grand-Clément. *Bytes and Battles: Inclusion of Data Governance in Responsible Military AI*. No. 308. Center for international governance and research, 2024. https://www.cigionline.org/publications/bytes-and-battles-inclusion-of-data-governance-in-responsible-military-ai/.

List of Contributors

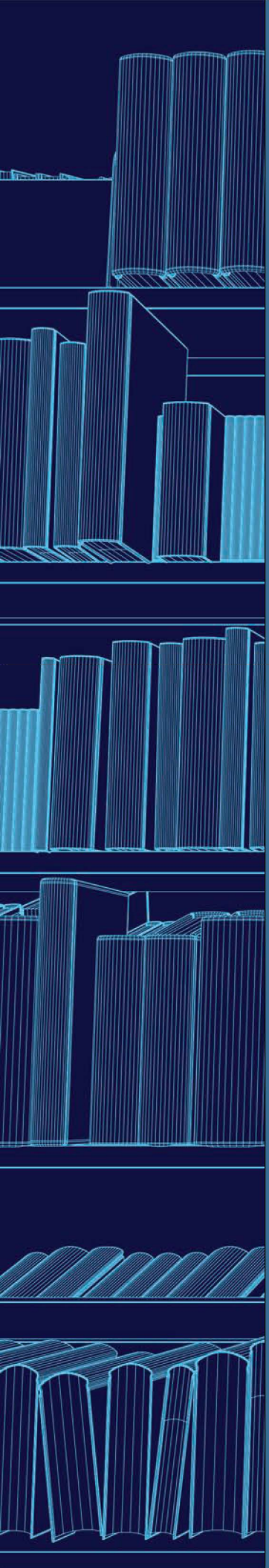
Gorana Grgić, Ph.D., is a Senior Researcher in Transatlantic Security and Acting Head of the Swiss and Euro-Atlantic Security team at the ETH Zürich's Center for Security Studies. She is also a Senior Lecturer at the United States Studies Centre at the University of Sydney and a non-resident Senior Fellow at the Atlantic Council's Scowcroft Center for Strategy and Security.

Tanna Krewson is a sociocultural psychologist and one of the leading experts on cognitive warfare. She is the architect of NATO's Cognitive Warfare Concept and advises governments, international organizations, and security institutions. She has trained senior military and diplomatic leaders from 43 countries and provides strategic counsel to private sector organizations in the OSINT and AI fields. Her work focuses on strategic communications, the psychology of influence, and how narratives and identity impact conflict, shaping how democratic nations understand and contest adversarial influence in the cognitive dimension.

Dominika Kunertova, Ph.D., is a research scholar with over a decade of transatlantic professional experience in academic, think tank, and international organization settings. Her research covers emerging and disruptive technologies and their impact on international security and warfare. Dr. Kunertova is currently a Research Fellow at the Harvard Kennedy School's Belfer Center. She is also a non-resident senior fellow at the Atlantic Council and an affiliate researcher at Peace Research Center Prague. Her research on future drone warfare and military artificial intelligence received grants from the NATO Science for Peace and Security and NATO Chief Scientist programs.

Sofia Romansky is a strategic analyst at The Hague Centre for Strategic Studies as well as the Project Coordinator and Penholder of the Global Commission on Responsible Artificial Intelligence in the Military Domain (GC REAIM). Her primary research concerns the impact of artificial intelligence on the social and military domains, specifically the centrality of the concept of responsibility and the intersection of generative artificial intelligence with disinformation in online spheres as hybrid threats. Sofia has a master's degree in international relations and diplomacy from the University of Leiden and the Clingendael Institute.

Vlasta Zekulic, Ph.D., is Director Strategic Management and Communications at NATO Allied Command Transformation in Norfolk, Virginia, and author of Strategic Force Advising in the NATO Context: Principles and Norms that Support Security Force Assistance (NATO Security Force Assistance Center of Excellence, 2022).



NATO

OTAN

NATO Academic Conference 2025

London,
United Kingdom
30 June - 1 July 2025