• *ANALYSIS*

NATO in the Technopolar World: "Deterrence, Norms and Challenges"

Erman Akilli

www.setav.org

20.yıl | SETA

JUNE 2026 NO 100

NATO IN THE TECHNOPOLAR WORLD: "DETERRENCE, NORMS AND CHALLENGES"

ERMAN AKILLI

SETA

SETA Yayınları
ISBN: 978-625-5703-51-4

Editorial Team: Ebrar Üzümcü, Sudib Sontoran
Layout: Said Demirtaş

SETA | SİYASET, EKONOMİ VE TOPLUM ARAŞTIRMALARI VAKFI
Nenehatun Cd. No: 66 GOP Çankaya 06700 Ankara TÜRKİYE
Tel: +90 312 551 21 00 | Faks: +90 312 551 21 90
www.setav.org | info@setav.org | @setavakfi

SETA | İstanbul
Defterdar Mh. Savaklar Cd. Ayvansaray Kavşağı No: 41-43
Eyüpsultan İstanbul TÜRKİYE
Tel: +90 212 395 11 00 | Faks: +90 212 395 11 11

SETA | Washington D.C.
1025 Connecticut Avenue, N.W., Suite 1106
Washington D.C., 20036 USA
Tel: 202-223-9885 | Faks: 202-223-6099
www.setadc.org | info@setadc.org | @setadc

SETA | Berlin
Kronenstraße 1, 10117 Berlin GERMANY
berlin@setav.org

SETA | Brussels
Avenue des Arts 27, 1000 Brussels BELGIUM
Tel: +3226520486

CONTENTS

> NATO will remain strategically relevant only if it adapts its deterrence logic, normative authority and internal cohesion to a security environment in which sovereignty also means the ability to govern algorithms, data corridors, compute infrastructures and cognitive ecosystems.

SUMMARY

This analysis examines NATO's future in the technopolar world, an international order increasingly shaped by artificial intelligence (AI), digital infrastructures, data flows, semiconductors, cloud systems and algorithmic authority. It argues that NATO's traditional sources of strength, including conventional military power, nuclear deterrence and institutional cohesion, remain essential but are no longer sufficient in a security environment where power is increasingly exercised through control over compute, data, models and cognitive infrastructures. In this context, NATO faces an integrated challenge composed of changing deterrence dynamics, the growing importance of responsible AI norms, technological asymmetry among allies and the rise of cognitive insecurity through disinformation, deepfakes and AI enabled manipulation.

The analysis situates these developments within the broader transformation from a military industrial security order to a technopolitical security order. Deterrence in this environment depends not only on the ability to retaliate, but also on the capacity to perceive threats autonomously, attribute attacks credibly and preserve sovereign control over digital and cognitive infrastructures. NATO's 2021 and 2024 AI strategies reflect this shift, moving from a primarily normative framework toward a more operational posture focused on generative AI, testing, evaluation, verification and validation. Yet the Alliance remains internally uneven, as some members possess mature AI strategies and advanced digital capabilities while others remain dependent on external models, infrastructures and regulatory templates. This internal digital asymmetry, reinforced by supply chain dependence on semiconductors, cloud infrastructure, critical minerals and advanced computing, represents one of the most significant challenges to Alliance cohesion.

Türkiye occupies a central place in this analysis as an ally that recognized the strategic importance of digital autonomy early and sought to transform AI from a technological instrument into a component of sovereign agency. Türkiye's National AI Strategy (2021-2025) and AI Action Plan (2026-2030) are presented as examples of a sovereignty centered approach that combines AI literacy, public data infrastructure, sovereign cloud capacity, national large language models and international norm entrepreneurship. The analysis concludes by proposing connected sovereignty as NATO's appropriate strategic posture in the technopolar world. Complete dependence undermines autonomous judgment, while autarky weakens cooperation and redundancy. NATO will remain strategically relevant only if it adapts its deterrence logic, normative authority and internal cohesion to a security environment in which sovereignty also means the ability to govern algorithms, data corridors, compute infrastructures and cognitive ecosystems.

INTRODUCTION

In the grim darkness of the Cold War years, the North Atlantic Alliance was built for a world whose currency of power could be counted in divisions, warheads and industrial output. For more than seven decades that arithmetic held, first against a bipolar adversary and then across a unipolar interval in which the Western narrative of military and economic primacy seemed settled. That world is now being displaced, crumbled by the challenges brought by the 21st century.

The decisive assets of contemporary competition are compute, data, models and the narratives that move through them. More importantly, this very competition and the actors who control these assets increasingly set the terms on which security itself is defined. Moreover, in the technopolar world[1], a systemic and structural reframing of the international order in which technological infrastructure, algorithmic authority and digital sovereignty have become the primary axes of geopolitical competition.

NATO therefore confronts an instrument and an era that no longer matches. The Alliance retains unmatched conventional and nuclear capability, yet the contest has migrated toward a domain where capability is necessary but no longer sufficient. This analysis argues that the challenge facing NATO is not a list of separate technological problems but a single integrated one with four faces. The first is a logic of deterrence the Alliance does not yet fully control. The second is a normative role it has only begun to claim. The third is an internal cohesion

1 Erman Akıllı, *Cognitive Diplomacy and Digital Autonomy: Statecraft in the Age of Artificial Intelligence*, Palgrave Macmillan, 2025, 25.

problem produced by deep and widening differences in technological capacity among allies. The fourth is a societal attack surface where the contested terrain is no longer territory but cognition. These four are aspects of one structural transformation, and they must be governed together. Throughout, the argument returns to Türkiye, an ally who recognized the stakes of this transformation early and who offers the Alliance both a working model and a norm entrepreneur from within.

THE TECHNOPOLAR WORLD AND THE TRANSFORMATION OF SECURITY

The concept of the technopolar world departs from and builds upon the more familiar idea of a technopolar moment[2]. Technopolar moment describes a transitional period in which a small number of technology firms come to rival states in their capacity to shape norms, public opinion and even geopolitical outcomes. The insight is valuable, but it is actor specific and temporally bounded, fixed to the rivalry between particular companies and particular governments at a particular instant. The technopolar world, by contrast, is not a moment but a standing condition. It is rooted in the deepening of the digital divide and is best understood as the international order adapting to a new and durable form of strategic imbalance, no longer organized around the ideological confrontation of the Cold War but around asymmetries in technological power[3].

That imbalance produces what earlier analyses term digital asymmetry[4], a structural reality in which the capacity to gather, process and govern digital systems is concentrated in a handful of dominant actors while the majority remain dependent, vulnerable and peripheral. The order divides into a technological core, composed of the states and corporate actors that dominate AI, advanced computing and semiconductor production, and a periphery that is structurally compelled to adopt standards and regulatory frameworks designed elsewhere. Sovereignty itself is being redefined in the process. It is no longer only the control of territory but the ability to act with digital autonomy, to make sovereign decisions over data, algorithms and infrastructures without coercion or compromise.

For an alliance, the implications are direct. The referent object of defense now extends beyond borders, airspace and sea lanes to include data corridors, cloud layers, model weights and the compute on which they run. An order whose founding logic predates its own primary axis of competition cannot simply add

2 Ian Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order", *Foreign Affairs*, 100(6), 2021.

3 Akıllı, *ibid*, 25-26.

4 Akıllı, *ibid*, 102.

technology to its agenda as one item among many. It must reconsider what it is defending and with what.

AI, DIGITAL INFRASTRUCTURE AND THE NEW LOGIC OF DETERRENCE

Deterrence has traditionally been discussed through the theoretical foundations laid by Thomas C. Schelling[5], whose conceptualization focused on the stark realities of brinkmanship. Accordingly, this framework was later formalized through Snyder's analysis of the *"chicken game"*[6] and Jervis's examination of Mutually Assured Destruction (MAD)[7], both of which target ultimate annihilation. However, deterrence in the technopolar world is harder to establish and harder to attribute than the deterrence the Alliance was designed to provide. Three features explain why traditional deterrence fails in this domain.

Deterrence in the technopolar world is harder to establish and harder to attribute than the deterrence the Alliance was designed to provide.

First, the attack surface is increasingly infrastructural and frequently falls below the threshold of armed forces. The submarine cable networks of the Red Sea offer the clearest illustration. Roughly seventeen of the world's submarine cables traverse that corridor, and it carries on the order of ninety percent of the data capacity between Europe and Asia[8]. An adversary who severs or degrades these arteries can paralyze financial settlement, cloud dependent commerce and logistics across three continents without firing a recognized shot. The damage can be obscured sixty meters underwater and attributed to a passing anchor or to seismic activity, exploiting what specialists call the attribution problem, the extreme difficulty of proving responsibility with the certainty that a deterrent threat requires[9]. As Schelling argues, deterrence rests on shaping the adversary's expectations by making the cost of aggression appear unacceptable, which requires both an identifiable opponent and a credible retaliatory commitment[10]. In other words, deterrence relies on the belief that threats prevent undesirable actions, but this very *"cost of living"* dissolves when the perpetrator can hide behind plausible deniability.

5 Thomas C. Schelling, *Arms and Influence*, New Haven: Yale University Press, 1966, 35–43.

6 Glenn H. Snyder, "'Prisoner's Dilemma' and 'Chicken' Models in International Politics," International Studies Quarterly 15 (1), 1971, 66-103.

7 Robert Jervis, The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon (Ithaca: Cornell University Press, 1989.

8 Alan Mauldin, "The Red Sea: A Key Subsea Cable Crossroads Under Siege", *TeleGeography*, 2024; Sean Monaghan, Michael Darrah, Eskil Jakobsen and Otto Svendsen, "Red Sea Cable Damage Reveals Soft Underbelly of Global Economy", *Center for Strategic and International Studies*, 2024; Erman Akıllı, "Hyper-Connectivity Put to Test: Israel/US and Iran War and Türkiye's Critical Role", *Anadolu Agency*, 2026.

9 Erman Akıllı, "Cutting Cables: How War in the Red Sea Could Trigger Digital Collapse", *Daily Sabah*, 2026.

10 Schelling, *ibid.*, 38.

Second, deterrence presumes that the deterring party can independently perceive the threat it intends to deter. Here the technopolar condition introduces a quieter vulnerability. When a state's algorithms, models and compute are externally controlled, the knowledge that state produces, is itself externally controlled[11]. This is epistemic dependency, a largely invisible condition that is more insidious than energy or supply dependency because it silently shapes threat assessment, foreign policy choice and strategic decision making[12]. An alliance that deters with borrowed models may not see, on its own terms, the danger it is meant to confront.

Third, NATO has taken real but partial steps. The Alliance recognized cyberspace as a domain of operations at the Warsaw Summit in 2016[13], elevating cyber threats toward the level of kinetic ones and bringing them within the logic of collective defense. These measures were necessary, yet they were designed for a narrower problem than the one now unfolding across the full stack of digital infrastructure. Capability without shared norms, moreover, is unstable, which is where the next face of the challenge begins.

RESPONSIBLE AI AND NATO'S NORMATIVE ROLE

NATO cannot out build the largest computing ecosystems, and it should not stake its relevance on trying. Its comparative advantage lies elsewhere, in its capacity to set norms for the responsible military use of AI. The Alliance has begun to claim this role. Its first AI strategy[14], adopted in October 2021, established six Principles of Responsible Use covering lawfulness, responsibility and accountability, explainability and traceability, reliability, governability and bias mitigation. NATO's AI Strategy underlined the critical necessity of maintaining technological autonomy and adopting responsible AI frameworks against sophisticated asymmetric threats.

Ultimately, the latest institutional push towards algorithmic resilience against sophisticated asymmetric threats was solidified during the 2024 Washington Summit, which underscores the imperative of securing sovereign computational capabilities within the Alliance. The revised strategy[15] released at the Washington

11 Akıllı, *Cognitive Diplomacy and Digital Autonomy*, 2025, 13-14.

12 Akıllı, 2026.

13 NATO, Warsaw Summit Communiqué, NATO Official Texts (July 9, 2016), https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

14 NATO, "NATO Artificial Intelligence Strategy", NATO Official Texts (October 22, 2021), https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy.

15 NATO, "NATO's Revised Artificial Intelligence (AI) Strategy", NATO Official Texts (July 10, 2024), https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy.

Summit in July 2024, took account of generative AI and of AI enabled information tools, named such tools as a concern for the first time, and committed the Alliance to building a testing, evaluation, verification and validation capacity drawing on the network of test centers associated with the Defense Innovation Accelerator for the North Atlantic.

The evolution between NATO's 2021 and 2024 AI strategies clearly demonstrates how rapidly the global technopolitical paradigm is shifting. The inaugural 2021 strategy served as a largely normative framework, positioning AI within the broader lexicon of emerging technologies while prioritizing the establishment of six core ethical principles. In contrast, the 2024 revised strategy reflects a decisive shift toward an operational and proactive defense doctrine, triggered by the asymmetric challenges of generative AI and large language models. While the initial document introduced initiatives like DIANA and the NATO Innovation Fund as visionary concepts, the 2024 update cements them as operationalized pillars designed to secure allied interoperability and data sovereignty. Ultimately, the alliance has transitioned from a phase of normative conceptualization to a pragmatic posture, treating AI not merely as an emerging capability, but as a critical geopolitical shield within the contemporary cognitive and cyber domains.

> NATO's value in this contest is to act not only as a military organization but as a normative one, anchoring the responsible use of military AI in law and democratic accountability.

Nonetheless, among the principles of NATO's AI Strategy, governability carries particular weight for deterrence and escalation control. It requires that applications allow appropriate interaction between humans and machines, that they permit the detection and avoidance of unintended consequences, and that they preserve the ability to disengage or deactivate systems that behave in unintended ways[16]. This represents the institutional expression of AI in statecraft, establishing that technology must augment human judgment rather than substitute for it, thereby keeping the human firmly in the loop[17].

The wider contest over AI norms is genuinely open. One pole, expressed in the human rights grounded approach of the UNESCO Recommendation on the Ethics of AI adopted by acclamation across the membership in November 2021[18], emphasizes human oversight, transparency and fairness. Another pole advances a model of cyber sovereignty in which states claim absolute jurisdiction over digital governance within their borders, directly challenging the vision of a unified global network. This fracturing of the digital domain represents the

16 UNESCO, Recommendation on the Ethics of Artificial Intelligence, UNESCO Official Texts (November 23, 2021), https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

17 OECD, "OECD.AI Policy Observatory: Dashboards on National AI Policies and Data," OECD Artificial Intelligence, accessed June 21, 2026, https://oecd.ai/en/dashboards.

18 UNESCO, *ibid.*

onset of what contemporary diplomatic discourse conceptualizes as *Pax Silica*[19]. NATO's value in this contest is to act not only as a military organization but as a normative one, anchoring the responsible use of military AI in law and democratic accountability. This normative posture is where Türkiye's contribution becomes visible, for she has positioned herself as a state seeking to shape rather than merely receive these standards.

NATIONAL AI STRATEGIES ACROSS THE ALLIANCE: A COMPARATIVE MAP

Beneath the Alliance's collective normative posture lies a strikingly uneven national landscape. The claim that NATO can shape standards for responsible AI assumes that its members are governing technology in broadly comparable ways. However, the diverse array of AI policy frameworks adopted across the thirty-two member states whether national strategies, action plans, or dedicated regulations fails to bear this assumption out. It reveals instead a spectrum that runs from early frameworks revised across several generations to drafts still in consultation, and in a few cases to the absence of any standalone document at all.

At one end stand the early movers. Türkiye sits within this early adopting group through her National AI Strategy for the years 2021 to 2025[20], and she is among the very few allies to have moved already to a second-generation text, Türkiye's AI Action Plan[21] for the years 2026 to 2030. Canada[22] adopted the world's first national AI strategy in 2017 and has since renewed it[23], while Finland[24], France[25], Germany[26] and Sweden[27] all published strategies between 2017 and 2018. Several of these states have revised their frameworks once or twice, with Czechia[28],

19 "Pax Silica Summit," U.S. Department of State, Fact Sheet, December 11, 2025, https://www.state.gov/pax-silica

20 "Ulusal Yapay Zekâ Stratejisi (2021-2025) ile İlgili 2021/18 Sayılı Cumhurbaşkanlığı Genelgesi", T.C. Resmî Gazete, Sayı: 31574, 20 Ağustos 2021, s. 1, https://www.resmigazete.gov.tr/eskiler/2021/08/20210820-22.pdf; OECD.AI Policy Observatory, "Türkiye's National AI Strategy," OECD.AI Policy Navigator, updated December 25, 2025, https://oecd.ai/en/dashboards/policy-initiatives/national-ai-strategy-6021

21 "Türkiye Yapay Zekâ Eylem Planı Açıklandı", T.C. Sanayi ve Teknoloji Bakanlığı, 13 Haziran 2026, https://www.sanayi.gov.tr/medya/haber/turkiye-yapay-zek%C3%A2-eylem-plani-aciklandi

22 Canadian Institute for Advanced Research (CIFAR), Pan-Canadian Artificial Intelligence Strategy, March 2017, https://www.cifar.ca/ai/pan-canadian-artificial-intelligence-strategy.

23 Innovation, Science and Economic Development Canada (ISED), "Canada's National Artificial Intelligence Strategy: AI for All," Government Official Official Statements, accessed June 21, 2026, https://ised-isde.canada.ca/site/ised/en/canadas-national-artificial-intelligence-strategy-ai-all.

24 Ministry of Economic Affairs and Employment of Finland, Finland's Age of Artificial Intelligence, December 2017, https://tem.fi/en/artificial-intelligence-programme.

25 Cédric Villani, *For a Meaningful Artificial Intelligence: Towards a French and European Strategy*, March 2018, https://www.aiforhumanity.fr

26 Bundesregierung, Strategie Künstliche Intelligenz der Bundesregierung, November 2018, https://www.ki-strategie-deutschland.de

27 Government Offices of Sweden, National Approach for Artificial Intelligence, May 2018, https://www.government.se

28 Ministry of Industry and Trade of the Czech Republic, Národní strategie umělé inteligence České republiky 2024, 2024, https://www.mpo.cz/en/guidepost/news/national-ai-strategy-of-the-czech-republic

Denmark[29] and Spain[30] among those issuing updated texts in 2024. A large middle group adopted dedicated strategies between 2019 and 2021, among them the Netherlands[31], Estonia[32], Lithuania[33], Luxembourg[34], Portugal[35], Poland[36], Latvia[37], Hungary[38], Bulgaria[39], Norway[40], Slovenia[41], the United Kingdom[42] and the United States[43], with the last two adding fresh action plans in 2025. A wave of recent adopters has followed, with Italy[44], Romania[45], Greece[46] and Iceland[47] all formalizing national documents in 2024.

A smaller set of members addresses AI inside broader digital transformation strategies rather than through a dedicated instrument. Slovakia situates its AI measures within the Strategy of the Digital Transformation of Slovakia 2030[48], and Croatia, while preparing a dedicated National Plan for the Development of AI to 2032, has so far governed the field largely through its Digital Croatia

29 Ministry of Digital Government, National Strategy for Artificial Intelligence - Strategic Update 2024, 2024, https://digmin.dk/en

30 Ministerio de Digitalización y Función Pública, Estrategia de Inteligencia Artificial 2024, May 2024, https://portal.mineco.gob.es/es-es/digitalizacionIA/Documents/Estrategia_IA_2024.pdf

31 Ministry of Economic Affairs and Climate Policy, Strategic Action Plan for Artificial Intelligence, October 2019, https://www.government.nl/documents/strategic-action-plan-for-artificial-intelligence

32 Government Office of Estonia, Estonian National AI Strategy (Kratt Report) 2019–2021, July 2019, https://www.kratid.ee/en

33 Ministry of the Economy and Innovation, Lithuanian Artificial Intelligence Strategy: A Vision of the Future, April 2019, https://eimin.lrv.lt/en

34 Department of Media, Connectivity and Digital Policy, Artificial Intelligence: a strategic vision for Luxembourg, November 2019, https://digital-luxembourg.public.lu

35 Ministry of Science, Technology and Higher Education, AI Portugal 2030: An Innovation and Growth Strategy, April 2019, https://www.portugal.gov.pt

36 Chancellery of the Prime Minister, Policy for the Development of Artificial Intelligence in Poland from 2020, shadows of EU directives, December 2020, https://www.gov.pl/web/ai

37 Ministry of Environmental Protection and Regional Development, On the Development of Artificial Intelligence Solutions, February 2020, https://www.varam.gov.lv/en

38 Ministry for Innovation and Technology, Hungary's Artificial Intelligence Strategy 2020–2030, September 2020, https://ai-coalition.hu/en

39 Ministry of Transport, Information Technology and Communications, National Strategic Framework for the Development of Artificial Intelligence in Bulgaria until 2030, December 2020, https://www.mtitc.government.bg

40 Ministry of Local Government and Modernisation, National Strategy for Artificial Intelligence, January 2020, https://www.regjeringen.no/en/documents/national-strategy-for-artificial-intelligence/

41 Government Office for Digital Transformation, National Programme for Artificial Intelligence (NpUI) until 2025, May 2021, https://www.gov.si/en

42 Department for Science, Innovation and Technology (DSIT), AI Opportunities Action Plan, January 13, 2025, https://www.gov.uk/government/publications/ai-opportunities-action-plan

43 The White House, "America's AI Action Plan," Government Official Statements, July 2025, https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

44 Agenzia per l'Italia Digitale (AgID), Strategia Italiana per l'Intelligenza Artificiale 2024–2026, March 2024, https://www.agid.gov.it

45 Ministerul Cercetării, Inovării și Digitalizării, Strategia Națională în domeniul Inteligenței Artificiale 2024-2027, 2024, https://www.mcid.gov.ro

46 Ministry of Digital Governance, Blueprint for Greece's AI Transformation: High-Level Advisory Committee Report, November 2024, https://mindigital.gr

47 Ministry of Higher Education, Innovation and Industry, Stefna Íslands um gervigreind (Iceland's AI Policy Framework), 2024, https://www.stjornarradid.is

48 Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization, "Strategy of the Digital Transformation of Slovakia 2030," Slovak Government Official Statements, October 2019, https://www.mirri.gov.sk/wp-content/uploads/2019/10/SDT-English-Version-FINAL.pdf

Strategy 2032[49]. The three most recent members in the Western Balkans are at an earlier stage still. Albania[50] opened a draft National AI Strategy for the years 2025 to 2030 to public consultation in 2025, Montenegro[51] presented a first AI Readiness Assessment in 2025 ahead of drafting a strategy, and North Macedonia[52] has no adopted standalone strategy, treating AI as a priority within its information and communication technology strategy.

The asymmetry within the Alliance is not only a matter of hardware and compute, as the supply analysis will show,but also of normative and strategic maturity.

Three conclusions follow, and each feeds the cohesion argument. First, the asymmetry within the Alliance is not only a matter of hardware and compute, as the supply analysis will show, but also of normative and strategic maturity. Around twenty seven of the thirty two members have adopted a dedicated national AI document, yet some have iterated through three generations of policy while others are drafting their first. Second, a strategy on paper is not a capacity in the field. Several states with sophisticated documents still run their models and their compute on foreign infrastructure, so that epistemic dependency persists even among the strategy rich, while the lighter footprint of the smallest members reflects scale and stage rather than neglect, with the European Union candidates among them converging through the EU AI Act[53].

Third, and most consequential for the Alliance, shared standards are harder to build when members sit at such different stages and when several of them effectively outsource their normative templates, whether to the EU AI Act or to whichever foreign models they deploy. Within this landscape Türkiye's trajectory is notable not for being typical but for being among the most advanced[54], an early adopter that has already moved to a sovereignty centered successor while several allies remain at the drafting stage. The unevenness mapped here is the substrate of the cohesion problem examined next.

49 Central State Office for the Development of the Digital Society, "Strategy Digital Croatia for the Period until 2032," Government of the Republic of Croatia, Official Translation, accessed June 21, 2026, https://mpudt.gov.hr/UserDocsImages/RDD/SDURDD-dokumenti/Strategija_Digitalne_Hrvatske_final_v1_EN.pdf

50 Council of Ministers of the Republic of Albania, "Decision of the Council of Ministers (DCM) No. 606, Dated 23.10.2025," National Authority for Electronic Certification and Cyber Security (AKSK), Official English Translation, January 2026, https://aksk.gov.al/wp-content/uploads/2026/01/DCM-no.-606-dated-23.10.-2025_English.pdf

51 UNDP Montenegro, "Artificial Intelligence Landscape Assessment (AILA)," United Nations Development Programme Publications, 2025, https://www.undp.org/montenegro/publications/artificial-intelligence-landscape-assessment-aila

52 Ministry of Digital Transformation of the Republic of North Macedonia, "Strategy for Development of ICT - SMART MK 2030," National Strategic Documents, accessed June 21, 2026, https://portal.mdt.gov.mk/post-body-files/strategija-za-razvoj-na-ikt-smart-mk-2030-file-mBdU.pdf

53 European Union, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)," Official Journal of the European Union, L 2024/1689, July 12, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689

54 Murat Yeşiltaş, "Türkiye's AI Strategy and the Coming Technological Order," Daily Sabah, June 16, 2026, accessed June 21, 2026, https://www.dailysabah.com/opinion/columns/turkiyes-ai-strategy-and-the-coming-technological-order; Erman Akıllı, "Teknokutup Çağda Türkiye'nin Yapay Zekâ Eylem Planı (2026-2030)," SETA Odak, 15 Haziran 2026, https://www.setav.org/teknokutup-cagda-turkiyenin-yapay-zeka-eylem-plani-2026-2030.

TECHNOLOGICAL ASYMMETRY AND THE CHALLENGE OF ALLIANCE COHESION

The fault line that most threatens NATO runs inside it. Allies differ in technological capacity not merely by degree but by kind. Some are producers and standard setters, while others are consumers structurally dependent on technologies designed and governed elsewhere. Applied to an alliance, epistemic dependency becomes an 'interoperability problem'[55] of a deeper sort than the one usually discussed. Divergence in models, clouds and data governance fragments not only technical systems but situational awareness itself, eroding the common operating picture that collective defense presumes. Allies who interpret the same events through different and externally supplied analytical layers may not arrive at a shared understanding of what is happening, let alone of what to do.

Asymmetry within the Alliance is therefore a deterrence problem and not only a fairness problem. An adversary chooses the least autonomous member as the point of entry, and the credibility of collective defense is set by its weakest digital link rather than by its strongest. The structural arrangements of the wider technological order sharpen this internal divide, as the next section shows, by ranking states, including NATO members, according to their place in supply chains they do not control.

SUPPLY CHAIN DEPENDENCE AND THE GEOPOLITICS OF CRITICAL TECHNOLOGIES

The asymmetry inside the Alliance is reinforced by the geometry of the technologies on which it depends. The most advanced semiconductors are fabricated almost exclusively in a few locations, principally by leading firms in Taiwan[56] and South Korea[57], while the extreme ultraviolet lithography equipment indispensable to leading edge production is effectively monopolized by a single Dutch company[58]. Each chokepoint is a potential instrument of coercion, and the con-

55 However, interoperability should be strengthened as a core capacity for NATO members, as stated in the revised AI Strategy of 2024. For details: NATO, "NATO's Revised Artificial Intelligence (AI) Strategy", NATO Official Texts (July 10, 2024), https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

56 Taiwan - Semiconductors Including Chip Design for AI," International Trade Administration, U.S. Department of Commerce, last modified December 1, 2025, https://www.trade.gov/country-commercial-guides/taiwan-semiconductors-including-chip-design-ai

57 "SK Hynix says ships samples of 12-layer next-gen HBM4E chips to major customers," Reuters, June 18, 2026, https://www.reuters.com/world/asia-pacific/sk-hynix-says-ships-samples-12-layer-next-gen-hbm4e-chips-major-customers-2026-06-17/; Semiconductor Industry in Korea," Invest KOREA, Korea Trade-Investment Promotion Agency (KOTRA), 2023, https://www.investkorea.org/ik-en/cntnts/i-312/web.do

58 John VerWey, "Tracing the Emergence of Extreme Ultraviolet Lithography: Lessons for Identifying, Protecting, and Promoting the Next Emerging Technology," Center for Security and Emerging Technology (CSET) Policy Brief, July 2024, p. 7, 9, https://cset.georgetown.edu/wp-content/uploads/CSET-Tracing-the-Emergence-of-Extreme-Ultraviolet-Lithography.pdf

centration of the most advanced fabrication near a contested strait constitutes what many analysts describe as a single point of failure in the global economy. Major powers have responded with national strategies, from large subsidy programs to coordinated export controls, yet none has achieved full domestic capacity, and the dependency remains[59].

This supply geometry is now being institutionalized into a geopolitical hierarchy. *The Pax Silica*[60] initiative launched by the United States Department of State in December 2025, its flagship effort on AI and supply chain security, organizes a coalition of trusted partners around secure access to critical minerals, semiconductors, compute and energy, explicitly in order to reduce coercive dependencies[61]. This initiative convert technological cooperation from a universal development good into a geopolitical filtering mechanism that sorts states into tiers, deepening digital asymmetry and pushing the excluded toward the periphery[62]. The point of consequence for the Alliance is that the inaugural *Pax Silica* declaration was signed by eleven states, and Türkiye, a NATO ally, was not among them.[63] An alliance whose cohesion depends on rough parity among members cannot be insulated from a supply order that ranks those same members. The lesson for an excluded ally is not to wait for inclusion but to build sovereign capability, a lesson Türkiye has drawn.

COGNITIVE INSECURITY, DISINFORMATION AND SOCIETAL RESILIENCE

The softest target in the technopolar world is the human mind, and it is here that the framework of cognitive diplomacy supplies the answering logic. Cognitive diplomacy[64] is the deliberate integration of human and machine intelligence to influence how information is received, interpreted and acted upon across borders, organized around three pillars, presence, practice and resilience, that together serve the larger goal of digital autonomy. In this account the state is no longer only a geopolitical actor but a cognitive agent that shapes and safeguards the informational environments in which political agency, legitimacy and consent are formed.

59 Chris Miller, *Chip War: The Fight for the World's Most Critical Technology*, New York: Scribner, 2022.

60 "Pax Silica Summit", U.S. Department of State, Fact Sheet, 11 December 2025, https://www.state.gov/pax-silica

61 Erman Akıllı, "Pax Silica and Türkiye's Choice in the Age of Computing Power," SETA, 2026, https://www.setav.org/en/pax-silica-and-turkiyes-choice-in-the-age-of-computing-power

62 Akıllı, 2025, 181.

63 Pax Silica Summit, *ibid.*

64 Akıllı, 2025.

The threat is acute and documented. Deepfakes, synthetic personas and narrowly targeted influence operations[65] now challenge the narrative integrity and public trust on which the will to defend ultimately rests. The fabricated 2022 video purporting to show a Ukrainian surrender, though quickly exposed, demonstrated how synthetic media can distort battlefield perception and mislead decision making[66]. The resilience pillar of cognitive diplomacy answers this with a deliberate division of labor between machine and human. AI can detect coordinated inauthentic behavior and disinformation patterns at scale, but attribution and strategic response must remain under human control, a principle that NATO's own strategic communications work has likewise affirmed[67]. Societal resilience completes the picture. The models pioneered by states such as Estonia, which embed media literacy across society and pair civic preparedness with technical defense, show that resilience is at once technical and societal[68]. For an alliance whose collective defense was written for armed attack, defending the cognitive domain against assaults that fall below that threshold is now a capability of the first order.

> The claim NATO must hear is therefore not that Türkiye seeks autonomy apart from the Alliance, but that a capable ally who converts dependency into agency strengthens collective resilience rather than straining it.

TÜRKİYE'S AI ACTION PLAN, DIGITAL SOVEREIGNTY AND NATO'S FUTURE ADAPTATION

Türkiye recognized the logic of the technopolar world early and drew the appropriate conclusion, that digital autonomy is a precondition of political autonomy rather than a luxury that follows from it. Her National AI Action Plan[69] for the period 2026 to 2030, announced in İstanbul in June 2026 by President Recep Tayyip Erdoğan, sets out this ambition across four axes rendered as perceive, harness, forge and govern[70]. The plan establishes a national literacy program reaching across all eighty-one provinces with the aim of training five million citizens within two years, alongside ten thousand advanced specialists and one

65 House of Commons Foreign Affairs Committee, Disinformation Diplomacy: How Malign Actors Are Seeking to Undermine Democracy, Fourth Report of Session 2024–26, HC 703, London: House of Commons, 2026, https://committees.parliament.uk/publications/52401/documents/290829/default/

66 "Deepfake footage purports to show Ukrainian President capitulating," Reuters, March 16, 2022, https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/

67 "Riga StratCom Dialogue 2026 Set to Take Place from 3 to 4 June 2026 in Riga, Latvia," NATO Strategic Communications Centre of Excellence (StratCom COE), 2026, https://stratcomcoe.org/events/riga-stratcom-dialogue-2026-set-to-take-place-from-3-to-4-june-2026-in-riga-latvia/90

68 Cybersecurity Education in Estonia: From Kindergarten to NATO Cyber Defence Centre," e-Estonia Briefing Centre, https://e-estonia.com/cybersecurity-education-in-estonia-from-kindergarten-to-nato-cyber-defence-centre/

69 Yeşiltaş, *ibid.*

70 Akıllı, "Teknokutup Çağda Türkiye'nin Yapay Zekâ Eylem Planı".

hundred thousand applied professionals. It opens a National Data Library of at least two thousand public data sets in fields including health, agriculture, defense and electronic commerce, raises the national data center capacity toward at least one gigawatt by 2030, and commits no less than two percent of the public investment program to AI projects, with the state acting as first buyer and reference for domestic solutions[71].

The producing axis is where sovereignty becomes concrete. The sovereign large language model *Bilge*, developed by the TUBITAK, sits alongside efforts from the country's defense and technology firms, expressing the conviction that a state which cannot build its own model cannot compose its own sentences in the digital world. The governing axis is the most strategically significant. Through a substantial sovereign cloud and data center mobilization and through active engagement at the OECD, the United Nations and the G20, Türkiye seeks to act as a norm entrepreneur rather than a norm taker. The most far reaching element is the initiative, pursued with the Organization of Turkic States, to develop a shared Turkic large language model spanning the Oghuz, Kipchak and Karluk branches of the language family. This is not a cultural project wearing a technological label. It is an act of epistemic entrepreneurship[72], an attempt to shape the cognitive infrastructure of a vast geographic space before that space is absorbed into model architectures designed in San Francisco or Shenzhen.

These are stated objectives rather than completed achievements, and they should be read as the deliberate reflex of a capable state rather than as accomplished facts. Their direction, however, is unmistakable, and it carries a structural contribution to the Alliance. As earlier analysis of the Red Sea vulnerabilities argued, Türkiye's data localization and domestic infrastructure already cushion her against shocks that would cripple wholly cloud dependent neighbors, and her potential to serve as a terrestrial digital corridor, flanking the planned overland routes between Asia and Europe, offers the wider system a secure alternative to contested maritime chokepoints[73]. The claim NATO must hear is therefore not that Türkiye seeks autonomy apart from the Alliance, but that a capable ally who converts dependency into agency strengthens collective resilience rather than straining it.

CONCLUSION: NATO'S TECHNOPOLAR FUTURE

Türkiye case generalizes into a single governance principle for the Alliance. Resilience in the technopolar world is best understood as connected sovereignty, a

71 *Ibid.*

72 *Ibid.*

73 Akıllı, "Cutting Cables: How War in the Red Sea Could Trigger Digital Collapse".

balance between autonomy and strategic interdependence rather than a choice between dependence and isolation. In the technopolar world, neither pole serves the Alliance. Complete dependence undermines the capacity for autonomous judgment, whereas autarky sacrifices the benefits of cooperation, diversification and systemic redundancy. The Alliance shall execute four distinct yet interconnected steps to realize and secure its position in the technopolar world.

First, the Alliance should consolidate shared norms for the responsible use of military AI, building on its principles of responsible use so that the human judgment preserved by the governability principle becomes a common standard rather than an uneven national practice. Second, it should treat redundancy and diversity in critical infrastructure and supply as collective defense tasks, recognizing that a corridor or a chokepoint failing for one ally degrades the whole. Third, it should establish sovereign capability floors so that the least autonomous member does not set the deterrent value of the entire Alliance. Fourth, it should institutionalize cognitive resilience as a standing function, pairing the machine scale detection of manipulation with human control over attribution and response and with the society wide literacy that sustains public trust. Governance designed along these lines would treat the four faces of the technopolar challenge as the single problem they are.

This strategic pivot effectively bridges the operational gap identified at the outset. Deterrence, norms and cohesion in the technopolar world all rest on the same foundation, namely who controls the digital and cognitive infrastructure of security. An alliance that grasps this can adapt its deterrent logic to infrastructure and attribution, claim a normative role commensurate with its values, repair the asymmetries that divide its members, and defend the cognitive domain on which consent depends. An alliance that does not will find its conventional and nuclear strength intact yet increasingly beside the point.

Türkiye stands as the proof that the technopolar order rewards states which build agency early. By treating digital autonomy as the precondition of political autonomy, by investing in sovereign models and infrastructure, and by reaching for the role of norm entrepreneur from the Balkans to Central Asia, she demonstrates a path that strengthens the Alliance from within. NATO's technopolar future depends on whether the Alliance as a whole can internalize this systemic logic across its entire membership, moving past fragmented national frameworks to embrace a unified strategic posture. Ultimately, the survival of the Alliance hinges on its capacity to redefine sovereignty in this tech-driven era, recognizing it not merely as the Westphalian defense of physical borders, but as the absolute capacity to govern algorithms, data corridors, and the sovereign compute architectures upon which the modern international order now rests.

ERMAN AKILLI

Prof. Dr. Erman Akıllı is currently serving as a faculty member in the Department of International Relations at Ankara Hacı Bayram Veli University. His areas of expertise include artificial intelligence in foreign policy, digital diplomacy, the Turkic World, the Africa region, public diplomacy, and its sub-branches. Throughout his academic career, he has published articles in peer-reviewed journals indexed in SSCI and WOS; and has contributed as an author and editor to books published by prestigious publishing houses such as Routledge, Palgrave MacMillan, and Springer Nature. Additionally, he continues his work as an assistant editor for the Insight Turkey journal published by SETA Foundation.

NATO in the Technopolar World: "Deterrence, Norms and Challenges"

Erman Akilli

This analysis examines NATO's future in the technopolar world, an international order increasingly shaped by artificial intelligence (AI), digital infrastructures, data flows, semiconductors, cloud systems and algorithmic authority. It argues that NATO's traditional sources of strength, including conventional military power, nuclear deterrence and institutional cohesion, remain essential but are no longer sufficient in a security environment where power is increasingly exercised through control over compute, data, models and cognitive infrastructures. In this context, NATO faces an integrated challenge composed of changing deterrence dynamics, the growing importance of responsible AI norms, technological asymmetry among allies and the rise of cognitive insecurity through disinformation, deepfakes and AI enabled manipulation.

The analysis situates these developments within the broader transformation from a military industrial security order to a technopolitical security order. Deterrence in this environment depends not only on the ability to retaliate, but also on the capacity to perceive threats autonomously, attribute attacks credibly and preserve sovereign control over digital and cognitive infrastructures. NATO's 2021 and 2024 AI strategies reflect this shift, moving from a primarily normative framework toward a more operational posture focused on generative AI, testing, evaluation, verification and validation. Yet the Alliance remains internally uneven, as some members possess mature AI strategies and advanced digital capabilities while others remain dependent on external models, infrastructures and regulatory templates. This internal digital asymmetry, reinforced by supply chain dependence on semiconductors, cloud infrastructure, critical minerals and advanced computing, represents one of the most significant challenges to Alliance cohesion.

Türkiye occupies a central place in this analysis as an ally that recognized the strategic importance of digital autonomy early and sought to transform AI from a technological instrument into a component of sovereign agency. Türkiye's National AI Strategy (2021-2025) and AI Action Plan (2026-2030) are presented as examples of a sovereignty centered approach that combines AI literacy, public data infrastructure, sovereign cloud capacity, national large language models and international norm entrepreneurship. The analysis concludes by proposing connected sovereignty as NATO's appropriate strategic posture in the technopolar world. Complete dependence undermines autonomous judgment, while autarky weakens cooperation and redundancy. NATO will remain strategically relevant only if it adapts its deterrence logic, normative authority and internal cohesion to a security environment in which sovereignty also means the ability to govern algorithms, data corridors, compute infrastructures and cognitive ecosystems.

20.yıl | SETA

ANKARA • İSTANBUL • WASHINGTON D.C. • BERLİN • BRUSSELS

www.setav.org