BIZTPOL AFFAIRS

JUNE – JULY 2026

VOLUME 13. NUMBER 2.

1 Technology Cold War in the 21st Century: U.S.-China Competition in Semiconductors and AI

ESZTER SZŰCS

19 The Evolution of NATO's Cybersecurity Framework in the Age of Hybrid Warfare

SÁNDOR RÁCZ

33 NATO and Hybrid Warfare: The Invisible Front

GÁBOR MAROSFI

CORVINUS
KÜLÜGYI ÉS KULTURÁLIS EGYESÜLET

CORVINUS SOCIETY FOR FOREIGN AFFAIRS AND CULTURE

corvinusculture.com

BIZTPOL AFFAIRS

VOLUME 13. NUMBER 2.

JUNE–JULY 2026

BUDAPEST

Published by Corvinus Society for Foreign Affairs and Culture, 2026

© Biztpol Affairs

ISSN 2064-3152

Editor-in-Chief

Dr. Péter Rada, Dr. Péter Stepper

Copy editor

Ágnes Stepper

Cover design

Tamás Oláh

Supported by

Nemzeti Együttműködési Alap

Published by Corvinus Society for Foreign Affairs and Culture

Budapest

Responsible publisher:

Dr. Péter Rada

© CORVINUS SOCIETY FOR FOREIGN AFFAIRS AND CULTURE

corvinusculture.com

ESSAY

TECHNOLOGY COLD WAR IN THE 21ST CENTURY: U.S.-CHINA COMPETITION IN SEMICONDUCTORS AND AI

Eszter Szűcs

ABSTRACT

This article examines the U.S.-China competition for technological supremacy in semiconductors and artificial intelligence as a zero-sum strategic rivalry. The article analyses the United States' two-pronged strategy of domestic renewal and external denial. It first examines domestic renewal through the CHIPS and Science Act, then evaluates external denial through export controls targeting ASML's EUV lithography systems. It also analyses China's counter-strategies, including the National Integrated Circuit Industry Investment Fund ("Big Fund") and leverage over critical materials such as gallium and germanium. The findings suggest that although U.S. measures have preserved a short-term technological lead, they have also accelerated China's drive for self-sufficiency.

Keywords: technology cold war, semiconductors, U.S.-China rivalry

INTRODUCTION

The intensifying U.S.-China rivalry over semiconductors and artificial intelligence has transformed advanced technology from an economic asset into a central instrument of geopolitical power. In this emerging "technology cold war," technological leadership is no longer understood primarily in terms of innovation or market advantage, but as a source of military capability, economic leverage, and systemic influence. This article argues that the competition is best understood as a zero-sum strategic contest structured around containment, counter-leverage, and the growing fragmentation of global supply chains.[1]

Artificial intelligence has evolved from a long-standing scientific field into a strategic domain with broad military and economic implications. In public discourse, AI is often equated with generative tools such as ChatGPT, Gemini, or Perplexity, yet in geopolitical terms its significance lies less in user-facing applications than in the computing infrastructure required to develop advanced models. AI is therefore not only software but also a massive consumer of computational power, and access to that power increasingly shapes international hierarchies.[2]

This makes semiconductors indispensable to the contemporary technological order. In geopolitical context, the most important chips are not simple consumer components but advanced logic chips, especially GPUs, that enable large-scale AI training. Their production depends on highly specialized manufacturing processes and tightly concentrated supply chains. At the center of this system stands EUV lithography. ASML remains the only company capable of producing EUV machines, while crucial components are supplied through a narrow transnational network, including Zeiss optics in Germany and U.S.-linked technologies embedded in the wider production chain.[3]

This concentration has elevated semiconductor manufacturing into a strategic chokepoint. The United States has used its leverage over allied export-control regimes to restrict China's access to foundational technologies, especially advanced lithography systems. China, in turn, has responded through state-backed industrial policy, intensified self-

sufficiency efforts, and leverage over critical raw materials and mineral processing. The result is a competitive dynamic in which both sides increasingly treat technology as a matter of national security rather than market efficiency.[4]

Against this background, the article addresses the following research question: what containment strategies are available to the United States and its allies to maintain technological superiority over China in semiconductors and AI? It approaches this question through four related sub-questions: how the CHIPS and Science Act supports domestic re-shoring; to what extent export controls on ASML's EUV systems constrain China's technological development; how China's dominance in gallium and germanium functions as counter-leverage; and how this rivalry contributes to the fragmentation of global supply chains.

The article contributes to the literature in three ways. First, it treats the U.S.-China technology conflict not merely as an extension of trade competition but as a zero-sum security rivalry in which technological advantage is directly linked to military and economic power. Second, it emphasizes the asymmetrical structure of interdependence by focusing on chokepoints such as ASML and rare-material processing. Third, it argues that the most consequential outcome of this rivalry may not be decisive victory by either side, but the emergence of a durable "balance of loss" characterized by parallel technology systems, weakened global integration, and rising systemic costs.[5]

Methodologically, the article relies on qualitative analysis of secondary sources, including academic literature, policy documents, strategic reports, and industry materials. This approach is well suited to a topic defined by state strategy, supply-chain complexity, and rapidly evolving institutional responses. At the same time, the study is limited by its dependence on available English-language materials and the uneven accessibility of primary Chinese-language sources.

The article proceeds as follows. The next section outlines the theoretical framework, combining realism, techno-nationalism, and weaponized interdependence. It then examines the two pillars of U.S. containment strategy: domestic renewal through the CHIPS and Science Act and external denial through export controls on ASML's EUV systems. The following section analyses China's strategic

response through industrial policy and critical-material leverage. The final substantive section considers the broader global consequences, particularly supply-chain fragmentation, parallel technology stacks, and the emerging "splinternet."

THEORETICAL FRAMEWORK

This article adopts a realist and techno-geopolitical perspective to explain the U.S.-China rivalry in semiconductors and artificial intelligence. At its core is the claim that advanced technology has become a strategic asset tied directly to state power, security, and influence. In this context, competition over chips, AI, and supply chains is not adequately explained through market logic alone; it must also be understood through theories of relative power, coercion, and systemic rivalry.[6]

A first key concept is techno-nationalism, understood here as a state-led approach that treats advanced technologies as instruments of national strength and survival rather than merely as economic goods. Both the United States and China increasingly pursue techno-nationalist strategies through subsidies, export restrictions, industrial planning, and efforts to reduce dependence on foreign suppliers. This reflects a broader shift away from the neoliberal assumptions of globalization toward a framework in which states intervene directly to preserve technological advantage.[7]

Realism offers the main analytical lens for interpreting this shift. From a realist perspective, states operate in a competitive international environment in which relative gains matter more than absolute efficiency. In the U.S.-China case, technological progress by one side is increasingly interpreted by the other as a strategic loss. This logic helps explain why semiconductors and AI have become securitized: they are now seen not simply as drivers of growth, but as foundations of military capability, strategic autonomy, and long-term hegemony.[8]

Related realist concepts further clarify the dynamics of the rivalry. The security dilemma helps explain how measures adopted by one side for defensive purposes, such as re-shoring production or tightening export controls, generate insecurity and countermeasures on the other side. Power transition theory and the broader debate associated with

the "Thucydides Trap" illuminate why technological rivalry intensifies when a rising power challenges an established hegemon. In this sense, the semiconductor and AI race is part of a wider struggle over the future distribution of power in the international system.[9]

At the same time, liberal theories of interdependence remain relevant chiefly as a point of contrast. Earlier assumptions that deep economic integration would reduce the likelihood of conflict are increasingly strained in the present context. Here the concept of weaponized interdependence is especially useful. It highlights how states can exploit asymmetries within global networks to exert pressure on rivals by controlling chokepoints in finance, trade, or technology. In semiconductor supply chains, such chokepoints include lithography systems, advanced design tools, and the materials and equipment required for high-end manufacturing.[10]

This perspective helps explain why the United States has been able to transform interdependence into a containment tool. By leveraging its influence over critical technologies, intellectual property, and allied export-control regimes, Washington can slow China's access to advanced manufacturing capabilities. Yet interdependence is not unilateral. China's role in critical-material processing creates forms of counter-leverage that expose Western vulnerabilities and complicate the logic of technological denial.[11]

Taken together, realism, techno-nationalism, and weaponized interdependence provide the conceptual foundation for the article's central argument: the U.S.-China technology conflict is best understood as a zero-sum security rivalry unfolding through control over chokepoints, strategic industrial policy, and the fragmentation of previously integrated global supply chains.

U.S. CONTAINMENT STRATEGY

The first pillar of U.S. containment is domestic renewal. For decades, the United States was content to retain high-value chip design while outsourcing much of semiconductor fabrication to East Asia. As advanced chips became inseparable from AI development, defense systems, and economic competitiveness, that arrangement came to be seen as a strategic vulnerability rather than an efficient division of labor. The U.S. response has therefore been to rebuild

domestic capacity in advanced semiconductor manufacturing and reduce dependence on external chokepoints.[12]

This shift reflects a broader move from the liberal logic of absolute gains to a realist emphasis on relative gains. Earlier policy assumed that all participants in global supply chains could benefit from efficiency and technological exchange. In the context of U.S.-China rivalry, however, policymakers increasingly judge technological development in comparative terms: what matters is not only whether the United States advances, but whether China is prevented from closing the gap. This logic has elevated techno-nationalism from a peripheral policy tendency to a central organizing principle of U.S. strategy.[13]

The CHIPS and Science Act of 2022 institutionalized this turn. Signed into law on 9 August 2022, the Act marked the most significant U.S. state intervention in semiconductor manufacturing and research in decades. It allocated roughly $52.7 billion for semiconductor-related support, including $39 billion for manufacturing incentives and around $11 billion for research and development. In strategic terms, the Act does more than subsidize industry: it redefines semiconductor production as a national-security priority and treats domestic industrial capacity as part of the United States' long-term geopolitical position.[14]

A central purpose of the Act is re-shoring. Through grants, tax credits, and public-private coordination, Washington has encouraged companies such as Intel, TSMC, Samsung, and Micron to expand fabrication capacity on U.S. soil. These incentives have supported major projects in Arizona, Ohio, Texas, and New York, while also channeling resources into the wider semiconductor ecosystem. By early 2026, the Act had helped mobilize hundreds of billions of dollars in private investment across a wide range of projects. These investments are directed not only at increasing output, but also at restoring domestic control over the most advanced manufacturing nodes that are essential for AI training and high-performance computing.[15]

The Act also contains a longer-term technological logic. Its "science" component supports R&D, innovation hubs, and workforce development in semiconductor design, materials, and advanced computing. This reflects the view that technological leadership

depends not only on fabrication capacity, but also on the ability to sustain a multi-decade innovation advantage. In that sense, domestic renewal is intended to create a generational lead rather than merely solve short-term production shortages.[16]

Equally important are the Act's guardrails. Firms receiving support are restricted from materially expanding advanced semiconductor manufacturing capacity in countries of concern, especially China. These provisions are designed to prevent U.S. subsidies from indirectly strengthening a strategic rival, while also reducing the transfer of sensitive technological knowledge. The guardrails therefore link domestic industrial policy directly to containment strategy: the goal is not simply to build capacity at home, but to do so in a way that limits China's access to advanced production and expertise[17]

This effort also serves a broader geopolitical purpose: building a domestic buffer against external shocks, particularly those associated with Taiwan. The extreme concentration of advanced logic-chip production in Taiwan remains a major vulnerability for the United States and its allies. Re-shoring does not eliminate this vulnerability, but it reduces dependence on a single offshore chokepoint and creates greater redundancy within the U.S. production base. Major investments by TSMC in Arizona illustrate this logic especially clearly, as they are meant to anchor a more resilient domestic semiconductor ecosystem.[18]

The results remain mixed but strategically important. U.S. production costs are still significantly higher than those in Asia, and labor shortages continue to slow implementation. Yet the broader direction is clear: domestic renewal has already begun to reverse decades of industrial decline and to reposition semiconductor manufacturing as an element of national power. In that sense, the CHIPS and Science Act is not merely industrial policy. It is the internal pillar of a wider containment strategy designed to preserve U.S. technological superiority in a zero-sum rivalry with China.[19]

External Denial of ASML and Export Controls

The second pillar of U.S. containment is external denial. If domestic renewal seeks to rebuild capacity at home, external denial aims to slow China's technological progress by restricting access to critical inputs, equipment, and knowledge. This strategy is especially visible in the semiconductor sector, where chokepoints in global supply chains can be used to impose asymmetric constraints on a rival. In this sense, U.S. export controls exemplify the logic of weaponized interdependence: interconnected networks are not treated as neutral economic structures, but as instruments of strategic leverage.[20]

ASML occupies the most important position in this system. The Dutch company retains a virtual monopoly over EUV lithography, the technology required for manufacturing the most advanced logic chips used in high-performance computing, AI, and defense-related applications. Because no equivalent alternative exists at the same level, EUV has become one of the most consequential chokepoints in the global semiconductor industry. ASML's machines also depend on a highly specialized transnational supply chain, including key components linked to U.S. technologies and advanced optics produced in Germany. This creates the conditions for American leverage over a formally foreign firm.[21]

The U.S. strategy has therefore focused on denying Chinese firms access to ASML's most advanced systems. Under escalating export-control measures, and with sustained diplomatic pressure on the Netherlands and other allies, China has been prevented from obtaining EUV machines. Without EUV access, Chinese firms face major obstacles in producing leading-edge chips at the most advanced nodes. They can still rely on older DUV systems and workarounds such as multi-patterning, but these are more expensive, less efficient, and technologically limiting.[22]

The legal and institutional basis for this regime was built gradually. The Export Control Reform Act of 2018 expanded U.S. authority over emerging and foundational technologies. This was followed by the Trump administration's restrictions on Huawei and increasing pressure on allied governments to withhold export licenses for advanced semiconductor equipment. Under the Biden administration,

the strategy became broader and more systematic. The October 2022 export-control package targeted advanced computing, AI-related semiconductors, and manufacturing equipment, while extensions of the Foreign Direct Product Rule widened U.S. jurisdiction over foreign-produced items containing American technology or software.[23]

Multilateral coordination proved essential. Since the United States does not itself produce EUV machines, it relied on allied cooperation, particularly from the Netherlands and Japan, to convert unilateral restrictions into an effective denial regime. Dutch controls on advanced DUV immersion systems and Japanese restrictions on related equipment and chemicals extended the chokepoint beyond EUV itself. In practice, this transformed export control from a national instrument into an alliance-based mechanism of technological containment.[24]

The short-term effects have been significant. China has remained cut off from EUV systems, while firms such as SMIC have had to depend on less efficient manufacturing processes that raise costs and reduce competitiveness. U.S. and allied controls have therefore helped preserve a technological gap in advanced semiconductor production and AI-related capability. From a realist perspective, that outcome matters even if it does not stop Chinese progress entirely: slowing the challenger may be strategically sufficient if it preserves relative advantage for the incumbent hegemon.[25]

Yet the strategy also faces limits. China has responded through stockpiling, gray-market procurement, accelerated domestic innovation, and long-term state investment in self-sufficiency. The restrictions may therefore buy time, but they also intensify the incentives for China to reduce dependence on Western technology. At the same time, the regime imposes costs on allied firms, encourages supply-chain fragmentation, and risks turning ASML itself into both a strategic asset and a single point of failure within the Western containment framework.[26]

The broader implication is that external denial is effective but inherently unstable. It has succeeded in creating a powerful chokepoint around lithography and in constraining China's immediate access to the most advanced tools of chip production. At the same time, it reinforces the zero-sum logic of the rivalry and deepens the structural incentives for decoupling, reciprocal pressure, and long-

term fragmentation. Together with domestic renewal, external denial forms the second pillar of a U.S. containment strategy that seeks not simply to advance American technology, but to manage the pace and direction of China's technological rise.[27]

CHINA'S STRATEGIC RESPONSE

China's response to U.S. external denial is the logical counterpart to the chokepoint strategy built around advanced semiconductor tools. As Washington seeks to preserve technological superiority by restricting access to lithography systems, design tools, and high-end manufacturing inputs, Beijing has accelerated efforts to reduce dependence on foreign technology while also exploiting its own strategic leverage in critical materials and processing. In this sense, U.S. containment has not simply slowed China; it has also intensified China's push for self-sufficiency and helped transform technological rivalry into a condition of mutual vulnerability.[28]

The central institutional vehicle of this response is the National Integrated Circuit Industry Investment Fund, or "Big Fund." Since its establishment in 2014, the Fund has operated through successive phases that have become larger and more strategically targeted over time. Its purpose is to channel large-scale state resources into the domestic semiconductor ecosystem, especially those segments most exposed to foreign restrictions. Rather than serving only as an industrial subsidy mechanism, the Big Fund functions as a geopolitical instrument of technological catch-up, designed to sustain China's long-term autonomy in advanced manufacturing.[29]

This strategy has produced visible gains. China has expanded domestic capabilities in selected segments of the semiconductor chain, including equipment localization, packaging, and mature-to-intermediate manufacturing processes. Firms such as SMIC and Huawei have continued to operate through technical workarounds, including multi-patterning on DUV systems and advances in packaging and chiplet-based design. These adaptations do not eliminate China's dependence on foreign technology, but they reduce the immediate coercive effect of U.S.-led export controls and allow continued progress in strategically important sectors.[30]

China's response, however, is not limited to industrial investment. It also relies on asymmetric counter-leverage through critical materials. Beijing's dominance in the processing of gallium, germanium, and other rare-earth inputs gives it influence over parts of the global semiconductor and electronics ecosystem that remain highly concentrated. Because these materials are essential to defense-related electronics, telecommunications, EVs, and advanced chip production, restrictions on their export can expose vulnerabilities across Western supply chains. This turns China's role in the global economy into a source of geopolitical pressure, much as the United States has done through export controls and technological chokepoints.[31]

From a strategic perspective, this material leverage is significant because it alters the structure of the rivalry. U.S. policy aims to deny China access to the tools of advanced manufacturing; China can respond by threatening access to some of the materials and processing capabilities on which those industries also depend. The result is not symmetry in a strict sense, but a reciprocal form of pressure that complicates any simple containment narrative. American dominance in advanced tools is increasingly balanced by Chinese leverage over foundational inputs.[32]

At the same time, China's response faces clear limitations. Despite major investment and measurable adaptation, China still trails global leaders in the most advanced lithography capabilities and remains dependent on costly and inefficient workarounds. Forced localization can generate higher costs, lower reliability, and duplication of effort, while past Big Fund scandals have highlighted the risks of corruption and inefficient capital allocation. Stockpiling, rerouting through third countries, and gray-market procurement may ease short-term pressure, but they do not resolve the underlying technological gap.[33]

These mixed outcomes point to a broader geopolitical conclusion. China's response has made U.S. containment less decisive than intended by converting unilateral denial into mutual vulnerability. Rather than permanently constraining Beijing, the U.S. strategy has accelerated Chinese self-reliance while deepening techno-nationalism on both sides. This dynamic strengthens the article's central argument: the rivalry is moving not toward reintegration, but toward a durable "balance of loss" in which both powers preserve selected

advantages while the global technology system becomes more fragmented, more costly, and less stable.[34]

GLOBAL CONSEQUENCES

The cumulative effect of U.S. domestic renewal, external denial, and China's counter-leverage is a broader transformation of the global technology order. What began as a bilateral contest over semiconductors and AI has increasingly produced systemic fragmentation. The rivalry is no longer confined to national industrial strategies or export controls; it now shapes the structure of global supply chains, digital infrastructure, and third-country alignment choices.[35]

A central outcome of this process is the emergence of parallel, increasingly incompatible technology stacks. As the United States and China seek to reduce exposure to one another in semiconductors, AI, cloud systems, digital standards, and critical inputs, firms and states face growing pressure to align with one technological ecosystem or the other. This divergence is driven not only by security concerns but also by industrial policy, regulatory barriers, export controls, and the broader logic of techno-nationalism. What had once been a relatively integrated global technology environment is gradually being replaced by segmented systems with fewer shared standards and weaker interoperability.[36]

This fragmentation extends into digital infrastructure, often described as a deepening "splinternet." Platforms, AI models, digital services, and governance frameworks are becoming more regionally and politically differentiated. Systems designed for one ecosystem may not function smoothly in another, forcing firms to maintain separate production, compliance, and technological pathways. The result is a more expensive and less efficient international environment in which political-security priorities increasingly override the earlier logic of open technological integration.[37]

The broader economic effects are substantial. Permanent decoupling, reshoring, and friend-shoring raise production costs by duplicating supply chains, reducing economies of scale, and forcing localization into politically preferred rather than economically optimal locations. This does not eliminate vulnerability; it often redistributes

it. The United States and its allies may reduce dependence in one area while creating new forms of exposure elsewhere, especially in relation to critical materials and processing capacity that remain highly concentrated.[38]

The consequences are also intellectual and strategic. Fragmentation slows innovation by reducing collaboration across firms, researchers, and production ecosystems. At the same time, it increases the risks associated with crisis escalation. Mutual deterrence through tools, materials, and chokepoints may create certain forms of restraint, but it also raises the possibility that supply routes, export controls, or technological breakthroughs become flashpoints in a wider geopolitical confrontation. In this environment, non-state actors and large private firms may gain influence by operating across the gaps and inconsistencies between rival systems.[39]

These developments extend far beyond the United States and China. Middle powers and non-aligned states are increasingly developing their own techno-nationalist or regulatory responses. The European Union is building a distinct regulatory model, while countries such as India and other actors in the Global South seek to preserve autonomy by mixing technologies, building domestic infrastructure, or avoiding full alignment with either bloc. This suggests not only bipolar division, but a more complex form of technological regionalism in which multiple partially overlapping systems coexist.[40]

Taken together, these trends support the article's central argument. The U.S.-China rivalry has moved from bilateral competition to systemic fragmentation. The relative gains secured by each side have come at heavy absolute cost: higher production expenses, slower innovation, weaker global integration, and greater instability. Rather than producing decisive containment, the interaction between U.S. strategy and Chinese counter-response has generated a durable "balance of loss" that now shapes the wider international system.[41]

CONCLUSION

This article set out to examine what containment strategies are available to the United States and its allies to maintain technological

superiority over China in semiconductors and artificial intelligence. The analysis shows that the United States has pursued a two-pronged strategy based on domestic renewal and external denial. Through the CHIPS and Science Act, Washington has sought to rebuild advanced manufacturing capacity, expand long-term R&D, and reduce dependence on vulnerable offshore nodes. Through export controls and allied coordination, especially around ASML's EUV lithography systems, it has also tried to slow China's access to the most critical technologies of advanced chip production.

In the short term, this strategy has achieved important results. Domestic renewal has strengthened U.S. industrial capacity and created a strategic buffer, while external denial has imposed a meaningful chokepoint on China's access to frontier semiconductor tools. These measures have preserved relative U.S. advantage in advanced chips and AI-related capability and therefore represent realistic containment options within a zero-sum technological rivalry.

At the same time, the strategy has clear limits. China has responded with a combination of state-led industrial investment and critical-material leverage, reducing the one-sidedness of U.S. pressure and turning containment into a condition of mutual vulnerability. This response has not erased the technological gap, but it has made containment less decisive and accelerated China's drive toward self-sufficiency. In that sense, U.S. success has been partial and time-sensitive rather than final.

The broader significance of these developments lies in their systemic consequences. The rivalry has contributed to the emergence of parallel technology stacks, a deepening splinternet, and the fragmentation of global supply chains. What began as a contest for strategic advantage in semiconductors and AI has become a wider transformation of the international system, in which interdependence increasingly serves as a source of coercion rather than shared prosperity. Techno-nationalism has thus become a dominant pattern in high-technology international relations.

Looking ahead, three broad trajectories remain plausible. The most likely is continued fragmentation, in which the United States and China deepen separate technological ecosystems and force firms and third countries into alignment choices. A second possibility is limited cooperation in non-sensitive areas, where selective engagement could

mitigate some of the costs of decoupling without reversing strategic competition. A third, more dangerous trajectory is escalation, particularly if one side perceives that the other is nearing a decisive breakthrough in AGI, advanced chips, or critical materials. In each case, the basic pattern remains the same: the relative gains pursued by the great powers impose wider absolute costs on innovation, integration, and stability.

The central argument of the article is therefore confirmed. The United States has developed credible containment strategies and has achieved short-term success in preserving technological superiority. Yet those same measures have accelerated Chinese adaptation and contributed to a more fragmented and less stable global order. Rather than delivering lasting hegemony, the rivalry increasingly produces a permanent "balance of loss" in which both powers preserve selected advantages while the broader international system absorbs the costs.

REFERENCES

[1] Segal, A. (2019, December 18). Year in review 2019: The U.S.-China tech cold war deepens and expands. Council on Foreign Relations. https://www.cfr.org/blog/year-review-2019-us-china-tech-cold-war-deepens-and-expands; Allison, G., Klyman, K., Barbesino, K., & Yen, H. (2021, December 7). The great tech rivalry: China vs the U.S. (Avoiding Great Power War Project Paper Series). Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/pantheon_files/GreatTechRivalry_ChinavsUS_211207.pdf

[2] UNESCO. (2022). Recommendation on the ethics of artificial intelligence. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence; Mitre, J., Horowitz, M. C., Henry, N., Borden, E., & Predd, J. B. (Eds.). (2025, September 24). The artificial general intelligence race and international security (Research Report No. PE-A4155-1). RAND Corporation. https://doi.org/10.7249/PEA4155-1

[3] Miller, C. (2022). Chip war: The fight for the world's most critical technology. Scribner.; Reinsch, W. A., Whitney, J., & Schleich, M. (2024, November 19). The double-edged sword of semiconductor export controls: Semiconductor manufacturing equipment. Center for Strategic and International Studies. https://www.csis.org/analysis/double-edged-sword-semiconductor-export-controls-semiconductor-manufacturing-equipment

[4] Sullivan, J. (2023, April 27). Remarks by National Security Advisor Jake Sullivan on renewing American economic leadership at the Brookings Institution [Speech transcript]. The White House. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution/; Nguyen-Tien, V., & Harper, G. (2025, October 31). The US-China rare earths deal shows the importance of critical materials in a new era of strategic interdependence. LSE USAPP Blog. https://blogs.lse.ac.uk/usappblog/2025/10/31/the-us-china-rare-earths-deal-shows-the-importance-of-critical-materials-in-a-new-era-of-strategic-interdependence/

[5] Reinsch et al., 2024.; Freund, C., Mattoo, A., Mulabdic, A., & Ruta, M. (2024). Is US trade policy reshaping global supply chains? Journal of International Economics, 152, Article 104011. https://doi.org/10.1016/j.jinteco.2024.104011 ; U.S.-China bipolar rivalry in the digital age. (2020, Fall). Belfer Center Newsletter. https://www.belfercenter.org/publication/us-china-bipolar-rivalry-digital-age).

[6] Mercadal, T. M. (2021). Zero sum game. In EBSCO Research Starters. EBSCO Information Services. https://www.ebsco.com/research-starters/economics/zero-sum-game; Fakhar, M. F. (2025, October 16). Opinion – The US-China tech hegemony contest: A threat to the neoliberal world order. E-International Relations. https://www.e-ir.info/2025/10/16/opinion-the-us-china-tech-hegemony-contest-a-threat-to-the-neoliberal-world-order/

[7] Sullivan, 2023; Kennedy, S. (2015, June 1). Made in China 2025. Center for Strategic and International Studies. https://www.csis.org/analysis/made-china-2025

[8] Mercadal, 2021; Fakhar, 2025.

[9] Allison, 2017; Organski, A. F. K., & Kugler, J. (1980). *The war ledger*. University of Chicago Press.; Webb, M. C., & Krasner, S. D. (1989). Hegemonic stability theory: An empirical assessment. *Review of International Studies*, 15(2), 183–198. https://doi.org/10.1017/S0260210500112999

[10] Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence: World politics in transition*. Little, Brown.; Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351 .

[11] Powers-Riggs, A., Hart, B., Funaiole, M. P., Thomsett, S., Zieleniewski, S., & Rose, T. (2025, July 17). Beyond rare earths: China's growing threat to gallium supply chains (CSIS Brief). Center for Strategic and International Studies. https://www.csis.org/analysis/beyond-rare-earths-chinas-growing-threat-gallium-supply-chains

[12] Miller, 2022; Sullivan, 2023).

[13] Mercadal, 2021; Sullivan, 2023.

[14] CHIPS and Science Act of 2022; NIST 2026. CHIPS for America. U.S. Department of Commerce. https://www.nist.gov/chips .; NASEM, 2024. Summary description of the CHIPS and Science Act of 2022. In Strategies to enable assured access to semiconductors for the Department of Defense (pp. 175–177). The National Academies Press. https://doi.org/10.17226/276244

[15]U.S. Department of Commerce. (2025, January 17). U.S. Department of Commerce announces CHIPS incentives awards with Corning, Edwards Vacuum, and Infinera to

increase domestic production capacity of chips and equipment critical for U.S. technological leadership [Press release]. https://www.commerce.gov/news/press-releases/2025/01/us-department-commerce-announces-chips-incentives-awards-corning; SIA. (2026).Semiconductor supply chain investments. https://www.semiconductors.org/chip-supply-chain-investments ; TSMC, 2026. TSMC Arizona. https://www.tsmc.com/static/abouttsmcaz/index.htm

ASML. (2026, January 28). ASML reports €32.7 billion total net sales and €9.6 billion net income in 2025 [Press release]. https://www.asml.com/en/news/press-releases/2026/q4-2025-financial-results

[16] NASEM, 2024; Sullivan, 2023.

[17] Crowell & Moring LLP. (2023, September 27). Final rule from Commerce on national security guardrails for CHIPS Act funding: Restrictions on China and other countries of concern. https://www.crowell.com/en/insights/client-alerts/final-rule-from-commerce-on-national-security-guardrails-for-chips-act-funding-restrictions-on-china-and-other-countries-of-concern

[18] Chang, C., Chung, J., Tseng, Y., & Huang, F. (2026, January 15). TSMC's Fab 2 in Arizona to begin mass production in 2nd half of 2027. Focus Taiwan. https://focustaiwan.tw/business/202601150025 ; Hunnicutt, T. (2026, January 16). US and Taiwan reach trade deal, with semiconductor chips and investments at core. Reuters. https://www.reuters.com/world/china/us-taiwan-reach-trade-deal-focused-semiconductors-commerce-department-says-2026-01-15 ; Bao, A., & Butts, D. (2026, January 19). What the U.S.-Taiwan deal means for the island's 'silicon shield'. CNBC. https://www.cnbc.com/2026/01/19/us-taiwan-chip-deal-silicon-shield-tsmc-trump-tapei-ai-semiconductor-supply-chain.html

[19] SIA, 2025; SIA, 2026; Sullivan, 2023.

[20] Farrell & Newman, 2019; Reinsch, Whitney, & Schleich, 2024.

[21] Miller, 2022; ASML, 2026; Reinsch, Whitney, & Schleich, 2024.

[22] Allison et al., Bao, Y. (2025, December 22). Goldman Sachs: The AI gap between China and the US has narrowed to '3-6 months,' while DouBao's mobile app heralds a 'shift in the application traffic landscape.' Moomoo. https://www.moomoo.com/news/post/63200451/goldman-sachs-the-ai-gap-between-china-and-the-us?level=1&data_ticket=1767113799873656 ; Browne, R. (2024, October 16). ASML just gave us a first glimpse into how U.S. chip export curbs will dent its China sales. CNBC. https://www.cnbc.com/2024/10/16/asml-2025-outlook-shows-us-chip-export-curbs-impacting-china-sales.html.

[23] Soliman M., & Carchidi V. (2024, September 23). Re-balancing the strategy of tech containment. Foreign Policy Research Institute. https://www.fpri.org/article/2024/09/re-balancing-the-strategy-of-tech-containment/ ; CFR. (2025, April 15). U.S.-China relations. https://www.cfr.org/timeline/us-china-relations; Sullivan, 2023.

[24] Reinsch, Whitney, & Schleich, 2024; Browne, 2024; Soliman M., & Carchidi V., 2024.

[25] Bao, 2025; Reinsch, Whitney, & Schleich, 2024.

[26] Reinsch, Whitney, & Schleich, 2024; Browne, 2024; ASML, 2026.

[27] Sullivan, 2023; Reinsch, Whitney, & Schleich, 2024.

[28] Kennedy, 2015; Nguyen-Tien & Harper, 2025; Reinsch, Whitney, & Schleich, 2024.

[29] Lee, L. C. (2024, June 6). China's Big Fund 3.0: Xi's boldest gamble yet for chip supremacy. The Diplomat. https://thediplomat.com/2024/06/chinas-big-fund-3-0-xis-boldest-gamble-yet-for-chip-supremacy ; Reuters. (2024, May 27). China sets up third fund with $47.5 bln to boost semiconductor sector. https://www.reuters.com/technology/china-sets-up-475-bln-state-fund-boost-semiconductor-industry-2024-05-27/ Tabeta, S. (2025, January 7). China's 3rd semiconductor 'Big Fund' starts spending $47bn war chest. Nikkei Asia. https://asia.nikkei.com/business/tech/semiconductors/china-s-3rd-semiconductor-big-fund-starts-spending-47bn-war-chest TrendForce. (2025, September 26). [News] China's "Big Fund III" invested RMB 450 million in semiconductor equipment. https://www.trendforce.com/news/2025/09/26/news-chinas-big-fund-iii-invested-rmb-450-million-in-semiconductor-equipment

[30] Allison et al. 2021; Reinsch, Whitney, & Schleich, 2024.

[31] (Powers-Riggs et al., 2025; Atlantic Council. (2025, June). Mapping China's strategy for rare earths dominance. https://www.atlanticcouncil.org/wp-content/uploads/2025/06/Mapping-Chinas-strategy-for-rare-earths-dominance.pdf; Zhiyenbayev, M. (2025, September 5). Securing the new resource frontier: Critical minerals in an era of great-power rivalry (Strategic Security Analysis No. 43). Geneva Centre for Security Policy. https://www.gcsp.ch/publications/securing-new-resource-frontier-critical-minerals-era-great-power-rivalry .

[32] Nguyen-Tien & Harper, 2025; Reinsch, Whitney, & Schleich, 2024.

[33] Reinsch, Whitney, & Schleich, 2024; Nguyen-Tien & Harper, 2025.

[35] Freund et al., 2024; Han, P., Jiang, W., & Mei, D. (2024). Mapping U.S.–China technology decoupling: Policies, innovation, and firm performance. Management Science. Advance online publication. https://doi.org/10.1287/mnsc.2022.02057.

[36] Gertz, G. (2026, January 15). U.S.-China competition accelerates across the tech stack. Center for a New American Security. https://www.cnas.org/publications/commentary/u-s-china-competition-accelerates-across-the-tech-stack; Freund et al. 2024.

[37] Lemley, M. A. (2021). The splinternet. Duke Law Journal, 70(6), 1397–1427. https://scholarship.law.duke.edu/dlj/vol70/iss6/3 ; Park, J. (2022, February 9). Breaking the Internet: China-US competition over technology standards. The Diplomat. https://thediplomat.com/2022/02/breaking-the-internet-china-us-competition-over-technology-standards/

[38] Freund et al., 2024; Powers-Riggs, et al. 2025).

[39] Allison, 2017; Mitre et al. 2025).

[40] Park, 2022; Gertz, 2026.

[41] Freund et al., 2024; Reinsch, Whitney, & Schleich, 2024.

ESSAY

THE EVOLUTION OF NATO'S CYBERSECURITY FRAMEWORK IN THE AGE OF HYBRID WARFARE

Rácz Sándor

ABSTRACT

In the 21st century, although traditional kinetic warfare remains central to military conflict, cyberspace marked the emergence of a new operational domain. In modern security environment, the combination of cyber operations and physical attacks is effectively undermining adversary's military and political will. This multi-domain approach is known as hybrid warfare, combines conventional military force with irregular tactics including cyber operations, economic coercion, and disinformation campaigns. Hence, modern states are ready for cybersecurity challenges, so does the NATO, which this article is about.

Keywords: cybersecurity hybrid warfare, NATO.

INTRODUCTION

This article aims to explore the systemic tension within the North Atlantic Treaty Organisation (NATO) that mainly comes from its multilateral alliance structure. Moreover, this paper examines how NATO's cybersecurity framework has evolved in response to hybrid warfare and what institutional, legal, and operational limitations continue to constrain its effectiveness. To answer this question, official NATO doctrines, international legal treaties, and cyber exercise data were evaluated to provide a picture of the alliance's strategic approach. This essay argues that NATO's cybersecurity framework has effectively developed from a technical support role into an integrated, cooperative framework, where the discord between the preservation of national sovereignty over cyber capabilities and collective defence aspirations significantly limits its strategic efficacy.

CYBER THREATS AND HYBRID WARFARE

The vulnerability of modern societies to digital threats and disruption became undeniable during the 2007 coordinated cyberattacks against Estonia. The distributed denial-of-service (DDoS) and attacks targeted governmental networks and media organisations, which served as a warning for NATO. The Estonian incident acts as the catalyst that coerced the alliance to create its cyber defence.[1]capabilities, shifting from an ad hoc technical issue approach to a core pillar of collective security.[2] From a military perspective, cybersecurity extends beyond civilian IT network protection; it contains the active protection of military command and control (C2) networks, incorporates defensive cyber operations into coordinated campaign planning, and maintains mission assurance in compromised circumstances. The cyberspace where these operations exists defined by NATO as "the electronic World created by interconnected networks of information technology and the information on those networks"[3] Cyberspace is determined by its unique structural features such as: the lack of physical borders, the extensive reliance on privately owned infrastructure, and the widespread identification challenge of attackers.

These attributes make incoming cyber threats even more problematic to tackle. The advantage of cyber operations within hybrid warfare is in their ability to achieve high-impact military and political effects while staying below the threshold of open armed conflict. Moreover, this enables state and state-sponsored actors to take advantage of the cyber domain to disrupt communication lines, degrade infrastructure resilience, or conduct media influence operations while maintaining plausible deniability. It is technically difficult to identify the true perpetrators behind sophisticated cyber campaigns, and it is also difficult to hold them legally accountable.[4] In cyberspace,multi-node routing, advanced obfuscation networks, and false-flag indicators are useful tools and methods used by adversaries to misdirect defence professionals. Advanced Persistent Threats (APTs) often employ self-deleting malware[5] and scrub system logs, which result in extensive „dwell times" where state actors remain undetected within critical infrastructure for months.

The ongoing Russian-Ukrainian war is a perfect representation of the operations of these methods. From both sides, coordinated cyber operations have consistently preceded kinetic operations, targeting satellite communications and power stations; thereafter, strikes in the physical domain, such as artillery barrages on critical infrastructure, were adopted. Even though both Ukraine and Russia have great cyber offensive operations, the conflict shows that the limitations of Russia's standalone cyber actions have reduced their effectiveness when met with proper cyber resilience and international defensive cooperation.

NATO'S DOCTRINAL AND INSTITUTIONAL CYBER FRAMEWORK

At the 2016 Warsaw Summit, NATO formally institutionalised its structural shift, where member states officially recognised cyberspace as a distinct operational domain supplementary to the already existing ones. This declaration means that cyber capabilities had to be fully adopted into defensive military planning and carried out simultaneously inside join multi-domain operations (MDO). Therefore, cyber operations can no longer be considered independent secondary technical support. The Allied Joint Doctrine for Cyberspace

Operations (AJP-3.20) is the main doctrinal form of this important integration. This framework guides how cyber operations are planned and executed in NATO.[6] AJP-3.20 created standardised concepts for situational awareness within the shared operational digital picture and defines how local cyber effects influence the broader picture of war. In addition to this, commanders of conventional forces can treat cyber components as reliable assets within a unified command structure.

Complementing AJT-3.20 doctrine's framework, specialised institutional bodies were designed to secure NATO's operational networks. One of them is the NATO Communication and Information Agency (NCI Agency), which acts as the central technical authority, tasked with constructing, deploying, and defending the secure IT infrastructure required for Allied communication and C2 capabilities.[7] NATO maintains centralised oversight of its institutional network through the NCI Agency, providing the technological bases that are essential to prevent unauthorised intrusion and maintain data collection across transnational commands.

LEGAL AMBIGUITY OF CYBER OPERATIONS

The implementation of cyberspace into a military alliance creates complex legal challenges under public international law. More precisely, regarding the thresholds for the use of force, armed attacks, and the invocation of collective defence.[8]

Under Article 2 (4) of the United Nations Charter, the prohibition of threat and use of force in international relations, states are prohibited from the use of force against the territorial integrity or political independence of any state or in any manner inconsistent with the purposes of the United Nations (UN).[9] According to legal consensus and the scale-and-effect test, a cyber operation is considered an illegal use of force if its effects are similar to those of a conventional kinetic strike, that is, if it results in physical destruction, injury or death.[10] However, a higher legal threshold must be met to trigger the right of individual or collective self-defence under Article 51 of the UN Charter, which requires an armed attack. Although all armed attacks includes use of force, not every minor use of force reaches the magnitude of an armed attack. Cyber operations that

cause temporary system outages, economic loss, or data theft generally fall into a legal grey zone below this threshold, remaining legally non-forcible interventions.

Independent of the use of force, cyber operations can violate state sovereignty or the international law principle of non-intervention.[11] A violation of sovereignty occurs when a state conducts unauthorised digital operations within the physical territory of the cyber infrastructure of another sovereign state without consent, seeking to forcefully influence choices that belong within the target state's sovereign domestic reach, such as the manipulation of democratic electoral infrastructure or the forced hindering of essential governmental administrative systems.[12]

Within the Alliance, a similar classification of legal thresholds shapes the potential application of Article 5 of the North Atlantic Treaty. In theory, a severe cyberattack targeting a NATO country can trigger the Article 5 collective self-defence mechanism. In practice, however, this invocation is non-automatic. The North Atlantic Council evaluates the cyber incidents on a case-by-case basis, taking into consideration their scale, effects, and the availability of evidence regarding attribution. Since most hybrid cyber threats deliberately target dual-use[13] critical infrastructure, such as national power stations and grids, railways, or bridges, the assessment of these actions is difficult. The ambiguity of these operations allows aggressors to conceal their identities using proxies and false-flag operations. Therefore, establishing the level of certainty regarding state responsibility is required to justify an Article 5 collective military response, which is a legally and politically complex task.

To handle these ambiguities, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) funded an independent academic initiative. As a result, the Tallinn Manual on the International Law Applicable to Cyber Operations has been created.[14] However, the Tallinn Manual is not an official NATO doctrine, nor does it constitute binding international law. The manual conducts a comprehensive academic study by preeminent legal experts interpreting how existing international humanitarian law (IHL) and peacetime legal regimes apply to the cyber domain.

The initial volume (2013) focused on the laws of armed conflict (jus in bello[15]), detailing how traditional IHL core principles like

distinction[16] and proportionality[17] operate in cyberspace.[18] However, the subsequent Tallinn Manual 2.0 (2017) expanded its scope to peacetime international law. It provides an analytical framework that describes the responsibilities of states, the violations of sovereignty, and the legality of state countermeasures below the threshold of open warfare. The manual is an essential resource for Allied policymakers to assess the legality of defensive choices and possible cyber responses.[19]

OPERATIONAL READINESS: CCDCOE, SCEPVA AND LOCKED SHIELDS

On the one hand, NATO's operational readiness is mostly sustained through practical multilateral mechanisms and realistic simulations, for instance „the Russian-style cyber warfare simulation on NATO" carried out by Ukrainian soldiers in the summer of 2026.[20] On the other hand, legal and doctrinal frameworks provide legal boundaries to Allied states.

NATO's most vital training and research hub is the CCDCOE, which was established in 2008 in Tallinn, Estonia. Even though it is the NATO-accredited Centre of Excellence, most experts and staff members do not come from NATO's central military command structure but rather directly by member states. The usefulness of this, firstly odd-looking attribute, is that it serves as a connection between the military commands part of NATO, industry experts from prominent industries such as Siemens or CrowdStrike and academic institutions, for instance the Tallinn University of Technology or Stanford University. They all contribute to navigating across the highly disparate national networks to ensure proper interoperability.

One of the most critical structural nodes in NATO's cyber structure is shown in the mechanism of Sovereign Cyber Effects Provided Voluntary by Allies (SCEPVA).[21] Several scholars argue that the preservation of Westphalian state sovereignty within a collective security alliance[22] is important to maintain. However, SCEPVA was designed to respect this foundational norm while solving the tension that it poses. To fully comprehend its operational and strategic

implications, SCEPVA must not be seen merely as a technical workaround, but also as a deliberate political tool.

Unlike the traditional military domains (air, sea, ground), where NATO commands assign standing forces, for instance the Standing NATO Maritime Groups or the Baltic Air Policing mission, the Alliance has no centralised offensive cyber capabilities.[23] Cyberspace operation inherently different from conventional strikes. They are non-kinetic, use perishable codes and specialised hardware intercepts to precisely disrupt, overload, or mislead the enemy command structure, communications or critical infrastructure.[24] Several scholars argue[25] that under SCEPVA (2016), when a NATO military operation requires an offensive cyber effect to undermine the enemy air defence grid or mislead command-and-control (C2) nodes, NATO cannot simply order a cyber unit to carry out this operation. Instead, commanders must formally request that individual member states voluntarily deploy their national cyber capabilities to carry out the mission on the objective.[26] To comprehend how NATO conducts cyber operations, the matrix below demonstrates the decentralised operational structure.

Operational phase	Actions and Decisions
1. Target Identification	NATO Allied Command Operations identifies a strategic requirement to degrade adversarial networks (e.g., overriding a hostile C2 or radar node)
2. Formal Request	Because NATO lacks organic offensive tools, it issues a formal request to capable member states via the SCEPVa mechanism.
3. Divergent Alignment	Allied Nation (A) approves the request and deploys its covert capabilities. Concurrently, Allied Nation (B) denies the request due to political constraints, moral or legal issues.

However, this structural design presents an operational dichotomy. In NATO, joint doctrines, for instance AJP-3.20, standardise MDO; in reality, to enforce these doctrines, actual tools are required that only a few technologically advanced member states possess. These member

states are the United States, the United Kingdom and the Netherlands.[27] This results in a forked, divided alliance where the majority of member states are tasked to focus exclusively on passive network defence, while a few member states maintain the capability to project digital prowess.[28] Therefore, offensive cyber impacts cannot be consistently hard-coded into long-term strategic targeting operations; a joint force commander can never be most certain of the asset's final availability until the precise time of national execution.

Jensen argues[29] that the nature of this cautious SCEPVA model lies behind the perishable attribute of offensive cyber weaponry itself. In conventional warfare, a certain type of missile, artillery shell or a type of bullet is a physically visible and repeatable tool. Repeatable in the sense that using them any time will expectably have the same effect, and showcasing them to allies or foes will not reduce their lethality. Unlike military offensive cyberspace operations capabilities (OCOC), which mostly rely on day zero exploits and undiscovered vulnerabilities in software code.[30] This creates an extremely restrictive lifecycle for OCOC:

Discovery → Weapon Development → Deployment/Multilateral Exposure → Adversary Patching → Obsolescence

The moment an offensive cyber tool is executed, its source code and target mechanism are exposed to the target, and once they are exposed, the enemy can quickly fix the breach by patching the vulnerable parts. Moreover, they can analyse the digital signature and even repurpose the code to use it in a counteroffensive.[31] Therefore, the highest level of national classification is required to safeguard advanced cyber powers' offensive arsenal. To create a centralised permanent NATO command structure, member states are required to share this sensitive, highly classified technical data with other nations, which they consider an unacceptable risk of intelligence leakage. This lack of centralised transparency further complicates the joint battle damage assessment (BDA) and synchronisation. According to Jensen[32], it is very challenging for joint staff to measure the exact duration and scope of the digital disruption because the state supplying the cyber effect under SCEPVA frequently conceals from NATO commanders the specific technical mechanisms of the attack to protect its source code. Gady argues[33] that to achieve cross-domain synergy, the core principles of MDO, which demand clear visibility and

synchronised coordination across all operational domains, are frequently being violated by the technical isolation of member states. The effect of this can be seen in a possible scenario where a NATO commander does not fully understand how or when a cyber effect will reduce the enemy capabilities, for instance, an enemy radar system; they cannot synchronise the kinetic strike in the physical domain to have a compact, safe, and successful hit on the target objective.[34]

Credible deterrence requires 3 elements: capability, communication and credibility (C3). However, SCEPVA weakens this credibility of NATO's collective cyber prowess. According to Jensen[35], the individual capabilities of key allies are formidable; however, the collective communication and credibility of the alliance are undermined by the fragmented, voluntary architecture of SCEPVA. Adversaries operate unified cyber commands that can easily integrate offensive cyber operations with state disinformation and economic warfare in an instance.[36] They possess the information that a compulsory political discussion among member states is required before NATO acts collectively, and they are also aware that cyber offensives are dependent on voluntary national exceptions.[37] In most cases, this vulnerability is most severe in operations that do not qualify as armed attacks under Article 51 of the UN Charter.[38] Knowing this, adversaries can launch sustained, sub-threshold cyber operations against vulnerable NATO allies, while still being in this grey zone. Targeting maritime shipping registries or hospital record data will probably not invoke an Article 5 declaration, due to the struggle to find consensus among member states on it.[39] In these sub-threshold scenarios, relying on SCEPVA means that instead of a collective defence response, any proactive cyber countermeasure would be executed by independently active states.

However, to test collective defence capabilities under SCEPVA, the CCDCOE annually hosts Locked Shields, which is the world's largest cyber defence simulation.[40] This practice includes a highly technical environment, where international Blue Team (defenders) protect the interconnected critical infrastructure against a real-time, evolving onslaught from an expert Red Team (adversaries) in a fictional scenario. Locked Shield is much more than a basic technical IT troubleshooter simulation. IT experts must coordinate their tasks while cooperating with legal advisors, strategic communication

specialists, and even governmental decision-makers.[41] The smooth coordination of these experts in each field is the key to repelling harmful cyberattacks. Legal units must rapidly evaluate whether the digital intrusion meets the threshold of sovereignty violation or opens the opportunity for a lawful countermeasure under international law. Meanwhile, media experts must combat disinformation campaigns designed to confuse the public and undermine public opinion of the infrastructure failures. Overall, Locked Shields is one of the most useful ways to maintain operational readiness practices in unexpected scenarios and share knowledge through practical simulations. It also improves cross-functional and cultural communication, endorses rapid joint decision-making, and enhances the psychological resilience of experts who must face real scenarios in the future while being under the pressure of intense information ambiguity.

Strategic Limitations and Remaining Gaps

Despite the significant institutional progress that NATO has shown since the appearance of the first cyberattack incident, systematic vulnerabilities keep limiting the strategic efficacy of the Alliance's collective cybersecurity mechanisms.

The SCEPVA mechanism is good at preventing violations of sovereignty; however, insufficient as a model to effectively, rapidly, and collectively enable member states to respond to cyberattacks. SCEPVA, as mentioned before, relies entirely on voluntary contributions, which can result in operational failures during crisis situations. Whether the SCEPVA model will be modified to reduce operational friction and improve the combat readiness of cyber capabilities is a complex legal and political question.

Besides SCEPVA, the attribution-response dilemma was also discussed in this paper. To conclude, the attribution process is inherently political and time-consuming. Weeks or months are needed to forensically establish state responsibility in an unclear cyber incident. It can hinder the North Atlantic Council's ability to reach a consensus on collective diplomatic, economic, or military responses.

Although this essay does not examine the differences between NATO-EU and EU-US cyber defence cooperation, it is worth noting that many of the challenges associated with the implementation of a common cyber defence framework within the Alliance come from the legal and regulatory differences. For instance, compliance requirements under the NIS2 Directive can create challenges for U.S. companies operating in the European market, while data protection rules under the General Data Protection Regulation (GDPR) impose restrictions on the processing and cross-border transfer of personal data[42]. These legal requirements add complexity to enhancing cyber defence cooperation between the United States and the European Union, and thus to the cooperation with NATO as well.

CONCLUSION

NATO's cybersecurity framework evolution is a vital paradigm shift in the Alliance's structure and approach to the cyber domain to tackle the digital challenges of the twenty-first century. Three primary pillars improved NATO's defence.

Firstly, the recognition of cyberspace as an independent domain via AJP-3.20 and enhancing its technological prowess through the NCI Agency. Secondly, the Alliance has greatly benefited from the legal guidance of the Tallinn Manual 2.0, which has helped clarify the legal thresholds in cyberspace. Thirdly, NATO has improved operational readiness through the CCDCOE and multinational exercises, for instance, Locked Shield, which strengthens the technical skills and helps spread the experience of national experts throughout the Alliance.

NATO's cyber defence network still has serious structural flaws despite these implementations. The speed, consistency and predictability of collective actions are limited by the Alliance's reliance on sovereign national cyber capabilities under the SCEPVA model. Coordinated cyber operations are made more difficult by ongoing attribution issues, overlapping obligations with the European Union, and legal and regulatory differences among allies. These issues show that cyber defence is as much a legal task as it is a political or strategic task that requires continuous adaptation to overcome the difficulties posed by the cyber domain. As cyberspace continues to grow as a

contested and turbulent domain, maintaining credible collective cyber defence will require continuous adaptations to new technologies and legal obstacles, as well as cooperation and unity among member states.

REFERENCES

[1] The main difference between cybersecurity and cyber defence is that while the former focuses on preventing cyberattacks, the latter actively fights to repel, reduce, and diminish them once they breach the defensive walls and being noticed.
[2] NATO. "Centres of Excellence." Last modified January 25, 2025. https://www.nato.int/en/what-we-do/deterrence-and-defence/centres-of-excellence.
[3] Costigan, Dean S., and Michael A. Hennessy. Cybersecurity: A Generic Reference Curriculum. Norfolk, VA; Kingston, ON; Garmisch, Germany: NATO, National Defence, and PfP Consortium of Defense Academies, 2016.
[4] JLCW Editor. "Cyber Warfare Legal Frameworks and International Law." Journal of Law & Cyber Warfare, 2026. https://www.jlcw.org/articles/cyber-warfare-legal-frameworks.
[5] Smeets, Max. "The Strategic Promise of Offensive Cyber Operations." Strategic Studies Quarterly 12, no. 3 (2018): 90–113.
[6] North Atlantic Treaty Organization. Allied Joint Doctrine for Cyberspace Operations. Allied Joint Publication AJP-3.20, Edition A, Version 1. Brussels: NATO Standardization Office, 2020. https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320.
[7] NATO. "NATO Communications and Information Agency (NCI Agency)." April 4, 2022. https://www.nato.int/en/about-us/organization/nato-structure/nato-communications-and-information-agency-nci-agency
[8] Kailius, Marius. "International Law on the Use of Force and Hybrid Warfare." Acta Prosperitatis 15, no. 1 (2024): 92–100. https://doi.org/10.2478/acpro-2024-0008
[9] United Nations. Repertory of Practice of United Nations Organs, Supplement No. 7, Volume I, Article 2(4) of the Charter of the United Nations. New York: United Nations, 2010. https://legal.un.org/repertory/art2/english/rep_supp7_vol1_art2_4.pdf
[10] Roscini, Marco. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2016.
[11] Schmitt, Michael N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017
[12] Schmitt, 2017.

[13] Civilian-military used objectives
[14] Schmitt, 2017.
[15] Jus in bello regulates the conduct of parties engaged in an armed conflict. IHL is synonymous with jus in bello; it seeks to minimize suffering in armed conflicts (International Committee of the Red Cross, 2015) - International Committee of the Red Cross. "What Are Jus ad Bellum and Jus in Bello?" 2015. https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0.
[16] Discriminating between civilian and military networks
[17] Ensuring collateral civilian digital harm is not excessive relative to the concrete military advantage anticipated
[18] Pipyros, Kimon, Charilaos Thraskias, Lilian Mitrou, Dimitris Gritzalis, and Theodoros Apostolopoulos. "A New Strategy for Improving Cyber-Attacks Evaluation in the Context of Tallinn Manual." Computers & Security 74 (2018): 371–83. https://doi.org/10.1016/j.cose.2017.04.007
[19] Schmitt, 2017.
[20] Kutielieva, Iryna. "NATO Narrowly Repels Attack in Russian-Style Cyber Warfare Simulation." Ukrainska Pravda, June 7, 2026. https://www.pravda.com.ua/eng/news/2026/06/07/8038166/.
[21] Arik, Marko, Ricardo Gregorio Lugo, Rain Ottis, and Adrian Nicholas Venables. "Optimizing Offensive Cyber Operation Planner's Development: Exploring Tailored Training Paths and Framework Evolution." Frontiers in Computer Science 6 (2024): 1–12. https://doi.org/10.3389/fcomp.2024.1400360.; Jensen, Mikkel Storm."Five Good Reasons for NATO's Pragmatic Approach to Offensive Cyberspace Operations." Defence Studies 22, no. 3 (2022): 464–88. https://doi.org/10.1080/14702436.2022.2080661.
[22] Fidler, David P. "NATO, Cyber Defense, and International Law." St. John's Journal of International and Comparative Law 4, no. 1 (2013): 1–24.
[23] Arik et al. 2024.
[24] Gady, Franz-Stefan. Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2020.; Smeets, Max. "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis." In Proceedings of the 11th International Conference on Cyber Conflict (CyCon), 1–15. Tallinn: NATO CCDCOE Publications, 2019. https://doi.org/10.23919/CyCon.2019.8756634.
[25] Arik et al. 2024. and Jensen 2022.
[26] Arik et al., 2024.
[27] Jensen 2022; Smeets, 2019.
[28] Jensen 2022.
[29] Jensen 2022.
[30] Smeets 2019.
[31] Jensen 2022.
[32] Jensen 2022.
[33] Gady 2020.
[34] Gady, 2020; Jensen, 2022.
[35] Jensen 2022.
[36] Gady, 2020; Jensen, 2022.

[37] Jensen, 2022.
[38] Fidler, 2013; Roscini, 2016.
[39] Fidler, 2013.
[40] Smeets, Max. "The Role of Military Cyber Exercises: A Case Study of Locked Shields." In Proceedings of the 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), 9–25. Tallinn: NATO CCDCOE Publications, 2022. https://doi.org/10.23919/CyCon55549.2022.9811018.
[41] Sarjakivi, Pekka, Jari Ihanus, and Pertti Moilanen. "Using Wargaming to Model Cyber Defense Decision-Making: Observation-Based Research in Locked Shields." In Proceedings of the 23rd European Conference on Cyber Warfare and Security, 457–64, 2024. https://doi.org/10.34190/eccws.23.1.2270.
[42] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union L119 (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj; European Union Agency for Cybersecurity (ENISA). NIS360 2024: Comprehensive Assessment of NIS2 Cybersecurity Maturity across Critical Sectors. Luxembourg: Publications Office of the European Union, 2024.

ESSAY

NATO AND HYBRID WARFARE: THE INVISIBLE FRONT

Gábor Marosfi

ABSTRACT

This article examines why NATO and the EU have struggled to deter Russian hybrid warfare despite stronger strategies, resilience measures, and intelligence sharing. It argues that fragmented national responsibilities, limited non-military tools, political caution, and weak coordination reduce collective effectiveness. It calls for a more adaptive NATO–EU approach combining resilience, coordinated action, clearer legal frameworks, and greater political willingness to impose costs.

„NEITHER PEACE NOR WAR"

It has been over twelve years since the Western community was shocked by Russian hybrid warfare through the occupation of Crimea and the emergence of the "little green men." In the fifth year of Russia's war against Ukraine, NATO and the EU are fully aware of the threat posed by hybrid warfare. Both organisations have adopted high-level strategies and action plans, developed counter-hybrid toolkits, various mechanism and established a Centre of Excellence in Helsinki for knowledge-sharing. Despite all these efforts, the scope and intensity of Russian hybrid actions against the Western community — for the purpose of this study understood as NATO Allies and EU member states — has been increasing steadily[1]. These Russian hybrid actions evidently fall into a wider strategy in the context of the ongoing war of aggression against Ukraine. While not reaching the threshold of an armed conflict the current situation in the words of NATO Secretary General Mark Rutte in February 2025 "it is neither peace nor war"[2].

Considering all the Allied efforts aimed at strengthening NATO's deterrence, why does it seem to be ineffective restraining Russian hybrid activities, as evidenced by the number of incidents? What are the strategic and policy limitations? Is there a Western 'grand strategy' against Russian hybrid warfare? How could NATO and EU deliver its political commitment (expressed in joint declarations since 2016) in practical terms?

From the perspective of Summer 2026, this essay attempts to outline some of NATO's dilemmas in countering hybrid. Although the primary focus of this paper will be Russia, being currently the most significant actor employing hybrid methods, they are certainly not the only actors in this field. The growing number of state and non-state actors employing hybrid methods, their interactions and 'learning processes', the accelerating technological development and social change have brought about a dramatic evolution of hybrid warfare. Irrespective of the outcome of the war in Ukraine, this evolution will continue dynamically. In a world moving towards multipolarity, asymmetric methods of warfare will play an even more prominent role. All this begs the question: how sustainable and adaptable is the strategy currently pursued by NATO and Allies?

YOUR FROG IS SERVED, SIR!

The slowly boiled frog has become the metaphor of Western complacency and inaction facing hybrid warfare. The illustration is dramatic but not entirely fair: hybrid warfare has been widely recognised, analysed and conceptualised in NATO and the EU as organisations and at the level of member states, and this knowledge and first-hand experience have been built into various political-military strategies and responses at the highest levels[3]. The frog is still alive, and it certainly feels the ambient temperature reaching uncomfortable levels.

As a result of the increasing military threat posed by Russia in the decade since the annexation of Crimea — and especially since the beginning of Russia's full war against Ukraine — NATO's military posture has been completely transformed in preparation for a possible armed conflict with Russia[4]. Nevertheless, the military measures strengthening deterrence and collective defence have not been followed by (visible) comparable measures to deter activity below the threshold of armed conflict. Paradoxically, the success of NATO's military deterrence against Russia seems to have resulted in the increase of the use of hybrid methods by Russia.

This, however, does not mean that the problem has been ignored or that non-military measures are entirely absent.

NATO adopted its first counter-hybrid strategy in 2015. Its three-part structure and task framework — prepare, deter, defend — have essentially remained in force to this day[5]. This threefold framework was intended to be effective against all actors, i.e. meant to be 'actor-agnostic', including Russia. The continuous intensification of hybrid activities against the Alliance and Allies, however, demonstrates its weaknesses: the strategy is either based on false assumptions, and/or it is not being properly implemented. The reasons are examined in the following section.

"LOST IN TRANSLATION"

The practical implementation of the strategy has raised several fundamental questions. What can be considered as a "hybrid action/measure/method"? Based on the theoretical debates of the past

decade (in numbers enough to fill a small library), a coherent conceptual framework has emerged for the definition of "hybrid," with definitions that might differ ('asymmetric', 'unconventional', 'non-linear' warfare/methods) but certainly describing the same thing. The definition remains a moving target in time and space, as adversaries' tactics are continuously evolving.

The difficulty of coming to a common understanding about hybrid has been aggravated by differences in national perceptions. What might constitute a hybrid act/event in one country without a hint of doubt, may not reach the 'detection threshold' of another, especially if it is not a kinetic event (e.g., disinformation). The event can be simply ignored for political reasons and convenience, reflecting simple ignorance or wilful negligence in some cases. Awareness matters: while, for example, NATO's integrated air and missile defence has a 'recognized air picture', providing 24/7 awareness of ballistic and air threats, hybrid events have lacked a similar unified 'threat board' for many years. Since reaching a common understanding and recognition – including attribution, i.e. linking the hybrid event to a specific actor/perpetrator – is a precondition for joint actions, recent developments in this area have proved to be a small breakthrough.

The 2016 NATO Warsaw Summit was the first high-level Alliance forum to substantively address the issue of hybrid warfare and laid down the basic principles of defence that have remained valid ever since: "Responding to this challenge, we have adopted a strategy and actionable implementation plans on NATO's role in countering hybrid warfare. The primary responsibility to respond to hybrid threats or attacks rests with the targeted nation. NATO is prepared to assist an Ally at any stage of a hybrid campaign. The Alliance and Allies will be prepared to counter hybrid warfare as part of collective defence. The Council could decide to invoke Article 5 of the Washington Treaty. The Alliance is committed to effective cooperation and coordination with partners and relevant international organisations, in particular the EU, as agreed, in efforts to counter hybrid warfare."[6].

A striking feature of the strategy is its fundamentally defensive nature. This can be considered self-evident by an Alliance based on collective defence, though it also indicates the limits and scope of action. The 2022 Strategic Concept essentially reaffirmed these principles[7]. At the same time, it failed to provide further guidance how

to operationalise or translate principles into action, or how to introduce them into NATO's military and non-military instruments of power (so-called NMIoPs). While serving the goal of strategic ambiguity, it also lacked the necessary granularity to draw the line between individual (national) and collective responsibilities.

THE LIMITS OF COLLECTIVE ACTION

The 2015 counter-hybrid strategy clearly placed primary responsibility for defence and preparation within the domain of national responsibility, as a task straightly derived from Article 3 of the North Atlantic Treaty: "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."[8]. Allied preparedness can be increased primarily through the strengthening of individual national resilience, requiring a whole-of-government effort across practically all sectors of society. The sheer magnitude of efforts required explains that although Allies have made significant progress in the following decade, there is still much to be achieved in this field. This recognition was reflected in the common commitment adopted at the 2025 Hague Summit: "And Allies will account for up to 1.5% of GDP annually to inter alia protect our critical infrastructure, defend our networks, ensure our civil preparedness and resilience, unleash innovation, and strengthen our defence industrial base."[9].

The declared raison d'être of the Alliance is to guarantee the security of nearly one billion citizens of its member states through collective defence[10]. Accomplishing this 'mission objective' and meeting expectations are far more difficult than issuing regular political statements.

What can a defensive alliance do against an adversary that intentionally blurs the traditional boundaries between peace, crisis and conflict/war? How to counter the full spectrum of DIMEFIL (diplomacy, information, military, economic, financial, intelligence and legal/law enforcement) available to a major nuclear power? What defensive options are available? What is the division of labour and

tasks between the political and military sides? The underlining problem can be summarised as follows.

Over the past seven and half decades the Alliance has developed and operated a sophisticated civilian-military decision-making organisation ranging from the North Atlantic Council and its subordinate committees to the Military Committee and the integrated military and command structure. Running the military structure and using the military instruments of power with its precise rules and procedures, all geared and trained for conducting and winning a kinetic war if necessary, have become the bread-and-butter daily routine for the Alliance. Countering hybrid warfare, however, requires a very different approach, mostly through employing non-military instruments of power with the civilian structure taking the leading role. And the adversary happens to target the this very centre of decision making.

It is commonplace that NATO's strength lies not in wielding its military instrument of power, but in the political cohesion among its members, which also constitutes the Alliance's political centre of gravity. This embodies its most critical vulnerability. Eroding political cohesion employing "reflexive control" theory [11] was an eminent Soviet objective during the Cold War[12], often targeting an Ally or Allies considered to be the weakest link(s). The fundamental objective has not changed and Russian methods and means have expanded significantly. The maxim has survived the fall of the Soviet Union: there is always a weakest link. Russia has been systematically mapping vulnerabilities, finding political rifts and cleavages among Allies for later exploitation.

CONSULTATION AND RESPONSIBILITIES

NATO's history is marked by political crises ultimately resulting in the strengthening of political consultation, as evidenced by the 'Three Wise Men' report in 1956, the 'Harmel Report' in 1967, or the 'NATO 2030' initiative launched in 2021. Consultation is not just matter of self-preservation: it is the lifeline of the Alliance, as enshrined in Article 4 of the North Atlantic Treaty "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is

threatened." It is worth noting that at the time of the signature of the Treaty, the Alliance did not yet have a Council in permanent session, and lacked a supporting committee structure[13]. Today, the daily operation of NATO Headquarters and the regular meetings of dozens of committees are considered as the manifest of Article 4, without calling it as such. However, in the event of a serious security incident any Ally can seek consultations to be held formally under Article 4 – always at the level of the North Atlantic Council. The purpose of such a meeting is primarily to send a political message of Allied solidarity and to convey that NATO gives the issue thorough consideration. The outcome of the meeting is usually a statement issued by the Council, expressing its concern and announcing any decision or action taken that could be publicly communicated. Article 4 consultations are infrequent to preserve the gravity of the occasion and to prevent "decision inflation": in the history of the Alliance about 10 such consultations have taken place.

Although Article 4 and 5 of the Treaty are sequential in numbering but neither depends on the other; and neither of them automatically entails the use of military instruments of power or use of force.

This is all relevant from the perspective that countering hybrid threats is perfectly achievable through political means and NATO's regular run-of-the-mill consultative function, even when it is not explicitly discussed formally under Article 4. Conducting 'meaningful consultations' still leaves the problem of the availability of non-military instruments of power at the disposal of Allies and the Alliance as a whole.

This is exactly the area where Allies and NATO face the greatest difficulty. Hybrid actions most frequently (physically) manifest themselves at national level. NATO is an intergovernmental political-military Alliance of sovereign member states, as an organisation simply does not possess collectively those the non-military instruments of power that would enable action against hybrid acts below the military threshold[14].

These non-military instruments – unsurprisingly – reflect NATO's intergovernmental character and belong to individual Allies as national means of power: diplomacy, information, military economic, financial, intelligence and legal/law enforcement. Except for the military domain, where the Alliance has developed joint structures

and mechanisms, the other instruments (elements of DIMEFIL) are frequently considered as integral and closely guarded parts of national sovereignty: the bigger the Ally, the better sheltered they are. With a few exceptions, small and medium-sized Allies are usually more willing to consider jointly use their national instruments. In the domains of diplomacy, information and intelligence(sharing), and to a limited extent legal aspects, NATO provides the framework for consultation. While there were some efforts (in the 1950-1970s) to include economy in consultations, the rapid advance of European integration has overtaken these initiatives.

One of the most important lessons of the past decade, however, that although Allies can retain primary responsibility at the national level, the Alliance as a whole, can respond more effectively through joint actions. Accordingly, NATO's central role is no longer disputed in countering hybrid — within the limits of national sovereignty, of course. It is still often recalled that NATO does not have a comprehensive political mandate or structure to implement certain decisions (e.g., economic sanctions cannot be discussed, and legal matters also fall outside the scope). However, as others point out, the Alliance can play a consultative and limited coordinating role by sharing best national practices and comparing legal frameworks[15]. At the same time all agree that NATO current decision-making mechanisms and supporting structures are less effective against destabilisation efforts. This is a hard-earned lesson where the Alliance has some homework to do.

In order to overcome this apparently inhibiting factor the relevant NATO strategy envisages "voluntary national measures and actions" to "constrain and contest Russia's aggressive actions and to counter its ability to conduct destabilising activities towards NATO and Allies"[16]. Allies' willingness and readiness to take national actions and accept commensurate risks greatly differ.

HOW TO DETER HYBRID ACTIONS?

According to agreed NATO-terminology, deterrence is: "The convincing of a potential aggressor that the consequences of coercion or armed conflict would outweigh the potential gains. This requires the maintenance of a credible military capability and strategy with

the clear political will to act."[17]. According to traditional theories, deterrence is based either on denial or punishment. But how can all this be interpreted in a hybrid context?

As declared, "NATO's deterrence and defence posture is based on an appropriate mix of nuclear, conventional and missile defence capabilities, complemented by space and cyber capabilities".[18]. NATO is ready to "employ military and non-military tools in a proportionate, coherent and integrated way to respond to all threats to our security in the manner, timing and in the domain of our choosing." The 'all threats' include hybrid ones, of course.

Above the threshold of armed conflict, this strategy appears to be successful — as there are no open hostilities with Russia. Below this threshold, however, serious doubts linger about the effectiveness of deterrence: Russian hybrid activities against Allies have been steadily increasing over the past decade[19]. The conclusion is evident.

Can we deter Russia from using hybrid against NATO and/or Allies at all? Measuring the effectiveness of deterrence is sometimes jokingly referred to as "not being a science but guessing, mostly based on intuition". Even game theory often concludes that "the opponent's cognitive processes and decision-making is a static uncertainty that cannot easily be resolved and has to be accepted"[20].

In Russian strategic thinking, the concept of deterrence differs significantly from what generally accepted and used in NATO (as a sidenote: differences exist even between major Allies). According to the Russian concept, deterrence presupposes maintaining escalation dominance[21]. In relevant Russian literature, the purpose of asymmetric warfare is often asserted to prepare the theatre of operations for major kinetic warfare (in this section we will use "asymmetric warfare" instead of "hybrid", as Russian literature defines "hybrid" as the perceived non-military coercion methods employed by the West to destabilise Russia, e.g., "orange revolutions" etc.). The existence of the concept of "zero phase of kinetic operations" is confirmed by political statements of leaders (most frequently by former Russian president Dmitry Medvedev). In Russian perception, the country has been in 'full conflict' with the West for at least a decade[22].

However, this conflict remains an "invisible front" for most in the West.

Apparently, Russia is ready and willing to use and unlimited amount of limited non-military power to prepare the ground for a possible open confrontation with NATO, utilising the full spectrum of means available to the Russian state. In this approach, non-military instruments are preferred to avoid direct confrontation, but military instruments are not necessarily excluded, if they are fundamental to achieving Russian objectives. In this extremely pragmatic approach, the only limiting imperative is to avoid direct attribution to Russia and avoid inadvertently crossing the (assumed) NATO threshold of armed conflict – in which Russia, by its own calculation, would almost certainly be at a disadvantage. Hybrid actions against NATO and Allies (asymmetric warfare from the Russian perspective) therefore indicate the recognition of Russia's military inferiority.

Should then NATO and Allies tolerate/accept a certain level of Russian hybrid actions as a tool for managing escalation and prevent open conflict, "for the sake of peace"? If the answer is yes, where should Allies / the Alliance draw the line? So far, the West has been following precisely this logic: prevent escalation at all costs, emphasise the "denial" side of deterrence, strengthen and build national and institutional resilience.

The fallacy of this strategy is apparent. Democracies are often reluctant to go to war, but they are also prone to ignore that deterrence and defence might not be sufficient to prevent them. The absence or insufficiency of Western countermeasures against Russian hybrid actions, denying or exceeding the gains available for Russia, has further encouraged the Russian leadership to increase its 'operational tempo'. The absence of active actions (i.e. punishment or retaliation) by the West results in a positive feedback loop for further actions by Russia. The fear of escalation and self-restraint by the West drive escalation[23].

On the other hand, Russian deterrence against the West — frequently based on harsh nuclear rhetoric — has been successful. Although Russian "red lines" has continuously shifted in parallel with the increase in Western support for Ukraine, Russian messaging and deterrence have played an eminent role in limiting active Western actions against hybrid actions.

Over the past five years many Allies have recognised this strategic blunder and have started to call for a more assertive NATO approach,

sometimes dragging other reluctant Allies and the entire Alliance along the way. This 'new approach' has been demonstrated by the efforts to curtail the activity of the Russian 'Shadow Fleet'.

BEYOND DETERRENCE: ARTICLE 5 AND WHAT FOLLOWS

Although the Russian determination to maintain escalation dominance — as a central element of the Russian deterrence concept — and to keep it under tight political control remains obvious, its successful outcome cannot always be guaranteed. Russian "diplomats" accredited to NATO (before they were restricted to visit NATO HQ) had made considerable efforts to learn what Allies would consider as an "armed attack" under Article 5 of the Washington Treaty. Moscow is aware of the enormous risk of miscalculation; reading and learning NATO'perceptions correctly therefore is essential to keep hybrid actions under the threshold. As Russia has been increasingly forced to "outsource" the execution of hybrid operations to criminal groups (as Russian intelligence operations in the West were significantly damaged by expulsions), the potential slip of political control represents a mounting danger [24] in managing escalation.

NATO's potential responses to hybrid actions are often confused with collective defence under Article 5. In 2015, the Alliance declared, and has since reaffirmed on numerous occasions, that "hybrid operations against Allies could reach the level of armed attack and lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty"[25]. Despite being NATO's 'core business', Article 5 remains somewhat mystified. As a collective political declaration, its significance cannot be overstated – still, it has no immediate automatic military consequences. Theoretically, the Alliance is quite capable (and within its legal rights, pursuant to Article 51 of the UN Charter) of defending itself without calling actions Article 5 or using the full power of its military instruments. NATO can act with or without formally calling it Article 5. NATO's responses may not necessarily be of military nature, and may take place "in the manner, timing and in the domain of the choosing" of the Alliance. However, given the shortcomings of the availability of non-military instruments

of power, as described above, there is a grey zone between military and non-military responses. The cumulative effects of separate hybrid actions could also tip the scales in favour of collective action. As the one and only instance of NATO acting under Article 5 demonstrated in 2001, Allies first required attribution before committing to action. "The Council agreed that if it is determined that this attack was directed from abroad against the United States, it shall be regarded as an action covered by Article 5 of the Washington Treaty, which states that an armed attack against one or more of the Allies in Europe or North America shall be considered an attack against them all"[26]. Actions followed only six weeks later in early October 2001, following attribution shared with Allies by the United States. Attribution has remained Allies' sovereign national prerogative, and collective attribution by NATO (with very carefully crafted expressions!) has remained quite rare.

The answer to the "Russian inquiries", (hopefully) has always been the same by everybody in NATO: the only "threshold" recognised by Allies is enshrined in Article 5; it is 'armed attack'. To maintain strategic ambiguity, the Alliance will never define 'armed attack' or the 'red lines' triggering collective military action. This strategic ambiguity works both ways: while it maintains the political freedom of manoeuvre for Allies, it creates the same room for manoeuvre for hybrid actors. Narrowing this space may be a useful direction of travel to improve Allied responses.

As outlined above, even a collective NATO response to hybrid actions reaching the threshold of armed attack does not necessarily and automatically mean the use of kinetic force. Non-kinetic responses are possible, for example in the cyber domain of operations. Decision-makers will have to make careful choices: which instruments of power do serve better the objective of restoring deterrence and defence? Direct or indirect, strictly proportionate or disproportionate responses? Can democratic states apply mirror-image, tit-for-tat responses, including using the hybrid methods? Currently, there are no simple or clear answers to these questions.

OUTLOOK: "NOT GREAT, NOT TERRIBLE"

Hybrid methods, in their various forms and manifestations will remain an integral part of exerting influence. Actions below the threshold of armed conflict, or asymmetric warfare (regardless of terminology) will remain an attractive and cost-effective method, for an increasing number of state and non-state actors in a multipolar world. Among the numerous lessons drawn from the Iran war, the importance of asymmetric methods will certainly be included. "Post-truth Western societies" will continue to constitute lucrative targets with their inherent vulnerabilities. Russia, facing its dire economic prospects and military inferiority vis-à-vis the West, will be increasingly dependent on using hybrid methods. No change can be expected in Russian doctrine or deterrence concept, either. In light of its declining military prowess in Ukraine, Russia might be willing to undertake high-risk hybrid operations against the West to stop the flow of military support to Ukraine. Desperate actions by a desperate Russian leadership increase the danger of unintended escalation. Russia will continue its hybrid campaigns as long as it is achieving success and its own strategic calculus remains positive, reflecting the doctrine "never reinforce failure, always exploit success."

China pays close attention to Russian experience and would not necessarily follow Russian patterns of behaviour. Beijing's approach to hybrid – as experienced in the West – is much less understood but appears to be different, more complex and indirect in its methods, presumably rooted in the country's different strategic culture, with more emphasis on economic and financial instruments. The mutual learning process, however, is apparent in the Sino-Russian 'partnership without limits'[27].

The good news is that NATO and Allies are learning, too. Intelligence sharing and situational awareness of hybrid actions – the 'threat board' – have significantly increased among Allies. Converting assessment and knowledge into political decisions still fall short of expectations. The difficulty of overcoming the psychological phenomenon of 'learned helplessness' seems to be applicable at the level of nation states and organisations. Nevertheless, the

increasingly intensive and coordinated actions of some Allies against vessels of the Russian "shadow fleet" over the past 12 months already indicate a new, campaign-like approach[28].

A scalable and adaptive non-military "toolbox" remains essential for confronting the adversary. The current situation bears a distant resemblance to the debate in the early 1960s within the Alliance about using nuclear weapons, which ultimately led to the adoption of the doctrine of "flexible response" instead of "massive retaliation". Responses must remain scalable and adaptable to preserve freedom of action and political control. The framework for their employment needs also to be created. The European Union's relevant strategy [29] fundamentally reflects NATO's approach, focusing on the non-military elements of DIMEFIL. In these fields the EU possesses (in certain cases at supranational level) much broader toolbox, primarily in the economic dimension (sanctions) and in countering disinformation, building democratic institutions and national resilience. Despite sharing 23 members with NATO, close cooperation remains a promise to be fulfilled.

There are several directions of travel currently under consideration in the Alliance. One of them is rendering the non-military instruments of power at Allies' (national) disposal more available at multinational level. This would primarily entail their coordinated use to better calibrate Allied responses. This approach would help to solve the "hitting a fly with a sledgehammer" problem, responding to hybrid actions proportionately with non-military means, while ensuring escalation management. This may be complemented by more effective and targeted strategic communication, although the demarcation of sovereign national and Alliance competences constitutes a limitation.

Expanding the non-military toolbox is fundamental but not sufficient for improving the effectiveness of responses. The most important factor remains enhancing Allies' political willingness to act, which requires crossing mental thresholds in several Allied nations. This presupposes improving the awareness of the political leadership and society at large of the threat posed by hybrid warfare, without triggering siege-mentality. Some Allies –mostly Nordic and Baltic Allies closer to the source of the threat – have achieved a high level of awareness. Another factor requires surpassing the peace–war dichotomy: national legal systems are most often not suitable for the

effective handling of hybrid actions because of the absence of appropriate legal frameworks and the strict demarcation of civilian and military competences and responsibilities. For example, civilian authorities and police in many Allies lack the necessary authority and instruments to counter drones as the domestic use of military force may be subject to a special legal state.

Many Western democracies — for ethical, moral, political and many other reasons — are not willing to engage in an eye for an eye, tit-for-tat, mirror-image exchange in responding to hybrid warfare. The (somewhat late) recognition that certain offensive action against hybrid threats must be unavoidable is beginning to take root in major European Allied countries – as expressed by the director of the German foreign intelligence service (BND)[30]. A similar approach has been proposed to the EU[31].

Hybrid warfare is often perceived as individual actions happening in different Allies. While we see separate frames and respond accordingly, our adversaries are watching a continuous movie, retaining the freedom for ad hoc actions within a campaign. Against the coordinated strategy pursued by our adversaries, a similar campaign-like approach is needed, incorporating both defensive and offensive elements. On the technical side, the exploitation of artificial intelligence (AI) offers enormous prospects both for detection, analysis and countermeasures.

But as always, the scope and limits of Allied actions will be defined by national sensitivities and risk appetite.

REFERENCES

[1] Jones, Seth G. (2025). *Russia's Shadow War Against the West*. Center for Strategic and International Studies, 18 March 2025 https://www.csis.org/analysis/russias-shadow-war-against-west; Edwards, Charlie & Seidenstein, Nate. (2025) *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*. International Institute for Strategic Studies. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf

[2] Rutte, Mark. (2025, January 13). *Remarks by NATO Secretary General Mark Rutte at the European Parliament's Committee on Foreign Affairs and Subcommittee on Security and Defence. NATO.* https://www.nato.int/en/news-and-events/events/transcripts/2025/01/13/remarks

[3] NATO. (2022). *NATO 2022 Strategic Concept.* https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

[4] NATO. (2024). *Relations with Russia.* https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-russia;

NATO. (2025a). *Deterrence and defence*. https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence

[5] NATO. (2026). *Countering hybrid threats*. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

[6] NATO. (2016). *Warsaw Summit Communiqué.* https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique

[7] NATO. (2022). *NATO 2022 Strategic Concept.* https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

[8] NATO. (1949). *The North Atlantic Treaty.* https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty?selectedLocale=en

[9] NATO. (2025b, June 25). *The Hague Summit Declaration issued by the NATO Heads of State and Government participating in the meeting of the North Atlantic Council in The Hague.* https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration

[10] NATO. (2025a). *Deterrence and defence.* https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence

[11] Vasara, Antti. (2020) *Theory of Reflexive Control.* Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy. Finnish Defence Studies 22. National Defence University. Helsinki. ISBN 978-951-25-3126-4 (pdf). https://www.doria.fi/bitstream/handle/10024/176978/Vasara_FDS22_Theory%20of%20Reflexive%20Control%20%28web1%29-1.pdf

[12] Andrew, Christopher, Vasiliy Mitrokhin. *The Mitrokhin Archive: The KGB in Europe and the West*. Penguin, 2018. ISBN 978-0141989488

[13] NATO. (1949). *The North Atlantic Treaty.* https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty

[14] NATO. (2026). *Countering hybrid threats*. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

[15] NATO. (2026). *Countering hybrid threats*. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

[16] NATO. (2026). *Countering hybrid threats*. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

[17] AAP-06, ed. 6. 2021. *NATO glossary of terms and definitions.* https://www.collegesidekick.com/study-docs/5341783

[18] NATO. (2025a). *Deterrence and defence.* https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence

[19] Jones, Seth G. (2025). *Russia's Shadow War Against the West.* Center for Strategic and International Studies, 18 March 2025 https://www.csis.org/analysis/russias-shadow-war-against-west; Edwards, Charlie & Seidenstein, Nate. (2025) *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure.* International Institute for Strategic Studies. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf

[20] Frelin, Jan: (2026) *Theory-Based Assessment of Deterrence*, 2026. ISBN 978-92-837-2638-8. https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-196/MP-SAS-196-31.pdf; Mazarr, Michael J. (2018). *Understanding Deterrence*. RAND. DOI:10.7249/PE295. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf

[21] Charap, S. (2020). *Strategic Sderzhivanie: Understanding contemporary Russian approaches to "deterrence".* George C. Marshall European Center for Security Studies. https://www.marshallcenter.org/sites/default/files/files/2020-09/Security%20Insights%2062%20-%20Charap%20-%20RSI%20-%20Strategic%20Sderzhivanie%20-%20IMAGE%20IDEAS%20%28002%29.pdf

[22] Institute for the Study of War. (2026). *Russian phase zero operations in Europe, date range: September 9, 2025 to February 27,* 2026. https://understandingwar.org/map/russian-phase-zero-operations-in-europe-date-range-september-9-2025-to-february-27-2026/

[23] Charap, S. (2020).

[24] Hajdu, D. (Ed.). (2025). *Russia's crime-terror nexus: Criminality as a tool of hybrid warfare in Europe.* GLOBSEC – International Centre for Counter-Terrorism. https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf; Politico. (2026, March 18*). Russia's newest spy may be someone you know.* https://www.politico.eu/article/russia-newest-spy-may-be-someone-you-know-foreign-intelligence-sabotage/

[25] NATO. (2024).

[26] NATO. (2001). *Statement by the North Atlantic Council, 12 September 2001.* https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2001/09/12/statement-by-the-north-atlantic-council

[27] Aukia, Jukka & Kubica, Lucjan (2023). Russia and China as hybrid threat actors: The shared self-other dynamics. *Hybrid CoE Research Report No. 8*. ISBN 978-952-7472-70-5 (web). https://www.hybridcoe.fi/wp-content/uploads/2023/04/NEW_Hybrid_CoE_Research_Report_8_web.pdf

[28] Institute for the Study of War. (2026).

[29] Council of the European Union. (EUCO 2022). *Council conclusions on a framework for a coordinated EU response to hybrid campaigns.* https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

[30] Reuters. (2026, February 13). *German spy chief calls for more operational freedom to counter threats.* https://www.reuters.com/world/german-spy-chief-calls-more-operational-freedom-threats-2026-02-13/

[31] Brown, W., Kobzova, J., Popescu, N., & Torreblanca, J. I. (2026). *From shield to sword: Europe's offensive strategy for the hybrid age*. European Council on Foreign Relations. https://ecfr.eu/publication/from-shield-to-sword-europes-offensive-strategy-for-the-hybrid-age/

***

CORVINUS KÜLÜGYI ÉS KULTURÁLIS EGYESÜLET
corvinusculture.com