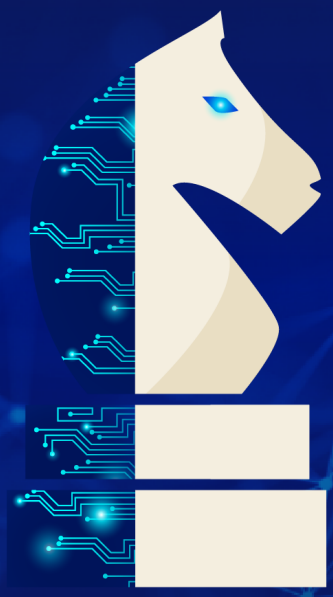
"Those who have the privilege to know, have the duty to act."— Albert Einstein

GEOSTRATEGIC PULSE

No. 309 July - August 2026 | www.pulsulgeostrategic.ro



BILINGUAL-BIMONTHLY PUBLICATION OF GEOPOLITICAL ANALYSIS

office@pulsulgeostrategic.ro

CONTENT

CONTENT

EDITORIAL

Minilateralism is the Method and Multipolarism is the SystemicFinal Result for the New World Order

PhD. Eng. Stelian TEODORESCU (Romania)

"The first principle in life: never give up on people or events."
Marie Curie

In the context of current regional and global developments, we can say that the global order is undergoing one of the most profound transformations since the end of the Cold War. Geopolitical fragmentation, disruptions in the supply chain of various resources, climate risks, technological competition and the increasing gaps in development financing have exposed the limits of the multilateral architecture that existed until recently. As a result, it is more necessary than ever to analyze in detail this minilateralism that characterizes the entire world today and involves the formation of small groups of countries that cooperate in the field of various interests categorized as strictly common interests in economic, technological or defense and security terms specific exclusively to their own interests and not to the common interests promoted by major international institutions, such as the UN, which has lost enormously of its decision-making role at the international level. Some of these groups that highlight minilateralism are:

Source: https://www.fairobserver.com/economics/the-agency-of-middle-powers-in-a-fragmented-and-polarized-world/

• *The Shanghai Cooperation Organization (SCO)* - was founded in 2001 in Shanghai by China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. By 2026, it had grown to ten member states—India and Pakistan joined in 2017, Iran in 2023, and Belarus in 2024—with Afghanistan and Mongolia as observer states and fifteen dialogue partners. Kyrgyzstan assumed the rotating chairmanship after the SCO summit in Tianjin in 2025, adopting the theme "25 Years of the SCO: Together for Peace, Development, and Sustainable Prosperity". The Bishkek summit, held from August 31 to September 1, coincided with the opening of the sixth edition of the World Nomad Games in Kyrgyzstan on August 31.

• *CRINK (China, Russia, Iran, North Korea)* - operates as a transactional, informal, alignment of convenience, rather than a formal unified bloc, helping member states circumvent international sanctions and coordinate geopolitical opposition.

• *The Mecca Joint Defense Agreement between Türkiye, Saudi Arabia, and Pakistan* – signed on August 7, 2026, establishing a trilateral security pact in which an attack on one of these countries is considered an attack on all and addressing immediate regional threats, a perceived lack of reliability of traditional US security guarantees, and local deterrence. China is closely following the emerging defense partnership between Saudi Arabia, Turkiye, and Pakistan, a security framework that could reshape the strategic dynamics in the Middle East and South Asia. In this context, it is noteworthy that Chinese Foreign Minister Wang Yi expressed his strong support for the agreement, while signaling Beijing's interest in working with the

three countries. Although the pact has been widely discussed as a potential "Islamic NATO," it is not officially a NATO-like military alliance. However, closer defense coordination between Saudi Arabia, Türkiye, and Pakistan could lay the foundation for a broader security network encompassing key parts of Eurasia.

• *BRICS* - operates on a larger scale, but much of its practical work relies on minilateral economic coordination, alternative financial mechanisms, and localized currency settlements between groups of member states. Starting in August 2026, under the Indian presidency, with the theme "Building for Resilience, Innovation, Cooperation, and Sustainability," BRICS comprises 11 full member states and 10 partner countries. Recent assessments highlight the bloc's growing economic weight—accounting for over 35 percent of global GDP and an estimated 46-48 percent of the world's population—and its ongoing transition toward a functioning infrastructure and sovereignty platform for the Global South.

The 18th BRICS Summit took place on September 12–13, 2026, under India's presidency; notably, in the lead-up to the event in New Delhi, an agenda centered on resilience and institutional reform had already been brought to the forefront:

Focusing on the official theme for 2026—"Building for Resilience, Innovation, Cooperation, and Sustainability"—BRICS member states concentrated particularly on adapting the bloc and global governance networks to withstand current economic and geopolitical shocks.

The BRICS bank, the New Development Bank (NDB), is consolidating its position as an alternative financial pillar for developing economies, operating under its medium-term strategy (2022–2026). The NDB operates as an entity extended beyond the BRICS political format, integrating new approved members (such as Colombia, Uzbekistan, Bangladesh, UAE, Egypt and Algeria) to provide financing dedicated exclusively to the Global South. In July 2026, the NDB successfully issued a benchmark bond worth USD 1.75 billion (3-year maturity, listed on the London Stock Exchange and Nasdaq Dubai), the issue being oversubscribed 1.8 times. This demonstrates the solid confidence of global institutional investors, despite the restrictions maintained on projects in the Russian Federation.

Although the format of these aforementioned groups seems to be a mini-lateral one, their cumulative impact is fundamental to the intensification of multipolarity that the world is facing today.

• They actively dilute the hegemony of other states by creating diplomatic, financial and military architectures as new alternatives for a world order that is in a full process of accelerated and unpredictable change.

• They strongly reflect the policies of great and middle powers that shape their strategic autonomy, regional self-sufficiency and regionally localized security networks.

In short, minilateralism is the method, while multipolarism is the systemic final result.

For example, the BRICS and CRINK highlight and confirm as accurately as possible both multipolarism and minilateralism. These types of groupings use minilateral methods (small, flexible coalitions) to pursue a broader multipolar global order, through which the dominance of the major Western actors is reduced, but we must recognize that the role of international institutions and organizations is accentuated, giving rise, at the same time, to an anarchism that has become almost impossible to control.

<u>Highlighting multipolarism</u>

• Common purpose: Both configurations explicitly or functionally aim to end a unipolar international order.

• Global rebalancing: BRICS acts as a diplomatic and economic vehicle for the Global South to assert its independent power.

• Strategic alignment: CRINK functions as a network of revisionist states that counter Western sanctions and security frameworks.

<u>Highlighting minilateralism</u>

• Flexible formats: Rather than universal and comprehensive treaties, these are based on transactional and targeted cooperation between selected capitals.

• Practical convergence: These coordinate where interests overlap - such as energy trade, sanctions evasion or diplomatic vetoes - without requiring total ideological or institutional conformity.

• Sub-global coalitions: These function as "small circles" or limited clubs that work outside traditional global governance structures.

As a result of the accelerated and often unpredictable developments in today's world, the growing importance of economic, technological, artificial intelligence and resilience capabilities has also emerged as a recurring theme in the intense discussions and debates that regularly take place at regional and global levels.

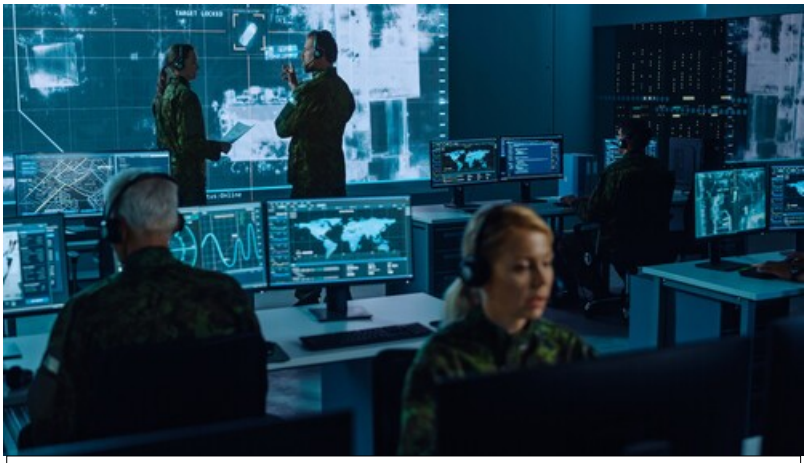
RESILIENCE IN THE MULTIPOLAR ERA

AI-Enabled Cyber Operations and the Resilience of Coalition Command: A Strategic Architecture for the Multipolar Era

John Keith KING (USA)

Abstract

Artificial intelligence (AI) is changing both the velocity of cyber conflict and the architecture required to command multinational operations. AI can help coalition defenders correlate telemetry, identify anomalous behavior, prioritize vulnerabilities and recommend responses at machine speed. The same technologies can enable adversaries to automate reconnaissance, discover and chain vulnerabilities, generate deception and attack the data, software and decision processes on which coalition command depends. The challenge is therefore not simply protecting networks. It is preserving legitimate, timely and trustworthy command decisions while communications, identities, data, software and AI models are contested. This article proposes a Federated AI-Cyber Mission Assurance Architecture comprising seven mutually reinforcing layers: mission governance, federated identity, trusted data, resilient cloud-edge infrastructure, bounded AI-enabled cyber defense, continuous interoperability assurance and continuity of command. Its purpose is to enable multinational forces to operate through disruption, degrade gracefully and recover without surrendering national sovereignty or human command responsibility. In the multipolar era, resilience must be measured by mission continuity and decision integrity—not merely system availability.



Source: https://tdhj.org/blog/post/cyberspace-cyber-operations/

Keywords: artificial intelligence, cybersecurity, coalition command, NATO, interoperability, mission assurance, multi-domain operations, zero trust, federated networks, resilience.

Central Argument

The decisive test of coalition cyber resilience is not whether every network remains available. It is whether commanders can continue making lawful, timely and trustworthy decisions when communications, identities, data and AI-generated information are simultaneously under attack.

Command under Persistent Digital Contest

The strategic environment is being reshaped by great-power competition, regional conflict, technological diffusion and the growing capacity of state and non-state actors to disrupt critical infrastructure. Cyberspace is no longer a supporting arena that can be separated from political or military operations. It is a continuously contested domain through which adversaries can collect intelligence,

influence public perceptions, disrupt logistics, manipulate data and interfere with command-and-control systems before and during a crisis.

Artificial intelligence intensifies this environment. AI-enabled systems can analyze data, identify patterns and propose actions at a speed beyond unaided human capacity. Properly employed, they can improve situational awareness and help defenders manage the enormous volume of activity across coalition networks. Improperly governed or inadequately secured, the same systems can magnify uncertainty, spread errors at machine speed and create dependencies that an adversary can exploit.

The problem is especially acute for coalitions. A nation can impose common technical standards, security authorities and operating procedures across much of its force. A coalition must integrate sovereign nations with different laws, classifications, capabilities, languages, risk tolerances and procurement cycles. Some members may possess advanced cloud, space and AI capabilities. Others may contribute essential forces while operating older communications and information systems. All must still be able to share enough trusted information to act together.

NATO's 2026 Alliance Digital Strategy emphasizes secure, resilient and interoperable digital capabilities, data-centric operations and human-machine collaboration. [1] Its Digital Transformation Implementation Strategy 2.0 describes a federated digital backbone connecting sensors, decision-makers and effectors across organizational, national and security-domain boundaries. [2]

These developments establish an essential direction. The remaining challenge is translating strategy into an operational architecture capable of preserving coalition command while the digital environment is being actively contested.

No realistic architecture can guarantee uninterrupted availability against a capable adversary. The correct objective is to ensure that commanders retain sufficient trusted information, communications and authority to continue the mission, manage risk and recover from disruption.

AI and the New Tempo of Cyber Operations

AI creates a dual-use acceleration problem. It gives defenders new capabilities while reducing the time and expertise required to conduct sophisticated attacks.

For defenders, AI can correlate network, endpoint, cloud, identity and application telemetry that might otherwise overwhelm a security operations center. It can detect deviations from expected behavior, prioritize vulnerabilities according to mission consequences, identify coordinated activity and generate possible courses of action. AI can also assist software analysis, configuration review, threat hunting, malware triage and the translation of technical events into information usable by commanders.

For adversaries, AI can automate target discovery, generate convincing social-engineering content, analyze exposed software, adapt malicious code and coordinate activity across numerous targets. Frontier models may help attackers connect individually minor weaknesses into complete attack paths. AI can also generate false intelligence, synthetic imagery, deepfake audio or fabricated orders intended to undermine confidence in coalition command.

ENISA's 2026 assessment of cybersecurity in the frontier-AI era describes a structural change in the pace of attack and defense. It warns that the interval between vulnerability discovery and exploitation may shrink from months or days to hours or minutes. ENISA also identifies an "authority gap": organizations may possess the technical ability to respond but remain unable to authorize action within the time available to counter an automated attack. [7] This authority gap is particularly dangerous in multinational operations. A cyber incident may cross national, organizational and classification boundaries within seconds. Authority to isolate a system, revoke an identity, change a shared configuration or disconnect a participant may be divided among several commands. If those authorities have not been defined in advance, machine-speed detection will not produce machine-speed defense.

The solution is not unrestricted autonomy. An AI system permitted to act without meaningful constraints could create disruption comparable to the attack it was intended to stop. The answer is bounded automation: pre-authorized and reversible actions operating within clearly defined technical, legal and operational limits.

An AI-supported defensive system might automatically increase monitoring, isolate a low-consequence endpoint, revoke a short-lived machine credential or redirect suspicious activity into a controlled environment. Actions with strategic consequences—such as disconnecting a nation, modifying operational priorities or altering targeting information—must remain under designated human authority.

The governing principle should be clear: automate at the speed of the threat, but constrain automation according to the consequence of error.

The Coalition Command Problem

Coalition command depends on more than connectivity. It requires shared meaning, sufficient trust

and recognized authority.

A system may successfully transmit data while still failing operationally. The receiving organization may not understand the format, may be unable to verify the source, may lack release authorization or may not know whether the information was generated by a person, sensor or AI model. Data that cannot be interpreted, trusted and acted upon does not create interoperability.

NATO's Federated Mission Networking framework provides an important foundation by treating coalition networking as a combination of people, processes and technology. [5] Its federated model allows participants to retain sovereign capabilities while joining a governed mission environment. This is preferable to attempting to centralize all coalition systems under a single technical or national authority.

AI introduces additional questions:

- Which data may be used to train or update a coalition AI capability?
- How are the provenance, classification and releasability of that data represented?
- Who validates the model, and against what operational conditions?
- How does the coalition detect poisoned data, model manipulation or unsafe behavior?
- Which AI-generated recommendations may cross national boundaries?
- What happens when national AI systems reach conflicting conclusions?
- Who may authorize automated defensive action?
- Can essential command functions continue if cloud connectivity, satellite communications or a shared AI service becomes unavailable?

These are architectural and governance questions, not merely software questions. They must be resolved before a crisis.

The Federated AI-Cyber Mission Assurance Architecture

The proposed Federated AI-Cyber Mission Assurance Architecture, or FACMA, connects policy, people, data and technology to the operational requirement of preserving coalition command. It complements rather than replaces NATO and national frameworks.

Figure 1: The Seven-Layer FACMA Model

Layer	Principal function	Operational assurance question
1. Mission governance and authority	Defines purposes, authorities, limits and escalation thresholds	Can commanders stop, override or constrain automated action?
2. Federated identity and trust	Continuously verifies people, devices, services and AI agents	Can access be reduced without unnecessarily breaking the mission?
3. Trusted mission data	Preserves provenance, integrity, classification and releasability	Can users determine where information originated and whether it was modified?
4. Resilient cloud-edge infrastructure	Sustains essential services during disrupted connectivity	Which command functions continue when cloud or satellite access is lost?
5. Bounded AI-enabled cyber	Detects, prioritizes and responds within approved limits	Are automated actions explainable, traceable and reversible?
6. Continuous interoperability	Tests complete multinational mission threads	Does information retain its meaning and trust across national systems?
7. Continuity, recovery and assurance	Restores trustworthy operations and incorporates lessons	Can the coalition operate while degraded and prove what occurred afterward?

Layer One: Mission Governance and Delegated Authority

The architecture begins with the mission, not the technology.

Every AI-enabled capability should be tied to a defined operational purpose, responsible authority and understood consequence of failure. Coalition leadership must specify what a system is authorized to observe, recommend or execute. It must identify prohibited actions, escalation thresholds and conditions

requiring human intervention.

NATO's principles for the responsible use of AI—lawfulness, responsibility and accountability, explainability and traceability, reliability, governability and bias mitigation—provide an appropriate foundation. [3] Operational implementation requires these principles to be translated into mission-specific rules.

Pre-authorization can permit low-risk, reversible defensive actions while reserving higher-consequence decisions for human commanders. Every automated action should produce a tamper-evident record identifying the triggering information, model or rule, confidence level, action taken and responsible authority.

Governability also requires a positive ability to intervene. A system cannot be considered governable if it cannot be stopped, isolated, rolled back or placed into a safe operating state.

Layer Two: Federated Identity and Continuous Trust

In coalition operations, identity is a foundation for both interoperability and defense. The architecture must authenticate people, devices, software services, sensors and AI agents—not only users signing into a network.

Traditional perimeter security assumes that activity inside an approved network is relatively trustworthy. That assumption is no longer adequate. Coalition environments should apply zero-trust principles in which access is continually evaluated using identity, mission role, device condition, behavior, location and the sensitivity of the requested resource.

Federation allows each nation to remain responsible for its identities while adopting common credential and assurance standards.

Machine and workload identities deserve particular attention. AI agents and automated cyber tools should use short-lived, narrowly scoped credentials. They should not inherit broad access simply because they operate for an authorized user. If an automated capability is compromised, its possible effect must remain limited by design.

Trust should also be adjustable. A participant, device or service may remain part of the mission while receiving reduced access because its security condition has changed. This is operationally preferable to the binary alternatives of complete trust or total disconnection.

Layer Three: A Trusted Mission Data Fabric

AI systems depend on data, but coalition effectiveness depends on trusted data.

Operationally significant information should carry machine-readable metadata describing its source, time, classification, releasability, integrity status and, where applicable, the AI model involved in producing or modifying it. Provenance should accompany the information throughout its lifecycle.

This chain of evidence allows human and machine users to distinguish among a confirmed sensor report, an intelligence assessment, an AI-generated prediction and an unverified submission.

Data architecture must also account for national sovereignty. Not every nation will release raw operational data into a common repository. Federated analytics can allow participants to contribute approved results, indicators or model updates while retaining sensitive source data under national control.

Coalitions should establish minimum mission data compacts before operations begin. These agreements would identify essential data elements, semantic standards, quality requirements and release procedures for priority mission threads. The purpose is not unrestricted sharing. It is assured access to the minimum trusted information required for collective action.

When data quality falls below an established threshold, an AI system should lower its confidence, notify operators or revert to a conservative mode.

Layer Four: Resilient Cloud, Edge and Transport Services

A coalition digital backbone must be designed for contested and intermittently connected operations.

Cloud services provide scale, common tools and rapid access to information. They should not become single points of operational failure. Essential capabilities must extend to regional and tactical edges, where selected data and AI models can continue functioning during disrupted communications.

A tactical headquarters should not require continuous access to a centralized model for every decision. Approved models, rules and mission data should be distributable to protected edge environments. When disconnected, those environments should continue providing bounded capabilities, record their actions and reconcile with the federation when connectivity returns.

Communications should use diverse paths and providers where appropriate, including terrestrial, satellite and deployable systems. Store-and-forward mechanisms, bandwidth-aware applications and

prioritized synchronization can preserve essential functions when full connectivity is unavailable.

Graceful degradation must be deliberate. The architecture should specify which services continue, become read-only, revert to manual operation or stop when trust is lost. A system that fails predictably is more resilient than one that remains nominally available while producing untrustworthy information.

Layer Five: Bounded AI-Enabled Cyber Defense

AI should strengthen coalition cyber defense by helping personnel sense, understand, recommend, act and learn.

It can correlate telemetry, identify relationships among events, estimate mission consequences and present prioritized courses of action. Automated action should initially focus on bounded and reversible functions, such as increasing collection, quarantining a file, expiring a machine credential or blocking a confirmed malicious indicator.

The AI capability must itself be treated as part of the attack surface. Models, prompts, training data, retrieval sources, software dependencies and deployment pipelines require protection and monitoring. Model artifacts should be signed and verified. Changes must be attributable. Testing should address data poisoning, evasion, prompt injection, unsafe tool use, model extraction and manipulated outputs.

AI recommendations must communicate uncertainty. A tentative assessment presented with false precision may be more dangerous than a system that produces no answer. Operators need supporting evidence, alternative interpretations and the ability to challenge the recommendation.

Layer Six: Continuous Interoperability and Mission Assurance

Interoperability cannot be treated as a certification event shortly before deployment. Software, models, data formats and security policies change continuously. Assurance must therefore become continuous.

NATO's 2026 Coalition Warrior Interoperability Exercise brought together more than 4,000 participants from 46 Allied and partner nations and conducted more than 30,000 interoperability tests. [6] The scale demonstrates both NATO's commitment and the complexity of multinational integration.

Testing should increasingly evaluate complete mission threads rather than isolated interfaces. A thread might begin with a sensor observation, pass through national and coalition systems, receive AI-supported analysis, reach a commander and generate an authorized response. Testing must verify not only that the information moved, but that it retained its meaning, provenance, security markings and operational utility.

AI models should also be evaluated under multinational conditions, including language differences, uneven data quality, adversarial inputs and degraded communications. Technical compatibility cannot compensate for unclear procedures or absent trust among operators.

Layer Seven: Continuity of Command, Recovery and Learning

The final layer assumes that prevention will sometimes fail.

Coalition commands need rehearsed procedures for operating when major services, identities or data sources are unavailable or untrusted. Essential configurations and mission information should have protected, immutable and geographically separated recovery copies. Manual procedures and alternate communications must be exercised rather than merely documented.

Recovery is not complete when servers return to service. The coalition must reestablish confidence in the integrity of identities, software, data and previous decisions. Reconstitution criteria should include both technical restoration and operational validation.

Lessons from incidents and exercises should be shared in an appropriately releasable form. Nations may not be able to disclose every technical detail, but they can often exchange defensive patterns, indicators, anonymized telemetry and procedural lessons.

A Hypothetical Coalition Scenario

At 03:20, a coalition headquarters receives an urgent audio instruction purportedly from a senior commander. The message directs an immediate change to the disposition of critical communications assets.

At almost the same time, a privileged partner identity begins accessing information outside its normal mission pattern. Satellite connectivity becomes intermittent, and several monitoring systems report conflicting data. An AI-enabled security platform assesses that the events may be related but assigns only moderate confidence.

A traditional network-centered response might treat each event separately. The audio could be forwarded for manual verification, the identity investigated by another organization and the

communications outage managed as a technical problem. The resulting delay would create an opportunity for the adversary.

Under FACMA, the events are evaluated as a possible attack on command integrity:

1. The trusted-data layer identifies that the audio lacks an approved digital signature and possesses no verified chain of provenance.
2. The identity layer detects abnormal activity and automatically reduces the account to minimum mission access without disconnecting the partner nation.
3. Edge services preserve the last verified operational picture and continue essential functions during intermittent satellite connectivity.
4. The defensive AI correlates the events, presents supporting evidence and recommends reversible containment measures.
5. Pre-established governance prevents the AI from independently changing operational dispositions.
6. The command verifies the instruction through an alternate authenticated channel.
7. Tamper-evident records preserve the event sequence for investigation, recovery and multinational learning.

The most important outcome is not that every service remained available. It is that the coalition prevented manipulated information from becoming a legitimate command decision while continuing essential operations.

Measuring Resilience Through Mission Outcomes

Traditional cybersecurity metrics remain necessary, but counting blocked attacks or measuring system uptime does not demonstrate that coalition command remained effective.

Mission-assurance measurements should include:

- Time required to detect, contain and recover from an attack;
- Percentage of priority mission threads validated across participating nations;
- Duration for which essential command functions can operate without central cloud or satellite connectivity;
- Percentage of operational data carrying verified provenance and releasability metadata;
- Time required to reduce access for a compromised person, device or machine identity;
- AI performance under adversarial and degraded-data conditions;
- Percentage of automated actions that are reversible and traceable;
- Recovery-time and recovery-point performance for essential services;
- Frequency and success of manual-command and human-takeover exercises;
- Completeness of decision records following AI-supported actions.

The decisive metric is whether the coalition can continue making timely, lawful and trustworthy decisions while under attack.

Strategic Priorities for NATO and Partner Coalitions

First, coalition leaders should establish standing AI-cyber mission-assurance governance connecting operational commanders, cyber authorities, intelligence organizations, legal advisers, data owners and technical architects. Its purpose should be to define authorities, approve use cases and resolve cross-national risks before deployment.

Second, the digital backbone should be funded and governed as an operational capability rather than administrative information technology. Command, data, cyber defense and interoperability are now inseparable from deterrence and operational effectiveness.

Third, coalitions should adopt minimum mission data compacts establishing the information required for priority mission threads, together with common semantics, provenance, quality and release rules.

Fourth, AI adoption should begin with bounded applications delivering measurable defensive value. Threat correlation, vulnerability prioritization, malware triage, configuration analysis and decision support are appropriate starting points. Autonomous authority should expand only through evidence obtained from testing and exercises.

Fifth, interoperability should be designed and tested continuously. Standards, interfaces, data models, security policies and AI behavior must be evaluated before operations depend upon them.

Sixth, coalitions must train human-machine teams. Commanders need sufficient AI literacy to understand uncertainty, limitations and manipulation. Cyber professionals need operational context, while

policy and legal personnel must participate in exercises involving machine-speed decisions.

Seventh, architecture must assume disruption. Degraded operations, local processing, manual fallbacks, recovery and reconstitution should be incorporated into requirements and evaluated under realistic conditions.

Finally, coalitions must treat trust as an operational asset. Trust is produced by transparent governance, shared standards, repeated testing, professional relationships and confidence that each participant will act responsibly under pressure.

Conclusion

Artificial intelligence will not eliminate the uncertainty of coalition operations. It will accelerate and redistribute it.

The coalitions that achieve strategic advantage will not necessarily possess the largest AI models or the greatest volume of data. Advantage will belong to those capable of combining sovereign national systems into a trusted operational federation, employing AI within clear authorities and continuing to command through disruption.

Resilient coalition command requires verified identities, attributable data, secure cloud-edge services, bounded automation, continuous interoperability testing, practiced recovery and commanders prepared to exercise judgment when machine outputs conflict or fail.

The objective is not perfect connectivity or unlimited autonomy. It is decision superiority under contested conditions.

This capability also contributes directly to deterrence. An adversary is less likely to expect strategic benefit from cyberattack, deception or infrastructure disruption when a coalition has demonstrated that it can absorb the attack, preserve command legitimacy, recover rapidly and continue operating. By denying the adversary confidence that digital disruption will produce political paralysis or operational collapse, resilience changes the strategic calculation itself.

In the multipolar era, the ability to preserve trustworthy coalition command under sustained digital pressure will be both an operational advantage and a stabilizing source of deterrence.

Author's Disclaimer

The views expressed in this article are those of the author and are based exclusively on publicly available information. They do not represent the official position of any current or former employer, government agency, military organization or international institution.

References:

1. NATO. "Alliance Digital Strategy." January 13, 2026. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/01/13/ alliance-digital-strategy

2. NATO. "NATO's Digital Transformation Implementation Strategy 2.0." May 26, 2026. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/ natos-digital-transformation-implementation-strategy

3. NATO. "Summary of NATO's Revised Artificial Intelligence Strategy." 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

4. NATO. "Cyber Defence." Updated July 30, 2024. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

5. NATO Allied Command Transformation. "Federated Mission Networking." https://www.act.nato.int/activities/federated-mission-networking/

6. NATO Allied Command Transformation. "CWIX 26 Strengthens NATO's Digital Interoperability and Operational Readiness." June 30, 2026. https://www.act.nato.int/article/cwix-2026-concludes/

7. European Union Agency for Cybersecurity. "ENISA's View on Cybersecurity in the Frontier AI Era." July 2026. https://www.enisa.europa.eu/sites/default/files/2026-07/ ENISA%20view%20on%20cybersecurity%20in%20the%20frontier%20AI%20era_en_0. pdf

8. European Union Agency for Cybersecurity. "ENISA Threat Landscape 2025." October 1, 2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

9. National Institute of Standards and Technology. "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile." NIST AI 600-1, July 2024. https://doi.org/10.6028/NIST.AI.600-1

10. National Institute of Standards and Technology. "Cybersecurity Framework Profile for Artificial Intelligence." NIST IR 8596, Initial Preliminary Draft, December 2025. https://doi.org/10.6028/NIST.IR.8596.iprd

AEROSPACE CONFLICT

The Invisible War

Paul SZYMANSKI
(USA)

Calogero BONASIA
(Italy)

Anatomy of orbital conflict and the institutional paralysis at its heart

I. The Infrastructure of Daily Life, and Its Vulnerabilities

Every morning, before anyone has finished breakfast, she has already depended on satellites at least four times. Her phone synchronized its clock through GPS timing signals. The weather forecast she glanced at was computed from data collected by polar-orbiting meteorological satellites. Her contactless payment at the café was authorized through a transaction chain whose timing relies on atomic clocks aboard navigation satellites and satellite communications. And if she drove to work, her route was calculated by a constellation of more than thirty satellites orbiting at 20,200 kilometers above the Earth's surface, each transmitting at roughly 25 watts, so that by the time the signal completes its journey it arrives at her dashboard approximately one thousand times weaker than the thermal noise floor of the device that receives it.

Source: https://www.popularmechanics.com/space/satellites/a19433822/us-space-force-reasons/

Every detail in the preceding paragraph is literal: a technical description of the first ninety minutes of an ordinary Tuesday in any Western city.

The objects that make this possible are remarkably small and astonishingly fragile. A GPS III satellite has an on-orbit mass of approximately 2,160 kilograms and measures just over four meters in length. These machines orbit at velocities between 7,000 and 28,000 kilometers per hour, depending on altitude, in an environment where no atmospheric drag slows any object down and where a one-kilogram fragment of debris, traveling at a relative velocity of ten kilometers per second, releases kinetic energy equivalent to twenty-two kilograms of TNT. They are unarmored, un-maneuverable in any tactically meaningful sense, and, with very few exceptions, entirely undefended.

The scale of dependence is measurable. In 2024, the Brattle Group estimated the cost of a total GPS outage in the United States alone to be 1.6 billion dollars for a single day, 12.2 billion for a week, and 58.2 billion for a month. These figures account only for direct economic losses in transportation, telecommunications, energy grid synchronization, and financial services. They do not include military consequences,

cascading infrastructure failures, or the effects of public disorder when payment systems, emergency response coordination, and air traffic control systems degrade simultaneously. The United States is one country. Europe, China, India, and the rest of the global economy depend on the same orbital infrastructure, through GPS, Galileo, BeiDou and GLONASS. In July 2024, Admiral Thad Allen, chairman of the U.S. National Space-based Positioning, Navigation, and Timing Advisory Board, issued a formal memorandum warning that America's continued over-reliance on GPS makes critical infrastructure vulnerable to a range of well-documented threats that can be accidental, natural, or deliberate.

The European reader may believe this is an American problem. The evidence says otherwise. In 2024, European aviation and maritime authorities documented dozens of significant GNSS interference events, the majority traced to Russian electronic warfare transmitters operating from Kaliningrad, Crimea, and other positions along the eastern perimeter of NATO. Commercial airliners flying Baltic and Black Sea corridors were forced to reroute. Cargo vessels in the Mediterranean reported GPS coordinates placing them at inland airports, the characteristic signature of a spoofing attack that substitutes false position data for genuine signals. At the Port of Gdansk, Poland according to testimony presented at the 2025 PNT Leadership Summit, autonomous cargo-handling systems dropped out of precision mode in bursts that operators associated with emissions from Kaliningrad, halting operations that depend on five-centimeter positional tolerances. Offshore, a wind farm contractor suspended survey and cable-laying work because the navigation precision required for the operation had dissolved into guesswork. In addition, the 23 Feb 2022 1800 "AcidRain" cyber-attack on the ViaSat satellite system left 5,000 power windmills across Europe non-functional.

These incidents occupy the grey zone between war and peace, a zone that functions as a strategic instrument in the hands of those who exploit it.

The vulnerability extends beyond navigation. Modern satellite infrastructure serves functions that were inconceivable when the legal framework governing outer space was drafted. The Outer Space Treaty of 1967 prohibits the placement of nuclear weapons and other weapons of mass destruction in orbit. It says nothing about conventional weapons. It says nothing about cyber weapons. It says nothing about the deliberate interference with satellite signals, the physical manipulation of satellites through proximity operations, the use of directed energy to blind optical sensors, or the deployment of co-orbital devices capable of inspecting, shadowing, and, at the appropriate moment, disabling a target satellite without generating a single piece of trackable debris. The treaty was written to prevent the Cold War from extending into orbit. It succeeded in that narrow objective. It has no answer to the war that is actually being fought there now.

II. Eleven Space Wars: The History that Has Never Been Told

Paul Szymanski has documented at least eleven distinct space conflicts since the 1960s. These episodes have never been collectively recognized as what they are, because the legal and strategic frameworks required to name them did not exist when they occurred and have not been created since. The cumulative effect of the omission is that a form of warfare with more than fifty years of operational history is treated, in public discourse and in most political deliberation, as a future possibility. This is because countries love the secrecy that space provides and limits their leadership's potential embarrassment in front of their citizens of failure in space operations.

The pattern became unmistakable in the twenty-first century. On 11 January 2007, the People's Republic of China destroyed its own defunct weather satellite, Fengyun-1C, using a kinetic kill vehicle launched from a ground-based ballistic missile at Xichang Satellite Launch Center. The closing velocity at impact was approximately 8 kilometers per second. The test created the largest field of artificial debris in the history of spaceflight: more than 3,000 traceable fragments and an estimated 150,000 pieces of debris large enough to damage or destroy an operational satellite. Nearly two decades later, much of that debris remains in orbit, a permanent contamination of the 800-kilometer altitude band and a demonstration that a single national decision can degrade a common resource for generations.

In February 2008, the United States responded with Operation Burnt Frost, destroying its own errant reconnaissance satellite USA-193 with an SM-3 missile modified for the purpose. The stated justification was the risk posed by the satellite's hydrazine fuel tank upon reentry. The operational significance was unmistakable: the United States possessed and was prepared to use a kinetic anti-satellite capability. The debris generated by the strike reentered the atmosphere within weeks, a difference that American officials emphasized but that did not alter the demonstration.

In March 2019, India conducted Mission Shakti, destroying the Microsat-R satellite at 283 kilometers altitude using a Prithvi Delivery Vehicle Mark-II modified from its ballistic missile defense program. The low altitude limited the debris lifetime, and India framed the test as a demonstration of deterrent capability rather than an operational posture. The international response was muted, reflecting both the technical precautions India had taken and the established precedent set by China and the United States.

In November 2021, Russia destroyed Kosmos-1408 with a direct-ascent anti-satellite missile, generating more than 1,500 traceable fragments in an orbit that threatened the International Space Station and forced its crew to shelter in their evacuation vehicles for several hours. Condemnation was swift and nearly universal. No binding legal consequence followed. It was apparent that this Russian test was a warning to American space weapons capabilities just as the second Ukrainian conflict was about to start. Because this test threatened cosmonauts on the International Space Station, this test indicated that the Russians were serious enough to invade Ukraine later.

Four kinetic tests by four different nations in fourteen years. Four confirmations that kinetic anti-satellite capability is now a feature of great-power arsenals. Zero treaty constraints added to the 1967 framework.

Alongside these kinetic demonstrations, a quieter and more operationally significant pattern has been developing: the systematic use of electronic warfare, cyber operations, and proximity maneuvers to deny, degrade, deceive, and disable satellite services without producing a single piece of traceable debris. Russian inspection satellites have approached French and Italian military spacecraft closely enough to provoke formal diplomatic protests. The Russian satellite Olymp-K has repeatedly maneuvered between commercial Intelsat satellites in geostationary orbit. Multiple states have developed and tested co-orbital capabilities that allow one satellite to approach, observe, and potentially interfere with another. The distinction between a satellite that inspects and a satellite that attacks is a matter of intent, and intent is precisely what the orbital environment makes impossible to determine from the outside.

The proof that this pattern has crossed into active warfare came on a single day. At approximately 03:02 UTC on 24 February 2022, the same morning Russian ground forces crossed the Ukrainian border, a cyber attack disabled tens of thousands of broadband modems connected to ViaSat's KA-SAT satellite network. The attack exploited a misconfigured VPN appliance at a management center in Turin, Italy, through which the attackers gained access to the trusted network segment and executed legitimate management commands that overwrote the flash memory of residential modems across Europe. The immediate objective was to degrade Ukrainian military satellite communications at the moment of maximum need. The operation achieved that objective. The spillover did not stop at the Ukrainian border. In Germany, remote monitoring and control of 5,800 Enercon wind turbines went dark. In France, nearly 9,000 subscribers of a satellite internet provider lost connectivity. Across Germany, France, Hungary, Greece, Italy, and Poland, approximately a third of 40,000 additional subscribers were affected.

The forensic investigation by SentinelOne identified the wiper malware used in the attack, designated AcidRain, and documented developmental similarities with VPNFilter, a 2018 campaign previously attributed by the FBI to Russian military intelligence. In May 2022, the European Union, the United States, the United Kingdom, and a dozen EU member states formally attributed the attack to the Russian GRU. Nearly twenty governments issued coordinated statements condemning this cyber-attack.

The attack targeted a commercial satellite communications network. It was executed through ground infrastructure, not from orbit. It produced no debris, no kinetic impact, no physical destruction of any satellite. It achieved, in the first hours of a conventional military invasion, the functional equivalent of destroying the enemy's communications architecture.

No international legal framework classifies this event as an act of space warfare. No treaty defines the threshold at which interference with satellite services constitutes an armed attack. No doctrine establishes when a cyber operation against satellite ground infrastructure triggers the right of self-defense under Article 51 of the United Nations Charter. The absence of these definitions is itself the condition under which space conflict actually operates: below the threshold of legal recognition, above the threshold of strategic consequence, and entirely within the capabilities of any state with a competent signals intelligence service. Since electrons do not have serial numbers attached to them, the United States considers cyber warfare as "non-attribution" and cannot be proven in any court of law.

III. The 24-Hour Rule: The Physics of Decision Collapse

Szymanski's Space Warfare Analysis Tools (SWAT) software has produced the most extensive unclassified dataset on orbital attack dynamics. The methodology subjects randomly selected satellite targets to simulated attacks using realistic orbital mechanics and adversary capabilities documented in open-source literature. The results describe a problem that cannot be solved through faster processing or better sensors, because the problem is physical, embedded in the orbital mechanics themselves.

The SWAT simulations show that 95 percent of attacks on randomly selected satellites can be completed in under 24 hours without optimized trajectories or starting positions. The remaining 5 percent are completed within 48 hours. Under optimized conditions, the timelines collapse further. A satellite at 500 miles altitude travels at approximately 16,672 miles per hour. A retrograde anti-satellite weapon in a head-on engagement approaches its target at a relative velocity exceeding 33,000 miles per hour. At those closure rates, the interval between detection and impact permits no evasive maneuver. In addition, attacks

from Lagrange Points and Lunar trajectories can counteract maneuvering satellites by slightly changing their angle of attack while still far away.

Evasive maneuvering is, in any case, constrained by fuel economics. A satellite designed for a fifteen-year operational life carries propellant calibrated for routine station-keeping and end-of-life on orbit. Large evasive burns drain this reserve. Each burn measurably shortens the satellite's operational lifespan, a fact that Szymanski has emphasized repeatedly: the attacker who forces the defender to maneuver wins even if the attack is ultimately avoided, because the defender's future operational capacity has been diminished. An adversary can potentially appear to be attacking, but maneuver away just at the last moment to assess the adversary's response times, tactics, and to drain its fuel reserves even if there is no conflict going on. Upon interception, a single anti-satellite weapon converts into a shotgun pattern of fragments, each moving at orbital velocity, each capable of destroying additional satellites and of remaining in orbit for decades or centuries.

The gap between orbital tempo and institutional tempo is the central structural problem of space warfare. A terrestrial military command structure can convene a decision conference in hours. An alliance consultation mechanism, such as NATO's North Atlantic Council, operates on a cycle measured in days. A political authorization for the use of force, in most democratic systems, requires deliberation that is measured in days or weeks. The attack these structures are asked to address will have concluded before the first meeting is convened, and thus we end up self-deterring.

Szymanski has proposed, as a partial doctrinal response to this temporal compression, a Space Defense Identification Zone (SDIZ) and a Combined Action Execution Zone (CAEZ), parallel to the Air Defense Identification Zone concepts that have governed air control since the Cold War. The SDIZ would define a volume around critical satellites within which unauthorized approach triggers pre-defined defensive protocols. The CAEZ would define a combined set of assets and authorities pre-positioned to execute response actions within operationally relevant timeframes. These proposals, and the Space DEFCON alerting system of which they are components, represent attempts to adapt the structural logic of terrestrial air defense to the orbital environment. They have not been adopted. Their adoption would require a level of political consensus on the weaponization of space that the international system has yet to produce.

IV. The Structural Impossibility of Total Space Surveillance

The temporal compression described above is compounded by three irreducible constraints that make the total surveillance and control of the orbital environment impossible. Szymanski has formulated these constraints as Vastness, Obscurity, and Complexity.

Vastness. The orbital volume between low Earth orbit and the Moon encompasses approximately 4.81 times ten to the sixteenth power cubic miles, a volume that exceeds the volume of Earth's oceans by a factor of more than one hundred forty-six million. Within that volume, the United States Space Surveillance Network tracks approximately 47,000+ objects. The tracking is dense in low Earth orbit and geostationary orbit, the two regimes of greatest commercial and military activity. The regions between and beyond, including the Lagrange points and the cislunar volume, receive sporadic attention at best.

Stealth in orbit is achievable through elementary techniques. Attitude adjustments that minimize the cross-section presented to sunlight can significantly reduce solar reflections, the primary method by which ground-based optical sensors detect objects in high orbit. Maneuvers conducted over Antarctica or the Southern Ocean exploit gaps in ground-based radar coverage, because the Space Surveillance Network's sensors are concentrated in the Northern Hemisphere. Highly elliptical orbits, such as the Molniya type used by Russian communications and early warning satellites, spend the majority of their period at apogee, far beyond the effective range of most tracking systems. A satellite in such an orbit is observable for a fraction of its orbital period and invisible for the rest, especially for the high Northern orbits employed by Russian satellites.

Obscurity. Of the 47,000+ tracked objects in the current catalog, approximately 35-40% of them are classified as Analyst Objects of unknown nature and ownership. These are objects that the Space Surveillance Network has identified but cannot confidently associate with any registered launch, operator, or mission. One Russian satellite was lost by Western tracking systems for approximately twenty years before being reacquired only after Russia announced its orbital parameters. The NORAD catalog famously tracked waste discharge from the Mir space station as if it were the station itself, an illustration of the operational limits of current surveillance at the routine level of discrimination.

Complexity. The physics of orbital mechanics permits attack vectors that have no precedent in terrestrial warfare. An anti-satellite weapon deployed from the Earth-Moon Lagrange points requires minimal delta-V to reach geostationary assets, because the Lagrange points sit at gravitational equilibrium from which small perturbations produce large displacements. A retrograde orbital attack from trans-lunar space against a geostationary target presents the defender with a threat that approaches from a direction no

sensor is oriented to observe. A bi-elliptic transfer attack can position a weapon from an apparently distant orbital location to the target's orbit through maneuvers that appear, to any individual observation, to be unrelated to the eventual target. The inspection of spent booster stages from 1960s-era launches, many of which remain in orbit, is operationally impossible: any one of them could, in principle, conceal an ASAT payload placed there decades in advance or more recently.

These constraints, taken together, establish that the orbital theater is, in any operationally meaningful sense, unobservable at the resolution required to distinguish hostile action from orbital mechanics if a potential adversary is purposely trying to obscure a potential attack. The system that governs the use of force in terrestrial domains is built on the assumption that the theater of war can be mapped, that movements within it can be detected and interpreted, and that hostile intent can be inferred from observed behavior. None of these assumptions holds in the orbital environment.

V. The Attribution Paradox and the Mechanism of Self-Deterrence

The temporal and perceptual constraints described in the preceding sections produce a specific operational consequence: the collapse of attribution.

In every major conflict of the past three centuries, the identity of the attacker could be established through direct observation, signals intelligence, or forensic analysis in time to inform the response. An army crosses a border. A missile leaves a launch site. A fleet sorties from port. Even in the most sophisticated denial-and-deception operations of the twentieth century, attribution was difficult but achievable within the operational tempo of the conflict.

In orbital warfare, the situation is categorically different. Szymanski has documented the problem in its full structural form. An attacking satellite carries no national markings. Its components are statistically likely to include Western-manufactured parts regardless of its country of origin, because the global supply chain for space-rated components has concentrated in a small number of Western firms. An attacker with moderate technical sophistication can launch from third-country territory, use commercial or civil launch services, register the payload under a commercial entity, and conduct the attack through autonomous software that requires no further communication with ground stations once deployed. Post-attack attribution may require weeks or months of forensic analysis. The conflict it initiated in space will have been decided on the ground due to command hesitation, and the defender will face the choice between retaliating without certainty or failing to retaliate at all.

The problem of attribution is compounded by the problem of intent. A space attack may be a localized show of force, a theater-specific defensive action, a prelude to nuclear exchange, or conventional war supporting effort. Each of these possibilities requires a categorically different response. A localized show of force calls for diplomatic and economic responses calibrated to preserve escalation control. A theater-specific defensive action calls for proportional military response within the theater. A prelude to nuclear exchange calls for activation of nuclear alert postures. Conventional war support calls for immediate counterforce operations. The decision-maker who cannot identify the attacker also cannot determine the purpose of the attack, and therefore cannot calibrate the scale, domain, or intensity of any response without risking catastrophic miscalculation. Even if two adversaries are currently in conflict on the Earth, an attack in space might actually be a third party try to stir things up.

The historical record offers no direct parallels, but it offers instructive analogies. At Pearl Harbor in December 1941, American intelligence possessed extensive warning signs of Japanese military movement, including decrypted diplomatic communications. The signs were not integrated, not acted upon, and not transmitted to the commanders whose ships were destroyed. In the Battle of the Bulge in December 1944, Allied intelligence had compiled approximately 11,000 Ultra intercepts documenting the German buildup in the Ardennes. The intercepts were dismissed because they contradicted the prevailing institutional assumption that the German army was incapable of a major offensive. In the Yom Kippur War of October 1973, the Israeli Bar-Lev Line suffered approximately 90 percent casualties among its forward positions because Israeli intelligence had concluded that an Egyptian attack was impossible and had refused to update that conclusion in the face of mounting evidence. A quote from General George S. Patton is appropriate here: "*If everyone is thinking alike, then somebody isn't thinking*."

These failures share a structural feature. The information required to prevent the disaster was available. The institutional mechanisms required to act on it were not. Intelligence was collected but not integrated. Warnings were issued but not believed. The defending institution treated the threshold of action as equivalent to certainty, and certainty was impossible to establish within the operational tempo of the attacker.

The orbital environment structurally amplifies these failure modes. The temporal compression described in Section III means that the window for integration, consultation, and belief-revision is narrower than any terrestrial conflict has ever presented. The perceptual opacity described in Section IV means that the information required for attribution may never be available in a form that meets institutional evidentiary

standards. The attribution problem described in this section means that even the information that is available may be susceptible to multiple interpretations, each of which would justify a categorically different response. When all of these constraints operate simultaneously, the institutional machinery designed to govern the use of force produces no answer at all. The system enters the state that Szymanski has called self-deterrence: the paralysis of the defender through the structural impossibility of meeting the evidentiary and procedural requirements that his own institutions demand before force may be authorized. The defender is not defeated by the attacker. The defender is defeated by the gap between the conditions under which his own institutions are designed to function and the obscure and fast paced conditions that the orbital environment imposes.

VI. The Kessler Threshold: When War Destroys Its Own Theater

Alongside the institutional problem of self-deterrence, the orbital environment imposes a physical constraint that has no precedent in the history of warfare. The physical integrity of the theater is a function of the operational restraint of the combatants. In 1978, Donald Kessler and Burton Cour-Palais published a model describing the conditions under which orbital debris would become self-sustaining. Beyond a certain density threshold, they argued, collisions between orbital objects would generate fragments that would cause further collisions, producing a cascade that could render entire orbital regimes unusable for decades or centuries. The model was theoretical at the time of publication. It is no longer theoretical. On 10 February 2009, the defunct Russian Cosmos 2251 satellite collided with the operational Iridium 33 communications satellite at approximately 790 kilometers altitude. The collision produced more than 2,000 traceable fragments and an estimated tens of thousands of non-traceable fragments. It was the first recorded hypervelocity collision between two intact satellites. Donald Kessler himself has described it as the opening move of the cascade phenomenon he predicted. Some fraction of the Iridium-Cosmos debris has already contributed to subsequent near-miss events. The cascade has possibly begun.

The European Space Agency's 2025 Space Environment Report confirms that the debris environment has entered a self-sustaining growth phase. Even without a single additional launch, the population of orbital debris would continue to grow, because fragmentation events are now generating new debris faster than atmospheric drag can remove it. In 2024 alone, several major fragmentation events added at least 3,000 new tracked objects to the orbital catalog. The Chinese Long March 6A upper stage breakup in August 2024 generated more than 700 fragments in sun-synchronous orbit, a region densely populated by Earth observation and climate monitoring satellites. In the first half of 2025, SpaceX's Starlink constellation executed 144,404 collision avoidance maneuvers, one every two minutes, day and night, for six months. Each maneuver consumed propellant. Each consumption of propellant shortened the operational lifespan of the satellites. Each shortened lifespan brought forward the date at which the satellite itself would become debris, if not de-orbited. The strategic logic of this environment is unlike any other military domain. In terrestrial warfare, the destruction of enemy assets preserves the theater for future operations. A tank destroyed in 1943 did not prevent the use of the field in which it burned. In orbital warfare, the destruction of enemy assets, if conducted through kinetic means in densely populated orbital regimes, can render the regime itself unusable for the victor as well as the vanquished. The Kessler threshold is the category without military precedent: the first domain in which victory through destruction and self-destruction are identical outcomes.

This is the strategic imperative behind Szymanski's book *100 Methods to Attack Satellites Without Space Debris*. The title is frequently misread as a humanitarian proposal, an argument for restraint based on the interests of third parties or future generations. The actual argument is operational. The book is about theater preservation, based on the self-interest of the attacker. A state that develops and maintains orbital assets has a vital interest in ensuring that the orbital environment remains usable after any conflict in which it participates. The exclusion of kinetic weapons from responsible space warfare doctrine is dictated by the physics of debris, as a function of operational survival rather than ethical restraint. The implication is that the space warfare of the future, if it is conducted rationally, will consist almost entirely of electronic warfare, cyber operations, directed-energy weapons, and proximity operations that degrade or disable without destroying. This is, in fact, the pattern already documented in the eleven space conflicts Szymanski has catalogued. The Viasat attack fits this pattern. The GNSS interference operations in Europe fit this pattern. The approach operations of Olymp-K and similar satellites fit this pattern. The kinetic tests of 2007, 2008, 2019, and 2021 were demonstrations of capability for political purposes, not operational employments. The operational space war has been and will continue to be conducted through methods that leave no debris and therefore no unambiguous evidence of attack.

VII. The Architecture of Blindness

The six preceding arguments converge on a single conclusion. The institutional machinery that

governs the use of force in the contemporary international system was designed under three foundational assumptions, each of which fails in the orbital environment.

The first assumption is temporal. Military attacks on Earth unfold over hours, days, or weeks, long enough to convene decision-makers, assess options, consult allies, and authorize a response. This assumption held from Thermopylae to the Falklands. In orbital warfare, as the SWAT data demonstrate, the decision window is compressed to the point of uncertainty of paralysis.

The second assumption is epistemic. The identity of the attacker in Earth conflicts can be established through direct observation, signals intelligence, or forensic analysis in time to inform the response. In orbital warfare, attribution may require weeks or months of analysis after the attack has concluded, and even when attribution is achieved, the intent of the attacker may remain ambiguous among possibilities requiring categorically different responses.

The third assumption is perceptual. The theater of war on the ground is physically accessible to human senses or their instrumental extensions. The orbital theater is, in any operationally meaningful sense, unobservable at the resolution required to distinguish hostile action from orbital mechanics or accidental encounters.

When all three assumptions fail simultaneously, the institutional machinery produces no answer at all. Self-deterrence is the operational result, but the underlying cause is architectural. The institutions are functioning exactly as designed. They are applying rules that were adequate for every conflict environment human beings have inhabited for three thousand years. The environment has changed. The rules have yet to follow.

The implications extend beyond military doctrine into the foundations of political accountability. In every democratic system, the authority to use force is grounded in a chain of legitimacy that runs from the electorate, through elected officials, to military commanders. That chain presupposes a decision: a human being, vested with political authority, evaluates evidence, weighs consequences, and authorizes action. The chain cannot function without the decision. And the decision cannot function without time, attribution, and situational awareness, the three resources that orbital warfare systematically denies.

In addition, governments desire secrecy in their actions so that potential failures cannot be readily perceived by the citizens. Space provides this secrecy where governments can show intent, will and resolve upon their adversaries without necessarily cause terrestrial conflicts or political embarrassments.

Satellites are invisible. Their signals are imperceptible. Their failure modes are silent and ambiguous: a GPS receiver that drifts is indistinguishable, to the user, from a GPS receiver that has been spoofed. The infrastructure is so deeply embedded in the substrate of daily life that its absence would be experienced as a simultaneous, unexplained degradation of everything: transport, finance, communications, energy distribution, emergency response, and the capacity of governments to coordinate any coherent action at all.

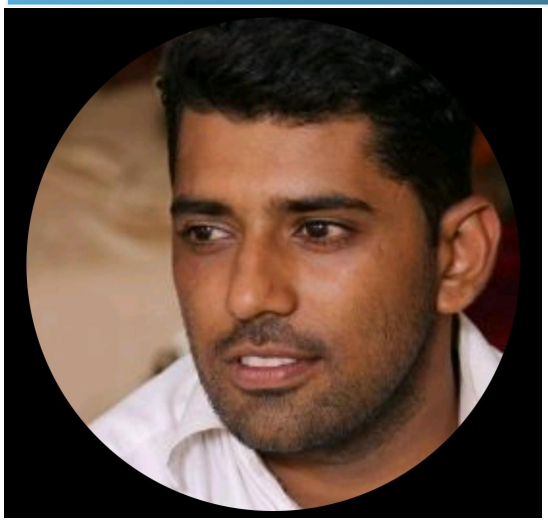
The questions that emerge from this analysis are precise and unanswered. Who decides when the commander lacks attribution? Who decides when the politician lacks time? Who decides when the alliance lacks a consultation mechanism calibrated to minutes rather than days? If the answer is an artificial intelligence system, on what political legitimacy does it act? If the answer is a pre-authorized doctrine, what happens when the doctrine prescribes a response the decision-maker cannot authorize because the evidence the doctrine itself requires has yet to be produced? If the answer is no one, then the defender has already lost, and the only remaining question is whether he will recognize the loss before or after the satellites begin to fall.

These questions are the operational reality of a world in which the most critical military infrastructure is deployed in a domain that no existing institution of governance was designed to comprehend, let alone control. They demand engagement from the audience that has so far been absent from the conversation: the European public, the Atlantic alliance, and the political and intellectual class whose inherited assumptions about sovereignty, security, and institutional legitimacy are now in direct collision with the physics of the orbital environment.

Szymanski's work, developed over five decades of direct involvement with American space warfare programs, provides the doctrinal foundation on which any serious response must be built. The Space Operational Art and Design (SOAD) framework, the Space Escalation Ladder, the Space Warfare Analysis Tools (SWAT), the Space Attack Warning (SAW) methodology, and the extensive analyses contained in *The Battle Beyond: Fighting and Winning the Coming War in Space*, the *Sun Tzu and the Art of War Applied to Space War* series, and *100 Methods to Attack Satellites Without Space Debris* constitute the most comprehensive unclassified body of work on how space wars are actually fought, how they escalate, and how they might be controlled.

The first step toward an answer is to recognize that the questions are real, that they are already upon us, and that the silence of existing institutions is itself the most precise measurement of their inadequacy to the moment.

SYNTHETIC INTELLIGENCE (SI)



Synthetic Intelligence and the Counterfeit Economy

Anand RADJOU (India)

We Thought Counterfeiting Was About Fake Products.
Synthetic Intelligence Has Other Plans.

How real consumer money can move into counterfeit and substandard markets, weaken the visible economy, and become a geopolitical risk.

"The product may be fake. The money paying for it is not."

1. The Real Concern || Real Money, Fake Goods

Counterfeiting is still treated mainly as a product problem. Find the fake bag, charger, brake pad, cosmetic, medicine or food item, seize it, and move on. But by the time the product is found, the transaction is already complete. A consumer has paid with his/her genuine currency. A legitimate business may have lost a sale. The state may have lost taxable activity. That is the part we often miss. Counterfeit and substandard markets do not need fake currency. They need real purchasing power. Small amounts leave ordinary households one purchase at a time and can accumulate inside informal, unreported or criminal networks.

Counterfeit and substandard goods are not identical. A counterfeit product deliberately pretends to be genuine. A substandard product fails a required quality or safety standard and may or may not carry a fake brand. For the buyer, the common problem is simple, what looks normal may not be genuine, safe, compliant or properly taxed.

INTERPOL treats illicit-goods trafficking as transnational crime and links it with smuggling, tax evasion, corruption, bribery and money laundering. OECD and EUIPO research published in 2025 and 2026 also finds a strong relationship between counterfeit trade, informality and labour exploitation. In other words, the fake product is only the visible end of a much larger system.

2. Updating the Number || What Can 2026 Honestly Support?

The last widely used global benchmark is the OECD/EUIPO estimate of **USD 467 billion** in international trade in counterfeit and pirated goods in 2021. It was equal to about 2.3% of global imports. That figure is important, but it is also 5 years old by the time this article is published.

The easy temptation is to simply double it. The data do not support that shortcut. IMF World Economic Outlook data put nominal world GDP at about USD 98.4 trillion in 2021 and USD 126.3 trillion in 2026 - an increase of roughly 28%.

If the 2021 counterfeit estimate simply moved in line with nominal world GDP, the 2026 equivalent would be about roughly USD 0.60 trillion. That is a useful baseline. It is not an official 2026 measurement.

The real uncertainty is intensity. Counterfeiters now operate through smaller parcels, online marketplaces, social media, encrypted communication and increasingly synthetic content. Domestic counterfeit production, undeclared sales, laundering, tax leakage and substandard goods are not fully captured by customs-based international-trade estimates. So, the measured number is better treated as a floor than as the whole economy.

The product mix also matters. Counterfeiting is not a luxury-handbag story and it is not a pharmaceutical story. OECD/EUIPO data cover clothing, footwear, electronics, cosmetics, toys, automotive parts, batteries, food products and many other everyday categories or non-perishable materials. The more ordinary the product becomes, the easier it is for the loss to disappear inside normal household spending. One fake charger or one diluted cosmetic does not look like a macroeconomic event. **Millions of such purchases do.**

Distribution has also become harder to see. OECD/EUIPO reported that shipments containing fewer than 10 items rose from 61% of counterfeit customs seizures in 2017–2019 to 79% in 2020–2021. The 2025 OECD/EUIPO report further confirms that around 65% of seizures now involve small parcels and mail. That is strategically important. A container is visible. Thousands of small parcels moving through e-commerce, postal systems and local fulfilment networks are much harder to stop.

YTHICS 2026 analytical range (scenario, not official estimate)

Scenario	Assumption	2026 value
GDP-scaled baseline	2021 intensity unchanged	~USD 0.60T
Accelerated	25% higher intensity than baseline	~USD 0.75T
High-risk	50% higher intensity than baseline	~USD 0.90T

Figure 1: *YTHICS scenario range. Baseline scales the OECD/EUIPO 2021 estimate by IMF nominal world-GDP growth to 2026. Accelerated cases are stress-tests, not measured facts.*

Recent enforcement data show that the problem has not faded. EU authorities detained about 112 million counterfeit items in 2024 with an estimated retail value above EUR 3.8 billion. The OECD/EUIPO 2025 report still describes counterfeit trade as a global threat worth up to USD 467 billion annually and adds new evidence connecting it with forced labour and informality. The number has not become smaller because the measurement is old; the measurement simply has not yet caught up with 2026.

3. Synthetic Intelligence || Counterfeiting the Story Around the Product

“Counterfeiters once had to copy the object. Now they can copy the environment around it.”

YTHICS uses the term Synthetic Intelligence here as an analytical description of AI systems that can manufacture convincing signs of authenticity at scale. A fake seller can have a polished profile. A fake product can have professional images. Reviews, invoices, certificates, customer replies, translations, advertisements, voices and even identities can be generated in minutes. That changes the question from 'Is the product fake?' to 'Can the entire story around the product be trusted?' A consumer may see the right logo, the right review language, the right-looking invoice and a convincing seller conversation - and still be inside a counterfeit transaction.

There is not yet enough global evidence to assign a precise AI multiplier to counterfeit trade. We should not invent one. But adjacent criminal markets give a warning. INTERPOL's 2026 Global Financial Fraud Threat Assessment (March 2026, 2nd Edition) confirms that AI-enhanced fraud is 4.5 times more profitable than non-enhanced tactics and describes the industrialization of fraud through synthetic identities, cloned voices and AI-generated personas. Global fraud losses reached USD 442 billion in 2025. That is financial fraud, not counterfeit trade - but the strategic lesson is clear: when deception becomes cheaper and more scalable, criminal markets gain operating leverage.

This is why Synthetic Intelligence matters more than the label 'AI'. Artificial intelligence describes technology. Synthetic Intelligence describes the consequence; authenticity itself can now be manufactured.

The danger is not limited to making a fake advertisement look better. Synthetic systems can lower the cost of operating an entire deceptive storefront. One person can generate product descriptions in several languages, answer customers around the clock, create social proof, alter images, draft invoices and move quickly when a seller account is removed. That makes enforcement a speed problem as much as a detection problem.

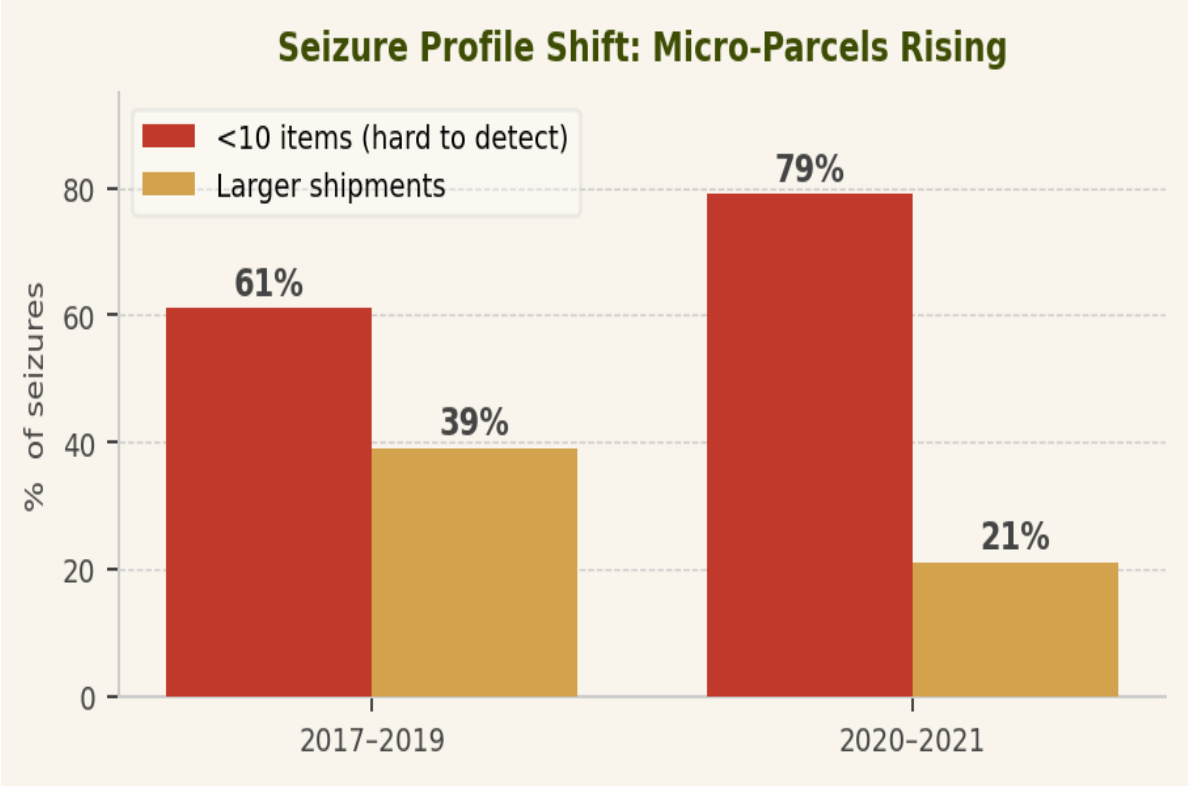


Figure 2: *OECD/EUIPO seizure-profile shift. Micro-parcels (<10 items) rose from 61% of seizures (2017–2019) to 79% (2020–2021); 2025 data confirms ~65% of all seizures now involve small parcels and mail. A container is visible; thousands of postal packets are not.*

4. When Invisible Money Starts Changing Visible Politics

The geopolitical risk should be stated carefully. Counterfeit goods do not automatically cause terrorism, government collapse or regime change. But counterfeit and illicit markets can strengthen the same hidden financial, logistical and corrupt networks used by wider organised crime.

The economic chain is straightforward. Legitimate firms pay wages, tax, testing costs, compliance costs and environmental costs. Illicit operators can avoid many of them. If enough real consumer money moves into those channels, legitimate businesses lose revenue, tax authorities lose visibility, workers lose formal jobs and criminal networks gain cash flow.

Some of those proceeds may later be laundered or recycled through assets, businesses, real estate, gold, trade-based schemes or other channels designed to make illicit value appear legitimate. This does not mean every counterfeit sale ends in property or gold. It means the border between the illicit and legitimate economy can become porous.

This is also where asset-price distortion enters the discussion. A property price can rise without an equal amount of new currency being printed; credit, expectations and marginal transactions can reprice an entire market. But when undeclared or criminal proceeds compete for the same finite land, gold or businesses, they can add purchasing pressure that formal statistics struggle to explain. The issue is not that higher property values prove counterfeiting. The issue is that hidden capital can influence visible prices.

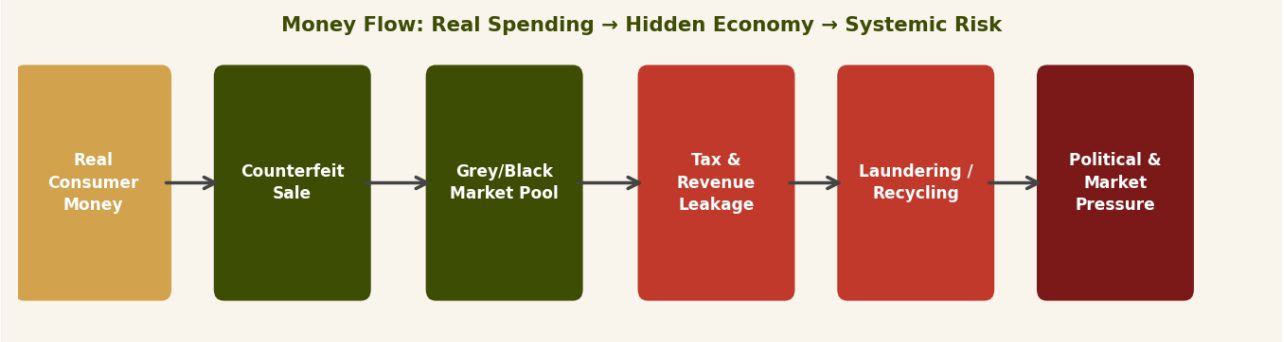


Figure 3: *YTHICS systemic pathway. The model shows how genuine consumer money can migrate into hidden economic channels and later return as market distortion or institutional pressure.*

That matters politically because economic stress rarely remains economic. Inflation, unemployment, low growth, weak public services and corruption affect public trust. IMF research on political fragility finds that low growth, high inflation, weak external positions, political instability and conflict can reinforce one another and raise the probability of political breakdown in structurally fragile countries. Separate IMF research also finds that price shocks are more likely to trigger anti-government unrest when economies are weak, institutions are poor and corruption is high.

Counterfeiting is therefore not a secret button that changes governments. It is an amplifier. In strong states, customs, tax systems, formal retail and financial intelligence can contain much of the damage. In weaker states, the same leakage can add pressure to unemployment, fiscal stress, corruption and public distrust. Over time, that can contribute to electoral swings, cabinet turnover, street unrest and, in the most fragile environments, more serious political disruption.

There is also a labour dimension that deserves plain language. Unemployment is one of the quiet suppliers of this economy: when people cannot find formal work, illicit networks find their workforce ready-made. And the loop runs both ways, because every formal job displaced by counterfeit trade adds someone to that pool. Equal and accessible labour opportunity is therefore not only a social objective; in this context it is a counterfeit-control instrument. A country that allows this loop to compound can drift, over years, toward a condition where parts of its economy stop functioning formally at all - and repairing that condition is measured in decades, not budget cycles.

2033: A Strategic Inflection Point, Not a Forecast

YTHICS uses 2033 as a stress-test horizon, not as a prediction that the world ‘breaks’ in that year. Starting from the roughly USD 0.60 trillion GDP-scaled 2026 baseline, 3 simple growth paths give a useful range. At 6% annual growth, the modeled value reaches about USD 0.90 trillion by 2033. At 8%, it crosses roughly USD 1.03 trillion. At 10%, it reaches about USD 1.17 trillion.

That makes 2033 a reasonable central scenario for a $1 trillion measured-equivalent threshold if counterfeit intensity grows faster than the formal economy. It is not an official forecast, and it does not include the full shadow economy. Its purpose is to show the cost of waiting.

The political meaning of that threshold is not a single global collapse. It is uneven pressure. Countries with strong tax administration, customs, digital payments and trusted institutions may absorb much of it. Countries already carrying high unemployment, debt stress, corruption or weak public services may not. In those places, even modest additional leakage can become politically expensive because citizens experience the outcome through prices, jobs and public services long before they see it in a national statistic.

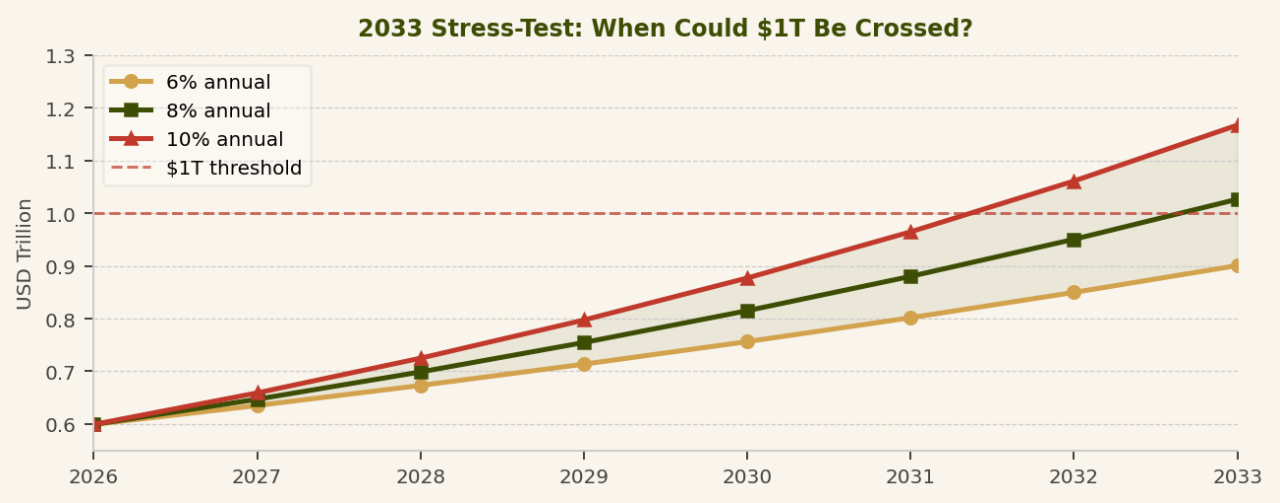


Figure 4: *YTHICS 2033 stress test. Starting point: ~USD 599B 2026 GDP-scaled baseline. Growth assumptions of 6%, 8% and 10% are analytical scenarios, not forecasts from OECD, IMF or EUIPO.*

5. What Needs to Change by 2030

The answer cannot be only 'inspect more products'. Trade is too large, too fragmented and too digital. The stronger response is to make the legitimate economy easier to verify than the illicit one.

One honest admission should frame everything that follows: counterfeiting is not completely fixable, but it is defendable. Like a malignancy that has already spread through the body, it cannot be treated one organ at a time once it has metastasized.

Defending early is therefore more important than fixing late - and defense is built into the system, not added after the damage.

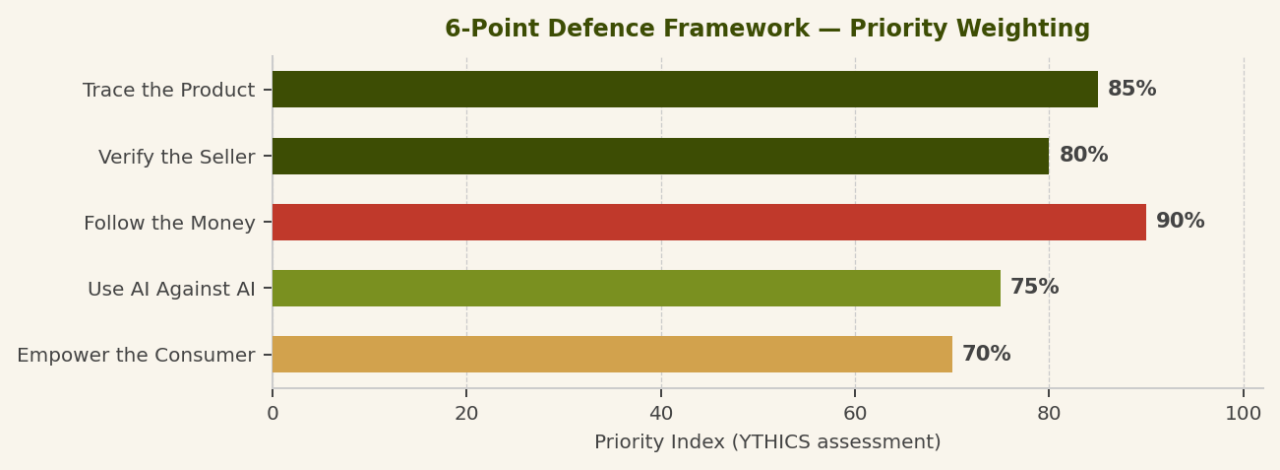


Figure 5: *YTHICS 6-point defence framework - priority weighting based on systemic impact assessment.*

1. **Trace the product -** Use serialisation, interoperable product identity and digital product-passport systems where they genuinely improve provenance - an approach the EU has already planned to implement. Critically, traceability must not remain a capability of governments and ministries alone; consumers should hold the right, and the tools, to verify what they are buying at the point of purchase.
2. **Verify the seller -** Marketplaces, distributors and payment systems should make repeated anonymous re-entry difficult and keep stronger records of who is selling what; this should be completely under Nation's core ministry control.
3. **Follow the money -** A counterfeit seizure should often start the investigation, not end it. Customs, tax authorities, financial-intelligence units, platforms, banks and rights holders need a shared picture.
4. **Use Synthetic Intelligence against Synthetic Intelligence -** AI can generate deception, but it can also compare images, detect seller clusters, flag unusual transactions and help investigators find patterns humans would miss.
5. **Measure the hidden impact -** Governments should track more than seizure value. Tax leakage,

repeat sellers, dangerous goods, job displacement, labor abuse, platform removals and links with wider organized crime all matter.

6. **Empower the consumer -** Consumer courts and grievance systems - including in developing economies - need to become fast, digital and inexpensive to use by citizens. When compliance is easy for honest sellers and redress is easy for buyers, transparency itself becomes a stabilizer; the market begins to defend itself long before enforcement arrives.

Conclusion

Counterfeiting is no longer only a fake product problem. It is a competition between a visible economy and an invisible one.

The visible economy pays workers, tax, compliance, testing and accountability. The illicit economy survives by using the gaps between them. Every counterfeit transaction begins with something genuine - **someone's income and someone's trust**. That is the quiet tragedy of this economy: good money, earned honestly and spent in good faith, ends up serving the wrong purpose.

Synthetic Intelligence raises the stakes because it can manufacture the signals that once helped people distinguish real from fake. If the product, seller, review, invoice, voice and identity can all look genuine, enforcement cannot stop at the package.

The policy question is therefore larger than 'Is this product real?' It is: Who sold it? Where did the money go? Can the transaction be traced? Can the evidence around it be trusted? And how much invisible economic activity can a state tolerate before it becomes a strategic weakness?

We thought counterfeiting was about fake products. Synthetic Intelligence has other plans.

Forecast note. The 2026 and 2033 figures above are YTHICS analytical scenarios built from the OECD/EUIPO 2021 measured trade estimate and IMF nominal world-GDP data. They are not official counterfeit-market estimates. The article deliberately separates measured evidence from strategic inference.

References:

1. OECD & EUIPO (2025). Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges. OECD Publishing. https://doi.org/10.1787/94d3b29f-en;
2. OECD & EUIPO (2026). From Fakes to Forced Labour: Evidence of Correlation Between Illicit Trade in Counterfeits and Labour Exploitation. OECD Publishing;
3. International Monetary Fund (2026). World Economic Outlook Database, April 2026. World GDP, current prices, US dollars;
4. INTERPOL (2026). Global Financial Fraud Threat Assessment, Second Edition, March 2026;
5. INTERPOL. Illicit goods - the issues. Transnational organised crime, corruption, money laundering and related offences;
6. European Commission DG TAXUD & EUIPO (2025). EU Enforcement of Intellectual Property Rights: Results at the EU Border and in the EU Internal Market 2024;
7. EUIPO & Europol (2020). IP Crime and Its Link to Other Serious Crimes - Focus on Poly-Criminality;
8. IMF (2024). Political Fragility: Coups d'État and Their Drivers. IMF Working Paper 2024/034;
9. IMF (2023). Social Unrests and Fuel Prices: The Role of Macroeconomic, Social and Institutional Factors. IMF Working Paper 2023/228;
10. YTHICS Research & Development (2024). Counterfeit Goods Surge Fuelling Global Economic Downturn. White paper, 26 September 2024.

Selected source links:

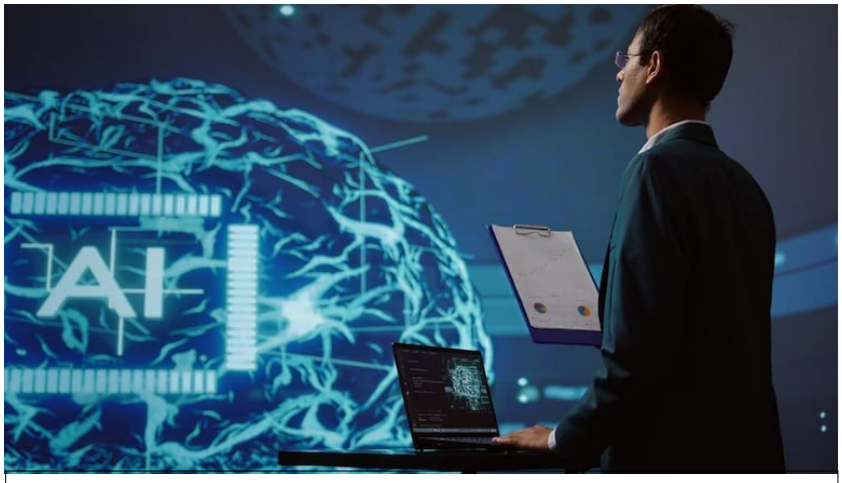
- https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en.html;
- https://www.oecd.org/en/publications/from-fakes-to-forced-labour_540dc43e-en.html
- https://data.imf.org/Datasets/WEO;
- https://www.interpol.int/en/content/download/24291/file/INTERPOL%20Global%20Financial%20Fraud%20Threat%20Assessment%202026.pdf;
- https://www.interpol.int/Crimes/Illicit-goods/Illicit-goods-the-issues;
- https://www.euipo.europa.eu/en/publications/eu-enforcement-of-intellectual-property-rights-results-2024;
- https://www.imf.org/en/Publications/WP/Issues/2024/02/16/Political-Fragility-Coups-dtat-and-Their-Drivers-544943;
- https://www.elibrary.imf.org/view/journals/001/2023/228/article-A001-en.xml.

ARTIFICIAL INTELLIGENCE (AI)

Infrastructure as Leverage: Chinese AI and Its Consequences

Jack LINDSTROM (USA)

In November 2025, as the world was swept up in the AI revolution, Singapore made a unique decision, relinquishing Meta's Llama and instead building it's sovergin AI model on Alibaba's Qwen. This development came after Singapore's SEA-LION program's deliberation, selecting Qwen due to its high scoring on Southeast Asian languages on the regional benchmark SEA-LION established, SEA-HELM. The program had previously been built on Llama and released a Gemma-based model only months prior; however, Singapore's official made this decision as one of advancing regional sovereignty, largely due to the fact that the model is open-source and forkable. This reflected a deeper pattern, one of the significance of Chinese technology in the default choices which stretch far beyond Beijing's formal orbit. It is this logic in China's commitment in AI standard-setting in a global scope, especially on territories in the Global South where Western influences and the vigilance for national security are not overwhelmingly prevailing, and the opportunist peripheries of the Global North (such as some less advanced economies within the EU), is predicated on the overarching logic of shared interests and thereby asymmetrical dependence. Put bluntly, dependence on infrastructure innately outlasts changes in governance.



Source: https://www.ndtvprofit.com/technology/china-explores-ai-to-predict-potential-dissenters-leaked-documents-show-11576360

Singapore's decision is one that establishes a concerning pattern of powers choosing infrastructure benefits in the short term, for a cheaper price than competitors, but with a long-term cost of dependence and policial leverage. China is the master of such negotiations, and this logic is embedded within Chinese domestic politics and forgien policies alike. It is an embodiment of China's strategic preference for transactional exchange of interests, i.e., Quid pro quo, and infrastructural hostage to lock down long-term political-economic benefits and adherence to the advantage of the ruling CCP both at home and abroad. One should note that this idiosyncratic tactic is deliberately devoid of Western values, ideologies, and idealism, such as democracy, universal human rights, and political accountability, as fundamental

principles to shape and constrain behaviors of state actors and govern human societies. Therefore, AI standard-setting is constantly modified and updated by competing political-economic forces, rather than a result of unimpeded technological dissemination and evolution into all possibilities and scenarios.

This dynamic is far from speechcraft and rhetorical influence. Beijing's 2018 China Standards 2035 push, as well as the 2021 National Standardization Development Outline following it, explicitly direct Chinese firms to increase their technical capabilities and export Chinese-set specifications internationally in priority sectors including AI, using Belt and Road projects and standards bodies as delivery channels. This is a large step from how Western-led standards bodies such as the International Organization for Standardization operate, as such institutions are voluntary and multi-stakeholder, aggregating competing input from firms and national delegations without a single government directing the outcome. China's approach is deliberately different, explicitly subordinating standard-setting to the state's industrial strategy.

Put bluntly, Beijing is actively seeking to establish projects that create international obedience to China through slow and deliberate standardization of Chinese technology.

The enthusiastically promoted One Belt, One Road Initiative (the BRI) aims at not only building physical infrastructure to integrate the Eurasian continent, but also absorbing countries and economies involved into China's orbit through, for example, technological dependence, and trade and investment reliance. The latter is intangible by nature, yet nonetheless addictive, country-specific, and potentially extortionate by coercive means at some point. China's AI standard is a technological shell with a monopolized political core inside. The Chinese authority wants to popularize and embed it as the default technological undercurrent for global adopters. The BRI reveals China's global ambition and expansive tendency under the disguise of multilateral co-development and a seemingly innocuous Chinese proposal for non-Western globalism. Once Chinese technological protocols, hardware specifications, and operating standards are organically integrated into the global AI blueprint, serving as the inherently exclusive and less compatible infrastructural foundation that applications rely critically upon to function, it can create enormous technological inertia for adopters. Extremely high switch costs to separate from it or simply to diversify by incorporating alternative systems can deter almost any second thought in a future scenario.

This is reflected from a ground perspective as well as a bird's-eye view, as Ecuador's ECU-911 system, established under a 2011 agreement, was financed by a $240 million loan from Beijing. Ecuador contracted the Chinese state-owned CEIEC and hardware supplier Huawei to establish a nationwide surveillance and emergency-response network which went into operational capability in November 2016. Within a few years, the system relied on more than 4,300 Huawei-supplied cameras nationwide, including a facial recognition capability deployed at the airports in Quito and Guayaquil as well as the city of Cuenca. This tool, meant to be a crime-fighting establishment to Ecuadorans, was later reported to have fed footage to the country's domestic intelligence service. Ecuador's dependence on Chinese-built and Chinese -manufactured hardware for core public safety functions is precisely the kind of technological trap described; once installed, the cost of removing the cameras, servers, and software is high enough that a change in government will not lead to a systemic replacement. It is, put simply, a one-way entry trap.

China dominates legacy chips through its remarkable manufacturing scale and extraordinary ability to cost-down. Weaponization of this competitive advantage by China is entirely possible. However, the country is strictly excluded from Extreme Ultraviolet Lithography (EUV) equipment provision that is monopolized by the Dutch firm, ASML, a restriction the Dutch government formalized through export-control regulations that took effect in September 2023 and tightened further in 2024. As well as advanced and high-capacity chips under the size of 7 nanometers, predominantly manufactured by TSMC for Nvidia, notably H100 and the Blackwell series, and others, exports of which have been subject to US licensing requirements since 2022. China's hostile and confrontational relationship with Taiwan carries a real, if debated, military risk rather than a fixed prediction. In 2021 the then-commander of US Indo-Pacific Command warned China could be capable of moving against Taiwan within six years, the so-called Davidson window, which runs through 2027, and a 2023 CSIS wargame of a Chinese amphibious invasion found that while a joint US-Taiwan-Japan defense would likely repel it, doing so would come at extraordinarily high military and economic cost to all sides, underscoring the risk to the security and stability of global advanced-chip supply chains. In addition, the intensifying competition and rivalry between the US and China for global preeminence, especially over high-techs that can be instrumentalized for defense, and military purposes or revolutionize economic productivity and sophistication, notably AI, add more geopolitical and geoeconomic uncertainties and contentions to an already volatile and tumultuous situation in the highly globalized semiconductor industry. AI serves as a modern catalyst for conflict; one must be wary of its implications for Chinese leverage.

For state actors that fall between the dueling giants in the US-China AI race, hedging between both powers is not a sustainable long-term strategy, especially from a strategic point of view. The key reasons behind this are America's secondary sanctions and American security and stability provisions for conflict-ridden regions, such as a 2023 nuclear umbrella extension to South Korea via the Washington Declaration,

wherein major semiconductors such as Samsung and SK Hynix are located. The enormous market capacity possessed by the US and China, respectively, with politically filtered entry barriers and operational regulations, serves another role in the same rationale of unsustainable longevity of this middle ground strategy. Lastly, ongoing and deepening derisking or decoupling driven by political incompatibility, divergent economic ambition and interests, as well as colliding national security pursuits, all prove a barrier to this long-term strategy. State actors at this time can choose either the US or China, but not both, no matter how great the opportunity cost may be.

Singapore might seem to be an exception, and the country is walking on a tightrope. This tiny yet commercially prosperous financial and logistical hub with both Eastern and Western heritages in Southeast Asia positions itself as a bridge between the US and China. This strategic choice actually requires extraordinary diplomatic skills and another crucial precondition, which is that its relationship with China does not jeopardize the security interests of the US in the region and beyond, and the reverse is also true from China's strategic perspective. However, as the US-China AI race escalates, it might not be attainable in reality when the space for diplomatic maneuverings and strategic ambiguity ceases to exist in any viable form.

Singapore's position reflects the strain established by these policies; in 2024, a Singapore-registered firm, Megaspeed, backed the Chinese gaming and cloud company 7Road. Megaspeed committed to purchasing billions of dollars in Nvidia GPUs, even as Singapore's share of Nvidia's reported revenue vastly exceeded the quantity of chips delivered within its borders. This gap drew US scrutiny after China's DeepSeek was released in early 2025 as a competitive AI model that appeared to rely in part on restricted hardware from FDPRs. By early 2025, Singaporean prosecutors had separately charged individuals accused of routing Nvidia-powered servers through the city-state to China, thus underscoring the difficulty for a sophisticated, rules-based hub to keep its balancing act above suspicion once chip flows themselves become the arena for great power competition.

It is noteworthy that China's infamous red supply chains have already infiltrated deeply into those of its neighboring countries and economies, notably Singapore, Malaysia, Taiwan, South Korea and even Japan. These destinations are plagued by rampant smuggling of advanced chips and servers to China's jurisdiction. Apart from document forgery and establishing shell companies, the Chinese state controls a large number of shadow agents and entities hidden in the gray zones and institutional loopholes of the vast and expanding logistical networks in Asia centered around major hubs and powerhouses of electronics, semiconductors, and AI-related, high-tech industries. These aforementioned Asian countries rely critically on America's military protection to a significant degree. Yet, they also desire China's enormous markets in combination. If they truly outweigh security over trade opportunity, then they should resist gradual encroachment of China's expanding sphere of influence and thoroughly eliminate any presence of red supply chains in explicit and/or covert forms from their own networks, as well as upgrade their institutionalized oversight mechanisms to better cooperate with the US authorities. Otherwise, they too might be excluded from the emerging democratic and rule-based supply chain ecosystem built on shared values, mutual trust, and collective security.

The Chinese action to deliberately expand into other nations for its own gain is nothing new; however, it is critical to halt when it takes place deep within US-allied nations and occurs in the field of the most volatile technology yet established.

Risks and their presence are not hypothetical by nature; they are either actualized or resting at a potential to become such. US federal prosecutors have documented networks that relabeled and redistricted Nvidia H100 and H200 processors, falsified end-user paperwork, and reputedly exported hardware through Southeast Asian intermediaries to reach Chinese buyers. One of these buyers was a US-based network the Department of Justice claimed exported or attempted to export more than $160 million in restricted GPUs between October 2024 and May 2025. This evidence presents a clear realization of this risk. China pursues constant AI standard-setting and infrastructure exports; it should then be evident that workarounds to the chip supply chain controls are not separate initiatives from these. Instead, it is the establishment of a long-term strategy to create a durable, asymmetrical dependence that partner states find difficult to reverse- it is fundamentally a one-way entry trap.

Both US policymakers as well as mid-sized and developing states which fall between the giants of Washington and Beijing have a response role to play. Washington must pair export-control enforcement, shuttering the transshipment loopholes exposed by Singapore, and retain an affordably priced alternative to Chinese infrastructure. Chinese leverage is a trap of economic appeal- Washington must respond with an even better one. Evidently, restriction does not work- at least not alone, and as such it is the economic counterpart of a deal to prevent abusive leverage from China taking hold.

Partner governments of Washington must build institutional capacity to audit their digital and telecommunications supply chains for undisclosed Chinese state involvement. This must occur before infrastructure one-way trapping suffocates that state with a scarcity of alternatives.

Without this combination of enforcement and alternatives, the shared interests Beijing offers will prove more durable, in practice, than the ad hoc coalitions Washington assembles to respond.

Wars are not won with responsive strategies; they are won with initiative.

CONTEMPORARY GLOBAL SITUATION

Ordo Pluriversalis[1] - The Fragmentation of the International System

Krzysztof ŚLIWIŃSKI (Hong Kong)

The future international system is likely to be characterised by divisions into distinct regions, each governed by what may be termed geopolitical dominions. This short paper identifies six such geopolitical dominions. This competition is expected to be violent, as history shows when major powers delineate their spheres of influence.

Source: https://www.labelsandlabeling.com/news/conventional-printing/koenig-bauer-launches-impact-strategy

The American Dominion

The US prioritises primacy by maximising offensive power. Under offensive realism, it sees great power competition as inevitable and seeks to prevent peer competitors by dominating key theatres[2]. This logic and geostrategic emphasis on the Eurasian "chessboard" shape its multi-regional posture[3].

U.S. operations show a rebalanced yet assertive global footprint. In the Western Hemisphere, Washington has intensified direct interventions—notably the 2026 removal of Venezuela's leadership—to reassert dominance in its sphere and deny extra-hemispheric rivals resources and influence, reflecting the realist imperative to secure the near abroad. In the Middle East, campaigns targeting Iranian infrastructure and blockading the Strait of Hormuz safeguard energy chokepoints and prevent broader Eurasian consolidation against American interests.

Across the Indo-Pacific, the focus remains deterring rising China through forward military presence, alliance reinforcement, and technological containment. This theatre exemplifies Mearsheimer's "tragedy" of great power politics: structural anarchy compels the hegemon to check the ascending peer. By contrast, Europe receives less commitment, as Washington urges allies to bear more against Russia.

The European Dominion (under German Leadership)

EU efforts centre on Europe and its rimlands. In Eastern Europe, operations include military-financial support for Ukraine, accelerated enlargement to Ukraine and Moldova, and hybrid countermeasures against Russian sabotage and disinformation. These aim to prevent Russian dominance, stabilise the eastern flank, and reflect Germany's post-"Zeitenwende" push for European responsibility.

Beyond the neighbourhood, the EU, under German guidance, pursues Indo-Pacific de-risking through trade agreements and technology standards, extending influence to secure chains. Relations emphasise defence autonomy and resilience amid U.S. shifts.

German leadership is not openly claimed. Instead, the 2023 National Security Strategy cites Germany's 'special responsibility' for peace, security, prosperity, stability, and establishing the EU Rapid Deployment Capacity[4]. German leadership posits Germany as a leader in European Security, declaring that becoming Europe's 'best equipped armed force' is important[5]. Former Chancellor Scholz openly claimed: "As the most populous nation and leading economic power at the continent's centre, our army must become Europe's cornerstone of conventional defence, the best-equipped force"[6]. Germans are pressing for a unified European army, which would give them access to French nuclear weapons—a bypass of international law that bars Germany from ever developing its own nuclear weapons[7].

The Russian Dominion

Russia deploys hybrid tools blending hard, soft, and informational instruments. Militarily, it uses coercive force and security guarantees to reintegrate the post-Soviet space as prudent geopolitics, countering fragmentation and maintaining depth[8]. Hybrid warfare fuses conventional operations with disinformation, cyber activities, and proxies to achieve objectives below conflict, as shown in Crimea[9]. Energy diplomacy: oil and gas pipeline control enables coercion across Europe and Eurasia, tying neighbours to Moscow's orbit.

"Russian World" (*Russkii Mir*) projects soft power through cultural and conservative ties among Russian-speaking diasporas and elites abroad, extending influence into Europe and Global South[10]. This aligns with consistent national-identity-rooted foreign policy prioritising sovereignty, great-power status, multipolarity over Western dominance[11].

Russia's geopolitical heft stems from geography-enabled advantages wielded through hybrid military-economic tools, soft-power narratives, and policies. Despite economic vulnerabilities, these instruments sustain its revisionist role, challenging the post-Cold War order as geography shapes ambitions, vulnerabilities, and adaptation.

The Chinese Dominion

Beijing operationalises reach through a toolkit emphasising economic statecraft, military modernisation and narrative power. The Belt and Road Initiative (BRI), launched in 2013, anchors influence, directing infrastructure investment across 140 countries to secure energy routes and extend leverage without coercion[12]. Rapid military transformation—A2/AD capabilities, blue-water naval expansion, and precision-strike systems—aims to deter intervention near China's shores while projecting power to dominate the region[13].

Territorial consolidation further underpins strategy; China has largely resolved land-border disputes to stabilise its periphery, freeing up resources for maritime assertiveness[14]. Ideational tools reinforce efforts: narratives of "peaceful development", multipolarity, and rejuvenation cultivate soft power via diplomacy, while techno-economic dominance embeds influence in governance.

China's power rests on geography-enabled scale and advantages, deployed through hybrid economic-military tools and grand strategy. Beijing challenges the U.S.-led order via connectivity, capability building, and assertiveness rather than confrontation, despite tensions with Washington. Regional backlash and domestic headwinds persist, yet fusion sustains China's trajectory as a competitor.

The Indian Dominion

New Delhi advances reach through a grand-strategic toolkit prioritising strategic autonomy, multi-alignment, and capability accretion over formal alliances. Diplomatically, India deepens the Quad with the United States, Japan, and Australia, while sustaining ties with Russia, engaging BRICS, and cultivating Global South partnerships[15]. Militarily, a nuclear triad, naval modernisation, and border infrastructure deter two-front threats and enable Indian Ocean Region (IOR) power projection, consistent with realist imperatives to maximise relative power[16].

Economically, initiatives such as "Act East", supply chain resilience, infrastructure diplomacy, and trade agreements extend influence without coercion. Soft power—rooted in credentials, cultural exports, and a 30-million-strong diaspora—amplifies India's appeal. This approach combines historical caution with pragmatic action[17].

India's geopolitical heft stems from geography-enabled centrality in a region, wielded through adaptive diplomatic, military, and economic tools and resilient autonomy. Despite economic asymmetries and neighbourhood challenges, these increasingly position India as a pole shaping Indo-Pacific balance and multipolar governance.

The Iranian Dominion

Iran's geopolitical power stems from its geographical position as a Eurasian crossroads and energy choke point. The world's 17th-largest country, Iran straddles the Persian Gulf and Caspian Sea, borders seven states, including nuclear-armed Pakistan and rivals Saudi Arabia and Iraq, and dominates the Strait of Hormuz, through which roughly one-fifth of global oil trade passes. Mountains and deserts provide defensive depth, while this geography gives Iran vulnerability through encirclement fears and leverage as a buffer and connector across Eurasian transit corridors[18].

Tehran operationalises this reach via an asymmetric, expeditionary toolkit compensating for conventional military inferiority to U.S. and Gulf adversaries. Central is the "axis of resistance"—a network of militant clients and proxies (Hezbollah in Lebanon, Hamas and Islamic Jihad in Gaza, Houthis in Yemen, Shia militias in Iraq and Syria)—used to project power, deter attack, and gain strategic depth without direct war[19].

Ballistic and cruise missiles, supplemented by drones, provide deterrence, while the nuclear program offers latent insurance against regime change.

Energy statecraft and ideological soft power complement tools. Threats to close the Strait of Hormuz or weaponise oil/gas flows coerce markets. Shia and anti-imperialist discourse attract non-state actors and audiences, framing Iran against hegemony[20].

Iran's influence stems from geography-enabled advantages—Hormuz dominance, buffer centrality, and defensive terrain—amplified by asymmetric tools, proxy networks, and missile deterrence. Despite sanctions, isolation, and limits, this strategy keeps Iran a revisionist actor challenging the U.S.-led order.

Conclusion

Two regions in particular are likely to witness the above-mentioned competition between such defined dominions: Africa, rich in resources and strategic locations, and the Arctic, which is emerging as a resource-rich and alternative passage due to climate change.

Apart from the six dominions, the fragmented international system features the growing importance of non-state actors, mostly Transnational Companies (TNCs), especially those developing Artificial Intelligence (AI) and ultimately perhaps even AI itself as a geopolitical actor along with traditional non-state actors such as international organisations (both IOs and NGOs), Transnational Organised Crime (TNOC) or terrorist organisations.

---

[1]*The term Ordo Pluversalis has been "borrowed" from Leonid Savin. See more: Savin, L. (2020). Ordo Pluriversalis: The End of Pax Americana and the Rise of Multipolarity. Black House Publishing.*
[2]*Mearsheimer, J. J. (2001). The tragedy of great power politics. W. W. Norton & Company.*
[3]*Brzezinski, Z. (1998). The grand chessboard: American primacy and its geostrategic imperatives. Basic Books.*
[4]*The Federal Government (2022) Speech by Federal Chancellor Olaf Scholz at The Charles University in Prague on Monday, August 29 2022. https://www.bundesregierung.de/breg-en/news/scholz-speech-prague-charles-university-2080752*
[5]*National Security Strategy. Robust. Resilient. Sustainable. Integrated Security for Germany (2023). Federal Foreign Office, Werderscher Markt 1, 10117 Berlin. https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf*
[6]*"Germany must become 'the best equipped armed force in Europe', Scholz says." Euronews, September 16, 2022. https://www.euronews.com/my-europe/2022/09/16/germany-must-become-the-best-equipped-armed-force-in-europe-scholz-says*
[7]*Germany. The International Campaign to Abolish Nuclear Weapons. Retrieved May 5, 2026, from https://www.icanw.org/germany*
[8]*Krickovic, A. (2014). Imperial nostalgia or prudent geopolitics? Russia's efforts to reintegrate the post-Soviet space in geopolitical perspective. Post-Soviet Affairs, 30(6), 503–528. https://doi.org/10.1080/1060586X.2014.900975*
[9]*Renz, B. (2016). Russia and 'hybrid warfare'. Contemporary Politics, 22(3), 283–300. https://doi.org/10.1080/13569775.2016.1201316*
[10]*Laruelle, M. (2015). The "Russian World": Russia's soft power and geopolitical imagination. Center on Global Interests. https://www.ponarseurasia.org/the-russian-world-russia-s-soft-power-and-geopolitical-imagination/*
[11]*Tsygankov, A. P. (2016). Russia's foreign policy: Change and continuity in national identity (5th ed.). Rowman & Littlefield.*
[12]*Doshi, R. (2021). The long game: China's grand strategy to displace American order. Oxford University Press.*
[13]*Swaine, M. D., & Tellis, A. J. (2000). Interpreting China's grand strategy: Past, present, and future. RAND Corporation.*
[14]*Fravel, M. T. (2008). Strong borders, secure nation: Cooperation and conflict in China's territorial disputes. Princeton University Press.*
[15]*Bajpai, K., Basit, S., & Krishnappa, V. (Eds.). (2014). India's grand strategy: History, theory, cases. Routledge.*
[16]*Mearsheimer, J. J. (2014). The tragedy of great power politics (Updated ed.). W. W. Norton & Company.*
[17]*Bajpai, K., Basit, S., & Krishnappa, V. (Eds.). (2014). India's grand strategy: History, theory, cases. Routledge.*
[18]*Fuller, G. E. (1991). The "center of the universe": The geopolitics of Iran. Westview Press. https://archive.org/details/centerofunivers00full*
[19]*Ostovar, A. (2018). The grand strategy of militant clients: Iran's way of war. Security Studies, 27(1), 130–158. https://doi.org/10.1080/09636412.2017.1416815*
[20]*Tabatabai, A. M. (2020). No conquest, no defeat: Iran's national security strategy. Oxford University Press.*

CONTEMPORARY GLOBAL SITUATION

Maritime Chokepoints: A Risk for Global Sea Trade

Christos BEZIRTZOGLOU (Greece)

1. Introduction to Global Sea Trade

Every day, tens of thousands of vessels navigate a complex network of global sea lanes to keep world trade moving. Around 80% of all international trade travels by sea! Global trade needs open maritime arteries. They need Maritime security, Strategic trade routes and Resilient global logistics.

Since 2020, international eCommerce[1] and global supply chains[2] have experienced major disruptions due to: Geopolitical risks (Hormuz strait crisis, Red Sea rerouting as a result of wars or piracy), Climate change (opening new routes as well as making other routes impracticable), Logistics crisis due to people (2024–2025 Canada Post labour dispute, 2024 United States port strike, 2022 Shanghai port lockdown, 2021 Ever Given accident in the Suez Canal), health issues (COVID-19 pandemic) and/or governments (multiplicity of customs rules, cyber attacks to manipulate navigation systems) and/or infrastructure (incompatible rail track gauge, inadequate port facilities).

Source: https://commoditieshub.ch/en/2026/07/06/the-worlds-maritime-chokepoints/

Straits, Passages and Canals are prime examples of strategic chokepoints. Their importance derives not from the countries surrounding them but from the volume of global trade that passes through them. Local instabilities that affect them have global economic repercussions. The essence of their asymmetric strategy lies exactly in the disproportionate cost-effectiveness (finance and logistic) ratio of alternative solutions.

Finally, we should stress that maritime trade has played a pivotal role in countries, such as China, South Korea or Japan, rising as eminent economic powers as most of the goods they export are transported by ships as well as the raw materials they import, such as hydrocarbons.

Maritime chokepoints have become critical instruments of geopolitical influence in the 21st century. Any disruption, whether it is caused by war, state coercion, piracy, or infrastructure failure, will trigger immediate effects on supply chains, insurance premiums, freight costs, and commodity prices worldwide.

---

[1]In this analysis, we are excluding digital trade transactions of services without need for physical transportation, notably digitally ordered, and either physically delivered —such as booking accommodations— or digitally delivered, like streaming media, cloud computing, or professional services provided online.

[2]In this analysis, we are excluding electrical energy interconnections, such as the Great Sea Interconnector (GSI) between Greece-Cyprus-Israel or the GREGY between Greece-Egypt, constituting parts of the greater economic corridor IMEC, which strategically connects India and Middle East with Europe.

2. Maritime Chokepoints and Mare Liberum

Napoleon said: `La politique des états est dans leur géographie` refering to the usage of geographical entities for political advantage.

Maritime chokepoints are relatively narrow or constrained waterways that, due to their physical characteristics including width, depth, length, and navigability, impose serious limitations on movement and "force traffic to converge" as they themselves have a "limited capacity to accommodate maritime circulation." The nature of a maritime chokepoint can also be measured in this respect by the existence or not of not only alternative maritime but also land-based routes circumventing the chokepoint in question.

The main reasons why they matter are:

1. They offer shorter transit times for faster global supply chains.
2. They help to lower shipping costs and to secure the movement of commodities, including energy.
3. They are the lifeline of global trade by connecting international markets in all continents.

The value of a maritime chokepoint is proportional to its degree of usage and thus be of considerable significance to several countries. That's why they are considered as "keys to the world", "geopolitical weapons" or "the geographical Achilles' Heel" of the global economy, trade, energy and food security. However, at the same time these maritime chokepoints are a strategic importance (economic, military, political) to those who control them. Finally, climate change and environmental concerns have become a risk multiplier as well as an opportunity enabler for the chokepoints.

Shallow canals and channels are also affecting the naval architecture by creating unique ship classifications (i.a. Suezmax, Panamax, Malaccamax, Chinamax) which is the absolute maximum dimensions a vessel can have to navigate their waters safely.

The concept of **Mare Liberum** is the guiding principle for freedom of navigation, global trade, and maritime security. Mare Liberum was revolutionary in the 17th century[3] because it challenged monopolistic claims over the seas and promoted the idea of shared access, which facilitated the rise of maritime powers and facilitated global trade. Contemporary applications include the regulation of shipping lanes, and the protection of global supply chains, emphasizing that oceans are a shared resource essential for commerce, security, and cooperation among nations.

In a nutshell, maritime chokepoints have become strategic pressure points where regional crises can rapidly generate global consequences.

3. Commodities trade flows affected

A diverse range of import and export commodities are affected when disruptions in a maritime chokepoint affect shipping schedules. The three types of effected global trade flows are:

1. **Energy products**, such as crude oil refined petroleum products and Liquefied Natural Gaz (LNG), mainly in the Middle East (straits of Hormuz, Bab el-Mandeb, Suez Canal) on the export side and Asia (straits of Malacca and Singapore) areas on the import side;
2. **Bulk commodities**, such as coal, iron ore, grain, fertilizers, and agricultural products;
3. **Containerised goods**, such as manufactured products.

The interconnected nature of these trade flows[4] creates problems both to exporting as well as to importing countries (i.e. the Gulf countries are major exporters i.a. of mineral fuels &oils, and fertilizers, while at the same time are major imports i.a. of vehicles & transport equipment, and pharmaceutical products).

Finally, any type of prolonged disruptions to transit through these maritime chokepoints[5] are putting additional pressure on global food security either by affecting the availability of key inputs (i.a. fertilizers) with vulnerable and rural regions experiencing the most severe impacts to their crop yields and/or by upsetting the flow of food to non-food producing countries.

---

[3]*Mare Liberum was formulated by the Dutch jurist and philosopher Hugo Grotius in 1604, following a legal confrontation between the Dutch and the Portuguese in relation to the seizure of the Portuguese carrack Santa Catarina in the Straits of Malacca. The central argument of Mare Liberum is that the sea is international territory, and no nation has the right to monopolize it. Grotius based this on what he considered a self-evident principle of natural law: every nation has the right to travel and trade with every other nation. From this, he derived the right of innocent passage over both land and sea, establishing a foundation for modern international maritime law.*

[4]*It is known that in case of crises a lot of money could be made by the dare devils and the innovators. The 2026 global geopolitical situation has given excess profits to ship owners as transport prices have doubled and tripled vis-à-vis the year before.*

[5]*Another aggravating factor that should be added to the food security equation is the climate phenomenon El Niño.*

3.1 The European Union Energy Diversification Strategy

The European Union (EU) is phasing out Russia's fossil fuels, but new dependencies on other providers (Gulf states and United States) were developed. The bloc's imports of Russian gas (including pipeline gas and LNG) fell by 75% between 2021 and 2025. EU imports of gas from Norway have been consistent in the last four years. The 2026 Middle East crisis destroyed the assumption that seaborne LNG was a strategically safer alternative to pipeline dependency.

An overreliance on United States (US) LNG, which is also the most expensive LNG for EU buyers, contradicts the REPowerEU[6] plan of enhancing EU energy security through diversification, demand reduction and making energy more affordable. The US now accounts for ~60% of U LNG imports. This reliance has created a high-risk geopolitical dependency that the US president has exploit it by explicitly linking LNG supplies to demands for modifications of EU legislation.

3.2 An Opportunity for African Countries

Africa's hydrocarbon reserves and proximity could offer the EU the needed extra supply diversification. Africa already supplies around 20% of Europe's gas needs through pipelines from **Algeria** & **Libya** in the north, **Nigeria** & **Mauritania** in the west, and **Mozambique** in the east. That share is growing as new LNG corridors are emerging in Senegal, Côte d'Ivoire, and Angola, while Nigeria holds the reserves to become a significantly larger supplier.

3.3 The Emerging South America Energy Landscape

The global energy map could undergo a profound transformation in the next decade if South America countries, such as **Guyana** (the world's fastest-growing oil producer), **Argentina** (increasing export capacity) and **Venezuela**[7] (holding the world's largest proven oil reserves), manage to attract international investment to become major energy players. These countries could transform their hydrocarbon wealth into lasting geopolitical influence, in particular the first two that are non-OPEC[8] countries.

4. Major Maritime Chokepoints in the World

The thirteen principal key maritime funnels that are used during the global seaborne trade are:

4.1 Four in Europe (Danish straits, Kiel Canal, English Channel & Straits of Gibraltar)
4.2 One in the Americas (Panama Canal)
4.3 Three in Asia (Malacca strait, strait of Singapore, Turkish straits)
4.4 Three in the Middle East part of Asia (Suez Channel, Bab el-Mandeb strait, strait of Hormuz)
4.5 Two in the outskirts of Asia (Eastern Mediterranean Sea, South China Sea)

4.1.1 Europe: Danish Straits (Great Belt, Little Belt, Øresund)

The three Danish Straits are the only sea connection between Baltic and North Sea/Atlantic. It's a critical seaway for northern/eastern EU (Sweden, Finland, Poland, the three Baltic states, eastern parts of Germany) and for residual Russian oil & LNG flows.

They are the key passage for Russia's "shadow fleet" of tankers. In addition to navigational hazards (i.a. high traffic density, shallow waters, narrowness of the straits), to the challenging winter environmental conditions (i.a. fog, ice, strong winds), the old and poorly maintained "shadow fleet" tankers poses a risk to maritime safety and environmental security.

4.1.2 Europe: Kiel Canal

The Kiel Canal is a 98 km long freshwater canal that links the German ports of Brunbüttel on the North Sea to Kiel on the Baltic Sea. The canal reduces the journey between the North and Baltic Seas by 460km by allowing ships to bypass the Jutland peninsula and the Danish Straits.

It was constructed between 1887 - 1895 and relies on a system of vulnerable century old locks.

---

[6]*REPowerEU was introduced in May 2022 in response to Russia's invasion of Ukraine and the resulting energy crisis. Its core aim is to rapidly reduce and ultimately eliminate the EU's reliance on Russian gas, oil, and coal while speeding up the clean energy transition.*

[7]*The importance of Venezuela, as well as the broad Caribbean area, could be understood from the "war for oil" narrative around the 2026 US military intervention to capture Venezuela's incumbent president.*

[8]*The Organization of the Petroleum Exporting Countries (OPEC) is an intergovernmental cartel enabling the co-operation of leading oil-producing and oil-dependent countries to collectively influence the global oil market and maximize profit for its 11 members (including Venezuela). A larger OPEC+ group consisting of OPEC members and 11 other oil-producing countries (including Brazil and Mexico), was formed in 2016 to better control the global crude oil market.*

4.1.3 Europe: English Channel

The 560 km long English Channel connects the North Sea with the Atlantic. The Channel is crucial for United Kingdom (UK)-EU trade as around 60% of trade is estimated to pass between the ports of Calais/Dunkirk and Dover/Folkestone. At the same time, it is a vital economic corridor for the EU connecting the ports of Antwerp (Belgium), Rotterdam (The Netherlands) and Hamburg (Germany) to the Atlantic Ocean.

The only shipping lane in the world that can be crossed underneath thanks to the Channel Tunnel connecting the UK and France!

The high traffic density (more than 180 000 ships per annum plus the multiply daily ferry crossings between France and UK), the frequently severe weather conditions (i.a. fog), and its funnel type geography (from 240km at its maximum width to only 34km at its narrowest) makes the possibility of collisions and/or groundings an unwanted disruptor for the European supply chains.

There are reports that Russia's "shadow fleet" of tankers avoid using this route (and take instead the long sea route around "neutral" Ireland) due to recent EU & UK forces seizure of sanctioned oil. Russia has even used military ship escorts for intimidation.

4.1.4 Europe: Strait of Gibraltar

The strait of Gibraltar is a 14km width gap that connects the Atlantic Ocean to the Mediterranean Sea and separates Europe from Africa. It's the sole natural sea entrance/exit for the entire Mediterranean. It handles ~10% of global maritime traffic; and it's essential for all Mediterranean EU ports (Spain, France, Italy, Greece, etc.) accessing Atlantic/Americas/Africa routes.

Statue of the pillars of Hercules in Ceuta

A combined Gibraltar and Suez closure could affect ~40% of EU seaborne trade. Key products transiting are crude oil and LNG (to/from Mediterranean refineries and markets, including West African and Middle Eastern flows); containers and bulk commodities (grain, fertilisers, ores, manufactured goods).

The multiple national and international interests of the three different jurisdictions (Spain [EU], Gibraltar [UK], and Morocco) are a potential source of tension. The United Nations has identified the Strait of Gibraltar (and the Canary Islands) as critical maritime chokepoints in the trafficking of cocaine from the Sahel countries into Europe.

It is also interesting to note that the Mediterranean loses more water than rivers and rain give back. Thus, it up to the Atlantic to fill up the deficit via the Gibraltar strait! Thus, the Atlantic waters enter the Mediterranean on the surface, whereas the denser Mediterranean waters flow into the Atlantic beneath them, creating tidal surges and hidden turbulence.

4.2 The Americas: Panama Canal

An 80km man-made engineering marvel connecting the Atlantic and Pacific Oceans, vital for American and West-East trade route. The canal created a much shorter connection between the Atlantic and Pacific Oceans, allowing ships to avoid the long journey around South America via Cape Horn or the Magellan strait and saving thousands of miles[9], time, fuel, and money.

Unlike sea-level canals, the Panama Canal uses a massive lock system powered by fresh water. Each vessel transit consumes 197 million Liters of fresh water from Gatún Lake!

France began a major attempt to build a canal across Panama in 1881, led by Ferdinand de Lesseps, who had previously been involved with the Suez Canal. However, difficult terrain, heavy rainfall, landslides, financial problems, and deadly diseases such as yellow fever and malaria caused the French project to collapse. The United States resumed construction in 1904. Instead of building a sea-level canal, American engineers created a massive lock system using Gatún Lake, which sits about 26 meters above sea level. The Panama Canal officially opened to world trade on 15 August 1914.

[9] *In example the route from San Fransico to New York will be 5 200 nautical miles instead of 13 100 when it was obliged to make the long and dangerous journey around the southern tip of South America.*

In 2016, the canal was expanded with new locks capable of handling much larger ships. However, as El Niño climate patterns influence hydrological conditions across Central America resulting in decreasing water levels in Gatún Lake (as was the case during the 2023 draught), the Panama Canal Authority has introduced reduced draft adjustments for its Neopanamax locks.

It handles around 5% of global maritime trade. It is of low relevance for Europe but of particular interest to the United States as the transiting trade is focused mainly on Americas-Asia and US East-West coast travel.

4.3.1 Asia: Malacca Strait

A vital 900km artery in Southeast Asia between the Malay Peninsula and the island of Sumatra, where it joins the Indian and the Pacific oceans. Handles around 60% of global maritime transport and 25% of globally traded goods. Of particular interest to transit hubs such as Singapore or to China for its global import and export energy and trade flow potential.

On top of collision risks between large vessels due to its narrow width and swallow waters, it is an active piracy affected area linked to overlapping jurisdictions that allows pirates to hide from law enforcement. The expression the "Malacca Dilemma" describes China pursue for alternative sea routes as currently is heavily reliant to this waterway for westbound exports and eastbound imports.

The Strait of Malacca is classified as an international strait, a natural sea lane that connects two exclusive economic zones. Within this category, the regime of transit passage applies meaning that all ships enjoy the right of passage that cannot be obstructed, suspended, or subjected to charges simply for transiting the strait.

Three countries (Indonesia, Malaysia, and Singapore) jointly manage the Malacca strait. Indonesia, whose exclusive economic zone covers roughly 70% of the waters of the Strait of Malacca, had captured ~5% of the strait's transhipment value. A gap that is actively pursuing by developing major port projects at Kuala Tanjung in North Sumatra, the Batu Ampar & Tanjung Sauh areas in Batam, and Sabang in Aceh as a deep sea port at the northern entrance of the strait. On the other hand, Malaysia continues to strengthen the position of Port Klang, which processes about 14 million containers annually and ranks among the ten busiest ports in the world, while developing Carey Island Port as a long term capacity expansion.

4.3.2 Asia: Singapore Straits (Phillip's Channel [known previously as Governor's Strait or Strait of John de Silva], New Strait & Strait of Johor)

The three Singapore Straits are a 113km long (with an average width of 19km and only 5km in its narrowest part) strategically important waterway located south of Singapore and north of Indonesia's Riau Islands, serving as one of the world's busiest shipping routes. It is located between the trading zone of greater Bay of Bengal in the west and the mainland & trading ports of the South China Sea in the east.

The Phillip's Channel, in particular, is extremely busy due to the presence of the Port of Singapore, one of the largest and most efficient ports in the world. It is the busiest transshipment port in the world, handling more than 40 million containers annually and serving as the largest bunkering hub on the planet. Thus, freedom of navigation is a condition for survival for the Singaporean economy that depend heavily on maritime trade flows.

The Singapore straits form the eastern extension of the Strait of Malacca and is a critical link between the Indian Ocean and the South China Sea handling around 50% of all global seaborne trade. The depth of the Singapore strait limits the maximum draft of vessels going through the strait of Malacca, having created the Malaccamax ship class.

The Singapore straits and the strait of Malacca sometimes are presented together as the Straits of Malacca and Singapore (SOMS) mainly due to their proximity.

4.3.3 Asia: Turkish Straits (Bosporus & Dardanelles)

Bosphorus[10], also known as the "Strait of Constantinople", is the world's narrowest strait used for international navigation, connecting the Black Sea with the Sea of Marmara. The Bosphorus has immense historical importance serving as a key trade route for centuries and played a central role in the history of the Byzantine Empire. The Dardanelles connect the Sea of Marmara with the Aegean Sea. Around 3-4% of global seaborn oil trade passes from these heavily busy straits.

Both straits separate Europe from Asia and are the sole maritime trade gate of the Black Sea

[10]*According to ancient Greek mythology, it was said that colossal floating rocks known as the Symplegades, or Clashing Rocks, once guarded both sides of the Bosporus and destroyed any ship that attempted to pass through the strait by crushing them. Their destructive power was finally overcome by the Argonaut hero Jason who managed to pass between them unscathed, whereupon the rocks became fixed, opening Greek access to the Black Sea.*

countries to the global markets. The Turkish straits are the only seaway for Bulgaria, Romania, Ukraine, south-western part of Russia, and Georgia to reach the Mediterranean Sea.

The two straits are critical for Eastern/Southern EU and global food security as it facilitates large grain (wheat, maize/corn, sunflower oil—major share of Black Sea/Ukraine/Russia/Kazakhstan exports equal to ~20%+ of global wheat), fertilisers, minerals, and steel exports. They also facilitate regional energy transportation, such as crude oil and petroleum products (from Russia, Caspian/Kazakhstan via Novorossiysk).

Their vulnerability, on top of navigational difficulties linked to the narrowness of the straits and the great density of traffic, has increased since the Russia's war of aggression against Ukraine.

4.4.1 Middle East (Asia): Suez Canal

A key artificial waterway in Egypt just west of the Sinai Peninsula linking the Mediterranean and Red Seas, shortening the voyages between Europe and Asia by avoiding circling Africa. Opened in 1869, it stretches about 193km. Roughly 11% of global petroleum and ~15% of global trade passes through the Suez Canal. It is a major source of revenue for Egypt.

The largest tankers to navigate the Suez Canal are Suezmax vessels and not the bigger Very Large Crude Carriers (VLCC). This fact means that Saudi Arabia can ship (using VLCC tankers) their oil only towards the south and this via either the strait of Hormuz or Bab el-Mandeb. Any blockage on these two chokepoints hurts directly the Saudi Arabian oil exports.

The Suez Canal charges hundreds of thousands of dollars per transit because of its status as artificial infrastructure under Egypt's full sovereignty.

Frédéric-Auguste Bartholdi originally proposed a massive statue for the entrance of the Suez Canal called "Egypt Bringing Light to Asia." When it was rejected, the design was repurposed to become the Statue of Liberty!

Its closure for six days during the *Ever Given* container ship grounding resulted in substantial delays, increased freight costs, and knock-on production effects noticeable globally. The incident illustrated the fragility of global logistics and the need to build resilient shipping as well as alternative networks.

4.4.2 Middle East (Asia): Bab el-Mandeb

The 29 km wide strait, which is narrower than the Strait of Hormuz, is situated between Yemen on the Arabian Peninsula and Djibouti &Eritrea in the Horn of Africa, linking the Red Sea to the Gulf of Aden and the Indian Ocean. Roughly 9% of global seaborne trade, ~11% of global petroleum and one third of India global trade pass through these straits. Together with the Suez Canal they form a critical Europe – Asia artery.

The Bab el-Mandeb Strait[11] (which translates from Arabic as the "Gate of Tears") has become increasingly significant due to security concerns arising from regional conflicts and attacks on commercial shipping (eventually forcing some vessels to select the longer and costlier trip around Africa).

4.4.3 Middle East (Asia): Strait of Hormuz

The 40km strait of Hormuz constitutes the only maritime way in and out of the Persian Gulf to the open seas, with its northern coast controlled by Iran, its southern coast by Oman, while its entry point from the Persian Gulf side is also connected to the United Arab Emirates (UAE).

It is the world's ultimate energy chokepoint, as roughly 26% of the world's LNG (mainly from Qatar and UAE) and 27% of global petroleum passes through its narrow two-mile-wide shipping lanes every single day (80% heading to Asia and 20% in Europe). A 28 million barrels per day oil export corridor for Saudi Arabia[12], Iraq, UAE, Iran (counting for 80% of its overall imports on top of its export needs), Kuwait and Qatar.

---

[11]There is also a significant underwater dimension of the Red Sea straits as around 90% of data traffic between Europe and Asia runs through undersea data cables. The heightened concentration of undersea cables is vulnerable either to intentional sabotage operations (such as the 2022 Nord Stream blasts, the 2023: Balticconnector gas pipe & cables, the 2024 Baltic fibre-optic communications & power cables, and the 2025-2026 telecoms cable incidents) or to ships sinking as a result of attacks by militia (case of the sinking of the Handymax-size Rubymar bulk carrier cargo ship in the vicinity of Bab-el-Mandeb due to Houthi attacks).

[12]In 2026 Saudi Arabia and 13 other countries have announced the creation of a Multinational Maritime Defense Alliance to safeguard freedom of navigation through the Bab el-Mandeb Strait, the Red Sea and the Gulf of Aden. The participating states share a conviction that maritime security is a shared responsibility and that cooperation and coordination among states constitute the cornerstone for confronting common and transnational maritime threats. They declared their intent to protect freedom of navigation, securing international trade routes and energy supply routes through the three waterways, which form a strategic maritime corridor linking the Indian Ocean to the Mediterranean.

Given its strategic importance, geopolitical tensions in the region frequently influence global energy markets.

4.5 Maritime Areas with Similar Characteristics

Other areas in the world that share similar characteristics to the above mentioned maritime chokepoints, such as intense geopolitical competition, high shipping density, discovery of hydrocarbon fields, limited sea lanes and increasing presence of military, are the **South China Sea**, in particular the Taiwan strait, and the **Eastern Mediterranean Sea**, in particular the Aegean, the Levantine, and the Libyan seas.

4.5.1 Eastern Mediterranean (Aegean Sea)

The Eastern Mediterranean includes Greece, Türkiye, Cyprus, Syria, Lebanon, Israel, Egypt and Libya. The region is strategically located at the crossroads of Europe, Asia, and Africa, connecting to the Atlantic via the Strait of Gibraltar, the Black Sea via the Bosphorus & the Dardanelles, and the Red Sea via the Suez Canal.

In particular Greece's Aegean Sea and its main ports (Piraeus, Thessaloniki and Alexandroupoli) located in the western end of the extended maritime system Bab el-Mandeb-Red Sea-Suez Canal-Aegean Sea, constitutes the EU entrance door of a single maritime line of transportation.

Nevertheless, the numerous Aegean Sea islands with their narrow passages as well as the limited sea lanes for the passenger ferries and pleasure navigation boats create a complex operational environment aggravated by delimitation disagreements from Türkiye.

Finally, it is interesting to note that since the Russia-Ukraine conflict, and particularly Ukarine's warfare activities in the Black Sea, the previous traditional presence of the Russian navy in the Eastern Mediterranean since early 2026 has ceased to exist.

4.5.2 South China Sea (Taiwan Strait)

The "silicon shield", Taiwan's dominance in microchip manufacturing at the level of 90% of the world's advanced semiconductors production, is their security lifeline. Any disruption, such as a blockade by China, of the **Taiwan Strait** will have severe consequences for Taiwan (energy strangulation) but would also significantly influence trade (approximately 20% of global maritime and 40% of EU trade passes from this strait) and the world economies via a tech driven crisis due to significant shortage of semiconductors.

In particular, the dangers for EU and the US are that it could severely affect their industrial manufacturing capacity and evolve risks of becoming even more dependent from Chinese products. Nevertheless, in such a scenario China will be affected negatively both at an economic (disruption of import and exports) but mainly from a reputational point-of-view (non-obeyance to the established rules-based international order).

5. Preliminary Conclusions

Whoever shapes maritime traffic through these narrow waterways shapes global energy markets, inflation, shipping costs, and ultimately political stability. It can be considered as the ultimate "geopolitical weapon" in times of overuse or misuse. Maritime chokepoints showcase their importance due to their dual nature as a milieu of power and opportunity for the controlling state(s) as well as an environment of constraints for all stakeholders.

As global trade continues to evolve, the most resilient economies will be those capable of integrating multiple transport corridors into flexible and adaptive logistics systems, thereby reducing their dependence on maritime chokepoints.

We are in the verge of a paradigm shift as we are experiencing a global security and law order under stress with global value chains and global energy flows in realignment. Geopolitical tensions are bringing critical dependencies and chokepoints into the spotlight. Taken together, these shifts suggest that the post-war growth model is eroding.

HYBRID WARFARE

The Human Dimension of Hybrid Warfare: Cognitive Resilience as a Strategic Capability

Aleksandar GRIZHEV (North Macedonia)

Introduction

For much of modern military history, strategic advantage has been closely associated with technological superiority. Precision-guided weapons, satellite systems, cyber capabilities, artificial intelligence and autonomous platforms have transformed the way armed forces prepare for and conduct military operations. It is therefore no surprise that discussions on future conflicts increasingly focus on technological innovation and the race to develop new capabilities. Yet, technology alone does not determine strategic success.

Source: NATO Allied Command Transformation, "Cognitive Warfare: Strengthening and Defending the Mind," 5 April 2023.

Every hybrid campaign, regardless of the tools it employs, ultimately seeks to influence people. Cyber attacks aim to create uncertainty and disrupt decision-making. Disinformation campaigns attempt to undermine trust in institutions and deepen existing social divisions. Artificial intelligence enables faster and more convincing manipulation, but it is still the human perception, judgement and behaviour that determine whether such efforts succeed or fail. Technology may amplify influence, but it does not replace the human dimension of conflict.

This is perhaps the most significant shift in contemporary strategic competition. The objective is no longer only to defeat an opponent's armed forces or destroy critical infrastructure. Increasingly, it is to shape perceptions, influence decisions and weaken the resilience of societies without crossing the threshold of conventional war[1]. The centre of gravity has gradually moved from the physical domain towards the cognitive one, where information, narratives, trust and human behaviour have become strategic assets.

For small and medium-sized states, this development carries implications. They are unlikely to compete with major powers in terms of technological or military resources alone. Their comparative advantage lies elsewhere: in resilient institutions, informed citizens, adaptive leadership and professional military education. These are not "soft" aspects of national security. They are essential elements of national resilience that determine how effectively a state can anticipate, absorb and recover from hybrid pressure.

[1]*NATO, NATO 2022 Strategic Concept, Brussels: NATO, 2022.*

This article argues that cognitive resilience deserves to be viewed as a strategic capability rather than merely a societal characteristic. Building advanced technological systems remains essential, but their effectiveness ultimately depends on the people who design them, operate them and make decisions based on the information they provide. In an era where strategic competition increasingly takes place below the threshold of armed conflict, investing in human resilience may prove just as important as investing in new technologies.

The Changing Character of Hybrid Warfare

For a long time, discussions about warfare were focused on the physical domain. Military success was measured through territorial gains, destruction of enemy forces, or control of critical infrastructure. Even when information operations became more prominent, they were often viewed as supporting activities designed to complement conventional military operations rather than as strategic instruments.

This perception has gradually changed. Strategic competition today increasingly unfolds below the threshold of armed conflict, where influence often replaces coercion and shaping perceptions becomes as important as demonstrating military strength. States no longer rely exclusively on military force to pursue political objectives. Economic pressure, cyber operations, disinformation, diplomatic influence, legal instruments and strategic communication are combined in ways that deliberately blur the distinction between peace and conflict[2].

Technology has undoubtedly accelerated this transformation. Artificial intelligence enables the rapid creation of persuasive content. Social media platforms allow narratives to spread globally within minutes. Data analytics make it easier to understand audiences and tailor messages to specific groups. At the same time, cyber capabilities create opportunities to disrupt essential services without firing a single shot. Yet these developments can sometimes create the impression that technology itself has become the decisive factor in hybrid warfare. This is a logical, but incomplete conclusion. Technology does not create fear. It amplifies it. Algorithms do not generate distrust. They accelerate its spread. Artificial intelligence does not weaken democratic institutions. It exploits existing vulnerabilities that already exist within societies.

The effectiveness of every hybrid activity ultimately depends on how individuals perceive information, how institutions respond under pressure, and how societies collectively interpret uncertainty. The same disinformation campaign may have very different effects in two countries with comparable technological capabilities, but different levels of institutional trust, media literacy or social cohesion. Likewise, sophisticated cyber capabilities achieve strategic impact only when they influence human decisions or undermine confidence in the state's ability to respond.

For this reason, the growing technological sophistication of hybrid threats should not divert attention from their primary objective. The target is rarely the technology itself. The target is the human being behind the screen, the public official making decisions under uncertainty, the military commander interpreting incomplete information, or the citizen deciding whom to trust[3]. Understanding this distinction is essential. It shifts the discussion from the tools used in hybrid warfare to the people they are designed to influence. Only then does it become possible to understand why cognitive resilience deserves far greater attention in contemporary security thinking.

Cognitive Resilience: The Decisive Strategic Capability

One of the challenges in discussing cognitive resilience is that the term is often used in very broad and sometimes vague ways. It is associated with media literacy, critical thinking, resilience against disinformation, psychological preparedness, or even social cohesion. While all these elements are important, none of them alone adequately explains why some societies remain resilient under sustained hybrid pressure while others become increasingly polarised, distrustful and vulnerable to manipulation.

At its core, cognitive resilience is the ability of individuals, institutions and societies to maintain sound judgement and effective decision-making despite uncertainty, information overload and deliberate attempts to influence perceptions. It is not about rejecting information or becoming immune to influence. Such an expectation would be unrealistic. Every society is exposed to competing narratives and every individual is susceptible to cognitive biases[4]. The real question is whether these influences affect a society's ability to make sound decisions and maintain trust in its democratic institutions. This distinction deserves greater attention. Much of the current debate still treats resilience primarily as a technological issue.

---

[2]Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies, 2007.

[3]NATO Allied Command Transformation, "Cognitive Warfare: Beyond Military Information Support Operations," 2023.

[4]Kahneman, Daniel. Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011.

Governments invest in cyber security, artificial intelligence, monitoring platforms and fact-checking mechanisms. These capabilities are undoubtedly necessary and will become even more important in the future. However, they address only part of the problem. A society equipped with advanced technologies may still struggle to respond effectively if its institutions fail to communicate in a coordinated manner, if public trust is already weak, or if political polarization prevents collective action during crises.

Perhaps this is where the human dimension becomes most visible. Hybrid campaigns rarely create entirely new social tensions. More often, they identify existing vulnerabilities and amplify them. They exploit uncertainty rather than create it, reinforce distrust rather than invent it, and deepen divisions that already exist within society[5]. Technology simply increases the speed, scale and precision of these processes. For that reason, cognitive resilience should be understood as something that extends beyond the individual. It operates simultaneously at several interconnected levels. At the individual level, it depends on critical thinking, media literacy, emotional self-awareness and the ability to evaluate information without reacting impulsively. At the institutional level, it reflects the capacity of public authorities to coordinate responses, communicate transparently and maintain credibility under pressure. At the societal level, it is closely linked to social cohesion, public trust and the willingness of citizens to support democratic institutions even during periods of prolonged uncertainty.

These levels constantly influence one another. Citizens who trust institutions are generally less vulnerable to manipulation, while institutions that communicate openly are more likely to preserve that trust. Conversely, when trust deteriorates, even accurate information may be questioned, official communication becomes less effective and opportunities for external influence increase significantly.

From this perspective, cognitive resilience should no longer be viewed as a desirable by-product of good governance. It represents an essential component of national security. In an era where strategic competition increasingly targets perceptions before infrastructure, confidence before capability and behaviour before territory, the resilience of the human domain becomes a strategic asset.

Preparing People for the Cognitive Battlefield

If cognitive resilience is to be treated as a strategic capability, it cannot be developed only during crises. Like every other capability, it requires continuous investment, training and adaptation. This is perhaps one of the most important lessons emerging from the changing character of hybrid threats. States have become increasingly aware of the need to protect networks, modernise military equipment and strengthen cyber defence, yet considerably less attention has been devoted to preparing people to operate effectively in complex information environments.

This challenge extends well beyond media literacy or the ability to identify disinformation. Decision-makers, military leaders and public institutions are expected to function under conditions characterized by uncertainty, incomplete information and competing narratives. They must make timely decisions despite ambiguity, communicate consistently during crises and maintain public confidence even when perfect information is unavailable. These are not purely technical competencies. They are cognitive and organisational skills that require deliberate development.

Professional military education has an important role to play in this process. Modern military professionals are expected not only to understand emerging technologies, but also to recognize how information influences behaviour, how cognitive biases affect decision-making and how adversaries seek to exploit organisational vulnerabilities. Developing critical thinking, ethical judgement, cultural awareness and the ability to challenge assumptions should therefore be regarded as operational requirements rather than academic aspirations.

The same applies beyond the military domain. Building cognitive resilience requires cooperation among government institutions, academia, civil society and the media[6]. No single institution possesses all the necessary expertise or authorities to address hybrid threats independently. Effective responses depend on trust, coordination and a shared understanding of the challenges rather than on isolated organisational efforts. In many respects, resilience becomes less a question of organisational capacity than of organisational relationships. Perhaps this is where one of the greatest misconceptions about hybrid warfare emerges. Hybrid threats are often described as something entirely new, requiring entirely new solutions. However, many of the capabilities needed to strengthen cognitive resilience are already familiar. Transparent institutions, credible public communication, professional education, adaptive leadership and public trust have always contributed to national security. What has changed is not their importance, but the strategic environment in which they operate. The cognitive domain has made these capabilities more visible, more contested and ultimately more decisive.

[5]*European External Action Service (EEAS), 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, 2025.*

[6]*NATO Allied Command Transformation, "What Resilience Means for NATO and Why It Matters Now," 19 December 2025.*

For small and medium-sized states, this observation is particularly relevant. While they may not always possess the technological or financial resources available to larger powers, they can invest in resilient institutions, well-educated professionals and a culture of informed decision-making. These investments are neither symbolic nor secondary. They constitute one of the most sustainable ways of strengthening national resilience against hybrid threats.

Rethinking National Security in the Cognitive Age

The growing emphasis on cognitive resilience does not imply that technology has become less important. On the contrary, technological innovation will continue to shape military capabilities and strategic competition for decades to come. Artificial intelligence, autonomous systems and advanced cyber capabilities are already transforming how information is collected, analysed and employed in support of political and military objectives.

The challenge is that technological superiority alone no longer guarantees strategic advantage. Modern conflicts increasingly demonstrate that highly capable institutions may still struggle when public trust erodes, when societies become deeply polarised or when decision-makers are overwhelmed by competing narratives and uncertainty. Strategic advantage therefore depends not only on what states possess, but also on how effectively they think, adapt and make decisions under pressure.

This observation has broader implications for national security policy. Investments in cyber defence, intelligence and advanced technologies should be accompanied by comparable investments in education, institutional learning and leadership development. These capabilities reinforce one another. Technology improves awareness and expands available options, while cognitive resilience enables individuals and institutions to interpret information, make sound judgements and respond coherently during crises.

Ultimately, resilience should not be understood as the responsibility of a single institution or sector. It is a whole-of-society capability that develops gradually through education, professional standards, transparent governance and public trust. Building such resilience is neither a short-term project nor a reaction to a particular crisis. It represents a long-term investment in national security that becomes increasingly valuable as strategic competition continues to evolve.

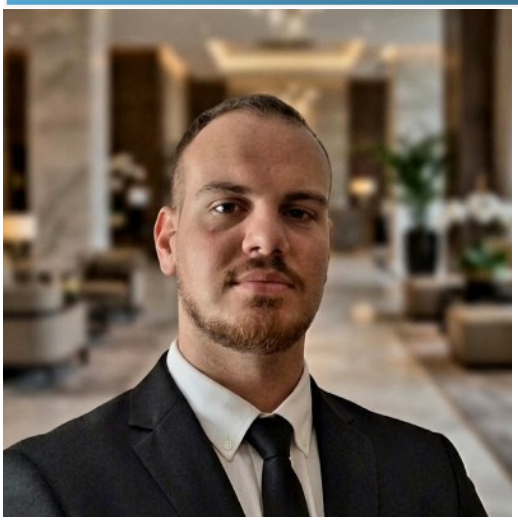
Conclusion

Hybrid warfare has reminded us that conflict is no longer confined to military operations or technological competition. Increasingly, it unfolds through influence, perception and decision-making. In such an environment, the human dimension deserves to receive the same strategic attention that has traditionally been devoted to military capabilities and technological innovation.

Cognitive resilience cannot prevent every attempt at manipulation, nor should it be viewed as a substitute for technological superiority. Rather, it enables societies to absorb pressure without losing their ability to think critically, trust legitimate institutions and make informed decisions under conditions of uncertainty. In that sense, it is not simply another component of national resilience; it is one of its foundations.

Perhaps the most important lesson is also the simplest one. Technology will continue to evolve, and hybrid threats will become increasingly sophisticated. Yet every cyber operation, every influence campaign and every artificial intelligence tool will ultimately seek to affect human judgement. Preparing people to understand, interpret and respond to these challenges may therefore prove to be one of the most important security investments of the coming decades.

HYBRID WARFARE



Hybrid Warfare: From Disinformation to Sabotage of Critical Infrastructures

Vasileios VLACHOS (Greece)

Conceptual Framework and Historical Overview

The term "hybrid warfare" first emerged in the early 2000s to describe a new form of conflict adapted to modern technological and geopolitical realities. Generally, it is defined as warfare conducted through the simultaneous combination of conventional (military) and unconventional methods and tactics. This broad spectrum of operations includes cyber warfare, terrorism, guerrilla warfare, psychological operations, coordinated disinformation, and ultimately any method capable of eroding an adversary's national power and social cohesion without requiring an open declaration of war. In international literature, this threat is also encountered under alternative terms such as "non-linear war" or "non-traditional war."

Frank Hoffman's Theory and the "Gray Zone"

The pioneer of the term, retired Marine Corps Lieutenant Colonel Frank Hoffman, pointed out that the essence of hybrid warfare lies in "blurring." Specifically, he noted that "...the blurring of modes of warfare, the blurring of who fights, and what technologies are fielded, produces a wide array of variety and complexity." According to Hoffman, hybrid wars incorporate a multi-layered spectrum of different modes of warfare, where conventional military capabilities, irregular tactics, terrorist acts, indiscriminate violence, and economic or psychological coercion coexist. This activity takes place in the so-called "Gray Zone"—an operational environment deliberately maintained below the threshold of for-mal armed conflict, making direct military response or the activation of collective defense clauses (such as NATO's Article 5) exceptionally difficult.

The evolution of hybrid warfare demonstrates that information operations and physical attacks should not be examined as separate phenomena. In a highly interconnected security environment, disinformation may prepare the operational environment, cyber operations may create vulnerabilities, and physical sabotage may ultimately transform those vulnerabilities into tangible disruption.

Disinformation as a Strategic Instrument

Disinformation has become an important component of contemporary hybrid warfare. Unlike conventional military operations, disinformation seeks to influence perceptions, decision-making and societal behavior without necessarily requiring a visible or attributable physical attack. Within hybrid campaigns, disinformation can undermine trust in institutions, deepen social divisions and amplify existing political and societal tensions. The rapid development of social media and digital communication has further increased the speed, reach and persistence of such operations Its strategic importance, however, extends beyond the information environment. Disinformation can create uncertainty, weaken institutional confidence and complicate the response to a developing crisis. When directed against critical infrastructure, false information concerning energy, telecommunications, transportation or essential services can further amplify the effects of cyber or physical disruption. Thus, information operations should not be viewed separately from other elements of hybrid warfare. Disinformation can shape the environment, cyber operations can exploit vulnerabilities, and physical sabotage can transform these vulnerabilities into tangible disruption. If disinformation can shape perceptions and influence the environment surrounding a crisis, cyber operations can provide the means to directly target the digital systems upon which modern critical infrastructure increasingly depends.

The Operational Chain of Hybrid Escalation

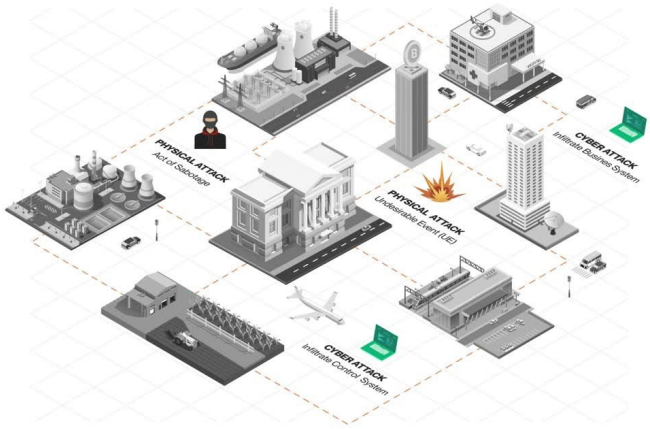
Stage	Hybrid Warfare Instrument	Primary Function	Strategic Effect
1.	Disinformation	Shapes the information environment and exploits societal vulnerabilities	Creates uncertainty, weakens trust and complicates crisis perception
2.	Cyber Operations	Exploits digital vulnerabilities and targets critical systems	Disrupts essential services and undermines operational continuity
3.	Physical Sabotage	Targets physical infrastructure and critical assets	Converts existing vulnerabilities into tangible disruption and material damage

Cyber Operations and the Vulnerability of Critical Infrastructure

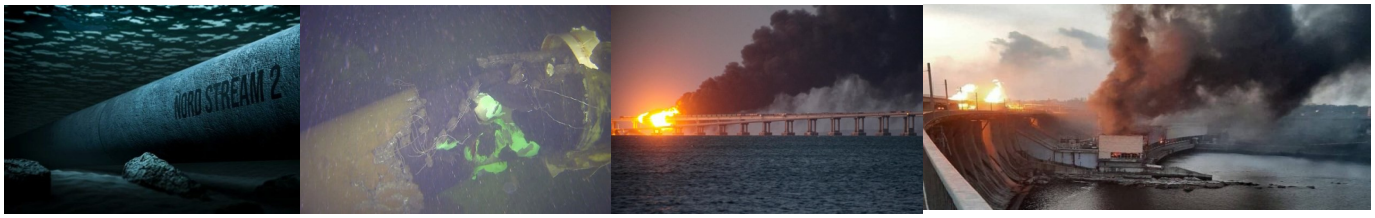
The increasing digitalization of critical infrastructure has created new vulnerabilities that can be exploited through cyber operations. Energy networks, telecommunications, transportation systems, financial services and other essential infrastructures increasingly depend on interconnected digital systems for their daily operation. Cyber operations within hybrid warfare can pursue different strategic objectives, including disruption of essential services, unauthorized access to sensitive information, manipulation of digital systems and the creation of operational uncertainty. Their impact can extend beyond cyberspace, particularly when digital systems support physical infrastructure and essential services. The significance of cyber operations there-fore lies not only in their ability to compromise information, but also in their potential to disrupt the physical and operational environment. A successful cyber intrusion can affect access-control systems, communications, monitoring capabilities, industrial processes or other functions essential to the continuity of operations. This creates a critical connection between the digital and physical dimensions of hybrid warfare. When digital vulnerabilities are successfully exploited, cyber operations can create the conditions under which physical disruption or sabotage becomes significantly more effective**.** The protection of critical infrastructure must therefore extend beyond traditional physical security measures. It requires an integrated approach

combining cyber security, physical protection, risk management, intelligence, crisis response and business continuity.

Physical Sabotage of Critical Infrastructure



Physical sabotage constitutes a significant dimension of hybrid warfare, particularly when directed against infrastructure essential to the functioning and resilience of a state or society. Its purpose is not necessarily the complete destruction of an asset, but rather the disruption, degradation or temporary incapacitation of essential services and capabilities. Critical infrastructure has become increasingly interconnected, creating dependencies between energy, telecommunications, transportation, water, healthcare, financial and digital systems. As a result, disruption to one component can generate cascading effects across multiple sectors, increasing the overall impact of an attack. Within a hybrid warfare framework, physical sabotage may be conducted independently or in combination with cyber operations, disinformation and other coercive activities. This cross-domain approach can increase uncertainty, complicate crisis response and make attribution more difficult. The strategic significance of physical sabotage therefore extends beyond the immediate physical damage. An attack can generate economic losses, interrupt essential ser-vices, undermine public confidence and place additional pressure on governmental and organizational decision-making. Consequently, the protection of critical infrastructure requires a shift from a purely asset-protection approach toward a broader resilience-based approach. This includes risk assessment, redundancy, continuity planning, emergency response capabilities, inter-organizational cooperation and the ability to rapidly restore essential functions following disruption. In the context of contemporary hybrid warfare, the vulnerability of critical infrastructure represents not only a physical security challenge but also a strategic national-security concern. The ability of a state and its private-sector partners to anticipate, withstand and re-cover from physical disruption is therefore becoming an increasingly important component of national resilience.



Nord Stream (2022)	Baltic connector (2023)	Crimea Bridge (2022/2023)	Ukrainian Energy Infrastructure
Energy infrastructure	Energy & telecommunications	Transportation & logistics	Energy infrastructure
Disruption of subsea pipelines	Damage to subsea infrastructure	Disruption of a strategic transport link	Repeated attacks and service disruption
Broader European energy and security implications	Increased concern over critical maritime infrastructure	Military and economic consequences	Impact on civilian resilience and national continuity

Hybrid warfare has transformed the contemporary security environment by combining disinformation, cyber operations and physical sabotage to exploit vulnerabilities across societies and critical infrastructure. The increasing interdependence of physical and digital systems means that even a localized attack can produce wider economic, social and security consequences. Critical infrastructure must therefore be protected through an integrated approach combining physical security, cyber security, risk management and resilience. Ultimately, the objective is not only to prevent attacks, but to ensure the ability of states and organizations to anticipate, withstand, respond to and recover from disruption.

References / Sources:

- Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies.
- NATO. (2021). NATO's Approach to Countering Hybrid Threats. North Atlantic Treaty Organization.
- European Union Agency for Cybersecurity (ENISA). (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity.
- European Commission. (2022). The EU's Cybersecurity Strategy for the Digital Decade. European Commission.
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Hybrid Warfare and Cyber Operations. Tallinn, Estonia.
- CISA. Critical Infrastructure Security and Resilience. Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security.
- Pomerantsev, P. (2019). This Is Not Propaganda: Adventures in the War Against Reality. New York: Public Affairs.
- International Energy Agency (IEA). (2022). A 10-Point Plan to Reduce the European Union's Reliance on Russian Natural Gas. Paris: IEA.
- NATO. (2023). Resilience, Civil Preparedness and Critical Infrastructure Protection. North Atlantic Treaty Organization.
- European Commission. (2024). Protecting Critical Infrastructure and Strengthening Resilience in the European Union. European Commission.
- International Maritime Organization (IMO). Subsea Infrastructure and Maritime Security. International Maritime Organization.

NATO

The Latency Trap: How Russia Attacks NATO's Decision Clock

Michael KEEN (USA)

Abstract

Russia's escalating pressure on NATO's eastern border is widely read as a military problem. This article argues it is a decision problem, one that exploits a specific seam in how the alliance decides under uncertainty, whether by design or by consistent effect. The deliberate drone incursions into Poland and Romania and the reconnaissance flights over the Baltic Sea, alongside the accidental Ukrainian-origin drone spillover into the Baltic states, all land in the same band: above the threshold the alliance can safely ignore, below the threshold that compels a clear collective response. What the pressure reaches, in effect, is not territory or forces. It is the interval between an ambiguous event and an agreed alliance response, the decision latency built into consensus. Romania supplies the sharpest case. Its detection-to-engagement time collapsed from roughly 50 minutes with no shot fired in September 2025 to a documented 5-minute kill on July 26, 2026, a measure of how quickly its operational decision-making speed hardened, while the alliance's political threshold, the Article 4 layer that Romania has pointedly not invoked, did not move at all. That asymmetry between operational hardening and alliance-political stasis is the article's central tension. Deterrence on the eastern flank fails not because NATO lacks the means to respond, but because the collective response is slow, negotiated, and ambiguous, and an adversary prices that predictability into each probe. The reform now debated inside the alliance, a tiered mechanism of pre-authorized responses that avoids emergency consultation for every violation, is a decision-architecture fix. The assessment holds with moderate-to-high confidence: capability investment that leaves the decision rule to consensus improves detection, not deterrence, and the border pressure will be answered at the decision layer or it will persist.

Source: https://www.nti.org/risky-business/natos-new-strategic-concept-what-it-is-and-why-it-matters/

Keywords: *NATO, Russia, deterrence, decision latency, eastern flank*

Russia's pressure on NATO's eastern border is read almost everywhere as a military problem. It is not, primarily. The deliberate incursions over Poland and Romania, the reconnaissance flights over the Baltic Sea, and even the accidental drone spillover from the war in Ukraine share one effect: they are not attempts to seize territory or degrade forces. They test a different target, the interval between an ambiguous event and an agreed alliance response. That interval is where deterrence on the eastern flank now succeeds or fails, and an adversary that probes it repeatedly learns to read it.

The pattern is consistent, whether it reflects deliberate design or the steady logic of a war spilling across a border. Each incursion sits in a narrow band, above the threshold NATO can safely ignore, below the threshold that compels a clear collective response. A single drone that strays is noise. Two dozen drones crossing into Poland in one night, some capable of carrying munitions, is a signal. But an incursion pitched just short of an unambiguous armed attack forces the alliance to consult rather than act. Whether each event is deliberately tuned or not, the effect is consistent. What the pattern targets, in outcome if not always by design, is not Polish airspace. It is the alliance's decision latency. Exploiting that latency is the method, and the goal it serves is larger: scenario analysis of the eastern flank identifies the fracturing of alliance cohesion, and the peeling away of exposed members into separate accommodations with Moscow, as the strategic objective that gray-zone pressure of this kind serves, whether or not any single incursion is planned with it in view[1].

The Threshold Is the Weapon

The September 2025 incursion into Poland is the clearest case. Between nineteen and twenty-three Russian drones entered Polish airspace over roughly seven hours. Poland scrambled aircraft, closed airspace over four airports, and invoked Article 4 of the North Atlantic Treaty[2]. Article 4 triggers consultation among allies. It does not authorize a response. The world's most powerful tactical air defenses engaged a handful of drones, and the alliance's formal response was to convene a meeting. Russia learned precisely what it came to learn: that a sub-threshold incursion buys a consultative response, not a kinetic one.

The 2026 record adds a complication that sharpens rather than weakens the point. Several drones crossed into Lithuania, Latvia, and Estonia in March, and again into Latvia in May, one striking an oil facility, but these were Ukrainian in origin, strays from Kyiv's campaign against Russian oil infrastructure, and Tallinn and Riga treated them as unintentional spillover. Poland separately intercepted a Russian reconnaissance aircraft over the Baltic Sea in July, and Romania recorded repeated violations during the same period, which are treated below[3]. The mix matters. Some incursions are deliberate Russian pressure, and some are accidental spillover from a neighboring war, yet the alliance's response machinery strains in the same way against both, because at the moment of detection, neither the origin nor the intent is known. Ambiguity is not a byproduct of these events. It is the operative condition. A drone whose origin cannot be established within the available minutes keeps the event below the response threshold, whether or not anyone launched it as a probe, and the cumulative effect normalizes the violation regardless of who is responsible.

Legal analysts have noted that the number and duration of the Polish penetrations and the hour-long Romanian flight would, by most states' readings, cross the threshold of a use of force, and that Russia appears to be signaling military capacity and readiness through them[4]. The signal is legible. The response is not automatic. That gap between a legible threat and a non-automatic response is the vulnerability, and it is a decision vulnerability, not a capability one.

Latency Is the Real Exposure

NATO does not lack the means to destroy a drone. It lacks a pre-agreed rule that converts a specific category of violation into a specific response without first convening the alliance. Under current arrangements, a member state's own armed forces acting on its own soil are not bound by NATO rules of engagement, while front-line states that depend on allied air policing are. The Baltic states have no fighter aircraft

---

[1]Eric Rosenbach et al., "Russian Threats to NATO's Eastern Flank: Scenarios, Strategy, and Policy for European Security", Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2026, available online at https://www.belfercenter.org/research-analysis/russia-nato-baltics-scenarios-europe-security, accessed 28 July 2026.

[2]On the Polish incursion of September 9-10, 2025: Reuters, "Poland shoots down suspected Russian drones in its airspace", September 10, 2025; CNN, "NATO shoots down Russian drones in Polish airspace", 10 September 2025. Prime Minister Donald Tusk reported to parliament 19 airspace violations between roughly 23:30 and 6:30, up to four drones downed with NATO support, four airports closed, and the activation of Article 4. The Polish Interior Ministry later confirmed 16 drones found on national territory.

[3]On the 2026 Baltic incidents: Al Jazeera, "Estonia, Latvia report drone incursions from Russian airspace", March 25, 2026; Euronews, "Latvian defence minister resigns following recent drone incursions", May 11, 2026. The drones that struck the Auvere power plant in Estonia (March 25) and the Kraslava area in Latvia (March 25), as well as the oil facility at Rēzekne (May 7), were of Ukrainian origin, strays from Kyiv's campaign against Russian oil infrastructure, and were treated by Tallinn and Riga as unintentional. On the interception of the Russian reconnaissance aircraft over the Baltic Sea, The Washington Times, "Poland intercepts Russian surveillance aircraft over Baltic Sea", July 14, 2026.

[4]"Legally Available Options in Response to Russia's Penetrations of NATO Airspace", Just Security, September 29, 2025, available online at https://www.justsecurity.org/121527/russia-nato-airspace/, accessed July 27, 2026. The authors note that the hour-long flight through Romanian airspace and the repeated incursions into Poland would, by most states' reading, cross the threshold of a use of force.

of their own and rely on NATO's Baltic Air Policing and Operation "Eastern Sentry", both of which operate under alliance rules of engagement[5]. The result is a seam: the states most exposed to incursion are the ones least able to respond without invoking a collective decision process, and that process runs more slowly than the events it must address.

This is the seam the pressure exploits. Not a gap in radar coverage or interceptor inventory, but the structural latency built into decision by consensus. Every incursion that produces consultation rather than consequence teaches the same lesson and lowers the political cost of the next one. Deterrence does not fail because NATO cannot act. It fails because Russia can predict that NATO's action will be slow, negotiated, and ambiguous, and can price that predictability into each successive probe. The point is not new to strategic theory. Richard Betts observed decades ago that miscalculation and sluggishness in political decisions are more the sources of surprise than any lack of information, and recent scenario analysis from the Belfer Center reaches the same conclusion for the eastern flank: in a fast-moving contingency, the binding constraint is the political decision-making among senior policymakers, not the intelligence or the hardware[6]. A threat deterrent depends on the adversary's expectation of a fast, certain response. Latency and ambiguity remove both.

Romania: Operational Speed, Political Stasis

Romania is where the two clocks separate most clearly. Its border with Ukraine places it inside the debris radius of nearly every Russian strike on Ukraine's Danube ports, and the incursion tempo rose sharply through 2026. By late July, the Ministry of National Defense counted thirty-three unauthorized entries into national airspace since the war began, a tally that had accelerated markedly in the preceding months. Three events in sixty days marked the shift from spillover to sustained pressure. On 29 May a Russian Geran-2 struck a residential block in Galați, injuring two, the first time such a strike hit a populated area in a NATO state during the war. On 5 June, a naval drone detonated inside the Port of Constanța after passing checkpoints undetected. Then, across 24 to 26 July, Romania shot down intruding drones on three consecutive days, summoned the Russian ambassador, and declared an embassy staff member persona non grata[7].

The engagement sequence is the quantitative core of the argument, and the Ministry of National Defense record documents it precisely across four points. In September 2025, Romanian F-16s tracked a drone for roughly 50 minutes and, after being granted authorization to fire, judged the collateral risk too high and let it exit the airspace unengaged. On 24 July 2026, radar detected a target at 09:39 east of Sulina and fighters destroyed it at 11:02, about eighty-three minutes later, after an Italian Eurofighter fired and missed and a Romanian F-16 completed the kill over uninhabited ground near Padina. Prosecutors confirmed that drone as a Russian-made Shahed. On 25 July, the same pilot downed a second drone near Sfântu Gheorghe, from radar detection at 08:22 to kill at 08:30, about eight minutes. On 26 July, a third drone crossed into Romanian territorial waters at 10:08 and was neutralized over the Black Sea at 10:13, five minutes later[8]. The progression is unmistakable. Detection-to-engagement collapsed from 50 minutes with no shot to 83 minutes, then 8, then 5 across a single year, as Romania's rules of engagement and pilot confidence hardened. That is operational decision speed improving in real time.

The alliance's political clock did not move with it. Romania has not formally invoked Article 4 over the 2026 incursions. Its foreign minister described Article 4 as an instrument the country can use, not as an invocation, and NATO's response to Romania has taken the form of solidarity statements and accelerated

---

[5]"Who Decides the Rules? NATO, Air Defence, and Russian Drone Incursions in Europe", NATO Association of Canada, December 20, 2025, available online at https://natoassociation.ca/who-decides-the-rules-nato-air-defence-and-russian-drone-incursions-in-europe/, accessed July 27, 2026.

[6]On the observation regarding the sources of surprise, Richard K. Betts, "Surprise Despite Warning: Why Sudden Attacks Succeed", Political Science Quarterly 95, no. 4 (1980-1981): 572. The parallel conclusion for the eastern flank appears in Rosenbach et al., op. cit., "Russian Threats to NATO's Eastern Flank".

[7]On the figure of 33 airspace violations since the start of the war and the three consecutive shoot-downs (July 24-26, 2026): Ministry of National Defence, cited in The Moscow Times, "Romania Shoots Down Third Russian Drone", July 26, 2026. On the summoning of the Russian ambassador and the declaration of a diplomat as persona non grata: Ministry of Foreign Affairs of Romania, July 26-27, 2026 (cited in Meduza and The Sofia Globe). For the specialist assessment of the incursion pattern as a deliberate test of NATO's response capacity, Institute for the Study of War (ISW), daily assessments of the Russo-Ukrainian campaign, July 2026, available online at https://www.understandingwar.org. See also UPI, "Romania says it shot down another Russian drone in its airspace", July 26, 2026, accessed July 28, 2026.

[8]The chronology is drawn from the communiqués of the Ministry of National Defence (MApN) and the official statements of Defence Minister Radu Miruță. July 24: radar detection at 09:39 roughly 20 km east of Sulina (Sulina-Brăila-Fetești-Buzău track), shoot-down at 11:02 near Padina, after an Italian Eurofighter missed and a Romanian F-16 completed the interception; prosecutors confirmed the drone as a Russian-made Shahed. July 25: detection at 08:22, shoot-down at 08:30 near Sfântu Gheorghe, the same pilot. July 26: the drone entered territorial waters at 10:08 and was neutralized at 10:13, roughly 12 km northeast of Sulina, per Minister Miruță's statement. For September 2025, the MApN communiqué specifies a flight of roughly 50 minutes, with the pilots granted authorization to fire but declining because of collateral risk. The communiqués are available through the news agencies (Reuters, Euronews, UPI, Kyiv Post, European Pravda), accessed July 28, 2026.

air-defense support rather than formal consultation, a pattern distinct from Poland's and Estonia's Article 4 consultations in 2025[9]. That is the asymmetry in one case: a member state can compress its kill chain from fifty minutes and no shot to a five-minute kill while the collective political threshold it operates beneath does not shift at all. An adversary observing both clocks needs only the slower one to set its expectations. The political threshold, not the kill chain, is what gets priced into the next probe.

The Alliance Is Debating the Right Problem, Slowly

The reform conversation within NATO has reached the decision layer, though it rarely calls it that. Analysts across the alliance's institutions are calling for a standing response mechanism for airspace violations that does not require emergency Article 4 consultation every time; a tiered system in which defined categories of violation trigger pre-authorized responses; and only the most serious incidents to demand full alliance consultation[10]. Belfer Center scenario planning makes the same recommendation, urging clearer thresholds for consultation paired with a standing set of coordinated response options, and noting that willing states can act bilaterally or in ad hoc coalitions before waiting for the alliance's formal consensus[11]. The stated rationale is precise: ambiguity may feel diplomatically safe, but it invites the very miscalculation everyone seeks to avoid.

That is a decision-architecture argument, and it names the shift the alliance most needs: from a reactive posture, which waits for each event and then negotiates a response, to a proactive one, which fixes the response before the event and removes the interval Russia exploits. Its logic is to remove latency by pre-committing the response, so that the adversary faces a known, automatic consequence rather than a negotiation. Operation Eastern Sentry, launched directly after the Polish incursion, marks a shift from an air-policing posture to an air-defense posture, and NATO describes it as enabling faster decision-making by connecting sensors, command systems, and effectors across the alliance[12]. The hardware and the posture are moving. The binding constraint is whether the political decision rule moves with them. Faster sensors feeding a slow decision process do not close the latency gap. They only measure it more precisely.

What This Means for Decision-Makers?

For the alliance and its member governments, the implication is that investment aimed only at capability - more interceptors, denser radar, the European drone-wall initiatives- addresses the visible symptom while leaving the exploited vulnerability intact. A drone wall that detects every incursion but still routes each response through consensus consultation has improved detection, not deterrence. The decisive variable is the pre-committed rule: which categories of violation carry an automatic, pre-authorized response, decided in advance and communicated clearly enough that Russia prices certainty rather than hesitation into its next probe. This is the whole distance between a reactive alliance and a proactive one, and deterrence lives entirely on the proactive side. Deterrence is restored at the decision layer, or it is not restored at all.

For the states on the flank, Romania and the Black Sea littoral among them, the exposure is more than military. A border regime in which violation is routine, and response is ambiguous, raises the risk premium on everything that depends on regional stability: energy corridors, port and maritime traffic, cross-border investment, and critical infrastructure within reach of the same deniable systems now testing airspace[13]. The latency that Russia exploits in its military response against the alliance applies equally to hybrid pressure on infrastructure, where attribution is slower, and the threshold for collective action is higher still.

The assessment turns on one variable. If NATO closes the decision gap, moving pre-authorized rules of engagement for defined violation categories from debate to standing policy, the incursion campaign loses its logic, because sub-threshold probing stops buying a consultative discount. Watch for that

---

[9]On the status of Article 4, The New York Times, "NATO, Article 4 and Romania", May 29, 2026, available online at https://www.nytimes.com/2026/05/29/world/europe/nato-article-4-romania-russia.html, where Foreign Minister Oana Țoiu describes Article 4 as "an instrument Romania can use", not as an invocation. On the Galați strike, ABC, May 29, 2026, accessed July 27, 2026.

[10]"Crafting a Unified NATO Response to Putin's Drone and Fighter Violations", Foreign Policy, October 22, 2025, available online at https://foreignpolicy.com/2025/10/22/russia-poland-nato-drones-airspace-planes/, which proposes a tiered response mechanism with pre-authorized responses, accessed July 27, 2026.

[11]Rosenbach et al., "Russian Threats to NATO's Eastern Flank", Recommendations and Priorities section, which recommends clearer thresholds for consultation, a standing set of response options coordinated through NATO, and bilateral or ad hoc coalition action ahead of the Alliance's formal consensus.

[12]"Eastern Sentry strengthens NATO's air defence posture on Eastern Flank", NATO Allied Air Command, June 2026, available online at https://www.globalsecurity.org/military/library/news/2026/06/mil-260604-nato-aircom02.htm, accessed July 27, 2026.

[13]On the warnings regarding Russia's possible use of captured drones against Poland and the Baltic states, Defense News, "Russia may use captured Ukrainian drones against Poland and Baltics, Warsaw warns", July 21, 2026, available online at https://www.defensenews.com/global/europe/2026/07/21/, accessed July 27, 2026.

move specifically, not for additional assets or exercises that address the symptom. If the alliance instead deepens capability while leaving the decision rule to consensus, expect the incursions to continue and widen, because the vulnerability they target remains open regardless of how many drones NATO can detect or destroy. Border pressure is a test of the alliance's decision-making process. It will be answered at that layer, or it will persist.

Russia is not probing NATO's defenses. It is probing NATO's decision latency, and reading the interval each time. The alliance holds every material advantage except speed and certainty at the moment of decision, and those are the two things deterrence cannot do without. A reactive posture concedes the interval by design. Only a proactive one, with the response fixed before the event, denies Russia the delay it is built to exploit, and the same discipline deters any other state that reads the same seam. Naming the target correctly is the first move, because an alliance that counters a decision attack with more hardware is fighting on the wrong layer, while the real one remains exposed.

References:

- Al Jazeera, "Estonia, Latvia report drone incursions from Russian airspace", 25 March 2026, available online at https://www.aljazeera.com/news/2026/3/25/estonia-latvia-report-drone-incursions-from-russian-airspace, accessed 28 July 2026.
- CNN, "NATO shoots down Russian drones in Polish airspace, accusing Moscow of being reckless", 10 September 2025, available online at https://www.cnn.com/2025/09/09/europe/poland-scramble-jets-russian-drone-reports-intl-hnk-ml, accessed 28 July 2026.
- "Crafting a Unified NATO Response to Putin's Drone and Fighter Violations", Foreign Policy, 22 October 2025, available online at https://foreignpolicy.com/2025/10/22/russia-poland-nato-drones-airspace-planes/, accessed 27 July 2026.
- "Eastern Sentry strengthens NATO's air defence posture on Eastern Flank", NATO Allied Air Command, June 2026, available online at https://www.globalsecurity.org/military/library/news/2026/06/mil-260604-nato-aircom02.htm, accessed 27 July 2026.
- Institute for the Study of War, daily assessments of the Russo-Ukrainian campaign, July 2026, available online at https://www.understandingwar.org, accessed 28 July 2026.
- Rosenbach, Eric, Carlo Giannone, Slavina Ancheva, Luc Hillion, Ethan Lee and Lukasz Kolodziej, "Russian Threats to NATO's Eastern Flank: Scenarios, Strategy, and Policy for European Security", Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2026, available online at https://www.belfercenter.org/research-analysis/russia-nato-baltics-scenarios-europe-security, accessed 28 July 2026.
- Euronews, "Latvian defence minister resigns following recent drone incursions that hit oil facilities", 11 May 2026, available online at https://www.euronews.com/my-europe/2026/05/11/latvian-defence-minister-resigns-following-recent-drone-incursions-that-hit-oil-facilities, accessed 28 July 2026.
- "F-16 downs drone in Romania's airspace for first time", Romania Insider, 24 July 2026, available online at https://www.romania-insider.com/f16-down-drone-romania-july-2026, accessed 27 July 2026.
- "Legally Available Options in Response to Russia's Penetrations of NATO Airspace", Just Security, 29 September 2025, available online at https://www.justsecurity.org/121527/russia-nato-airspace/, accessed 27 July 2026.
- Ministry of Foreign Affairs of Romania, communiqué on the summoning of the Ambassador of the Russian Federation, 26-27 July 2026 (cited in Meduza and The Sofia Globe).
- "NATO, Article 4 and Romania", The New York Times, 29 May 2026, available online at https://www.nytimes.com/2026/05/29/world/europe/nato-article-4-romania-russia.html, accessed 27 July 2026.
- "Romania Shoots Down Third Russian Drone", The Moscow Times, 26 July 2026, available online at https://www.themoscowtimes.com/2026/07/26/romania-shoots-down-third-russian-drone-as-president-calls-breaches-intolerable-a93340, accessed 28 July 2026.
- "Romania shoots down drone breaching its airspace, president says", Reuters, 24 July 2026, available online at https://www.reuters.com/business/aerospace-defense/romania-shoots-down-drone-breaching-its-airspace-president-says-2026-07-24/, accessed 28 July 2026.
- "Russia may use captured Ukrainian drones against Poland and Baltics, Warsaw warns", Defense News, 21 July 2026, available online at https://www.defensenews.com/global/europe/2026/07/21/, accessed 27 July 2026.
- UPI, "Romania says it shot down another Russian drone in its airspace", 26 July 2026, available online at https://www.upi.com/Top_News/World-News/2026/07/26/romania-says-shot-down-another-Russian-drone-airspace/9331785099814/, accessed 28 July 2026.
- "Who Decides the Rules? NATO, Air Defence, and Russian Drone Incursions in Europe", NATO Association of Canada, 20 December 2025, available online at https://natoassociation.ca/who-decides-the-rules-nato-air-defence-and-russian-drone-incursions-in-europe/, accessed 27 July 2026.

NATO

NATO 3.0 – The Start of Profound Transformations at the Level of the North Atlantic Alliance

PhD. Eng. Stelian TEODORESCU (Romania)

"Ability is what you are capable of. Motivation determines what you do. Attitude determines how well you do it."

Lou Holtz

NATO's pledge to spend more on defense dominated the headlines at this year's NATO Summit in Ankara. But beyond the debates over budgets, military hardware, and burden-sharing, experts say the North Atlantic Alliance is undergoing a deeper transformation—one that could redefine how it approaches security for decades to come.

Source: https://www.forumulsecuritatiimaritime.ro/nato-3-0-and-the-rebalancing-of-euro-atlantic-security/

As a result, it is crucial to highlight that NATO defense ministers and U.S. Secretary of Defense, Pete Hegseth, have proclaimed the birth of "NATO 3.0." With no prior explanation of what "NATO 1.0" or "NATO 2.0" entailed. It has been difficult to understand exactly what this new NATO model will look like. But for all his criticism of European allies' contributions to the common defense and their overreliance on American forces and capabilities, it seems a safe bet that NATO's future will mean Europe doing much more, and the United States significantly reducing its efforts. More than likely, the Alliance will be managed and resourced largely by Europeans. Already under pressure to spend more on defense and modernize their armed forces to meet a growing threat from Russia, the allies must now find even more capabilities to replace the troops and platforms that the Pentagon plans to withdraw from its NATO missions in Europe. P. Hegseth announced in Brussels a six-month Pentagon review of each individual ally to assess how much that ally contributes to NATO missions and how useful and valuable it is to the United States. The unprecedented review was largely driven by the Trump administration's frustration with NATO's perceived lack of support for US military action against Iran, particularly the denial of the use of air bases in the UK and Italy by US Air Force bombers, fighters and tankers. The US president concluded that the ungrateful allies had done far less to help the US than the US had done for them (with the exception of the efforts and deployments of European troops over 20 years in Afghanistan and Iraq).

The concept, increasingly referred to by analysts as "NATO 3.0", reflects a shift from an alliance built primarily around the concept of collective military defence to one focused on technological resilience, industrial capacity and emerging areas such as artificial intelligence, cyber security and cognitive warfare.

It is very clear that, to date, the evolution of the North Atlantic Alliance has been as follows:

• NATO 1.0 (Cold War): The original collective defence posture, designed to limit the influence and actions of the former Soviet Union through an active US military presence in Europe.

• NATO 2.0 (Post-Cold War): An era focused on crisis management outside the area, counter-terrorism and peacekeeping operations, characterised by a strong reliance on US capabilities, while European defence budgets have decreased significantly.

• NATO 3.0 (Current Change): A significantly rebalanced partnership highlighted at NATO level following recent strategic reviews and the Ankara Summit, all focusing on European strategic autonomy, increasing domestic defense industrial production, and managing regional hybrid threats.

The main pillars of the current change that are being relied on are the following:

• *A much more thorough burden-sharing:* European states are pressured to meet or even exceed defense spending targets and to train and equip military forces ready for military operations.

• *Development of industrial capacity:* Massive new procurement commitments and joint ventures (such as counter-drone initiatives and modernization of logistics infrastructure) are transferred to the level of European leaders.

• *Adjusting the US posture:* Washington is reducing its ground forces and military leaders in Europe, transforming itself into a supportive partnership backed by critical command resources and overall nuclear deterrence.

As a result, we can say that "NATO 3.0" is an informal strategic concept that describes a major shift in the North Atlantic Alliance, in which European member states assume primary responsibility for their own conventional defense, while the US shifts its primary military focus to other global priorities, such as the Indo-Pacific region.

Although the term "NATO 3.0" is not yet part of NATO's official doctrine, it was prominently featured in discussions among security researchers and experts who participated in the "NATO Allies in Ankara" forum, held in conjunction with the NATO Summit. Even Turkish President Recep Tayyip Erdoğan used the term in his opening speech at the NATO Summit. "For the vision of 'NATO 3.0' to achieve its goals, allies must end the restrictions they impose on each other," the Turkish president stressed.

NATO's long-standing transformation – often described as "NATO 3.0" – therefore extends far beyond adapting to the war between Russia and Ukraine. It reflects the broader effort of the North Atlantic Alliance to respond to an increasingly diverse and interconnected security environment, shaped by competition between both great powers and diverse groups/coalitions formed around various common goals and based on the concept of minilateralism, technological rivalry, cyber threats, and the increasing convergence of security at both the Euro-Atlantic and Indo-Pacific levels.

While much of the discussion around "NATO 3.0" has focused on its implications for Europe and the North Atlantic Alliance, an equally important question concerns how these developments are interpreted in other capitals around the world. Assessments of NATO's actual evolution by various international actors, rather than assessments of the Alliance's stated intentions, have a particular influence on the strategic calculations made by various competing states and, by extension, on the rapidly evolving and often unpredictable international security environment.

During the NATO Summit in Ankara, Kadir Temiz, President of the Center for Middle East Studies (ORSAM), provided expert analysis and commentary on the Alliance's new strategic statements and changes.

His key statements and insights during the Summit focused largely on defense industrial capabilities and changing geopolitical dynamics:

• *Emphasis on industrial capacity rather than military size:* K. Temiz highlighted that NATO's latest statement includes new defense procurement worth $50 billion. He noted that modern conflicts (drawing lessons from the wars in Ukraine and Iran) increasingly depend on industrial production capacity, advanced production of missiles, drones, artificial intelligence, and cutting-edge defense technologies, rather than simply maintaining larger standing armies.

• *Focus on joint production:* He highlighted NATO's emphasis on joint production, promoting innovation, and eliminating trade barriers in defense among allied nations.

• *Turkiye's strategic weight:* Commenting on the changing transatlantic landscape, US budgetary demands and issues of internal unity, K. Temiz highlighted the increasingly strategic, mediating and essential role played by Turkiye as a host nation navigating a highly volatile security environment.

K. Temiz said that NATO's next phase must be understood in the context of an increasingly complex security environment.

"Everyone is talking about 'NATO 3.0'," he told the media. "The main idea is to rebuild NATO from this perspective." For K. Temiz, the first pillar of 'NATO 3.0' is renewed collective action, built around a more balanced sharing of responsibilities among allies. "The first important issue in 'NATO 3.0' is collective action through new dimensions, including the European perspective of burden-sharing," he stressed.

The second pillar was described as adapting to a growing list of security challenges that now extend far beyond Russia's war in Ukraine. "The Middle East, the Balkans, Central Asia, the Russia-Ukraine war – all combine into a collective challenge for NATO members," K. Temiz said. According to him, the discussions in Ankara reflected growing optimism that the North Atlantic Alliance is starting to rethink its long-term strategic posture.

K. Temiz argued that Turkiye is entering this new phase of NATO's evolution from a position of relative strength. For decades, he noted, Ankara has been steadily investing in its defense industry, while expanding its exports to Europe, Africa, the Middle East and Asia. "Turkiye is ready," he said, referring to burden-sharing and increased defense spending. But at the same time, he warned that military capabilities alone will not solve current security challenges. "What we need is more diplomacy, more dialogue and more negotiations," as K. Temiz stated, adding that energy, food and climate security are becoming integral parts of a much more comprehensive security framework.

Also during the NATO Ankara Summit, Dr. Erman Akilli, a prominent professor of International Relations at Haci Bayram Veli University in Ankara and a SETA researcher, published a statement and analysis focused on NATO in a "technopolar" world. His assessment aligned directly with the concepts later codified in the official Ankara Summit Declaration, which emphasizes data sovereignty, artificial intelligence, and modernized alliance resilience.

E. Akilli said that NATO's transformation is driven both by technological disruption and geopolitics. "The battlefield is changing," he emphasized. "It's no longer just about physical force. Algorithms, data, and computing power are directly affecting the battlefield." E. Akilli referenced recent conflicts, including the war involving Iran, where U.S. officials have highlighted the increasing use of non-kinetic capabilities alongside conventional military operations. He argued that artificial intelligence, quantum technologies and advanced computing are becoming as strategically important as traditional military platforms. "When we talk about artificial intelligence and next-generation technologies, we often think of them as belonging to the future. No - they are already here," E. Akilli said, adding that: "We already live in a cognitive environment."

E. Akilli believes that the founding principle of the North Atlantic Alliance, collective defense under Article 5, remains essential - but is no longer sufficient. "NATO was built on collective security," he said. "But it must be transformed into collective resilience." In his opinion, future security will increasingly depend on the ability of member states to protect their digital infrastructure, technological supply chains and data sovereignty. "If a state cannot control its citizens' data, lacks algorithmic authority, computing power or the capacity to produce semiconductors and chips, it becomes vulnerable to systemic shocks," he warned. This, he argued, fundamentally changes the meaning of deterrence and "in the future, NATO deterrence will not be measured by the technological capability of its strongest ally, but will be measured by the technological resilience of its most digitally vulnerable member." E. Akilli also argued that hybrid threats and cognitive warfare require NATO to think beyond conventional military deterrence. "Cognitive warfare is happening even as we speak," E. Akilli emphasized.

At the same NATO Summit in Ankara, Defne Sadıklar Arslan, Director and Founder of the Atlantic Council Turkiye Program, orchestrated and participated in a series of high-level policy notes and related events to analyze Turkiye's strategic positioning within the Alliance.

D. Arslan moderated and spoke at an official side event of the NATO Summit in Ankara, entitled "Connecting Europe's Flanks: NATO, Germany, Turkiye, Italy and the Mediterranean", organized in partnership with the Friedrich-Ebert-Stiftung (FES) Turkiye, focusing on:

- How NATO can better connect its Eastern and Southern priorities through Mediterranean security.
- Improving burden-sharing and cooperation in the fields of defense and industry.
- Strengthening ties between the EU and NATO.

She promoted a critical strategic report by Atlantic Council member Pınar Dost, entitled "From Burden-Sharing to Strategic Delivery: NATO and Turkiye's Priorities Ahead of the Ankara Summit," which highlighted:

- Turkiye's growing regional influence and strategic autonomy.
- The implications of the US drawdown and the changes in transatlantic relations.
- The need to translate allies' verbal promises into concrete defensive actions.

D. Arslan said that Europe's efforts to strengthen its own defense industry open up new opportunities for closer cooperation with Turkiye.

She also highlighted growing defense partnerships involving Turkiye, Italy, and the United

Kingdom, as well as the collaboration between Turkish drone manufacturer Baykar and Italian company Leonardo. "I believe Turkiye will play an important role as Europe strengthens its defense capability," she added. D. Arslan also highlighted NATO's announcements regarding the expansion of satellite systems, radar capabilities and multinational industrial cooperation as examples of the North Atlantic Alliance moving beyond public procurement towards long-term industrial integration.

Analyzing the numerous studies carried out and the views expressed at the analytical and decision-making levels, at the global level, it was concluded that the main major risks identified in various expert environments in the field of defense and security at the regional and global levels are:

• threats to critical infrastructure at the EU and NATO levels;

• Russia's continued aggression in Europe;

• the reduction by the US of its security guarantees towards European allies at the North Atlantic Alliance level;

• the probable consequences generated by a military conflict between China and Taiwan that could generate immeasurable effects and according to a domino principle even for Europe.

In conclusion, it should not be overlooked that the leaders of NATO member states met in Ankara in the context of the greatest intensification of military actions that Europe has seen in recent decades. It has now become very clear that Russia represents the main threat to Europe and, implicitly, to the European member states of NATO. However, serious debates have also begun to arise regarding China, even if not all of them are open to debate.

For years, European governments have treated Beijing mainly as a trading partner and economic rival, but this opinion has begun to change rapidly behind closed doors. As a result, the EU is preparing to label both Russia and China as its main threats, presenting Beijing as a key ally and factor in Moscow's war in Ukraine. The Ankara Summit therefore came at an unusual time, as Europe is not only rearming against Russia – a threat it has acknowledged for several years – but is also starting to explicitly place China in the same category.

The NATO summit in Ankara reaffirmed NATO's "firm commitment" to Article 5 and collective defense, reaffirmed that Russia remains the main threat to Euro-Atlantic security, and reiterated support for the freedom, sovereignty, and territorial integrity of Ukraine. The final wording now appears to be very secure, with debates on escalation management, threat perceptions, and concerns about the challenges facing the North Atlantic Alliance very clear.

Perhaps most importantly, the final declaration reflected how much the debate on burden-sharing has evolved. A decade ago, European dependence on US military support was the defining feature of the transatlantic relationship. In 2022, few would have predicted that Europe and Canada would ultimately finance the vast majority of security assistance flowing to Ukraine. Yet NATO is now explicitly acknowledging this reality, demonstrating that burden-shifting is no longer just rhetoric.

Despite ongoing disagreements on issues such as Greenland, burden-shifting, and Ukraine and Middle East policies, NATO member states have nevertheless managed to reach consensus on the Alliance's core security priorities. Recognizing the need for the Alliance to adapt to a much broader and more unpredictable security environment demonstrates that NATO can address multiple security challenges simultaneously without losing strategic coherence.

EUROPE

Europe Between Strategic Autonomy and NATO Consolidation: The Industrial Impasses of a Decisive Decade

Aldo MUNGO (Belgium)

Europe chose its vocabulary before it chose its capabilities. For several years now, strategic autonomy has featured in every official speech, every white paper, every defense industrial strategy. Yet it has produced no major weapons system capable of standing alone against a first-rank power. The gap between the vocabulary and the hardware is the real subject of this decade.

Source: https://tdhj.org/blog/post/nato-eu-cooperation-benefits/

The MGCS program, meant to produce the joint successor to the French Leclerc tank and the German Leopard 2, illustrates this gap with almost clinical precision. Conceived as proof that two major defense industries could merge their doctrines and their production chains, it ran into a reality older than the project itself: France designs its land army for expeditionary projection, Germany for high intensity defense on NATO's eastern flank. These two doctrines produce two incompatible sets of requirements, and no industrial governance architecture has managed to reconcile them. While Paris and Berlin negotiated work-share arrangements, Rheinmetall moved forward alone with the KF51 Panther, proving that a single company, unconstrained by a politically negotiated division of labour, produces faster than a binational consortium.

The same pattern repeated with SCAF, the next-generation combat aircraft program bringing together France, Germany and Spain. Industrial tensions between Dassault and Airbus over intellectual property sharing and over the role of lead architect have slowed a program whose logic should have been purely capability-driven. Dassault has repeatedly hinted that a national program would remain an option should cooperation become ungovernable. Whether that threat is tactical or sincere, it reveals a structural truth: European industrial cooperation works better as a tool of political negotiation than as a method of producing weapons.

This difficulty is not unique to France and Germany. It runs through the entire European defense industrial ecosystem, built on a principle of geographic work-sharing rather than a principle of industrial efficiency. Every major multinational program must distribute production shares among participating countries, often in proportion to national orders rather than to available expertise. This model, inherited from decades of intergovernmental cooperation, produces lengthened timelines, unit costs higher than those of a single prime contractor, and recurring political blockages whenever one partner shifts its budgetary priorities.

The absence of strategic airlift capacity is a second symptom of the same illness. The A400M, meant to give Europe logistical autonomy, has suffered delays and capability limitations that have forced several European militaries to keep relying on American capabilities or, for certain missions, on Russian or Ukrainian solutions before the war. No European strategic heavy-lift program equivalent to the American C -17 has been launched. Europe built a projection force without the means to project that force beyond its own continent within timeframes compatible with a real crisis.

Europe's shortfall in tactical drones and autonomous systems completes the picture. While the war in Ukraine has demonstrated, on an industrial scale, the decisive importance of low-cost, mass-produced unscrewed systems, European industry remains structured around complex, expensive platforms produced in small quantities. The lag is not merely technological: it is industrial and cultural, inherited from a conception of warfare in which the unit quality of a system takes precedence over its ability to be produced and lost at scale.

Faced with this reality, consolidation around NATO remains, for a majority of member states, the most rational short-term option. American command, intelligence and projection capabilities have no credible European equivalent, and capability dependence on Washington remains the condition for the Alliance's deterrent credibility on the eastern flank. Strategic autonomy, as currently practiced, does not replace this dependence: it sits alongside it, without resolving the inconsistency between stated ambitions and the budgets actually allocated to an independent industrial base.

The coming decade will be decisive because it will force a choice that political ambiguity has so far allowed Europe to avoid. Either Europe accepts transferring a significant share of industrial sovereignty to a single prime contractor per major program, even if that contractor is not always the national one for each participating state, or it continues funding fragmented multinational programs whose political coordination costs exceed their capability benefit. The third path, one that would secure both full strategic autonomy and the preservation of the geographic work-share model, has not worked so far, and nothing suggests it will work better under the tight budgetary constraints most European states now face.

Europe has the combined budget, the industrial base and the skilled workforce needed to produce real strategic autonomy. What it lacks is not resources, but the will to accept the partial sovereignty sacrifices that this autonomy would require of each member state individually. As long as that will remains absent, strategic autonomy will stay a declaratory objective, and NATO consolidation will remain the operational reality.

EUROPE

Europe's Voice Cracks under Russian Bombs

Alistair HOLLOWAY (United Kingdom)

"Politics is the continuation of war by other means," Michel Foucault said[1].

European politics are ensnared in Russia's war against Ukraine. Now in its fifth year. The European Union's foreign policy chief Kaja Kallas called for the bloc to have a common voice to square up to all adversaries:

"We need to understand why they don't like the EU; why China doesn't like the EU, why Russia doesn't. It is because if we stick together, if we operate together, then we are equal powers, we are strong."[2]

Source: https://thenewglobalorder.com/world-news/report-one-year-into-the-war-the-eus-confusing-russia-policy/

Unity seems unlikely.

The continent is starting to split. On countering Russia's threat. On defence. On enlargement.

The Old West with the larger economies and legacy dominance of Germany and France. Rooted in the post-war consensus that built the EU, maintained peace and brought prosperity. Theirs is Europe as it ought to be. The product of conciliation, caution, process and dialogue.

There is the New North and East. EU member states after 1995. Sweden, Finland, the Baltic States, the former Warsaw Pact nations. With centuries of dealing with Russia. It was Estonian, Latvian and Lithuanian representatives that had long warned of Russia's threat to Central and Eastern Europe[3]. To too little heed. These nations are more ready to take a hard line with Moscow. They spend more per head on defence and direct support for Ukraine. Theirs is a Europe as it is, shaped mainly by events and geopolitical realities.

There is tension. Latvian Prime Minister Andris Kulbergs said in August he wants seven billion euros to help cover the military and economic costs of confronting Russia[4]. "I did not and do not believe in a peace agreement. Someone has to win and it has to be Ukraine," he said on August 24[5].

---

[1] *Michel Foucault, Society Must Be Defended, Picador, New York, 2003, p16.*

[2] *Antoaneta Roussi, US, China and Russia prefer a divided Europe, Kallas warns, Politico, 17 May 2026, https://www.politico.eu/article/us-china-and-russia-prefer-a-divided-europe-kallas-warns/.*

[3] *Leon Hartwell, Agne Rakstyte, Julia Ryng and Eriks K Selga, Winter is coming: The Baltics and the Russia-Ukrainian War, LSE !deas, December 2022, https://www.lse.ac.uk/ideas/Assets/Documents/reports/2022-12-05-BalticRussia-FINALweb.pdf.*

[4] *Max Griera, Latvia wants 7B euros from EU to cope with fallout from Russia's war, Politico, 17 August, 2026, https://www.politico.eu/article/latvia-pm-andris-kulbergs-7b-eu-funding-over-russia-costs/.*

[5] *Ukraine News, The West has talked about peace long enough...Ukraine must win, Facebook, August 24, 2026, https://www.facebook.com/100089774110537/videos/-the-west-has-talked-about-peace-long-enoughukraine-must-winlatvian-prime-minist/2295145071310928/.*

Politicians stress – depending on how the conflict ends – Latvia could be next. It's a question of survival. In the past five years the country more than doubled defence spending, re-introduced conscription and launched campaigns to push the message: defence is everyone's responsibility[6].

Polling showed – unsurprisingly – the greater proximity to Russia, the greater the fear. A YouGov survey last year found 62 percent of Danes and 57 percent of Lithuanians considered Moscow's aggression the greatest threat. It compares with 36 percent of Germans and 22 percent of French[7].

Europe Unheard

Europe has struggled to be heard with any collective voice at all. As recently as February 2025 its leaders were excluded from US-Russia talks on Ukraine. There's no guarantee the Americans won't bar Europeans from future talks[8]. Washington is now in a six-month review of its military presence in Europe. It has cut the number of troops on the continent to 80,000 from 100,000[9]. America's commitment to NATO's Article 5 assurance of mutual defence is under question[10].

Peace without Europe's involvement is diplomatically flawed and strategically dangerous[11].

France, Germany and the UK reportedly want a joint format for Ukraine peace negotiations. Additionally officials are said to be at work on contingency plans for a 'European NATO'.

It's Old Europe leadership when the continent needs new thinking. Commission President Ursula von der Leyen said in March:

"We urgently need to reflect on whether our doctrine, our institutions and our decision-making – all designed in a postwar world of stability and multilateralism – have kept pace with the speed of change around us. Whether the system that we built – with all of its well-intentioned attempts at consensus and compromise – is more a help or a hindrance to our credibility as a geopolitical actor."[12]

Time presses. EU Commissioner Andrius Kubilius – a Lithuanian – said Russia could be willing and able to attack an EU state by 2030[13].

He could be wrong.

It's dangerous to presume he is isn't.

Moscow for years has at war with Europe.

It continues grey-zone attacks. Russian President Vladimir Putin gives no sign of stepping back in his brutalisation of Ukraine. Security Council Deputy Chairman Dmitry Medvedev said in May: "Citizens of EU countries, you should realise your authorities have unilaterally entered into a war with Russia…So be vigilant and don't be surprised by anything. The peaceful sleep is over."[14]

That threat won't go away. Putin needs enemies. These wreckers of his promise to show Russia "was and will remain a great power"[15] are the means to rally and distract the nation. Adversaries are his Emmanuel Goldstein from George Orwell's *1984*. If they were all defeated, the straight man would leave the stage. The act fail. War, Russian victories – in Chechnya, Georgia, Crimea's annexation, eastern Ukraine, Syria – substantiate these fables.

When Putin announced the 'special military operation' in 2022, he blamed NATO expansion and "irresponsible Western politicians," invoked their interventions in Serbia, Libya, Syria, Iraq, their disregard

---

[6]Rebecca Pieder, A nation in arms: how Latvia is preparing for war to prevent it, New Eastern Europe, 23 March, 2026, https://neweasterneurope.eu/2026/03/23/a-nation-in-arms-how-latvia-is-preparing-for-war-to-prevent-it/.

[7]Csongor Koromi and Hann Cockerel, The closer to Russia the greater the fear, opinion poll finds, Polio, 20 October, 2026, https://www.politico.eu/article/russia-opinion-poll-closer-border-fear-yougov-eu-countries/.

[8]Kyiv Post, Europeans Seek Role in Ukraine Peace Talks Amid US Uncertainty, 15 August 2026, https://www.kyivpost.com/post/82407.

[9]The Economist, NATO ponders how to defend Eastern Europe as America Pulls Back, 2 July 2026, https://www.economist.com/international/2026/07/02/nato-ponders-how-to-defend-eastern-europe-as-america-pulls-back.

[10]Yuri Zoria, WSJ: Europe is quietly building a NATO fallback in case the US steps back, Euromaidan Press, 15 April, 2026, https://euromaidanpress.com/2026/04/15/wsj-europe-is-quietly-building-a-nato-fallback-in-case-the-us-steps-back/.

[11]Ambassador David Dondua, Why Europe Cannot Accept Being Sidelined in the Ukraine Peace Process, EU Awareness Centre, 30 July, 2026, https://euawareness.org/analytics/why-europe-cannot-accept-being-sidelined-in-the-ukraine-peace-process/.

[12]Ursula von der Leyen, Speech by President von der Leyen at the EU Ambassadors Conference 2026, European Commission, 9 March 2026, https://ec.europa.eu/commission/presscorner/api/files/document/print/da/speech_26_576/SPEECH_26_576_EN.pdf.

[13]Forum Europa, Defence Commissioner warns that "in five years or less" Russia could attack the EU, 11 April, 2025, https://www.forumeuropa.eu/news/defence-commissioner-warns-five-years-or-less-russia-could-attack-eu.

[14]Nina Golgowaski, Top Russian Official Warns All EU Countries Now At War With Russia: 'The Peaceful Sleep is Over', HuffPost, 29 May, 2026, https://www.yahoo.com/news/world/articles/top-russian-official-warns-eu-163512358.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAD9pI9G-fHt7qyseLp3r3iyt97w7UWxAhmd34awhzuBB6BOoJT9kIDsqN2bzshMUhYnNsSA5nqBKrTLj1aaFDfeqGBk8eihgWJt1wkbCSJHrYSz_svA4bUvzLlHuN82am1QQGljgSgmFmL8RVPK8MQctIUb89SOtKHRgkurE7JjC.

[15]Duncan Allan, To be a great power: Russia's quest to destroy the post-1991 order in Europe, New Eurasian Strategies Centre, 20 November, 2025, https://nestcentre.org/to-be-a-great-power/#h-introduction.

for international law. How the "collective West" fomented succession in southern Russia, seeks to contain Russia, supports nationalists and neo-Nazis in Ukraine. He talked about the "values, experience and traditions of our ancestors."[16]

He needs another victory – in Ukraine – now. Instead it's unravalling.

Not all Europe's leaders agree on the situation's urgency. Some want Europe's dealings with Russia to continue as if the war changed nothing. That once it's over the Grand Projet of old will resume.

Don't Mention the War

"Europe is not at war with Russia," Belgian Prime Minister Bart De Wever told the Davos World Economic Forum in January[17]. The next month he called for normalised relations with Russia to regain access to cheap energy[18].

De Wever's comments are appeasement based on the at-best blinkered assumption that engagement with Moscow can be normalised. That would be business as usual with Putin, an indicted war criminal[19] whose country continues to commit atrocities in Ukraine. That has long believed it's at war with Europe where it seeks to undermine public support for Ukraine, destabilise governments and disrupt. The Kremlin has attacked with laundered money, cyberattacks, undersea-cable mapping, airspace breaches, arson, poisonings, drone disruption at airports, electoral interference, the funding of extremist politics. And more.

In August alone an armed drone was found near a Ukrainian plane at Leipzig airport. A blast tore through an Italian munitions factory that supplied arms to Ukraine. A Russian plan to kill a Ukrainian-American citizen in Warsaw was thwarted. There's little outcry. Even if it doesn't all track to Moscow. After the Leipzig incident, Germany's Interior Minister Alexander Dobrindt said a "new threat" has spilled over from the Ukraine conflict. It's not new and it will continue..[20], Maksym Beznosiuk warned: "Europe and NATO cannot spend the remainder of 2026 discussing red lines without clearly defining or enforcing them. The Kremlin appears determined to step up its hybrid pressure to fracture European resolve."[21]

It's politically expedient in the West to not call call this 'war'. To define conflict only as the declaration of hostilities, border incursions and bombs. Dismiss the rest as isolated incidents. And not scare the voters. Defence stays down the domestic agenda, at the edges of spending priorities. Because money spent on health, law enforcement and education brings visible results. Defence – when it works best, as deterrence – produces absence. No sirens sound. No missiles land. It demotes the need for joint European action and protection and undermines."It is unclear, faced with competing national security priorities, how committed European capitals are to deterring Russia's unconventional war on Europe,Charlie Edwards and Nate Seiderstein wrote[22].

The debate cannot be skirted forever.

British Defence Secretary John Healey resigned on June 11 because of government unwillingness "to commit the resources that the nation needs to defend the country at this time of rising threats."[23] On June 22 Prime Minister Keir Starmer announced he too would step down. Healey's departure was just one reason.

And as time goes on, pro-Russian parties in Europe's biggest economies push forward. In September the Alternative for Germany (AfD) won a decisive victory – and fell short of a majority – in the eastern state of Saxony-Anhalt. Polls for France's 2027 presidential election show National Rally leader Marine Le Pen in a first-round lead with about one-third of voter backing[24].

---

[16]Vladimir Putin, Address by the President of the Russian Federation, President of Russia website, 24 February, 2024, http://en.kremlin.ru/events/president/news/page/299.

[17]Interfax, Belgian PM: We are not at war with Russia, can't seize assets, 22 January, 2026, https://interfax.com/newsroom/top-stories/115747/.

[18]Jennifer Rankin, Belgian PM condemned over call to repair relations with Russia to ease energy costs, Guardian, 16 March, 2026, https://www.theguardian.com/world/2026/mar/16/belgian-pm-bart-de-wever-call-repair-relations-russia-energy-costs-condemned.

[19]International Criminal Court, Vladimir Abramovich Putin, charge sheet, https://www.icc-cpi.int/defendant/vladimir-vladimirovich-putin.

[20]Maksym Beznosiuk and William Dixon, How Russia's Hybrid Warfare Will Escalate in 2026 and What Europe Must Do?, Globe sec, 13 January, 2026, https://www.globsec.org/what-we-do/commentaries/how-russias-hybrid-warfare-will-escalate-2026-and-what-europe-must-do.

[21]Maksym Beznodiuk, Why Russia Could Escalate Hybrid Warfare Against Europe, Carnegie Europe, July 21, 2026, https://carnegieendowment.org/europe/strategic-europe/2026/07/why-russia-could-escalate-hybrid-warfare-against-europe.

[22]Charlie Edwards and Nate Seidenstein, The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure, the International Institute for Strategic Studies, 19 August, 2026, https://www.iiss.org/research-paper/2025/08/the-scale-of-russian—sabotage-operations--against-europes-critical--infrastructure/.

[23]Letter from Rt Hon John Healey MP to the Prime Minister, 11 June, 2026, https://assets.publishing.service.gov.uk/media/6a2af42da3674dfd3eb50760/Letter_from_Rt_Hon_John_Healey_MP_to_the_Prime_Minister.pdf.

[24]Politico, France – Presidential election 2027 first round, September 2026, https://www.politico.eu/europe-poll-of-polls/france/.

Europe lags the changing nature of warfare, more defined – in Ukraine – by sustained innovation and adaptation than territorial gains. Unmanned systems, countermeasures and operating methods update on a never-ending loop. Ukraine champions a bottom-up model with hundreds of firms and volunteer groups working closely with frontline forces. Russia pursues a more-centralised approach in which the state dominates. Kyiv leads in some areas. Moscow in others. Both "have moved far beyond prevailing Western practices," Andriy Zagorodnyk wrote[25].

That showed in NATO's Hedgehog 2025 exercise when 10 Ukrainians acted as an opposing force. In half a day they effectively neutralised two NATO battalions[26].

Ukraine's former Commander-in-Chief Valerii Zaluzhnyi said his country is so far in front of NATO, it could never be a member. "It is impossible for the Ukrainian Armed Forces, given their current level of development, to join an organisation that is guided by World War II doctrine." Ukraine will most likely align with a European security bloc, he said[27]. One option is the Joint Expeditionary Force of the Nordic and Baltic States plus the Netherlands and UK. Ukraine already has enhanced partner status and President Volodymyr Zelensky said his nation is ready for full membership.

It's possible European defence could ultimately fracture into different groupings that work independently with Ukraine[28].

Ukraine's desire to join the EU is also divisive. Zelensky applied within days of Moscow's full scale invasion. Detailed negotiations are under way. Ukraine is not according-to-the-letter ready to take up membership. And the EU is far from ready to let it in. At the same time there are geopolitical imperatives. Not least Ukraine has Europe's strongest military. Its integration is – on paper – vital. Pangiota Manoli wrote: "Enlargement is now testing the EU's capacity to act collectively as an actor serving its interests and values. Despite diverse perceptions among elites on the flaws of enlargement policy, what clearly emerges is the urgency for strategic clarity rather than partial policy adjustments."[29]

Old vs. New

Old Europe is more likely than the New to fall into the "well-intentioned attempts at consensus and compromise" that Ursula von der Leyen warned of.

A joint statement from the French, British and German leaders in June called for an immediate ceasefire. It flies in the sense of reality. Russian Deputy Foreign Minister Sergei Ryabkov said in August that Moscow will only accept a peace proposal that aligns with Putin's military objectives and reflects "realities on the ground."[30] The maintenance of those maximalist demands makes talks a chimera. So the statement's other points are irrelevant – that current contact lines be the start point for talks, that Ukraine needs robust and legally-binding security guarantees, and the continent's security interest must be safeguarded[31]. The approach echoes French President Emmanuel Macron's words four years ago: "We must not humiliate Russia so that the day the fighting stops, we can build a way out through diplomatic channels."[32]

New Europe speaks differently.

Kaja Kallas – a former Estonian Prime Minister – cautioned that the Kremlin deals over military threats and political pressure to reinforce demands. A slight retreat is presented as compromise. To the disadvantage of Western negotiators. Their instinct is to split the difference, let the middle ground decide the direction and reply: "maybe we should accept this." She has said Moscow must lose in Ukraine. Then not

---

[25]Andriy Zagorodnyk, The New Revolution in Military Affairs, Carnegie, April 20, 2026, https://carnegieendowment.org/research/2026/04/ukraine-russia-war-changing-warfare-practice-military-strategy.

[26]Bryan Daugherty, 10 Ukrainians Humbled Two NATO Battalions. When Will NATO Wake Up?, War on the Rocks, 26 March, 2026, https://warontherocks.com/10-ukrainians-humbled-two-nato-battalions-when-will-nato-wake-up/.

[27]Tim Zadoroznyy, Ukraine will 'never' join NATO, ex-commander Zaluzhnyi says, The Kyiv Independent, 4 August, 2026, https://kyivindependent.com/ukraine-will-never-join-nato-ex-commander-zaluzhnyi-says/.

[28]Jacob Funk Kierkegaard, The European Union and the war in Ukraine: More money, but not more Europe, Peterson Institute for International Politics, January 2026, https://www.piie.com/publications/policy-briefs/2026/european-union-and-war-ukraine-more-money-not-more-europe.

[29]Panagiota Manoli, The EU must solve the credibility deficit in its enlargement policy, LSE European Politics, Blog, 9 March 2026, https://blogs.lse.ac.uk/europpblog/2026/03/09/eu-credibility-deficit-enlargement-policy/.

[30]New Voice of Ukraine, Kremlin not interested in peace talks as Putin maintains maximalist war goals, 22 August, 2026, https://english.nv.ua/nation/russian-official-confirms-kremlin-unwilling-to-hold-meaningful-peace-talks-isw-says-50634867.html.

[31]Prime Minister's Office, 10 Downing Street, Joint E3 Leaders' Statement with President Volodymyr Zelenskyy of 7 June, 2026, UK.GOV, June 7, 2026, https://www.gov.uk/government/news/joint-e3-leaders-statement-with-president-volodymyr-zelenskyy-of-ukraine-7-june-2026.

[32]Dan Sabbagh, Russia must no be humiliated in Ukraine, says Emmanuel Macron, Guardian, 4 June, 2022, https://www.theguardian.com/world/2022/jun/04/russia-must-not-be-humiliated-ukraine-emmanuel-macron

be allowed to rearm and reattack[33].

"Historically, empires change their behaviour only when they lose their last colonial war...Russia has to lose its."[34]

Finnish President Alexander Stubb said in his New Year's speech: "Our relations with Russia have changed permanently."[35]

Polish Foreign Minister Radislaw Sikorski told the United Nations last year:

"To the representatives of Russia, I have this to say. We know you don't care for international law and you are incapable of living in peace with your neighbours. Your insane nationalism contains a lust for domination that will not cease until you realise that the age of empires is over and that your empire will not be rebuilt...I have only one request to the Russian government. If another missile or aircraft enters our space without permission, deliberately or by mistake, and gets shot down and the wreckage falls on NATO territory, please don't come here to whine about it. You have been warned."[36]

Russia is at its weakest since it began its war in 2022. Putin had 85 percent approval heading into this year. That's now at 74 percent[37]. Europe has leverage. It can take the hard line.

Russia Isn't Winning

Moscow racks up casualties faster than it can recruit. Up to 40,000 a month killed, injured, lost or captured. And 1.5 million for the whole war[38]. Only about 1,000 daily volunteered for service over recent months. Regional sign-on bonuses rose to a record 1.65 million roubles in August[39]. Speculation is of wide-spread mobilisation after September's parliamentary elections[40], despite North Korea's ongoing supply of troops and weapons. Almost no land is gained. Most months this year Russia's had a net loss of territorial control[41].

Crimea – a main staging ground for Russia's 2022 invasion[42] – is now a "zone of constant losses."[43]. Strikes on transport and infrastructure has almost cut off the peninsula. Reportedly 70 percent of residents have suffered power cuts.

What *Foreign Affairs* magazine called Plans A, B and C have failed. The Kremlin hasn't won over US President Donald Trump; America still supplies intelligence and weapons to Kyiv – now mostly paid for by Europe[44]; Russia may not outlast Ukraine. Not military. Not economically. the Kiel Instutit said:

"The contours of a genuine economic endgame are coming into view for Russia. The economy has not collapsed, but the structural foundations have eroded fast." [45]

---

[33]Kaja Kallas, Ukraine: speech by High Representative/Vice-President Kaja Kallas at the European Parliament Plenary, Diplomatic Service of the European Union, 9 September, 2025, https://www.eeas.europa.eu/eeas/ukraine-speech-high-representativevice-president-kaja-kallas-ep-plenary_en.

[34]Nordic Defence Review, Kaja Kallas, Russia Has to Lose Its Last Colonial War, 8 March, 2026, https://nordicdefencereview.com/kaja-kallas-russia-has-to-lose-its-last-colonial-war/#:~:text=She%20said%20Moscow's%20diplomats%20and,have%20very%20good%20negotiation%20tactics.%E2%80%9D.

[35]Alexander Stubb, New Year's Speech by President of the Republic of Finland Alexander Stubb on 1 January, 2026, The President of the Republic of Finland, January 1, 2026, https://www.presidentti.fi/en/new-years-speech-by-president-of-the-republic-of-finland-alexander-stubb-on-1-january-2026/.

[36]Radislaw Sikorski, Deputy Prime Minister Radislaw Siskorski's speech at the UN Security Council emergency session at Estonia's request, 22 September 2025, file:///C:/Users/User/Downloads/Deputy_PM_Sikorski's_speech_at_the_SC_UN_at_Estonia's_request,_NYC_22092025.pdf

[37]Levada Center, Putin's Approval Rating, chart, https://www.levada.ru/en/ratings/.

[38]The New Voice of Ukraine, Russia surpasses 1.5 million casualties, eclipsing all post-WWII Kremlin losses, 9 September, 2026, https://english.nv.ua/russian-war/russian-casualties-cross-1-5-million-troops-since-2022-full-scale-invasion-50639756.html.

[39]Janis Kluge, Russian recruitment stabilises at 1,000 per day, Russianomics, Substack, 8 August, 2026, https://janiskluge.substack.com/p/russian-recruitment-stabilizes-at.

[40]Milan Lelich, Ukiana Bezpalkd and Daryna Vialko, Russian losses reach 40,000 a month: Is Putin preparing new mobilisation?, RBC-Ukraine, 3 August, 2026, https://newsukraine.rbc.ua/news/russian-losses-reach-40-000-a-month-is-putin-1785750188.html.

[41]Harvard Kennedy School, The Russia-Ukraine War Report Card Aug. 5, 2026, Russia Matters, 4 August, 2026, https://www.russiamatters.org/news/russia-ukraine-war-report-card/russia-ukraine-war-report-card-aug-5-2026.

[42]Pjotr Sauer, 'No electricity, no water, no fuel: Ukrainian drone strikes bring darkness to Crimea's summer, 21 July 2026, Guardian, https://www.theguardian.com/world/2026/jul/21/no-electricity-no-water-no-fuel-ukrainian-drone-strikes-bring-darkness-to-crimeas-summer.

[43]Kyiv Independent newsdesk, Ukraine war latest: Crimea now 'zone of constant losses', SBU says after strikes on Russian air defences, military airfields, 24 June, 2026, https://www.yahoo.com/news/world/articles/ukraine-war-latest-crimea-now-174830440.html.

[44]NATO, NATO Allies and partners fund over 4 billion in PURL packages for Ukraine, press release, 10 December, 2025, https://www.nato.int/en/news-and-events/articles/news/2025/12/10/nato-allies-and-partners-fund-over-4-billion-in-purl-packages-for-ukraine.

[45]Becker, T, Gregor, K, Bosnia-Herzegovina, A, Klein M., Earphone, I, Riboviria, E, Reisinger, L, Scarisbrick, M, Endgame The State of the Russian economy, Kiel Institute, June 2026, https://www.kielinstitut.de/publications/endgame-the-state-of-the-russian-economy-19855/.

At Limits

For five centuries wars were repeatedly won by the side with the more flourishing economic base. Power position parallels economic position. "A large military establishment may, like a great monument, look imposing to the impressionable observer; but if it is not resting upon a firm foundation...it runs the risk of collapse," Paul Kennedy wrote.[46]

Russia struggles to to finance its aggression.

Its consolidated first-half budget deficit was 5.4 trillion roubles ($64 billion). In June alone it grew by 488.6 billion roubles[47]. That can't be plugged on the foreign debt market, from which Russia is excluded. Investors anyway have reduced faith in Russia's ability to service what it owes.

The government suspended domestic bond sales in July after a series of failed auctions.[48]

Clearly finances are increasingly difficult. Even if sovereign default is not imminent.[49]

There are simply fewer sources to fill the gap. Liquid sovereign wealth assets – rainy-day cover – are at 1.8% of GDP compared with 6.5% in 2022. First-quarter oil and gas revenues slid 45% from the same period last year. That's crucial. Russia never truly diversified from its fossil-fuel economy. Before the full invasion, these commodities drove half Russia's export revenue, nearly a fifth of GDP and over 30% of budget income[50]. There is little indication the situation will improve. Ukrainian attacks have taken out 43% of Russia's refining capacity. Industry losses in the last year are an estimated $13.5 billion[51]. A nationwide petrol shortage has drivers queuing for capped supplies. Wheat farmers – with higher diesel costs and bad weather – face smaller harvests and profits[52].

Ukrainian attacks have knock-on effects.

A 40-day campaign that ended on 4 August saw over 20 Wildberries logistics centres struck. It could cost the firm up to $3.3 billion. Losses to merchants who use the online retailer may reach $6.1 billion[53]. The state takes less tax[54]. And the financial sector – strapped for liquidity even as it makes preferential loans to state-aligned firms – doesn't get loans repaid. Sberbank, Russia's biggest lender, reported loan-book deterioration in the second quarter. Executives said corporate borrowers face the pressures of slower economic growth, high interest rates and a strong rouble[55]. Russia's second-largest bank VTB[56] guaranteed multi-billion-rouble loans to firms in the Wildberries group. If both fall to bankruptcy, it could trigger sector collapse. The problem is made worse by people's fear the Kremlin will seize their accounts. There was $7.3 billion is account withdrawals in July. On top of $4.5 billion in June. August is set to top both figures.[57]

Ordinary Russians face inflation of 6%-7% this year, according to the Central Bank[58]. That's over twice the Eurozone average[59]. Economic growth sputtered to an annual 0.9% in the second quarter.

---

[46]Paul Kennedy, The Rise and Fall of the Great Powers, William Collins, London and Dublin, 2017, pxxvii, 573.

[47]Interfax, Russia's consolidated budget deficit widens to 5.45 trillion rubles in H1 – Treasury, 17 August, 2026, https://interfax.com/newsroom/top-stories/118736/#:~:text=2026%2017%3A37-,Russia's%20consolidated%20budget%20deficit%20widens%20to%205.45%20trillion%20rubles%20in,Treasury%20said%20on%20its%20website.

[48]Bloomberg News, Russia Halts Bond Auctions With More Monetary Easing in Question, 21 July 2026, https://www.bloomberg.com/news/articles/2026-07-21/russia-halts-bond-auctions-with-more-monetary-easing-in-question.

[49]Peter Boyd, Russia Suspends Bond Auctions: Is a Default Imminent? The Investor Standard, 30 July, 2026, https://theinvestorstandard.com.au/2026/07/30/russia-suspends-bond-auctions-default/.

[50]Tatyana Lanshina, Fossil Fuel of War, Riddle, 26 May 2025, https://ridl.io/fossil-fuel-of-war/.

[51]Maksym Panchonka, ANALYSIS: What Zelensky's 40-Day Oil Campaign Achieved – and What It Didn't, Kyiv Post, 5 August, 2026, https://www.kyivpost.com/analysis/81748.

[52]Pyotr Kozlov, Russia's Wheat Harvest Faces Fuel Crunch and Rain Concerns, Bloomberg, 26 June, 2026, https://www.bloomberg.com/news/articles/2026-06-26/russia-s-wheat-harvest-faces-fuel-crunch-and-rain-concerns.

[53]Alex Stezhensky, Putin downplays Wildberries strikes as losses could approach $12 billion, New Voice of Ukraine, 19 August, 2026, https://english.nv.ua/nation/putin-downplays-wildberries-strikes-as-losses-could-approach-12-billion-50634109.html.

[54]Alex Strezhensky, Ukraine's Wildberries strikes threaten Kremlin-linked empire and seller network, The New Voice of Ukraine, 6 August, 2026, https://english.nv.ua/nation/ukraine-s-wildberries-strikes-expose-kremlin-ties-and-threaten-russian-sellers-50630353.html.

[55]The Moscow Times, Russia's Sberbank Warns of Rising Corporate Credit Risks as Bad Loans Increase, 19 July, 2026, https://www.themoscowtimes.com/2026/07/29/russias-sberbank-warns-of-rising-corporate-credit-risks-as-bad-loans-increase-a93374.

[56]Sean Ross, The 5 Biggest Russian Banks, Investopedia, 19 November, 2025, https://www.investopedia.com/articles/investing/082015/6-biggest-russian-banks.asp,

[57]Catherine Belton, Russians pull billions from banks, fearing Kremlin will seize deposits for war, The Washington Post, 18 August, 2026, https://www.washingtonpost.com/world/2026/08/18/russians-pull-cash-banks-fearing-kremlin-will-seize-deposits-war/.

[58]Bank of Russia, Bank of Russia cuts the key rate by 25 bps to 14% p.a., press release, 26 July 2026, https://www.cbr.ru/eng/press/keypr/.

[59]Eurostat, Annual inflation down to 2.8% in the euro area, release, 17 July, 2026, https://ec.europa.eu/eurostat/web/products-euro-indicators/w/2-17072026-ap. h

That's expected to slow to 0.5% in the third[60]. There are myriad other problems. The frontline's demand for bodies created a labour shortage. Russia's Business expects demand to weaken[61]. Russia's regions are so pinched, nearly a quarter cut healthcare spending this year[62].

Putin cannot end his war without a victory to sell the nation. In his Vertical system, Putin is not just a man or an office, but a political production complex, a clearing house for transactions[63]. Kremlinarchs are loyal as long as he fulfils his role. Be the regime/public contact point. And keep the money rolling in. And – as with all wars – there's wealth to be had while the fighting continues. So he goes on. Even as events on the battlefield and in the economy head to Russia's defeat and corner him. Putin, like Macbeth, is "in blood stepped in so far, that, should I wade no more, returning were as tedious as go o'er."[64]

To Poke or Not to Poke the Russian Bear

European inaction is costly. Peter Dickinson wrote: "For two decades, successive Western leaders have embraced policies of appeasement in a bid to avoid provoking Putin."[65]

The record bears him out.

In 2008 Germany – then the largest importer of Russian fossil fuels – scuppered Georgian and Ukrainian NATO membership at the alliance's meeting in Bucharest. Officially, they would simply "become members of NATO"[66]. It meant, promised, nothing and raised Russian hackles. That August Moscow fought a brief war with Tbilisi. International reaction was muted. EU leaders calls for a ceasefire appeared to favour Kremlin interests[67]. Barack Obama – when became US president the following year – sought a 'reset' with Russia. Moscow still controls about 20% of Georgian territory.

Emboldened by the weak response[68] Russia seized Crimea in 2014 and and backed a separatist uprising in eastern Ukraine. Again with few consequences beyond sanctions. The West's rhetoric hardened. The substance of policy did not: refrain from upholding international law, sacrifice Ukraine's interest and continue business as usual[69].

In December a collective loss of imagination to accommodate Belgian concerns meant the EU failed to seize 210 billion euros worth of frozen Russian assets. Germany refuses to supply its Taurus cruise missiles[70]. This fear of Russia cripples Europe, which does enough to prevent Ukraine's military and economic collapse. Not enough for it to prevail. In a June 3 letter to UK MP Jess Asato, the UK's then Armed Forces Minister Alistair Carns wrote: "The Government does not intend to establish a no-fly zone over Ukraine. The Government understands that such a step would likely lead to the shooting down of Russian planes which, in turn, would lead to further escalation."[71]

The best example of fine words over action is, arguably, the over-30-nation Coalition of the Willing. With Starmer and Macron as figureheads. Its raison d'être of creating a peacekeeping force for Ukraine is undermined by the proviso 'in the event of a ceasefire'. Which it's been long clear that won't happen. Yet, there was no change of direction, no move to make a real difference for Kyiv on the ground. The Coalition could have given troops paid leave to volunteer with Ukrainian forces, or – if the fear of a shooting march with Russian soldiers is too great – helped the police at the borders with Belarus and Transnistria. Now the Coalition faces a "slow death," The Telegraph speculated. Starmer's gone. France elects a new president in 2027. Without Britain and France at the helm, "there are fears of a leadership vacuum that

---

[60]Interfax, Central Bank expects Russian YoY growth to slow to 0.5% in Q3 from 0.8% (sic) in Q2, 5 August, 2026, 5 August 2026, https://interfax.com/newsroom/top-stories/118616/.

[61]Amelia Wojciechowska, The economic crisis in Russia is becoming more visible, Defence24.com, 29 July, 2026, https://defence24.com/geopolitics/the-economic-crisis-in-russia-is-becoming-more-visible.

[62]Russian Life, Russia's Shrinking Health Budgets, 6 March, 2026, https://www.russianlife.com/the-russia-file/russias-shrinking-health-budgets/.

[63]Karen Dawisha, Putin's Kleptocracy, Simon Schuster Paperback, New York, 2015, p160.

[64]William Shakespeare, Macbeth, III.4, The New Penguin Shakespeare, London, p101, 1995.

[65]Peter Dickinson, Western weakness is encouraging Putin to test NATO, UkraineAlert, Atlantic Council, 11 August, 2026, https://www.atlanticcouncil.org/blogs/ukrainealert/western-weakness-is-encouraging-putin-to-test-nato/.

[66]NATO, Bucharest Summit Declaration, 3 April 2008, www.nato.int/cps/en/natolive/official_texts_8443.htm.

[67]Peter Dickinson, The 2008 Russo-Georgia War: Putin's Green Light, UkraineAlert, Atlantic Council, 13 August, 2018, https://www.atlanticcouncil.org/blogs/ukrainealert/the-2008-russo-georgian-war-putins-green-light/.

[68]Anna Kalandadze, Matthew Bryza: Western response to Russia invasion was soft, delayed, 13 August, 2018, https://civil.ge/archives/249058.

[69]Ariana Gic, Marko Mihkelson and Roman Sohn, Tragedy of the West: Sacrificing Ukraine and the Rules-Based Order, Royal United Services Institute, 3 December, 2025, https://www.rusi.org/explore-our-research/publications/commentary/tragedy-west-sacrificing-ukraine-and-rules-based-order.

[70]AFP, Merz says Ukraine no longer needs German Taurus missiles, Euroactiv, 25 March, 2026, https://www.euractiv.com/news/merz-says-ukraine-no-longer-needs-german-taurus-missiles/.

[71]Copy of letter emailed to author.

could leave Europe rudderless," Joe Barnes and James Crisp wrote. The "obvious candidate" is German Chancellor Friedrich Merz.[72] Why? Europe doesn't have to always be led by the Old West.

Change the Guard

Nordic, Baltic and Eastern EU member states dominate the top 10 defence spenders when measured as a percentage of GDP. Germany – Europe's largest economy – ranks 11th[73]. It's the same with direct aid to Ukraine[74], which Denmark heads[75].

Lithuania, Latvia and Estonia last year cut the remaining physical ties with the Soviet-era power infrastructure. And made Russia's Kaliningrad exclave an energy island[76]. The Baltic Defence Line is under construction along their eastern borders. So the homeland is protected "from the first metre."[77] Norway added air cover, an artillery and light-infantry battalion, intelligence company and rapid-reaction force to defend its Russian frontier. NATO forces led by Sweden will be based in Lapland. Finland – with its conscription – can call on 900,000 reservists. It has stocked six-months' fuel and lubricants. It controls long-range missiles for air, sea and land. Romania this year opened NATO's second-largest logistics centre. It will coordinate and supply arms to Ukraine in tandem with a hub in Poland.[78]

These are actions that back up the hard line elucidated by Northern and Eastern leaders, including Kallas, Stubb and Sikorski. The Old West's ways have not stopped Russia from continued aggression. New Europe must push its case to lead the continent. Because it's not just about now. It's also about what comes after. There's no reason to assume the Russia that emerges from its war will be any less a threat then now. Sean Wiswesser wrote: "The psychological and political effects on Russian society will endure for decades.

But we cannot be optimistic about any real change from it, rather than paving the way for liberalisation or democratic reform, the aftermath of the war will only reinforce a more closed, securitised and authoritarian Russian state...The true legacy of this war will not be territorial gain or loss, but the transformation of Russia into a permanently militarised state, one in which the trauma of war strengthens authoritarian control rather than weakens it."[79]

This is why Old Europe's "well-intentioned attempts at consensus and compromise" must be abandoned. Moscow cannot be deferred to or feared. Decisiveness is needed. Because Russia's total military defeat is the best guarantee of peace in Europe. It's time London, Paris and Berlin gave way to Helsinki, Tallinn and Warsaw.

---

[72]Joe Barnes and James Crisp, The slow death of the coalition of the willing, Daily Telegraph, 2 August, 2026, https://www.telegraph.co.uk/world-news/2026/08/02/the-slow-death-of-the-coalition-of-the-willing/.

[73]European Parliament, At a Glance: EU Member States' defence budgets, factsheet, https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/785659/EPRS_ATA%282026%29785659_EN.pdf?utm_source=openai. .

[74]Statista, Bilateral aid allocations as a share of donor country's gross domestic product (GDP) between January 24, 2022 and February 28, 2026, by country, graph, https://www.statista.com/statistics/1373346/eu-gdp-member-states-2024/?srsltid=AfmBOorXYvs11oXwB7S9pJSm9R1fFeHaQySL9pPaEBMTvjgGuoBV4d7C.

[75]Csongor Koromi and Hann Cockerel, The closer to Russia the greater the fear, opinion poll finds, Politico, 20 October, 2026, https://www.politico.eu/article/russia-opinion-poll-closer-border-fear-yougov-eu-countries/.

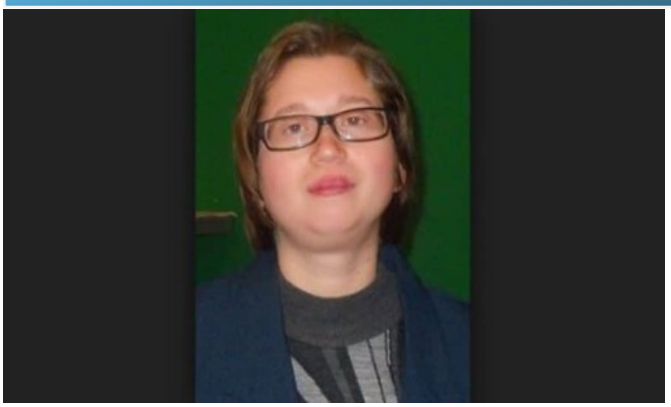
[76]SLDinfo.com, The Baltic Energy Cut-Off of Kaliningrad from Mother Russia, website, October 28, 2025, https://sldinfo.com/2025/10/the-baltic-energy-cut-off-of-kaliningrad-from-mother-russia/.

[77]Kevin Ryan, The New 'Baltic Way': Assessing the Baltic Defence Line Concept, Foreign Policy Research Institute, December 13, 2024, https://www.fpri.oYrg/article/2024/12/the-new-baltic-way-assessing-the-baltic-defensive-line-concept/.

[78]Bohdan Babaiev, Romania to open NATO's second-largest logistics hub to boost arms flow to Ukraine, RBC-Ukraine, December 21, 2025, https://newsukraine.rbc.ua/news/romania-to-open-nato-s-second-largest-logistics-1766334752.html.

[79]Sean Wiswesser, When the Guns Fall Silent: The Bleak Future of Postwar Russia, Proceedings, Vol. 152/8/1,482, August 2026, https://www.usni.org/magazines/proceedings/2026/august/when-guns-fall-silent-bleak-future-postwar-russia.

EUROPE - WESTERN BALKANS



Current Dynamics of International Relations and Geopolitical and Geo-Economic Changes in the Western Balkans: Divergent Positions and Regional Security Solutions

Monica AGRIGOROAIEI (Romania)

Summary

In recent years, the international security environment has been marked by intensified competition between great powers, Russia's war against Ukraine, the transformation of global supply chains and the acceleration of the energy transition. These developments have had a direct impact on the Western Balkans, a region characterized by an important geostrategic position, the persistence of unresolved political conflicts and economic, energy and institutional vulnerabilities. The European Union, the United States, Russia, China, Turkiye and the Gulf States pursue different objectives in the region, using economic, diplomatic, energy, technological and security instruments.

Source: https://www.kosovo-online.com/en/news/analysis/economies-western-balkans-should-cooperate-eu-also-seek-new-markets-10-1-2026

The war in Ukraine has increased the strategic importance of the Western Balkans for European security. At the same time, the process of European integration has acquired a more pronounced geopolitical dimension, and the EU is trying to reduce the region's economic and energy vulnerabilities through investments, reforms and progressive approximation to the single market. The European Commission has stressed in its recent assessments that progress towards accession depends on accelerating structural reforms, strengthening the rule of law and developing economies capable of withstanding the competitive pressures of the European market.

In this context, the stability of the Western Balkans depends on the capacity of the countries in the region to transform European integration into a concrete process of economic and institutional modernisation, as well as on the capacity of the EU and the transatlantic partners to provide a credible strategic perspective. The main priorities are strengthening the Serbia-Kosovo dialogue, stabilising Bosnia and Herzegovina, energy diversification, combating organised crime and disinformation, developing regional infrastructure and deepening rule of law reforms.

1. The Impact of Geopolitical Transformations on the Western Balkans

The transformations that have taken place in international politics in recent years have had a direct impact on the Western Balkans. The region was already characterized by a series of political, economic and social problems, but the war in Ukraine, changes in the energy market and competition between great

powers have made these vulnerabilities more visible. Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia are in a special situation: they are strongly linked to the European Union, but, at the same time, there are still important influences from Russia, China and Turkiye in the region.

From a political point of view, the most sensitive issue remains the relationship between Serbia and Kosovo. The lack of a definitive solution maintains a state of tension that can quickly return to the center of European attention when incidents occur. For the European Union, the issue is all the more important as the stability of the Western Balkans is directly linked to the security of the continent. An open conflict is not the most likely scenario, but the risk of repeated periods of tension cannot be ignored. In addition, any deterioration of the situation could further complicate the region's European integration process.

Serbia has a special role here. Belgrade is trying to maintain important economic relations with the European Union, without giving up traditional relations with Russia and without limiting cooperation with China. This policy gives Serbia some room for maneuver. At the same time, it complicates the relationship with Brussels, especially at a time when the EU is placing increasing importance on aligning candidate states with its foreign and security policy. Serbia is not the only state in the region trying to maintain relations with multiple actors, but it is probably the case where this strategy is most visible.

Bosnia and Herzegovina faces a different problem. Here, the main difficulty is represented by the functioning of a very complicated political system and the tensions between the different levels of power. Relations between central institutions and Republika Srpska remain a source of political instability, and reforms are progressing slowly. The situation is being closely monitored by the EU and the United States, as well as by Russia, which maintains relations with the Serbian leaders in Bosnia and Herzegovina. Thus, an internal problem also comes to have a geopolitical dimension.

Importantly, institutional vulnerability can become a security issue in itself. When institutions are weak, corruption is widespread, and political decisions are blocked by internal conflicts, a state becomes easier to influence from outside. Therefore, reforming the judiciary, combating corruption, and strengthening public administration should not be viewed solely as bureaucratic requirements imposed by the European Union. They are directly related to a state's ability to defend its own interests.

Economically, the situation is somewhat more favourable. The Western Balkans are closely linked to the European economy, and the European Union is the main trading partner and one of the most important investors in the region. This relationship gives Balkan states access to a very large market, investment, technology and infrastructure funds. At the same time, dependence on the European economy can become a problem when periods of economic slowdown occur in the EU.

The World Bank estimates moderate economic growth for the region in the coming years and draws attention to structural problems that may limit long-term development. These include an aging population, emigration, labour shortages and low productivity. The question is not only how fast the economies of the Western Balkans grow, but also whether this growth manages to reduce the gap in living standards with EU member states.

Emigration is one of the most visible consequences of this gap. Many young people in the region choose to work or study in EU countries, where salaries and job opportunities are better. In the short term, the money sent home by the diaspora helps national economies. In the long term, however, the departure of a significant part of the active population can become a serious problem. States lose labour, and certain areas end up facing a shortage of qualified personnel. Therefore, the economic development of the Western Balkans must also be viewed through the lens of the demographic problem.

Another important aspect is foreign investment. The European Union has a very strong position in the region, but it is not the only interested actor. China has invested in infrastructure, energy and transport projects, and Turkiye and the Gulf states have also become more active. For the governments of the Western Balkans, these investments are attractive because they can quickly bring money and projects to a region that needs modern infrastructure. The problem arises when a major project creates too much dependence on a single financier.

2. The Interests of External Actors

The Western Balkans are one of the few European spaces where the interests of several external actors meet directly. The importance of the region is not determined only by its economic or demographic size, but above all by its geographical position. The Balkans are located between Central Europe, the Adriatic Sea, the Aegean Sea and the Black Sea area and represent a link between the European Union and the Middle East. For this reason, controlling or influencing infrastructure, energy, trade and political relations in the region can have consequences that go far beyond the borders of the six states.

The European Union is currently the external actor with the greatest economic and institutional influence in the Western Balkans. However, the relationship between the EU and the region is different from its relations with other external partners, because for the Western Balkan states there is the concrete

prospect of accession. This prospect offers Brussels an instrument of influence that Russia, China or Turkiye cannot offer in the same form. The EU can condition the approach to the single market and access to certain funds on the implementation of political and economic reforms.

The fundamental interest of the European Union is the stabilization of the region and its progressive integration into European structures. From the perspective of Brussels, the problems in the Western Balkans cannot be separated from the security of the EU. Political instability, organized crime, illegal migration, energy dependence or tensions between Serbia and Kosovo can have direct effects on the member states. Therefore, European enlargement also has a security dimension. A region that is more stable and closer to the EU is, at the same time, a region that is less vulnerable to the influence of external actors.

The instruments used by the EU are varied. Accession negotiations are probably the most powerful political instrument, but they are complemented by European funds, investments, development programmes, technical assistance and institutional cooperation. The Growth Plan for the Western Balkans is important precisely because it seeks to deliver concrete economic benefits even before accession. The basic idea is relatively simple: if the countries in the region can have greater access to the European market and benefit from additional investment, their interest in moving closer to the EU increases and the economic gap with the member states can be reduced. However, European policy is not without its problems. The accession process is slow, and the reforms required by the EU are sometimes difficult to implement in countries where institutions are fragile or where there are strong political interests opposing change. In addition, there is a risk that the population in the region will perceive the European process as too technical and too distant from everyday issues. For the EU, this is a serious problem, because political influence cannot be maintained indefinitely simply by promising future accession. Visible results are also needed in infrastructure, economy, energy and living standards.

The European Commission's enlargement reports have consistently stressed that the Western Balkan states need to accelerate reforms in the rule of law, the functioning of democratic institutions, the fight against corruption and the independence of the judiciary. Therefore, the enlargement policy must be seen in two ways. On the one hand, it is a process of internal transformation of the candidate states. On the other hand, it is a way for the EU to expand its own political and security space.

The United States has a different approach. Washington does not have the same economic role as the European Union, but it remains one of the most important actors in terms of security. For the United States, the stability of the Western Balkans is linked primarily to the Euro-Atlantic security architecture and to maintaining NATO's influence in the region.

NATO's presence in Kosovo through KFOR is a very clear example. The mission is intended to contribute to maintaining a safe and stable environment and to reduce the risk of tensions between different communities escalating. At the same time, the US has invested in developing security relations with the states in the region, including through military cooperation, joint exercises and support for the modernization of the armed forces.

The US interest is essentially that the Western Balkans remain anchored in the Euro-Atlantic space. From this perspective, the accession of North Macedonia and Montenegro to NATO was an important development, and the rapprochement of Bosnia and Herzegovina and Kosovo with Euro-Atlantic structures remains a strategic objective. For Washington, the question is not only who controls the region politically, but also whether it can again become an area of instability requiring external intervention.

The relationship between the US and the EU in the Western Balkans is, in general, one of complementarity. The EU has the economic and institutional advantage, while the US has a greater military and security capacity. The two approaches complement each other in many situations, although there may be differences in the pace and methods used. For the states in the region, this combined presence provides a relatively stable security framework.

Russia has a different strategy and has more limited economic resources than the EU, but this does not mean that its influence can be ignored. Moscow's interest is primarily political and strategic. Russia seeks to prevent the full expansion of Euro-Atlantic influence and to maintain privileged relations with states or political groups that are favorable to it.

Serbia is Russia's main partner in the region. The historical, religious and political ties between the two states provide Moscow with a base of influence that it uses, in particular, on the Kosovo issue. Russia supports Serbia's position in the UN Security Council and opposes the recognition of Kosovo's independence. For Belgrade, Moscow's support is an important diplomatic tool, as Russia can block certain international initiatives that would disadvantage Serbia.

China is a different case. Beijing is not directly seeking to replace the EU as the main economic partner of the Western Balkans. Rather, it is trying to create its own footholds through investments and infrastructure projects. This approach is linked to China's broader policy of expanding trade and logistics connectivity.

In recent years, Chinese companies have been involved in road, rail and energy infrastructure projects in several states in the region. For Balkan governments, these projects are attractive because they can be completed in a relatively short time and provide access to financing for infrastructure that the region needs. From a geopolitical point of view, however, the issue is not only whether a project is built or not, but also who finances it, who builds it and who ends up controlling the infrastructure once it is completed.

3. Security, Hybrid Threats and Unresolved Conflicts

The security of the Western Balkans has changed considerably in recent years. If in the past, discussions about regional security focused mainly on military conflicts and the risk of confrontations between states, today the situation is much more complicated. A state can be destabilized without a war breaking out on its territory. Disinformation, cyber attacks, economic pressures, manipulation of social networks, energy dependence and external political influence can have significant effects on the stability of a country. These tools are increasingly associated with what specialists call “hybrid threats”.

The Western Balkans are particularly vulnerable to such threats because there are already a number of political, ethnic and social divisions. In a society where there is distrust in institutions, disinformation messages can have a greater effect than in a stable political system. False information about an ethnic incident, a government decision or the relationship with the European Union can spread quickly and provoke political reactions before the authorities have time to verify and correct the information.

This is one of the main difficulties of information warfare. It is not necessary for all false information to be believed by the majority of the population. It is enough for it to create enough distrust that people no longer know which sources are credible. In such an environment, any political or social crisis can become more difficult to manage. That is why information security has become an important component of national security.

Russia is one of the external actors trying to exploit these vulnerabilities. However, Russian influence in the Western Balkans should not be understood only through the prism of propaganda. Moscow uses a combination of political relations, historical ties, energy, mass media and contacts with local political groups. Serbia is the main example, but Russian influence can also be observed in Bosnia and Herzegovina, especially through relations with the Serbian part of the country.

After the Russian invasion of Ukraine, this problem became much more visible. Before 2022, some Western Balkan states were able to maintain a relatively balanced foreign policy between the EU, the US, Russia and China. However, the war made this position much more difficult. Pressure to align with European policy towards Russia increased, and the debate over the geopolitical orientation of the region became more intense.

An important aspect is that hybrid threats do not always come in the form of easily identifiable actions. A cyberattack on a public institution can be presented as a technical incident. A disinformation campaign can be presented as a simple journalistic activity. Economic pressure can appear in the form of a trade negotiation. It is precisely this ambiguity that makes it difficult for authorities to react. In the case of a military attack, responsibility is relatively clear. In the case of a hybrid threat, authorities must first establish who is behind the action and whether it is part of a broader strategy.

Cyberattacks represent another important vulnerability. The digitalization of public administration, banking systems, energy infrastructure and communications has brought important advantages, but has also created new vulnerabilities. An attack on a major digital infrastructure can have significant economic and social effects without the attacker being physically present in the country.

For the Western Balkan states, this problem is all the more difficult as the financial and human resources available for cybersecurity are more limited than in developed Western states. The lack of specialists, outdated IT systems and the different level of protection of public institutions can create significant gaps. Cooperation with the EU and NATO therefore becomes essential, as cyber threats do not respect national borders.

In 2026, the European Parliament continued to draw attention to hybrid threats in the EU’s neighbourhood, including information manipulation and foreign interference, cyber-attacks and pressures on infrastructure and energy security. The problem is increasingly being treated as one that affects European security as a whole, not just certain vulnerable states.

4. Solutions and Mechanisms for Regional Cooperation

The stabilisation of the Western Balkans cannot depend on a single institution or a single solution. The problems of the region are too different and, at the same time, too interconnected. European integration, regional economic cooperation, security, energy and institutional reform must be addressed together. From this perspective, the solution is not only for the states in the region to join the European Union as soon as possible, but also for them to be able to cooperate in the meantime, to reduce their

vulnerabilities and to build common mechanisms that work even when political divergences arise.

A first important mechanism is the Berlin Process. Launched in 2014, it arose precisely from the need to keep the Western Balkans on the European agenda at a time when the enlargement process was progressing relatively slowly. Its importance lies not only in the political meetings organized annually, but above all in the fact that it provides a framework in which the states in the region can discuss common problems and advance concrete projects. Cooperation in the fields of transport, energy, mobility and trade can produce results even before all the states become EU members.

An advantage of the Berlin Process is that it allows cooperation without all the political problems being resolved beforehand. This is important in a region where relations between states are sometimes difficult. If every economic project were conditional on resolving all political disputes, cooperation would progress very slowly. Instead, joint projects can create economic interests that, over time, make conflict less advantageous for the parties involved.

Another important mechanism is the Regional Common Market. The idea behind it is to gradually bring the economies of the Western Balkans closer together by reducing trade barriers, facilitating the movement of people and labour, recognising qualifications and developing common rules. In practice, a better integrated regional market can reduce costs for companies and make the region more attractive for investment. For relatively small economies, access to a wider regional market can be very important.

However, regional economic cooperation must be viewed realistically. It cannot replace EU membership. The difference between the two is fundamental. Regional integration can improve economic relations between the Western Balkan states, but only closer proximity to the European single market can provide access to the economic and institutional dimension of the EU. For this reason, regional projects are most valuable when they prepare the states for European integration, not when they are presented as an alternative to it.

An interesting example is the “Open Balkans” initiative, supported in particular by Serbia, Albania and North Macedonia. Its aim was to facilitate the movement of people, goods, services and capital between the participating states. However, the initiative has had a mixed reception in the region. Some governments saw it as a practical way to accelerate economic cooperation, while others were more sceptical, fearing that it could become a parallel project to the European integration process. This situation shows that, in the Western Balkans, even an economic initiative can quickly acquire a geopolitical dimension.

From a strategic point of view, the European Union has an interest in regional cooperation mechanisms being compatible with the accession process. In other words, if states start to cooperate more with each other in the fields of trade, transport or energy, these links should be built in such a way that they can later be integrated into the European system. This would reduce the risk of parallel economic structures emerging and would turn regional cooperation into an intermediate stage on the way to European integration.

The Growth Plan for the Western Balkans is important precisely from this perspective. Through this instrument, the EU is trying to offer countries in the region economic benefits before they actually join, but in exchange for concrete reforms. The logic is different from traditional enlargement policy. Instead of countries receiving the main benefits only after accession, they can gradually gain access to certain advantages of the European market if they demonstrate that they meet the established conditions.

However, the success of this policy depends very much on the capacity of national administrations. It is not enough for Brussels to provide funds. Countries must have institutions capable of preparing projects, following procedures, managing public procurement and demonstrating that the money is used efficiently. In a weak administration, even a very generous financial program can have a limited impact.

From this point of view, public administration reform is as important as infrastructure investment. A new road can be built in a few years, but developing an efficient administration takes much longer. Without institutions capable of planning and implementing projects, the economic gap with the EU may remain large even if European funds are available.

Regional organizations also have an important role, even if their influence is less than that of the EU and NATO. The Regional Cooperation Council, for example, aims to develop cooperation between states in the region in areas such as connectivity, economic competitiveness, mobility and human development. Its importance is more technical and coordination than geopolitical, but this very feature can be an advantage. Some issues can be discussed more easily in a regional framework than in one dominated by the great powers.

CEFTA, the Central European Free Trade Agreement, has an important function in facilitating regional trade. For the economies of the Western Balkans, the elimination of trade barriers and the simplification of customs procedures can have direct effects on companies. In the long term, such mechanisms can prepare economies for integration into the European single market.

The Black Sea Economic Cooperation Organization is also relevant for economic and trade

connectivity, although its role for the Western Balkans is more indirect. It provides a broader framework for cooperation between the Black Sea states and South-Eastern Europe, especially in the areas of transport, energy and trade. In the current geopolitical context, however, the functioning of these mechanisms is inevitably influenced by the deterioration of relations between Russia and Western states.

5. Short, Medium and Long-term Priorities

The analysis of developments in the Western Balkans shows that the region is not facing a single problem that can be solved by a specific political decision. Vulnerabilities overlap: there are unresolved security issues, still fragile institutions, economic and energy dependencies, demographic problems and an increasingly visible competition between external actors. For this reason, priorities must be ordered according to the time horizon. In the short term, there is a need to prevent crises and maintain stability; in the medium term, to strengthen economic and institutional resilience; and in the long term, to fully integrate the region into the European and Euro-Atlantic architecture.

5.1 Short-term Priorities

The first priority must be to prevent an escalation between Serbia and Kosovo. The issue can no longer be treated as a simple bilateral dispute, as any serious deterioration in the situation could have repercussions for the entire region. In recent years, incidents in northern Kosovo have demonstrated how quickly tensions can rise when security concerns overlap with political and identity disputes. For this reason, maintaining communication channels and incident prevention mechanisms must remain a priority for the EU, NATO and local actors.

The second short-term priority is to maintain stability in Bosnia and Herzegovina. The main risk should not necessarily be sought in a return to a large-scale military conflict, but in the gradual degradation of the functioning of state institutions. Contesting the authority of central institutions, political tensions between entities, and the polarization of society can weaken the state even in the absence of armed conflict.

The third priority is to combat hybrid threats. Currently, a political crisis can be amplified through social media, propaganda websites, coordinated accounts or the manipulation of sensitive topics such as national identity, migration, relations with the EU or the war in Ukraine. The European External Action Service considers disinformation and information manipulation as forms of hybrid threats that directly affect the Western Balkans and underlines the need for an approach that involves both governments and civil society and the media sector.

In the short term, states in the region need better capacities to monitor and analyze the information space, but also institutions that can communicate quickly and credibly during crises. It is not enough for authorities to say that information is false. They need to explain why it is false, provide the correct information and do this before the manipulative narrative consolidates.

The fourth priority is to accelerate European reforms. At this point, the question is no longer whether the Western Balkan states want to join, but whether their administrations are capable of implementing reforms. The European Commission's 2025 Enlargement Report shows that progress varies between states and that areas such as the rule of law, the independence of the judiciary, the fight against corruption and freedom of expression continue to determine the pace of rapprochement with the EU.

5.2 Medium-term Priorities

In the medium term, the main objective must be to reduce the region's structural vulnerabilities. The first of these is economic fragmentation. The six economies are relatively small, and administrative, customs and logistical barriers reduce the ability of companies to operate regionally.

The Common Regional Market can play an important role here. The regional market is conceived as a space based on European rules and standards and as an intermediate stage towards the single market. The European Commission estimates that deeper regional integration could bring significant economic benefits, including by reducing fragmentation and attracting investment.

However, an important distinction must be made here. Regional integration should not become a substitute for European integration. It should be a preparation for it. In other words, if the states in the region harmonise their rules, standards and procedures with those of the EU, the cost of economic accession will be lower when political integration becomes possible.

The new phase of the Common Regional Market for the period 2025–2028 follows exactly this direction. The leaders of the six Western Balkan states approved the new action plan in 2024, and the Regional Cooperation Council (RCC) has the role of supporting its implementation.

In the medium term, infrastructure development must also be accelerated. Roads, railways, energy networks and digital infrastructure should not be analysed in isolation. Together they form the strategic infrastructure of the region. A transport corridor that is not connected to European networks has less economic value than one that facilitates rapid access to EU markets.

The same principle applies to energy. Interconnecting electricity networks, diversifying supply sources and developing renewable energy can reduce geopolitical vulnerability. However, the energy transition must be done in a realistic way. Countries that are still dependent on coal cannot give up this source overnight without causing serious social and economic problems.

Therefore, energy policy must also include a "just transition" dimension. Mining regions must be given economic alternatives and workers must benefit from reconversion programs. Otherwise, the green transition may be perceived as a policy imposed from outside and may fuel political resistance to the EU.

Another priority is the modernization of public administration. This is perhaps one of the less spectacular but decisive problems. A weak administration means delayed projects, inefficient absorption of European funds, fewer investments and low-quality public services.

From this perspective, the economic development of the region depends not only on the amount of money invested, but also on the ability of states to transform investments into productivity. The World Bank warned in 2025 that although the region continues to grow, the prospects are strongly influenced by the evolution of the European economy and global uncertainty. In the autumn 2025 edition, the institution anticipated an aggregate growth of 3.1% in 2026 and stressed the need for policies oriented towards quality jobs, skills and digitalization.

More recent data from the spring 2026 edition of the Western Balkans Regular Economic Report, however, indicate a more cautious outlook, with a growth forecast of 2.8% for 2026. The World Bank links this revision to external uncertainties and emphasizes the importance of reforms, institutional capacity and the valorization of human capital. This is relevant for geopolitical analysis because it demonstrates that regional stability also depends on economic performance. An economy that does not generate enough jobs and opportunities for young people becomes more vulnerable to emigration, populism and external influence.

Therefore, economic policy must focus not only on GDP, but also on productivity, education, digitalisation, entrepreneurship and labour force retention. Youth migration to the EU is beneficial through remittances and skills transfer, but becomes a strategic issue if the region permanently loses its active population.

5.3 Long-term Priorities

In the long term, the strategic objective must be the full integration of the Western Balkans into European structures, provided that the accession criteria are met. This formulation is important because enlargement must not be transformed into a purely geopolitical process in which democratic criteria are abandoned for the sake of speed.

At the same time, the EU cannot afford to let the enlargement process remain indefinite. The geopolitical context has changed. Russia's invasion of Ukraine has shown that the existence of a "grey zone" between the EU and the Euro-Atlantic space can become a strategic vulnerability. From this perspective, enlargement is no longer just a neighbourhood policy, but also an investment in European security.

The European Commission stressed in the 2025 enlargement package that the process must remain merit-based and reform-based, with the pace of each state depending on progress in democracy, the rule of law and fundamental rights. The EU-Western Balkans summit declaration of December 2025 also presented enlargement as a geostrategic investment in peace, security, stability and prosperity.

In the long term, European integration should gradually reduce the region's vulnerability to external pressures. A state that is part of the single market, is connected to the European energy infrastructure, applies European law and participates in EU security mechanisms has fewer opportunities to be used as a geopolitical pressure point.

However, accession should not be seen as the end of the process. Even after European integration, states will need to protect their infrastructure, fight corruption and develop their defence and cybersecurity capabilities. The EU can reduce external vulnerabilities, but it cannot completely eliminate them.

6. Conclusions

The Western Balkans currently represent one of the most sensitive regions of Europe from a geopolitical point of view. Their importance does not stem from their economic or military size, but from their position at the crossroads of several strategic spaces and from the fact that the region retains political problems that have not been fully resolved.

From the perspective of a geostrategic analysis, the main vulnerability of the region is the combination of unresolved conflicts and still fragile institutions. Serbia and Kosovo are the most obvious examples. Bosnia and Herzegovina is another case in which stability depends to a large extent on the functioning of a complex institutional system vulnerable to political blockages.

These internal problems are amplified by external competition. Russia is trying to maintain its

political, energy and informational influence, especially through its relationship with Serbia and its position on the Kosovo issue. China mainly uses economic, infrastructural and technological instruments. Turkiye develops its influence through trade, investment, cultural relations and diplomacy. The Gulf states are mainly interested in investments and economic projects. None of these actors can compete with all the EU instruments at the same time, but each can exploit certain vulnerabilities of the region.

In this competition, the European Union starts from a structural advantage. The EU is the main economic partner of the Western Balkans and is the only external actor that offers the prospect of accession and integration into the single market. The problem is that this advantage needs to be transformed into a more credible strategy.

If the accession process is too slow, the gap between European promises and political reality can create frustration. If reforms are demanded without the population seeing concrete benefits, support for integration may decrease. On the other hand, if the EU manages to combine conditionality with gradual market access, investment and mobility, European integration can become much more attractive.

The Growth Plan is important precisely because it tries to change this logic. The plan aims to gradually move towards the single market in areas such as the free movement of goods, services and workers, access to SEPA, road transport, the integration and decarbonisation of energy markets, the digital market and integration into industrial chains.

References:

- European Commission. (2025). *2025 Enlargement Package: Commission assesses progress towards EU membership*. Directorate-General for Enlargement and Eastern Neighbourhood. Comisia Europeană – 2025 Enlargement Package;
- European Commission. (2024). *Commission adopts 2024 Enlargement Package*. Directorate-General for Neighbourhood and Enlargement Negotiations. Comisia Europeană – 2024 Enlargement Package;
- European Commission. (2023). *A New Growth Plan for the Western Balkans*. European Commission. Growth Plan for the Western Balkans;
- European Commission. (2025). *Growth Plan for the Western Balkans – Factsheet*. Directorate-General for Enlargement and Eastern Neighbourhood. Growth Plan – factsheet actualizat;
- European Commission. (2025). *Commission approves Reform Agendas of Albania, Kosovo, Montenegro, North Macedonia and Serbia, paving way for payments under the Reform and Growth Facility*. (Enlargement and Eastern Neighbourhood);
- European Commission. (2025). *Commission approves Bosnia and Herzegovina's Reform Agenda*. Directorate-General for Enlargement and Eastern Neighbourhood. (Enlargement and Eastern Neighbourhood);
- European Commission. (2025). *Allocations available for each beneficiary – Growth Plan for the Western Balkans*. (Enlargement and Eastern Neighbourhood);
- European Commission. (2025). *Common Regional Market*. Directorate-General for Enlargement and Eastern Neighbourhood. Common Regional Market – European Commission;
- European Council. (2024). *EU-Western Balkans Summit, Brussels, 18 December 2024*. Council of the European Union. EU–Western Balkans Summit 2024;
- European Council. (2025). *EU-Western Balkans Summit, Brussels, 17 December 2025*. Council of the European Union. EU–Western Balkans Summit 2025;
- European Union. (2025). *Brussels Declaration – EU-Western Balkans Summit, 17 December 2025*. (Enlargement and Eastern Neighbourhood);
- European External Action Service. (2025). *Countering Disinformation and Building Societal Resilience*. EEAS. EEAS – Countering disinformation and building societal resilience;
- European External Action Service. (2025). *EU-Western Balkans Summit: Strengthening Security and Stability Together*. EEAS. (European External Action Service);
- North Atlantic Treaty Organization. (2025). *NATO reaffirms its commitment to Western Balkans stability, as Secretary General Rutte wraps up visits to Sarajevo and Pristina*. NATO. NATO – Western Balkans stability;
- Regional Cooperation Council. (2024). *Western Balkans Six Leaders Declaration on Common Regional Market 2025–2028*. Sarajevo: RCC Secretariat. RCC – Common Regional Market 2025–2028;
- Regional Cooperation Council. (2025). *Western Balkans Economy Ministers Endorse Landmark Package of RCC-Facilitated Economic Deliverables*. RCC. (RCC);
- Regional Cooperation Council. (2026). *Common Regional Market*. RCC Secretariat. RCC – Common Regional Market;
- World Bank. (2025). *Growth in the Western Balkans Holds Firm Amid Global Uncertainty*. World Bank, Western Balkans Regular Economic Report. World Bank – Western Balkans Economic Growth 2025–2026;
- World Bank. (2025). *Jobs Critical to Sustaining Growth in the Western Balkans*. World Bank, Western Balkans Regular Economic Report. World Bank – Jobs and Growth in the Western Balkans;
- World Bank. (2026). *Western Balkans Regular Economic Report – Spring 2026: Adjusting to Shocks, Mobilizing Untapped Potential*. World Bank. World Bank – Western Balkans Regular Economic Report;
- European Council on Foreign Relations. (2025). Shopov, V. *Eyes Wide Shut: How to Read China's Playbook in the Western Balkans*. ECFR. ECFR – China's playbook in the Western Balkans;
- European Council on Foreign Relations. (2025). Kelmendi, T. & Maliqi, A. *Why the EU Should Use Kosovo's Election to Advance Its Goals in the Western Balkans*. ECFR. ECFR – Kosovo, Serbia and EU policy;
- European Council on Foreign Relations. (2025). Shopov, V. *The Next 'Big Bang': How the EU Can Fast-Track Enlargement Amid Geopolitical Tensions*. ECFR. ECFR – Fast-tracking EU enlargement;
- European Parliament, European Parliamentary Research Service. (2022). Russell, M. & Stanicek, B. *Russia's Influence in the Western Balkans*. European Parliament;
- European Parliament, European Parliamentary Research Service. (2023). *Russia and the Western Balkans: Geopolitical Confrontation, Economic Influence and Political Interference*. European Parliament;

- European Parliament. (2018). *Countering Hybrid Threats: EU and the Western Balkans Case*. European Parliament;
- European Parliament, European Parliamentary Research Service. (2026). Tothova, L. *EU Response to Hybrid Threats*. European Parliament;
- European Parliament. (2026). *Special Committee Adopts Proposals to Improve the European Democracy Shield*. European Parliament;
- CEFTA Secretariat. (2025). *CEFTA and Regional Economic Integration in the Western Balkans*. Central European Free Trade Agreement;
- OSCE. (2024–2025). *Regional Cooperation, Democratic Institutions and Rule of Law in South-Eastern Europe*. Organization for Security and Co-operation in Europe;
- European Bank for Reconstruction and Development. (2024–2025). *Regional Economic Prospects: Western Balkans*. EBRD;
- International Monetary Fund. (2025). *Regional Economic Outlook: Europe – Western Balkans*. IMF;
- Stiftung Wissenschaft und Politik. (2023–2025). *Western Balkans, EU Enlargement and Geopolitical Competition*. SWP Research Papers and Policy Briefs;
- Clingendael Institute. (2023–2025). *The Western Balkans and European Geopolitical Security*. Netherlands Institute of International Relations;
- International Crisis Group. (2023–2025). *Serbia-Kosovo Relations, Bosnia and Herzegovina and Western Balkans*. Crisis Group Reports.

EUROPE - BLACK SEA

The Dronification of the Black Sea: Civilian Shipping and the New Asymmetric Security Architecture

Ertürk ERYILMAZ (Turkiye)

Since 2022, the Black Sea has moved well beyond the model of a classical front line, becoming a laboratory in which unmanned systems have effectively erased the distinction between civilian and military targets. As the Russia-Ukraine war enters its fifth year, the center of gravity of the conflict has shifted from large naval platforms to cheap, mass-producible, high-precision unmanned aerial and maritime vehicles. This shift has turned a regional naval contest into a full-blown shipping-security crisis with direct consequences for global food and energy supply chains.

Source: https://arstechnica.com/gadgets/2026/08/romania-destroys-russian-drones-drifting-near-vital-european-offshore-gas-site/

1. From Platform Warfare to Swarm Warfare

The heavy losses suffered by Russia's Black Sea Fleet in the early phases of the war demonstrated that maritime dominance can no longer be secured through large-tonnage vessels alone, but increasingly through cheap, distributed systems. Ukraine's unmanned surface vessels (USVs) have expanded well beyond strike roles against surface targets, now also performing air-defense functions through air-to-air missiles mounted on the platforms themselves[1]. This evolution confirms a paradigm in which naval power is measured less by tonnage and armor than by sensor networks, satellite connectivity, and low-cost mass-production capacity.

Russia's response has, notably, moved outside the boundaries of classical naval defense: submarines and port facilities at Novorossiysk are now fitted with specialized anti-drone armor plating, floating barriers, and netting systems designed to intercept incoming unmanned threats before impact[2]. The same logic has since spread to the commercial fleet Suezmax-class oil tankers are having their superstructures wrapped in cage-style netting to prevent direct contact by explosive-laden drones, with water-filled tanks placed along the hull to absorb the shock of any resulting blast[3]. This is a striking case of battlefield doctrine the "cage armor" logic developed for armored vehicles migrating directly onto the civilian merchant fleet.

2. Turkish-Flagged and Turkish-Owned Vessels in the Crosshairs

As the coastal state with by far the densest commercial traffic in the Black Sea, Türkiye has become an involuntary but direct party to this asymmetric war. Between late 2025 and the first half of 2026, numerous Turkish-owned or Turkish-flagged merchant vessels including the *Cenk T*, *VIVA*, *Ant*, *Yaşar*,

and *Nadezhda* were struck by unmanned aerial vehicles shortly after departing Russian or Ukrainian ports[4]. The August 2026 attack on the *Yaşar* and *Nadezhda*, which occurred immediately after leaving the port of Novorossiysk and left Turkish crew members injured, prompted a sharply worded statement from the Turkish Ministry of Foreign Affairs warning of multidimensional negative consequences extending as far as global food security[5].

A notable development is the shift in the attack pattern itself: whereas earlier incidents targeted ships as they departed port, previously unseen strike profiles were recorded during the summer of 2026[6] evidence that targeting algorithms or operational doctrine are being actively revised. Equally significant is direct third-party intervention: according to the *Financial Times*, after drone strikes on tankers using the Caspian Pipeline Consortium (CPC) terminal to carry Kazakh crude rattled global oil markets, Kyiv at Washington's request pledged to refrain from targeting vessels not under Ukrainian sanctions and not carrying Russian oil or cargo[7]. This confirms that drone warfare in the Black Sea is no longer a purely bilateral affair; it has become a bargaining space shaped directly by the energy-security calculations of third states.

3. Montreux under Strain

The 1936 Montreux Convention restricted the passage of warships belonging to non-riparian states, placing responsibility for regional stability on the coastal states themselves. That framework never anticipated the legal status of unmanned aerial and maritime vehicles. Whether a USV qualifies as a "warship," and whether its transit through the Straits falls under Montreux at all, are questions that expose a ninety-year-old architecture increasingly out of step with today's technological reality. Türkiye finds itself caught in this ambiguity, simultaneously serving as guardian of the Montreux regime and bearing, through its own merchant fleet, the risks generated by the very legal gap it is charged with policing.

4. Cost Transmission to Insurance and Freight Markets

The intensification of attacks has made shipowners more cautious about the region, pushing freight rates and insurance premiums upward[8]. This cost pressure does not fall only on directly targeted vessels; it spreads across every commercial actor using Black Sea routes grain, sunflower oil, and crude oil shipments foremost among them. Over time, this dynamic is likely to force a redefinition of the traffic structure through the Bosphorus, of insurance regimes, and of any future "safe corridor" arrangements.

5. The Coastal State's Triple Bind

The drone-ification of the Black Sea confronts Türkiye with a three-dimensional bind: preserving the security of the Straits as guardian of the Montreux regime, sustaining diplomatic balance between the warring parties, and protecting its own merchant fleet inside what has become, in practice, an active combat zone. These three responsibilities are generating mounting, and increasingly incompatible, pressure on one another. In the near term, the expected response is a further spread of passive protective measures for civilian vessels netting systems, electronic jamming, convoy practices but these manage only the symptoms of the crisis, not its source. Durable stability will require nothing less than an explicit definition of the legal status of unmanned systems under the Straits regime and international maritime law, coupled with concrete, verifiable commitments from the belligerents to guarantee the safety of civilian navigation. Absent such steps, Türkiye's exposure will continue to grow in direct proportion to the intensity of a war it did not choose to fight.

---

[1] Milliyet, "How the Ukraine war spread to the Pacific: drone alarm thousands of kilometers behind the front," August 2026.
[2] UK Ministry of Defence satellite imagery; cited in Milliyet, op. cit.
[3] 7deniz Haber, "Russian tankers sailing under 'cage armor' amid attacks," August 2026.
[4] Haber7, "Why is Ukraine attacking Turkish ships?," August 2026.
[5] Statement by the Turkish Ministry of Foreign Affairs; cited in Yeni Şafak and Ensonhaber, August 2026.
[6] Haber7, op. cit.
[7] Financial Times; cited in Haber Denizde, "Netted countermeasures against drones," August 2026.
[8] 7deniz Haber, op. cit.

REGIONAL AND GLOBAL ACTORS

Türkiye's Strategic Rise: From Regional Actor to Global Power Projection

Eduard VASILJ (Croatia)

With a gross domestic product of approximately €1.32 trillion, sustained growth of 4.5% in 2023 and 3.2% in 2024, and a projected rate of around 3% for 2025, Türkiye is among the largest and most dynamic economies in the G20.[1] A population of around 85 million, a highly developed indigenous defence industry, and the second-largest military in NATO have further solidified Ankara's position as a regional power.

Over the past decades, Türkiye has systematically created the structural conditions to expand its geopolitical influence and evolve from a regional power into an increasingly globally active actor. This development is based on a long-term strategy that combines economic strength, efforts to achieve greater military autonomy, and a foreign policy approach that strategically draws on historical, cultural, and religious ties.

Source: https://www.globalpanorama.org/en/2026/06/the-power-of-being-needed-turkiyes-strategic-value-and-erdogans-domestic-consolidation-ahmet-erdi-ozturk/

Türkiye is increasingly extending its influence into regions that historically formed part of the Ottoman Empire, including the Western Balkans and the Caucasus, while simultaneously expanding its presence beyond its immediate neighbourhood into strategically significant regions, particularly the Red Sea and the Horn of Africa, to secure its trade routes. At the same time, the weakening of Russia due to the war in Ukraine and mounting pressure on Iran have altered regional power asymmetries, facilitating a partial reconfiguration of Türkiye's influence in these regions.

Integrated Economic and Infrastructure Expansion Model

Western Balkans

Türkiye's economic and infrastructural expansion in Southeast Europe and along the expanded Caucasus and Caspian Corridors does not follow a fragmented project pattern, but rather a structurally integrated architecture comprised of state institutions, semi-public development agencies, financial intermediaries, and private-sector implementation units.

This configuration allows for the systematic linking of economic presence, infrastructural control, and long-term political channels of influence. Overall, this creates a vertically organized model of economic policy influence in which capital export, infrastructure development, and strategic presence are functionally linked.

In the Western Balkans, the states with predominantly Muslim populations, such as Kosovo, Albania, and Bosnia and Herzegovina, serve as the central reference points for this structure. The Turkish Cooperation and Coordination Agency (TİKA) has already implemented several thousand projects in these countries, spanning education, health, and infrastructure sectors.[2] These measures should not be understood as isolated development interventions, but rather as institutional embedding mechanisms for a long-term presence within administrative, infrastructural, and societal systems.

Across the Western Balkans, Turkish economic engagement has been most prominently concentrated in Albania and Kosovo, where it has combined structurally significant FDI inflows - reaching up to 28% of annual inflows in Kosovo in selected post-independence years - with a steady expansion of investment stock in Albania, rising from approximately €381 million in 2014 to over €1.3 billion by 2025.[3] Overall, Türkiye ranks among the top ten investors in all of the aforementioned countries (even among the top five in Albania and Kosovo). Türkiye primarily invests in infrastructure projects, such as the operation of Pristina Airport by the Turkish company Limak Holding, the construction of Vlora Airport, and the joint establishment of Air Albania in a Turkish-Albanian joint venture.[4] In Montenegro, the Turkish company Global Ports Holding operates the container terminal at one of the largest ports in the Adriatic – the Port of Bar.[5]

This macroeconomic presence is complemented by an operational network of development institutions, the construction industry, and financial intermediaries. In Bosnia and Herzegovina, state-affiliated financial actors and banking systems play a central role in project financing, particularly banks within the extended Ziraat Bank structure, acting as lenders for housing, infrastructure, and urban development projects. An example of this is the financing of sections of the Sarajevo-Belgrade highway in Bosnia and Herzegovina.[6] In Serbia, the Turkish presence manifests itself primarily through infrastructure and construction projects, especially in road construction, energy infrastructure, and urban development programs, with EPC companies acting as operational implementation units.

For instance, the Turkish company Fortis Renewable Energy BV is planning the construction of a 270 MWp solar photovoltaic power plant in Sremska Mitrovica with an annual supply capacity for approximately 105,000 households.[7] In all its construction projects, Türkiye strategically seeks to secure financing and construction through collaboration between Turkish banks and companies.

Unlike its competitors in the region, such as China, Russia, and the UAE, Türkiye is not hesitant to extend its influence into the EU member states of the Balkans. In Croatia, this involvement is particularly evident in large-scale infrastructure, tourism, and real estate investments. The Doğuş Group operates in the Adriatic region with an investment volume exceeding €350 million, focusing on marina and real estate-based development strategies, and KENT Bank is involved as a financial partner.[8]

Caucasus

In the broader geopolitical space of the Caucasus and the Caspian Basin, a structurally comparable, but more energy- and transit-driven logic is evident. Azerbaijan functions as the region's central energy producer, while Georgia operates as a strategic transit corridor between the Caspian region and European consumption centres.

Türkiye is integrated into this architecture via the TANAP pipeline, which connects to the Trans Adriatic Pipeline (TAP), thus forming part of one of Europe's key southern energy supply routes.[9] This infrastructure represents not only an energy-related system but also a geopolitical corridor that functionally integrates production, transit, and consumption. Kazakhstan expands this structure as an additional Caspian energy and raw material player, increasingly involved in transcontinental logistics and energy flows.

While Türkiye acts less as a direct capital provider and more as an infrastructural and logistical hub, an expanded system of interdependence is emerging between Central Asia, the Caucasus, and Europe. This corridor logic is stabilized by long-term power purchase agreements, infrastructure consortia, and state-coordinated energy policy. Also, of interest with regard to energy supplies from the Turkic states is Türkiye's growing role in seeking to unlock the potential of Turkmenistan, which possesses enormous gas reserves (approximately 7.5 trillion cubic meters) but has so far had limited access to European markets, with Russia and Iran representing major geopolitical constraints.[10]

Overall, a dual structural model emerges: The Western Balkans are characterized by project-based development, construction, and financial architectures with medium capital volumes, while the Caucasus is characterized by large-scale energy and transit structures. Both regions, however, are linked by a common institutional logic in which state development actors, financial intermediaries, and private infrastructure companies operate in a functionally integrated manner and operationalize economic

expansion as a direct extension of strategic foreign economic policy.

Military-industrial Development, Integration of the Defence Industry, and Projection of Maritime Power

In addition to the economic and infrastructure-driven expansion architecture, Türkiye's military-industrial development forms an independent but structurally integrated block within the overall strategy.

The starting point for this development is the historical experience of external arms dependency and repeated embargo policies, particularly since the US arms embargo of the 1970s in the context of the Cyprus crisis.[11] This phase marked a structural turning point toward a more systematic pursuit of greater military autonomy, which has since gradually expanded across all key capability areas.

At the heart of this transformation is a largely indigenous defence industry complex that now integrates air, land, sea, and electronic warfare systems. In the aviation segment, unmanned systems such as the Bayraktar TB2 and Akıncı (developed by Baykar), as well as the Anka and Aksungur platforms (TAI/TUSAŞ), dominate. These platforms enable both tactical reconnaissance and precision strikes and serve as key export instruments in asymmetric conflict environments.

This is complemented by the TAI KAAN program, a fifth-generation combat aircraft that aims to achieve long-term substitution of external platform dependency in manned air combat systems.[12]

In the land segment, Türkiye's growing defence-industrial independence is reflected in modern armoured vehicles and main battle tank programs such as Altay (BMC/ASELSAN system integration), supplemented by mobile artillery and multiple rocket systems such as the T-155 Fırtına and TRG/TRG-300 missile systems (Roketsan). In the maritime sector, the so-called "Mavi Vatan" doctrine is operationalized through national frigate and corvette programs such as MILGEM (Ada and Istanbul classes), as well as through the integration of unmanned systems into naval platforms.[13]

The industrial infrastructure supporting this transformation is based on a tightly interwoven ecosystem of government procurement and governance institutions such as the Presidency of Defence Industries (SSB), research and development centres, and key private and semi-public companies such as ASELSAN (electronics and C4ISR), ROKETSAN (rocket and missile systems), TUSAŞ/TAI (aviation), Baykar (UAV systems), and BMC (land vehicles).[14] This configuration enables a vertically integrated value chain from research and production to export and significantly reduces external dependencies in critical technology segments.

NATO Membership and a National Middle Ground

Parallel to the development of greater military autonomy, Türkiye is establishing a strategically independent position within NATO structures. This is characterized both by the acquisition of Russian S-400 air defence systems and by the maintenance of military cooperation with Russia, including large-scale energy and nuclear projects such as the AKKUYU nuclear power plant, agreed upon in 2010, whose operational commissioning has been delayed, with the first unit now expected to enter service in 2026.[15] In this context, Türkiye is increasingly positioning itself as a balancing actor between its NATO commitments and its bilateral relationship with Russia, managing both frameworks in parallel without fully subordinating its strategic autonomy to either side.

At the same time, Türkiye, NATO's second-largest military, confidently pursues independent security interests and actively operationalizes these through military operations in Syria to enforce regional security and influence objectives.[16]

In parallel with this evolving defence-industrial capacity, an increasingly maritime and expeditionary component of military power projection is developing. This includes securing trade and energy corridors beyond the eastern Mediterranean region to the Red Sea and the Horn of Africa.

The military presence in Somalia (especially Camp TURKSOM in Mogadishu), together with Türkiye's broader logistical and security engagement along regional sea routes, contributes to securing strategic transport lines between the Suez Canal, the Indian Ocean, and the eastern Mediterranean.[17] This maritime expansion is functionally linked to the energy and infrastructure strategy and adds a security dimension to the economic corridor logic.

Cultural Integration, Historical Continuity, and Soft Power Architecture

Parallel to the economic, infrastructural, and security policy dimensions of Türkiye's foreign projection, cultural integration forms an independent, strategically functional block within the overall architecture. This is based on a combination of historical narrative formation, institutionalized religious diplomacy, media expansion, and the reactivation of shared civilizational reference systems. The primary goal is not symbolic representation but the long-term stabilization of cultural affinities as a structural complement to economic and political interdependencies.

In the Western Balkans, references to the Ottoman heritage play a particularly central role. In countries such as Bosnia and Herzegovina, Kosovo, North Macedonia, Albania, and parts of Serbia, this historical continuum is made visible through targeted restoration and infrastructure programs. The Turkish Cooperation and Coordination Agency (TİKA) is a key institutional partner in this effort, having invested for years in the restoration of mosques, bridges, caravanserais, and historical urban structures, thereby reconstructing tangible anchor points of shared historical narratives. This structure is complemented by the presence of the Presidency of Religious Affairs (Diyanet), which establishes an institutionalized religious link between Turkish and local Islamic communities through religious networks, imams, and educational programs.[18]

This cultural integration does not operate in isolation but is closely intertwined with political and economic presence, as it creates social opportunities for investment, infrastructure projects, and educational collaborations. Particularly in Kosovo and Bosnia, this creates a multilayered structure of religious, cultural, and economic interaction that strengthens long-term institutional ties.

In the broader context of the Caucasus, cultural integration is primarily organized through a pan-Turkic identity architecture. The Organization of Turkic States (OTS) serves as the central institutional framework for strengthening cultural, linguistic, and political commonalities between Türkiye, Azerbaijan, Kazakhstan, Uzbekistan, and other member and observer states.[19]

This structure operates less as a classic supranational organization and more as a platform for synchronizing cultural standards, educational cooperation, and historical identity narratives within a shared Turkic-language logic of civilization.

In parallel, the media and information architecture play an increasingly central role in the cultural connectivity of both regions. Turkish television stations, production companies, and digital media platforms have significantly expanded their reach in both the Western Balkans and the Caucasus.[20]

Series productions, news formats, and cultural content function as soft integration tools that reinforce linguistic proximity, cultural symbolism, and everyday narratives. In addition, Turkish newspapers, online portals, and transnational media networks contribute to the continuous presence of Turkish perspectives in the regional information space.

Taken as a whole, this soft power structure functionally complements the economic, infrastructural, and security policy dimensions of Türkiye's expansionist architecture. It acts as a long-term cohesion mechanism, intertwining historical continuities, cultural affinities, and media visibility, thereby stabilizing the structural embedding of Turkish spheres of influence in the Western Balkans and the broader Caucasus region.

Strategic Assessment: Geopolitical Dynamics and Power Volatility in the Caucasus

The economic, infrastructural, military-industrial, and cultural expansion axes of Türkiye described above do not operate within a static space, but rather within a dynamically shifting geopolitical environment. Ankara's long-term strategy is currently experiencing further acceleration due to structural power shifts in the broader post-Soviet space, particularly in the Caucasus and the adjacent Caspian system.

Central to this is the erosion of Russian influence capacities as a result of military and economic overextension in the context of the war in Ukraine. Russia is increasingly forced to concentrate resources on the European theatre of war, which has functionally weakened traditional mechanisms of influence in the South Caucasus - security guarantees, conflict mediation, and military presence. This does not lead to an abrupt withdrawal, but rather to a noticeable reduction in the density of its influence and its capacity for intervention.

This results in an expanded scope for action for Türkiye to consolidate and expand existing infrastructure, energy, and security corridors. The TANAP and TAP pipelines thus gain additional systemic importance within the European energy architecture.[21]

In parallel, Iran's influence profile is shifting. Internal economic restrictions, regional pressure, and ongoing sanctions are increasingly limiting Tehran's ability to project a sustained political and economic presence in the Caucasus.

The combined weakening of Russian and Iranian influence structures does not create a complete power vacuum, but rather a fluid competitive field in which actors with high institutional coherence and strategic consistency gain ground.

Türkiye is particularly favoured in this regard, as its existing architecture of economic integration, military-industrial self-sufficiency, cultural soft power, and institutional network politics is already geared toward expansion into precisely these areas.

The result is not an abrupt reorganization, but a gradual shift in regional hierarchies toward a multipolar, yet increasingly Türkiye-centric, sphere of influence in the broader Caucasus and Caspian Basin. At the same time, this development remains inherently fragile: it depends on the continuation of

external weakening processes affecting competing actors and is subject to growing competition from alternative models of influence, particularly capital- and infrastructure-driven engagements by external powers.

Against this backdrop, it becomes clear that Türkiye has evolved from a reactive regional actor into a structurally coherent power projector, combining economic expansion, infrastructural control, military-industrial capabilities, and cultural influence instruments into an integrated model. This architecture enables Ankara to operate effectively along strategic corridors from the Western Balkans to the Caspian region. However, the extent to which this geopolitical reach can be translated into sustained external expansion remains constrained by Türkiye's economic capacity.

Türkiye is not an economy in collapse; rather, high inflation and financing costs constrain the scale, speed, and sustainability of its external expansion. Its geopolitical reach can therefore exceed its capacity for capital-intensive expansion. At the same time, this model is not self-sustaining. Its long-term viability depends on Türkiye's ability to ensure macroeconomic stability, maintain continuous access to external capital, and preserve domestic economic and political control. Currency volatility, inflation dynamics, and energy dependencies represent potential limiting factors that could restrict the scalability of this expansion.[22]

Meanwhile, Türkiye operates in an increasingly competitive environment. In particular, China and capital-rich actors from the Gulf States are establishing parallel structures of influence that directly overlap with Turkish activities, intensifying competition for markets, infrastructure, and political alliances.

Overall, Türkiye's development should be understood neither as an inevitable rise to a permanent power nor as an overextension of a regional actor. Rather, it is a conditional transformation: the emergence of a potentially stabilizing power factor whose long-term role depends on the extent to which it succeeds in controlling internal structural limitations and maintaining a sustained strategic position in an increasingly multipolar and contested strategic environment.

---

[1]The World bank: 04/2026, https://www.worldbank.org/en/country/Turkiye/overview.
[2]Turkish Cooperation and Coordination Agency: 04/2026, https://tika.gov.tr/en/our-activities/.
[3]Bank of Albania: 04/2026, https://www.bankofalbania.org/home/.
[4]Limak. Holding: 04/2026 https://www.limak.com.tr/sectors/construction/projects/projects-completed/airports/prishtina-international-adem-jashari-airport-kosovo.
[5]Global Ports Holding: 04/2026, https://www.globalportsholding.com/our-ports/port-of-adria/.
[6]Euronews: 14.10.2024 by Sergio Cantone, https://www.euronews.com/2024/10/14/can-a-motorway-to-bosnia-strengthen-the-ties-between-serbia-and-Turkiye.
[7]Balkan Green Energy News: 19.02.2026 by Igor Todorovic, https://balkangreenenergynews.com/ebrd-mulls-investment-in-fortis-energys-solar-bess-project-in-serbia/.
[8]Croatia Week: 10.03.2016, https://www.croatiaweek.com/dogus-group-to-invest-e350-million-in-croatias-tourism-sector/#:~:text=Dogus%20Group%20to%20Invest%20%E2%82%AC350%20Million%20in,%20March%2010%2C%202016.%20*%20in%20Business.*
[9]Tanap Pipelines: 04/2026, https://www.tanap.com/en/tanap-project.
[10]American Enterprise Institute: 21.08.2020 by Michael Rubin, https://www.aei.org/op-eds/Turkiyes-new-gas-find-in-the-black-sea-wont-save-the-economy/.
[11]European Parliament: 04/2026, https://www.europarl.europa.eu/enlargement/briefings/1a2_en.htm.
[12]Türkiye Today: 14.09.2025, https://www.turkiyetoday.com/nation/tai-advances-kaan-fifth-generation-fighter-as-european-nations-express-interest-3206892.
[13]Centre for international maritime security: 18.09.2020, https://cimsec.org/Turkiyes-mavi-vatan-strategy-and-rising-insecurity-in-the-eastern-mediterranean/.
[14]Presidency of defence industries: 04/2026, https://www.ssb.gov.tr/en.
[15]Daily Sabah: 19.12.2025, https://www.dailysabah.com/business/energy/turkiyes-1st-akkuyu-nuclear-reactor-readied-for-2026-commissioning.
[16]The Guardian: 25.10.2024, https://www.theguardian.com/world/2024/oct/24/Turkiye-airstrikes-syria-iraq-attack-defence-firm-hq-ankara-kurdish-militant-pkk.
[17]The Washington Institute: 20.08.2025 by Ido Levy, https://www.washingtoninstitute.org/policy-analysis/halt-jihadist-advance-somalia-work-Turkiye-and-uae.
[18]Global Influence Operations Report: 21.10.2025, https://www.global-influence-ops.com/Turkiye-influence-operations-western-balkans-mosques/.
[19]Republic of Türkiye / Ministry of foreign affairs: 04/2026, https://www.mfa.gov.tr/turk-konseyi-en.en.mfa.
[20]European council of foreign relations: =3/2019 by Asli Aydintasbas, https://ecfr.eu/archive/page/-/from_myth_to_reality_how_to_understand_Turkiyes_role_in_the_western_balkans.pdf.
[21]Tap Pipeline: 04/2026, https://www.tap-ag.com/.
[22]Reuters: 09.02.2026 by Nevzat Devranoglu and Jonathan Spicer, https://www.reuters.com/world/middle-east/Turkiyes-inflation-fighting-quest-risks-stumbling-again-2026-02-09/#:~:text=Summary,cost%2Dof%2Dliving%20crisis.

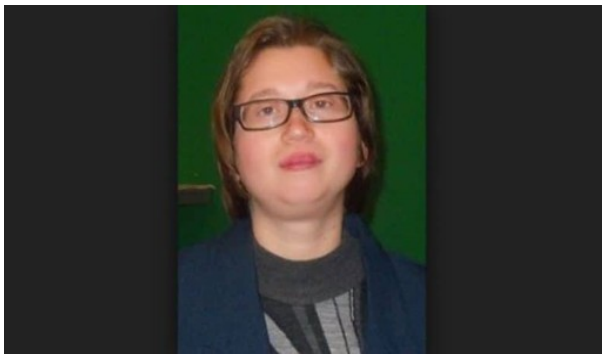
Biographies of the authors

❖ ❖ ❖

John Keith KING (USA)

John Keith King is the founder of Q Advisory and an enterprise architecture, cybersecurity, artificial intelligence and strategic communications adviser. His career spans more than four decades across defense, aerospace, telecommunications, cloud computing and national-security environments. His national-security service included supporting the White House as Lead Engineer for the U.S. Presidential Direct Communications Link, helping maintain secure strategic communications between the White House and the Kremlin. He has also served in senior enterprise architecture, technology leadership, cyber policy and program-management roles supporting four United States combatant commands and multinational missions. His work focuses on resilient digital infrastructure, AI-enabled cybersecurity, multi-domain interoperability and translating emerging technologies into practical strategic capabilities.

❖ ❖ ❖



Mona AGRIGOROAIEI (Romania)

She graduated in Political Science - Bachelor and Master in Political Marketing and Communication at "Al.Ioan Cuza" University in Iași. In 2023 she also graduated with a second master's degree "Security and Diplomacy" at SNSPA, Bucharest. She followed an internship at the "Center for Conflict Prevention and Early Warning during her studies at SNSPA. She specializes in academic research and exploration of Western Balkan political and security topics, publishing several analyzes in the media of this area in various newspapers in Albania , Kosovo, North Macedonia. Also published two books of poems in Albanian language in Pristina, Kosovo in 2014 and 2022.

❖ ❖ ❖

Eduard VASILJ (Croatia)

Eduard VASILJ holds degrees in Political Science and International Law from Goethe University Frankfurt am Main, as well as in Political Science and Organization from the University of Zagreb. After many years of international experience at executive board level, he advises global corporations and institutions on corporate governance, corporate security, geopolitical security issues, and foreign investments. He splits his time between Croatia and the German-speaking region.

❖ ❖ ❖

❖ ❖ ❖

Paul SZYMANSKI (USA)

The internationally acclaimed expert on space strategies and space warfare, Paul Szymanski is a major contributor to United States military space doctrine as an independent consultant. Paul Szymanski has more than 52 years of experience in all fields related to space control, including policy, doctrine, strategy, simulations, surveillance, survivability, threat assessment, long-range strategic planning, and command and control. In the past he has worked with the White House National Security Council (NSC), Congress, the U.S. Air Force, U.S. Army, U.S. Navy and Marines as well as civilian agencies like NASA, DARPA, and FEMA. His contributions range from working for the Air Staff at the Pentagon (Secretary of the Air Force - AQSC) to systems development at the Space and Missile Systems Center (SMC – ASP/XRJ) in Los Angeles, technology development at the Air Force Research Labs (AFRL/RD/RV/RI/RH) and as a member of the Independent Assessment Team general officer programmatic review board) in Albuquerque, New Mexico (USA) to operational field testing (China Lake Naval Test Center, California). Through this vast experience, he has a unique perspective of understanding all the divergent issues associated with each step of procurement processes. In addition, Paul Szymanski supported the NATO Supreme Allied Commander Transformation Group and has worked in critical space control programs (non-NRO) for 27 years, developing new concepts, analyses and simulations while managing technical programs critical to national U.S. security. He has administered or participated in multiple architecture studies that provided senior decision-makers with long-term strategic planning road maps and were being briefed to the Secretary of the Air Force, Secretary of Defense, Joint Chiefs of Staff, Congress, and the National Security Council.

Paul is also the founder of the Space Strategies Center. His works have been featured in the Strategic Studies Quarterly of the Air University of the U.S. Air Force, Aviation Week and he has been a frequent speaker at international conferences and exhibitions on satellite and space missions throughout the world. In total he has presented over 225 lectures and written publications in the last few years alone. He has also publishing 16 books on the topic of outer space warfare which serve as the foundation for modern space warfare planning and strategies. Paul Szymanski is available for conferences, seminars, and consulting.

❖ ❖ ❖

Calogero BONASIA (Italy)

Executive Program Manager with 35 years of experience across defence, public administration and regulated industries. As an Italian Air Force officer from 1991 to 1995, I commanded the NATO/ACCAM Communications Centre at the 41st Wing in Sigonella, with responsibility for 480 personnel, budgets, projects and the operational continuity of military and civilian networks in a classified environment. I subsequently worked with the Italian Army and Navy on document digitisation, process design, workflow and regulatory compliance. Since 2022, I have supported the leadership of a software division through portfolio governance, capacity and dependency management, risk oversight and executive performance analysis.

Core expertise:

-Complex programmes and governance programme and portfolio management, PMO, capacity, dependencies, progress, risk, KPIs and executive reporting;

-Defence and classified environments unit command, personnel and budget responsibility, military and civilian telecommunications, NATO/ACCAM experience and operational continuity.

-Security, risk and compliance ISO/IEC 27001, ISO 9001, ISO 31000, internal audit, information governance, controls and regulatory compliance.

-Systems, processes and data Jira, BigPicture, eazyBI, KNIME, Confluence, Linux, Unix, Solaris, SharePoint, workflow, DevOps and performance analysis.

❖ ❖ ❖

❖ ❖ ❖

Aldo MUNGO (Belgium)

Aldo Mungo is a recognized specialist in strategic studies and the doctrine of air power employment, with expertise built over more than thirty years in specialized defense journalism. After completing studies in political science and international relations at the Université Libre de Bruxelles (ULB), he quickly turned toward the defense and armaments sector. In 1984, he founded the monthly magazine Carnets de Vol, dedicated to military aviation, which he directed and relocated to Paris in 1986. From 1989 onward, he served as editor-in-chief and editorialist of the monthly Armées & Défense (the French edition of the Israeli-American magazine Defense Update). Both publications rapidly became essential references in military, industrial, and institutional circles. He held these roles until 2011, when he returned definitively to Belgium. His recognized expertise led to his selection as an auditor at the Institut des Hautes Études de Défense Nationale (IHEDN) in Paris (1988–1989 session), where he deepened his knowledge of defense policy, strategy, armaments, and the economics of defense. In 1990, the French Air Force General Staff integrated him into a six-week advanced training program at the US Air Force Weapons School, as part of the Red Flag exercise at Nellis Air Force Base (Nevada). Embedded within a French detachment, he took part in intensive, realistic combat-air training missions, benefiting from cutting-edge real-time performance analysis tools (RFMDS) and access to vast training ranges, including classified areas. Today, Aldo-Michel Mungo is still regarded as one of the leading civilian experts on the military doctrine of air vector employment. His analyses and contributions focus primarily on strategic, tactical, and technological developments in air power and defense.

❖ ❖ ❖

Prof. Krzysztof ŚLIWIŃSKI (Hong Kong)

Prof. Śliwiński Krzysztof Feliks is an Associate Professor at the Department of Government and International Studies of Hong Kong Baptist University (https://gis.hkbu.edu.hk/people/prof-krzysztof-sliwinski.html) and Jean Monnet Chair. He received his doctorate from the Institute of International Relations at the University of Warsaw in 2005. Since 2008, he has been employed at Hong Kong Baptist University. He has regularly lectured on European Integration, International Security, International Relations, and Global Studies. His primary research interests include British foreign policy and Security Strategy, Polish foreign policy and Security Strategy, Security and Strategic Studies, Traditional and Non-traditional Security Issues, Artificial Intelligence and International Relations, European Politics and the European Union, Theories of European Integration, Geopolitics, and Teaching and Learning.

Hong Kong Baptist University, ORCID ID: https://orcid.org/0000-0001-7316-3714, E-mail: chris@hkbu.edu.hk.

❖ ❖ ❖

❖ ❖ ❖

Michael KEEN (USA)

Michael KEEN is the Chief Intelligence Officer and Managing Partner of Ridgeline Advisory Group, where he advises executives, boards, investors, and institutions on geopolitical risk, geoeconomic exposure, strategic competition, and decision-making under uncertainty. His work examines how military competition, alliance cohesion, sanctions, export controls, energy security, industrial policy, supply chain concentration, and regulatory fragmentation affect national strategy and enterprise decisions. His areas of focus include NATO, Russia, European security, transatlantic relations, strategic infrastructure, economic statecraft, and the commercial consequences of geopolitical change. Michael is the creator of the Ridgeline Intelligence Operating System, or RIOS, and the Decision Signal System, or DSS. Michael combines geopolitical and strategic advisory experience with more than two decades of leadership in global technology, infrastructure, enterprise transformation, and executive operating environments across North America, Europe, the Middle East, Africa, and the Asia-Pacific region.

Areas of expertise:

- NATO, Russia, and European Security
- Geopolitical and Geo-economics Risk
- Strategic Competition and Economic Statecraft
- Transatlantic Security and Alliance Cohesion
- Energy, Infrastructure, and Supply Chain Security
- Sanctions, Export Controls, and Regulatory Risk
- Defense Industrial Capacity and Strategic Resilience
- Scenario Analysis and Strategic Foresight
- Intelligence Architecture and Structured Analysis
- Executive and Board-Level Decision Support
- Capital Allocation Under Geopolitical Uncertainty
- Technology Sovereignty and Critical Infrastructure

❖ ❖ ❖

Vasileios VLACHOS (Greece)

He is highly experienced Security Professional with a strong background in corporate, hospitality, and high-profile event protection. Proven track record in risk assessment, loss prevention, and team leadership. Skilled in managing diverse security operations for luxury hotels, resorts, and private enterprises while ensuring compliance with international safety standards. He has extensive experience in Security Operations & Supervision, Risk Assessment & Incident Management, VIP & Executive Protection, Loss Prevention Strategies, CCTV & Access Control Systems, Team Leadership & Training, Crisis & Emergency Response. He has attended and graduated numerous specialized studies in the country and abroad and obtained licenses and certificates of graduation in various fields such as: Security Risk Management, Psychological First Aid (Johns Hopkins University/USA), Understanding and Managing the Stresses of Police Work (University of Toronto/Canada), COSHH Manager Certification (The Knights of Safety), Open-source Intelligence (Institute of Governance in Basel/Switzerland), Certificate in Disaster Preparedness (University of Pittsburgh), HB1143 Firearms Safety Training Course (Washington Civil Rights Association/USA).

❖ ❖ ❖

❖ ❖ ❖

Alistair HOLLOWAY (United Kingdom)

Education:

- University College London, MA, Russian and Post-Soviet Politics, Distinction, 2019-2020
- Northumbria University, BA (Hons) English and History, 2:2, 1988 – 1991

Courses (Online):

- International Human Rights: War, Conflict and the Responsibility to Protect, ICE Cambridge University
- International Humanitarian Law in Theory and Practice; Universiteit Leiden

Returned to education after 25 years of international political, financial and economic journalism. Currently writing a second book on Russian politics, provisionally titled Mutant Markets: The Failure of Russian Capitalism.

- MA Russian and Post-Soviet Politics.
- Wrote Putin's Stories: How Russia Was Sold Into Ceaseless War. Published February 2025.
- Broke news by building relationships to gain exclusive access to political and business leaders.
- A career rooted in reporting on governments, economies and financial markets.
- Shorthand.
- Languages: Estonian, French, Finnish, Russian.

2025-2026: Write essays about Russian politics for my Substack page. Was interviewed by Fahd Hussain on Express 24/7, Pakistan's premier English language global affairs programme, July 2026.
2020-2024: Researched and wrote **PUTIN'S STORIES: HOW RUSSIA WAS SOLD INTO CEASELESS WAR,** Published February 2025.
2019-2020: MA RUSSIAN AND POST-SOVIET POLITICS: University College London, Distinction.
2017-2018: LUXEMBOURGER WORT/LUXEMBOURG TIMES: Was a reporter on a seven-person team to develop the English content of Luxembourger Wort – the Grand Duchy's biggest newspaper – into the Luxembourg Times. Covered Brexit, European ministers' meetings in Luxembourg and Brussels, the ECB, and institutions including the European Court of Justice and European Stability Mechanism.
2016: SOUTH CHINA MORNING POST: Hong Kong, Business Editor. Handled copy from reporters with English as a second language.
2014-2016: BRAIN LIGHTNING: Toronto. Taught English literature and language to Chinese and Chinese-Canadian students from grade one up to grade 12. A number of my pupils went on to pass university entrance exams.
2014: CHINA DAILY: Beijing. Senior Business Editor.
2012-2013: WALL STREET JOURNAL/DOW JONES NEWSWIRES: London. Editor. Edited stories for the Wall Street Journal's European webpages. This included pulling pictures into the text, adding link and creating a complete product for clients before putting them online. Handled market stories from reporters – on bonds, stocks, commodities, corporate news – and sent them to the Dow Jones wire.
2007-2011: BLOOMBERG: London. Reporter. Covered the commodity markets, primarily coal and shipping.
2005-2007: BLOOMBERG: Helsinki. Reporter. Wrote about the government and economy in Finland and the Baltic States. Also covered European Union stories on assignment in Brussels and went to Frankfurt to write about the European Central Bank.
2001-2005: REUTERS: Helsinki. Reporter. Covered Finnish stories, everything from bond issues to company results to sports and wife carrying.
1998-2001: REUTERS: Tallinn. Reporter/Deputy Bureau Chief. Worked in a two-person bureau. Followed Estonia's bids to join NATO and the European Union.

❖ ❖ ❖

❖ ❖ ❖

Jack LINDSTROM (USA)

a. Education:

1. UC San Diego, School of Global Policy and Strategy, San Diego, CA
Master of International Affairs, June 2028
Courses: Quantitative Methods, Microeconomics, Globalization, Strategic Studies

2. Thomas Edison State University, Orange, NJ
Bachelor of Arts, International Studies, specializations in Chinese History, Spanish, June 2026

b. Experience:

1. Mackinder Forum, London, UK
Junior Researcher, June 2026 – Present
- Assessed international events spanning geostrategy, geopolitical theory, history, and geoeconomics on a weekly basis, informing speaker vetting decisions for programming
- Authored geostrategy literature applying the Mackinder–Spykman framework to inform analysis of contemporary great power competition, working directly with Director Leonard Hochberg

2. Arctic Ledger, San Diego, CA
Founder | Lead Researcher, April 2026 – Present
•Founded an independent research and publishing platform covering Arctic geopolitics, critical minerals, chokepoints, and international governmental policy, under the mentorship of White House and House of Commons affiliates
•Recruited and managed research teams totaling 30+ researchers across 10 countries and 5 continents, compiling and publishing 2 volumes and 6 total essays of original peer-reviewed geopolitical research, pending publication through The Arctic Institute, SDWAC, and The La Jolla Strategic Institute
•Produced viable strategy for organization foundation, expansion, recruitment, and geopolitical strategy research, including policy briefs

3. Thomas Edison State University, Orange, NJ
Junior Sino-Policy Researcher, May 2026
•Produced research regarding US-Sino soft power transmission and imbalance, emphasizing US policy response and Chinese governmental strategy

4. City of Phoenix & Chengdu Municipal Government, Chengdu, China
Representative & Field Researcher, November 2024
•Represented Arizona in an official diplomatic capacity with the People's Republic of China through a formal sister-cities cultural exchange program, negotiating structured bilateral dialogue and cross-cultural communication
•Strategized with individuals from the Senate Committee on China to draft U.S.-China diplomatic proposals, leveraging diplomatic communication and conceptualization skills throughout bilateral sessions
•Presented public remarks on U.S.-China technological competition and cooperation and policy, focused on implementation through public speaking rooted in US-China relations

5. Civil Air Patrol, U.S. Air Force Auxiliary, Phoenix, AZ
Cadet Leader, November 2018 – April 2025
•Engaged in operational contributions to policy analysis and execution during real-world incident response
•Awards: Crisis Service Medal, Civil Air Patrol (October 2022), Master Rating in both Communications and Emergency Services, Civil Air Patrol

❖ ❖ ❖

❖ ❖ ❖

Anand RADJOU (India)

Chief HR Officer • Business Strategist - *Systems Thinker • Framework Architect • HR Transformation Leader.*
Multidisciplinary strategic architect with 17+ years of progressive leadership spanning corporate strategy, organizational transformation, and complete HR department ownership across IT, Technological start-ups, pharmaceuticals, nutraceuticals and international NGO sectors. Expert in building Business Systems & Frameworks and HR functions from ground up encompassing all 8 HR functional areas and architecting scalable business ecosystems, CoE, and compliance frameworks for sustainable growth.

1. HR Department Leadership & Complete Functional Ownership:

-Talent Acquisition & Workforce Planning
-Learning & Development
-Performance Management
-Compensation & Benefits
-Employee Relations
-HR Compliance & Governance
-HRIS & HR Technology
-Onboarding & Offboarding

2. Strategic Systems & Business Frameworks:

-Strategic Architecture
-Market Intelligence
-Governance & Leadership
-Communication & Elevation

3. Strategic Leadership Experience;

-Chief HR Officer & CISO
-Founder & Executive Director (Chief Strategy Officer)
-Strategic Campaign Consultant (Organic & Neutral

4. Earlier Career & Foundation:

-Head of HR & People Strategy (Sr. HR Generalist)
-Operations & Client Relations
-Business Operations & Financial Management

5. Education & Professional Certifications:

-MBA – International Business
-MBA – Human Resources
-B.E. – Electronics & Communication Valliammai

❖ ❖ ❖

Christos BEZIRTZOGLOU (Greece)

Christos BEZIRTZOGLOU was born in Athens (Greece) in 1966. He studied Physics with specialisation in Electronics and Computers. He worked in Greece as a trainer and consultant in Information and Communication Technologies for ten years. In 1994 he moved to Brussels (Belgium) to join the European Commission, where he occupied different posts both in policy Directorates-General (Environment, Competition, Regional Policy & Trade) as well as in policy coordination (Secretariat-General & Cabinet of Commissioner Diamantopoulou for Employment and Social Affairs).

❖ ❖ ❖

❖ ❖ ❖

Ertürk ERYILMAZ (Turkiye)

A Security Strategist, Regional Analyst, and Strategic Risk Analyst working at the intersection of social dynamics, geopolitical transformations, and the global security architecture; conducting interdisciplinary research on security policy, intelligence analysis methodologies, hybrid threats, the defense industry, cybersecurity, financial security, and regional power competition.

His work is grounded in strategic analysis, open-source intelligence (OSINT), intelligence analytics, strategic reporting, geopolitical assessment, and decision-support systems. His research focuses primarily on the Middle East, Central Asia, and the Turkic world, covering security policy, hybrid warfare, information operations, defense industry trends, economic security, and digital threat environments.

He aims to support public institutions, research centers, think tanks, and the private sector by evaluating multi-source data through analytical methods to contribute to strategic reporting, risk analysis, and decision-support processes.

Work experience:

Director – Chief Analyst

MIRAS GLOBAL – Mefkûre Intelligence, Risk Analysis and Strategy Center | *January 2026 – Present*

Leads the institution's strategic direction in security, intelligence, and risk analysis; manages multi-source analysis processes, strategic reporting activities, and decision-support studies.

Columnist

HasBahçe Gazetesi | *September 2025 – Present*

Writes regular columns on security, geopolitics, and strategic analysis topics.

Cyber & Financial Intelligence Consultant

Freelance | *January 2024 – Present*

P rovides advisory services in cyber risk and financial security; conducts risk assessment and intelligence analysis work for institutions.

Civil Society, Media & Cyber Analysis Studies

Freelance | *January 2022 – Present*

Conducts regional field research, societal risk analysis, and media/cyber domain studies for NGO and public support platforms.

Project and Investment Advisor

Eren Emlak | *Freelance*

Provides advisory support in real estate project and investment processes

Education:

Istanbul Topkapı University

M.A., Security Sciences and Applications

February 2026 – Present

Ahmet Yesevi University

M.A., Political Science and Government

September 2024 – January 2026

Atatürk University

B.A., Sociology

❖ ❖ ❖

❖ ❖ ❖

Aleksandar GRIZHEV (North Macedonia)

Aleksandar GRIZHEV is an Associate Professor and Head of the Department of Social Sciences and Humanities at the Military Academy "General Mihailo Apostolski" - Skopje, Goce Delcev University, North Macedonia. He holds a PhD in Sociology and a master's degree in psychology.

Before joining academia, he spent 15 years in the military security and intelligence service, including as Head of Analysis. His professional experience includes international deployments in Iraq and Afghanistan, as well as service with the OSCE Special Monitoring Mission to Ukraine.

His main areas of academic and professional interest include international security, hybrid threats and FIMI, cognitive resilience, strategic communication, Women, Peace and Security, and the human dimension of contemporary security challenges. He is actively involved in international defence and security cooperation, including activities within the NATO Science and Technology Organization (STO).

He is the author of two books and around 40 academic and professional publications in the fields of security, defence and the social sciences.

❖ ❖ ❖

PhD. Eng. Stelian TEODORESCU (Romania)

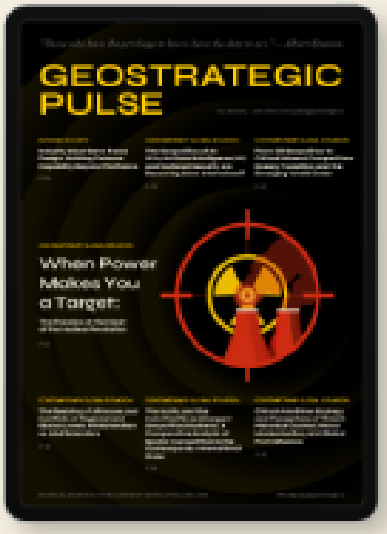
He is an aviation engineer and during his doctoral studies he was admitted to the SmartSPODAS Project - "Transnational network for the integrated management of smart doctoral and postdoctoral research in the fields of "Military Sciences", "Security and Information" and "Public Order and National Security" - Continuous training program for elite researchers - "SmartSPODAS", in this context participating in various research activities, among them being those organized by CRISMART in Sweden. During the first part of his career, he performed various executive within the Air Force Staff, and in the second part of his career, he was an executive and leadership positions within the Ministry of National Defence. He participated in various cooperation activities at the national and international level, gaining professional experience in the field of international relations and geopolitics. He carried out teaching activities in the academic environment (undergraduate and postgraduate studies).

❖ ❖ ❖

GEOSTRATEGIC PULSE

EDITORS

Pompilia VLĂDESCU
Stelian TEODORESCU



Starting from December 2010, Geostrategic Pulse has been registered in the international catalogue Index Copernicus Journal Master List.

SCAN IN ORDER TO ACCESS:

pulsulgeostrategic.ro

ISSN: 1843-701X FOUNDED IN 2017 | BUCHAREST

office@pulsulgeostrategic.ro