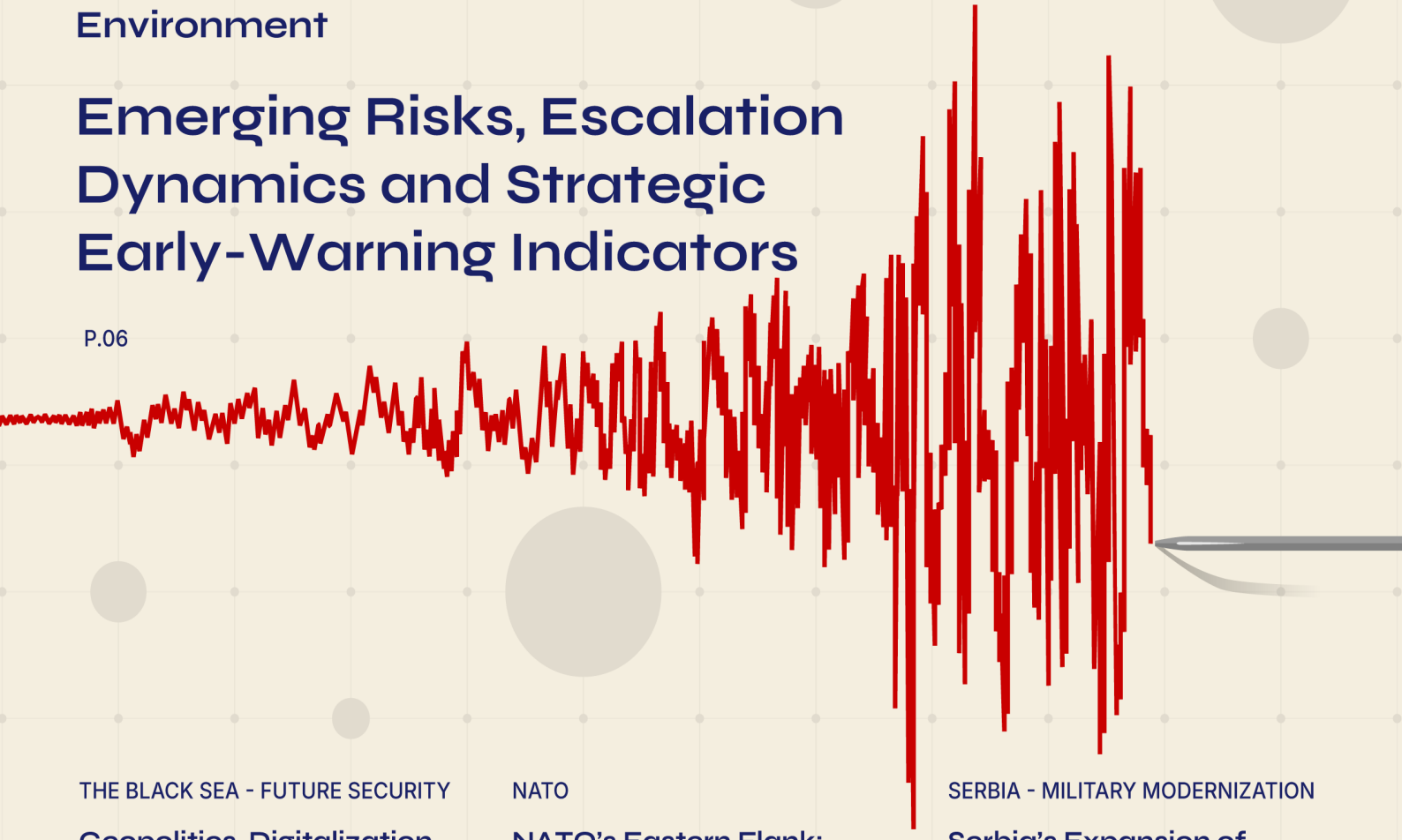
"Those who have the privilege to know, have the duty to act." — Albert Einstein

GEOSTRATEGIC PULSE

No. 307 March - April 2026 | www.pulsulgeostrategic.ro

Hybrid Competition in a Multipolar Environment

Emerging Risks, Escalation Dynamics and Strategic Early-Warning Indicators



BILINGUAL-BIMONTHLY PUBLICATION OF GEOPOLITICAL ANALYSIS

office@pulsulgeostrategic.ro

CONTENT

CONTENT

EDITORIAL

Minilateralism vs. Multilateralism – a Key Challenge for the New International Order

PhD. Eng. Stelian TEODORESCU (Romania)

As of 2026, the global diplomatic landscape is defined by a hybrid model in which minilateralism acts as an agile tool specific to the problems facing the world today, while multilateralism remains essential for universal legitimacy and long-term norms. Today's world shows increasing signs of moving rapidly towards a model of international relations characterized by minilateralism – small, flexible, and informal groups of nations collaborating on the platform of specific common interests, and relying less and less exclusively on large, universal, and often blocked multilateral institutions (such as the United Nations, the World Health Organization, or the World Trade Organization).

Source: https://www.britainsworld.org.uk/p/the-big-ask-03-2024

This emphasis on minilateralism is perceived and labeled as a key trend that will shape the global order in 2026 and beyond, designed to bypass bureaucratic inertia to address pressing security, defense, technological, and economic challenges. We can call 2026 the entry into the *"golden age of minilateralism"* which is characterized by small groups of like-minded nations advancing rapidly in technology, security, defense, and supply chains, while traditional multilateral institutions face bottlenecks, leading to a shift toward "trust blocs".

Prominent examples of minilateralism include:

• QUAD (US, Japan, Australia, India): Focused on maintaining a free and open Indo-Pacific and addressing regional security challenges.

• Group of Seven (G7): An international forum of governments of economically, technologically and militarily advanced countries (Canada, France, Germany, Italy, Japan, the United Kingdom of Great Britain and Northern Ireland and the United States).

• AUKUS (Australia, Britain, USA): A trilateral pact for technology transfer, particularly in the area of nuclear-powered submarines.

• I2U2 (India, Israel, United Arab Emirates, USA): Focused on regional economic, technology and energy cooperation.

• Japan-Philippines Defence Pact: A growing network of security partnerships in Asia, designed to strengthen maritime security.

• UAE-India-France Trilateral: A partnership encompassing defence, energy and technology cooperation.

• CRINK is a new acronym used by Western analysts and officials (starting around 2023-2024) to describe an informal but increasingly close alliance of four states: China, Russia, Iran, and North Korea.

Most experts do not see minilateralism as a complete replacement for multilateralism, but rather as a hybrid, complementary model. While minilateralism solves immediate problems, it cannot replace the global legitimacy, rules-based framework, and universality of traditional institutions like the UN.

The World Economic Forum's 2026 Global Risks Report warns of a *"global governance vacuum"* as knowledge and understanding of the weakening of multilateralism accumulate. In this world of profound uncertainty, global cooperation is finding other ways to evolve. Former World Economic Forum President and CEO Børge Brende[1] said: *"A new competitive order is taking shape as great powers seek to secure their spheres of influence. In this changing landscape, where cooperation looks significantly different than it did yesterday, collaborative approaches and a spirit of dialogue remain essential."* Such a model of collaboration is gaining ground, according to the latest Global Cooperation Barometer, an annual assessment of global collaboration. Smaller, more flexible groups of nations are working together to address specific common challenges. This approach – minilateralism – is reshaping the way countries collaborate, as cooperation finds new avenues. As Happymon Jacob, founder and director of the Council for Strategic and Defense Research, told the media in Davos: *"Some states in certain regions are coming together and talking about connectivity. They're talking about climate change. So even if multilateralism is failing… minilateralism is on the rise."*

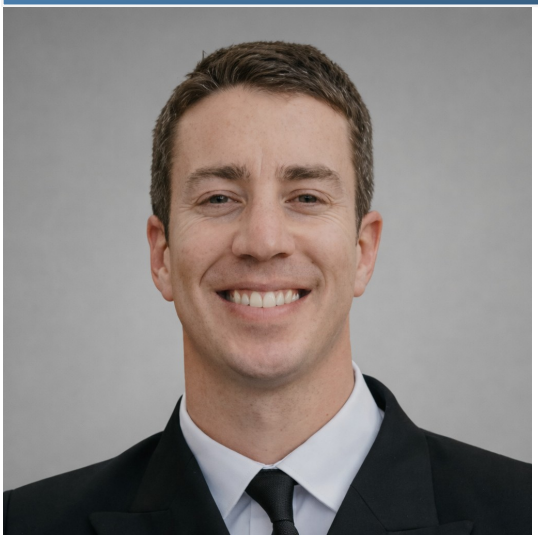
The crucial distinction is the emphasis: *minilateralism prioritizes common interests over shared values or ideology, allowing nations with different worldviews to cooperate pragmatically on specific and common issues.* As H. Jacob explains: *"You may not like a particular country… but you go sit down with that country… and you talk about the common good. There is that positive… proactive approach to the international world."* The I2U2 partnership between India, Israel, the United Arab Emirates, and the United States held its first leaders' summit less than a year after its formation, in 2022. Smaller groups bypass bureaucracy and political gridlock, allowing countries to act quickly on urgent challenges. However, minilateralism does not come without risks. The proliferation of coalitions could fragment and disrupt the international order, creating conflicting agreements that undermine universal institutions. If we sit down and think very carefully, we can conclude that minilateralism cannot replace multilateralism for all global challenges, and for some risks (such as weapons or biological, chemical or nuclear threats or even hazard) they are considered more effective in stimulating action. The latest report on global risks also suggests that the two are not mutually exclusive: *"It is essential that stakeholders from the public, private and civil society sectors continue to work together to support existing multilateral institutions wherever possible."*

Europe is experiencing a "minilateral" revolution, as its leaders come together with trusted neighbours and partners across the continent to build defence and security relationships. This political shift is driven by the dual challenge of growing threats, particularly from Russia, and the surprising stance taken by the Trump administration, which together have created an environment conducive to putting European leaders in a difficult decision-making position to seek new ways of shaping leadership for the whole of Europe. On 18 November 2025, British Prime Minister Starmer went to Berlin for a dinner with his German and French counterparts in the E3 format, a group originally created to represent Europe in the nuclear negotiations with Iran. The leaders expressed their support for collaboration in the field of foreign and security policy and highlighted cooperation with Poland and Italy, in such a context, the E5 group was formed - a group that had been established in early 2025 to bring together the largest defense actors on the European continent. The challenge of responding to the new international security and defense environment has highlighted the structural weakness of Europe's security architecture - in particular its dependence on the US. As uncertainty about the US commitment to Europe grows, the foundation of Europe's multilateral order is fracturing, and consensus-based multilateral formats are in an extremely difficult situation to respond to any risks and threats. Europe's response to the growing uncertainty is to increase its efforts to create a European pillar based on the production of the defense and security capabilities needed in the event of a US withdrawal from the continent. The EU is in the process of adapting to new geopolitical and geo-economic realities, and it is imperative to drastically reduce or even eliminate the inabilities to respond effectively to key challenges, due to the slow and cumbersome decision-making process, as well as due to the diverse perceptions of threats and security interests that have emerged among member states.

---

[1]Børge Brende, the former president and CEO of the World Economic Forum (WEF), announced his resignation in February 2026, following an internal investigation into his ties to Jeffrey Epstein. The decision came after revelations of meetings and exchanges of messages between Brende and Epstein. B. Brende had led the WEF since 2017 and was previously Norway's minister of foreign affairs, trade and the environment. Swiss Alois Zwinggi was appointed to take over.

MULTIPOLARISM AND HYBRID COMPETITION



Hybrid Competition in a Multipolar Environment: Emerging Risks, Escalation Dynamics and Strategic Early-Warning Indicators

Matías González POMMERENKE (Chile)

Introduction

Hybrid competition has consolidated itself as one of the most persistent and complex forms of contemporary strategic rivalry. Unlike conventional confrontation, it does not necessarily unfold through the direct and visible use of military force, but rather through the combination of political, economic, informational, cyber, technological, and, in certain contexts, limited military instruments. Its logic is to influence, wear down, disorganize, or constrain the adversary without unequivocally crossing the threshold of open conflict. In this sense, hybrid warfare and gray-zone activities should not be understood as anomalies of the international system, but as characteristic expressions of an environment in which ambiguity, plausible deniability, and gradual coercion offer advantages against superior adversaries or against response systems that are slow and normatively constrained (Cullen & Reichborn-Kjennerud, 2017; Rühle & Roberts, 2021).

The discussion becomes especially relevant in the current transition toward an increasingly multipolar international order. The diffusion of power, the emergence of new centers of decision-making, the fragmentation of normative consensus, and the relative erosion of global governance mechanisms do not imply

The appearance of "little green men" (irregular armed forces) in Crimea, Ukraine, ahead of its illegal annexation by Russia in March 2014, illustrates one type of hybrid threat. Other hybrid threats can be invisible. © Meduza

Figure 1. "Little green men" in Crimea as a visual illustration of a hybrid threat. Source: Rühle and Roberts (2021), NATO Review, photograph © Meduza.

the immediate collapse of order, but they do alter its operating conditions. In a system that is less hierarchical, more interdependent, and more contested, competition tends to manifest itself in multidomain and sub-threshold ways, favoring tools that make it possible to produce strategic effects without initially assuming the political and military costs of open war (Hersman, 2020; Kissinger, 2016).

The purpose of this article is to examine, from a strategic analysis and foresight perspective, how hybrid competition is changing in a multipolar environment, what its emerging risks are, and how escalation dynamics and strategic early-warning indicators may be identified. Rather than offering an exhaustive inventory of threats, it proposes an interpretive framework useful for decision-makers in defense, security, and intelligence.

Multipolarity and the Changing Strategic Environment

Contemporary multipolarity should be understood not only as a material redistribution of power, but also as a transformation of the political and normative architecture of the international system. The order that emerged from the global expansion of Westphalian principles and their subsequent liberal reformulation no longer operates on the basis of a sufficiently homogeneous consensus regarding the legitimacy of rules, the limits of sovereignty, or the effective authority of international institutions. Kissinger warned that the central problem of the contemporary world order lies not only in the presence of multiple centers of power, but also in the absence of a shared definition of the system itself, its rules, and the responsibilities required to sustain it (Kissinger, 2016). Where power and legitimacy cease to converge in a relatively stable manner, competition tends to shift toward more ambiguous and less regulated forms.

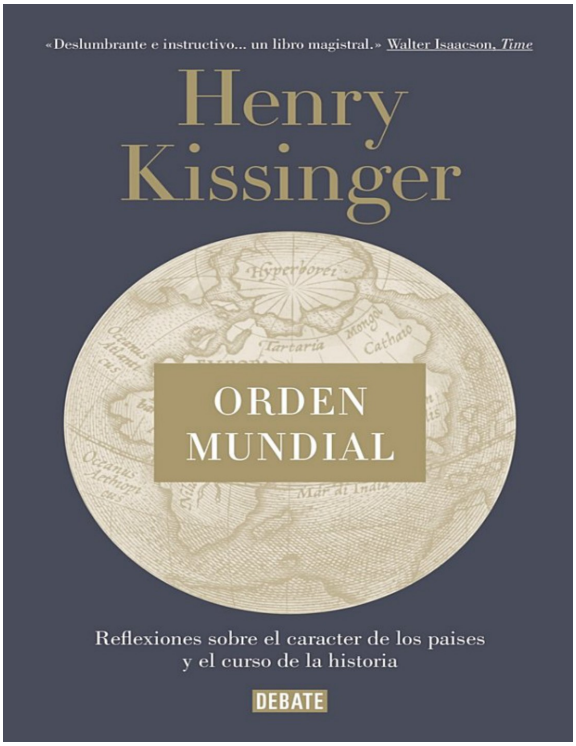


Figure 2. "World Order: Reflections on the Character of Nations and the Course of History." Source: Kissinger (2016), Debate.

This point is essential for understanding the rise of hybrid competition. In a system with several relevant powers, revisionist incentives, regional asymmetries, and different imaginaries of order, indirect coercion becomes especially attractive. Not all actors wish to, or can, resort to high-intensity conventional confrontation, but they may still seek to alter the strategic environment through influence campaigns, economic pressure, cyber operations, the instrumentalization of critical dependencies, the use of proxies, or the exploitation of internal tensions in third states. The multiplication of power poles therefore expands both the number of friction scenarios and the variety of tools used to manage them (Hersman, 2020; Martín González y Santiago, 2026).

Likewise, current multipolarity does not mechanically reproduce the classic patterns of the nineteenth-century European balance of power. It operates in an environment characterized by financial interdependence, digital connectivity, shared technological vulnerabilities, and the simultaneous presence of state and

non-state actors capable of producing strategic effects. Consequently, conflict is no longer expressed exclusively in terms of war and peace, but rather in an intermediate zone where coercive actions of low visibility, high political return, and uncertain attribution proliferate. It has been argued precisely that the expansion of hybrid warfare and gray-zone activities has shifted confrontation toward non-military domains aimed at influencing political will, social cohesion, and the decision-making capacity of states (Vendrell Martínez, 2026).

In this framework, multipolarity tends to reinforce four characteristics of the strategic environment: fragmentation of international authority, overlap among domains, acceleration of decision time, and expansion of the coercive repertoire. Hybrid competition finds especially fertile ground here because it allows for the gradual revision of the status quo, the testing of red lines, the saturation of the adversary's response capacity, and the exploitation of gaps between attribution, decision, and action.

The Evolution of Hybrid Competition

The literature on hybrid warfare has for years shown considerable conceptual dispersion. Part of the debate has focused on whether it is truly a new phenomenon or rather a contemporary reformulation of historical practices of irregular warfare, subversion, and limited coercion. Beyond terminological controversy, however, a growing consensus exists around certain functional characteristics. Hybrid warfare has been defined as the synchronized use of multiple instruments of power, tailored to specific vulnerabilities across the full spectrum of societal functions, in order to achieve synergistic effects (Cullen & Reichborn-Kjennerud, 2017). This formulation is particularly useful because it shifts attention from a simple inventory of means to the combinatory logic of action.

The evolution of hybrid competition may be summarized in four main transformations. The first is the shift from isolated actions to campaigns of cumulative pressure. It is no longer merely a matter of discrete episodes of disinformation, sabotage, or proxy use, but rather of sustained sequences of activities intended to progressively degrade the target's decision-making capacity, institutional resilience, and public confidence. It has been emphasized that hybrid warfare does not necessarily follow linear phases; it may evolve through simultaneous escalation and de-escalation across different planes, producing cumulative and non-linear effects (Cullen & Reichborn-Kjennerud, 2017).

The second transformation is the shift from an approach centered on capabilities to one centered on vulnerabilities. For this reason, contemporary emphasis lies on the relationship between instruments of power, pre-existing vulnerabilities, and desired effects. What matters is not only what the aggressor possesses, but how it synchronizes its means to affect the adversary's critical sectors, often without being clearly perceived at first.

The third transformation is the growing centrality of informational, cyber, and cognitive components. It has been observed that today the hybrid combination of military and non-military instruments introduces ambiguities that hinder situational awareness and, consequently, consensual and timely decision-making. Similarly, Hersman warns that digital influence tools, disinformation campaigns, and new means of operating through virtual proxies expand the strategic reach of sub-conventional coercion (Rühle & Roberts, 2021; Hersman, 2020).

The fourth transformation is the persistence of the proxy dimension in contemporary competition. Although public debate tends to associate "the hybrid" primarily with cyber attacks and disinformation, indirect support to third-party actors, militias, armed groups, criminal networks, or aligned political structures remains a relevant component. Harmon reminds us that violence by proxy is a recurrent feature of international relations, especially when sponsors seek to limit confrontation, preserve plausible deniability, or avoid direct retaliation (Harmon, 2023). From this perspective, hybrid competition is not simply a type of warfare, but a mode of strategic action designed to exploit the indeterminacy of the contemporary environment.

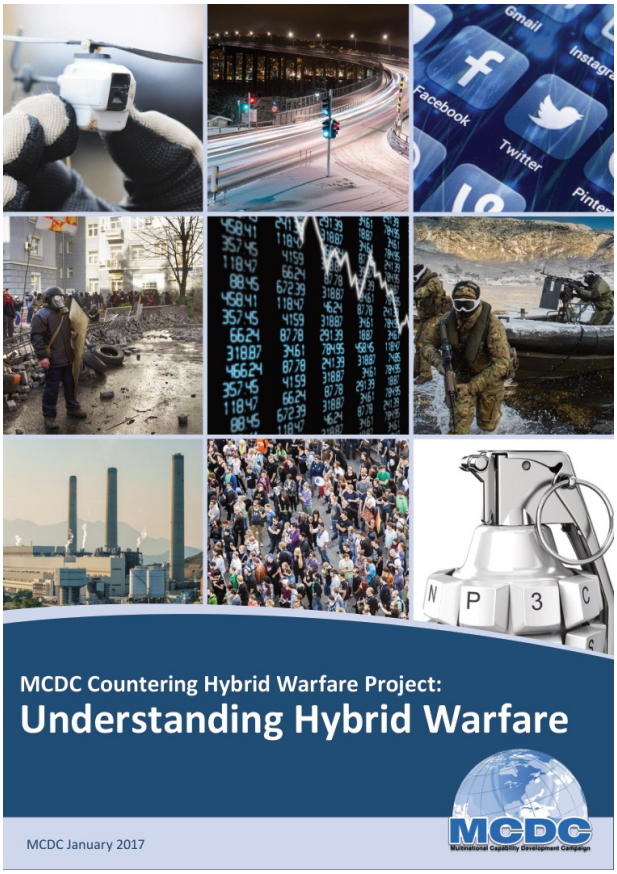


Figure 3. Cover of the report Understanding Hybrid Warfare.
Source: Cullen and Reichborn-Kjennerud (2017), Multinational Capability Development Campaign.

Emerging Risks and Escalation Dynamics

If multipolarity expands the incentives for hybrid competition, its main practical consequence is the emergence of new escalation risks. The problem no longer lies only in manifest hostility, but in the difficulty of distinguishing between dispersed incidents, sustained campaigns, and genuine strategic inflection points. Hybrid actions often operate through limited doses of coercion, adaptive adjustments, and combinations of means that, when viewed separately, may seem manageable or even routine. Yet their convergence may produce major effects on political cohesion, public perception, institutional stability, or deterrence credibility.

A first emerging risk is the normalization of the gray zone. When state and non-state actors discover that they can gain advantages through sub-threshold activities without suffering a proportional response, such practices tend to be repeated. The consequence is not necessarily an immediate major crisis, but rather a progressive erosion of the threshold of tolerance and of the political cost associated with behaviors previously regarded as exceptional. It has been pointed out that hybrid threats develop precisely in that "gray zone" where attribution is slower, collective response more difficult, and decision-making more vulnerable to ambiguity (Rühle & Roberts, 2021).

A second risk is the fragmentation of attribution. In contemporary hybrid competition, authorship may be diluted through proxies, technical outsourcing, layered operations, or manipulation of the information environment. The difficulty is not only evidentiary; it is also political. The more ambiguous the origin of an attack or campaign, the greater the likelihood of internal disagreement among allies, agencies, or national actors regarding the nature of the threat and the legitimacy of the response. Part of the effectiveness of hybrid action lies precisely in remaining below certain thresholds of detection and response, thereby obstructing the target's decision-making process (Cullen & Reichborn-Kjennerud, 2017).

A third risk relates to convergence across domains. Escalation should no longer be understood exclusively as a vertical movement from low levels of violence toward open war. Hersman proposes the idea of "wormhole escalation" to describe non-linear pathways through which sub-conventional competition may suddenly connect with higher strategic levels, bypassing the intermediate rungs assumed by classical models (Hersman, 2020). The combination of influence campaigns, cyber operations, economic pressure, and attacks against critical infrastructure may produce disproportionate strategic effects without passing

through an easily recognizable conventional military sequence.

A fourth risk is deterrence fatigue. Prolonged crises, the saturation of micro-incidents, and the repetition of ambiguous actions may degrade the credibility of red lines. When decision-makers are forced to manage minor incidents permanently, the ability to distinguish signal from noise diminishes, and the danger increases of becoming habituated to pressure that, cumulatively, alters the strategic balance. In such a scenario, repeated inaction may prove as dangerous as overreaction (Martín González y Santiago, 2026).

A fifth risk is the compression of strategic time. Digital technologies, permanent connectivity, and instant public exposure reduce the window for analysis and institutional coordination. This is particularly serious when hybrid competition affects electoral processes, financial systems, energy grids, or emergency infrastructures, that is, sectors where the political pressure to act is high, but initial information is often incomplete (Hersman, 2020; Pérez Franco, 2025).

A central idea follows from this: hybrid escalation is frequently cumulative and contextual. It does not usually present itself as a single decisive event, but as a combination of weak signals, exploited vulnerabilities, insufficient responses, and mutually reinforcing effects. For that reason, the challenge for strategic analysis is not merely to register events, but to interpret patterns.

Strategic Early-Warning Indicators

If one of the most dangerous traits of hybrid competition is its capacity to generate cumulative effects before being fully recognized, then the construction of strategic early-warning indicators becomes an analytical priority. It has been emphasized that responding adequately to hybrid warfare requires the identification of critical functions, the establishment of thresholds, the construction of baselines of normality, and the development of indicators capable of recognizing when a hybrid action or effect is taking place (Cullen & Reichborn-Kjennerud, 2017). This approach is particularly valuable because it prevents early warning from being reduced to the mere detection of obvious threats.

From a strategic perspective, early-warning indicators should be organized into at least five interrelated categories.

The first category is political-institutional. Here the aim is to observe signals of exploitable polarization, deterioration of strategic consensus, blockage of critical decisions, persistent disputes over threat attribution, or erosion of confidence in authorities and institutions. A divided institutional environment offers the hybrid actor a privileged opportunity to amplify tensions and delay responses.

The second category is informational and cognitive. Contemporary hybrid competition exploits the speed of narrative circulation, audience segmentation, and the vulnerability of information ecosystems. Relevant indicators include the coordinated emergence of divisive narratives on sensitive issues, the artificial amplification of content, synchronization between digital campaigns and critical political moments, and the growing disconnect between verifiable facts and dominant perceptions. In this domain, the analytical key lies in detecting patterns of convergence and opportunity rather than in the isolated content of each message (Rühle & Roberts, 2021; Hersman, 2020).

The third category is cyber and technological. Indicators here include an increase in intrusions against critical systems, reconnaissance activities against sensitive networks, campaigns targeting service infrastructures, disruptions in logistics or communications systems, and the combination of cyber operations with political or informational pressure. Cyberattacks are among the most frequently used instruments in hybrid campaigns, precisely because they may be operated by states, proxies, or private organizations, with high scalability and persistent attribution difficulties (Rühle & Roberts, 2021).

The fourth category is economic and critical infrastructure-related. Relevant indicators include selective restrictions on supply chains, signs of pressure on energy or financial sectors, opaque acquisitions in sensitive areas, anomalous fluctuations linked to political decisions, and sabotage or disruption events with potential plausible deniability. In a multipolar environment, where interdependence can be used as a tool of pressure, the economy ceases to be merely contextual and becomes a direct vector of coercion (Blackwill & Harris, 2016; Pérez Franco, 2025).

The fifth category is military and gray-zone related. Analysts should monitor unusual exercises near sensitive areas, ambiguous presence deployments, increased patrol activity combined with informational pressure, greater activity by intermediary actors, and changes in the employment patterns of dual-use capabilities. The importance of these indicators lies not only in their material dimension, but in their interaction with other signals.

Yet the usefulness of indicators does not depend on their mere enumeration. What is decisive is the capacity to integrate them into a system of persistent monitoring, capable of comparing signals against previously defined baselines and of interpreting thresholds not only sectorial, but systemical. It has also been stressed that without a clear notion of what is normal, it is difficult to "see" ambiguous actions that may form part of a hybrid attack (Cullen & Reichborn-Kjennerud, 2017). Early warning therefore requires continuity, integration, and contextualization. From the standpoint of strategic foresight, its purpose is not

to predict the future, but to reduce strategic surprise, improve reaction time, and enable more calibrated decisions.

Implications for Strategic Decision-Making

The implications for strategic decision-making are profound. First, hybrid competition requires abandoning the idea that security, defense, intelligence, economy, and public communication can continue to be managed as separate compartments. If the aggressor synchronizes instruments, the response must also be integrated. This implies interagency approaches, mechanisms for continuous information-sharing, and an institutional culture oriented not only toward reacting, but also toward interpreting trends, connecting signals, and assessing systemic risks (Cullen & Reichborn-Kjennerud, 2017).

Second, decision-making requires greater speed, but not at the cost of losing strategic judgment. The central problem is no longer only bureaucratic slowness, but the difficulty of deciding under persistent ambiguity. At this point deterrence remains relevant, but it must be adapted. Pérez Franco reminds us that deterrence consists, essentially, in influencing the adversary's cost-benefit calculation and decision-making process (Pérez Franco, 2025). In the hybrid sphere, this means raising costs not only through military means, but also through societal resilience, infrastructure protection, public exposure of hostile campaigns, attribution capacity, and calibrated multidomain responses.

Third, resilience ceases to be a complementary notion and becomes a central component of strategy. The need to strengthen resilience, cyber defense, and situational awareness as conditions of effectiveness against hybrid threats has been repeatedly stressed (Rühle & Roberts, 2021). A resilient society is not one that is immune to attack, but one capable of absorbing impact, sustaining essential functions, limiting the spread of damage, and preserving enough cohesion to decide under pressure. In a multipolar and technologically dense environment, resilience becomes a form of deterrence by denial.

Fourth, strategic decision-making must better incorporate the foresight dimension. This means going beyond reactive analysis of consolidated threats in order to work with scenarios, indicators, and plausible trajectories. It is not about predicting the future, but about identifying combinations of change that may alter the environment. Hybrid competition, precisely because of its incremental nature, demands anticipation based on weak signals and emerging patterns.

Finally, strategic decision-making in this field requires clarity regarding priorities and proportionality. Not every hybrid pressure deserves the same response; not every signal justifies political escalation; not every crisis should translate into militarization. But the absence of criteria also benefits the aggressor. A state or alliance that has not thought in advance about how to classify, prioritize, and respond to subthreshold activities will always arrive late.

Conclusion

Hybrid competition has become a central modality of contemporary strategic rivalry because it responds effectively to the conditions of a more fragmented, interdependent, and contested international environment. Multipolarity does not automatically produce this form of confrontation, but it does expand its utility by multiplying actors, centers of power, zones of friction, and disagreements regarding the legitimacy of order. In this context, gradual coercion, operational ambiguity, plausible deniability, and the synchronization of means offer clear advantages for those who seek to modify balances without initially assuming the costs of open war.

This article presents three main conclusions. The first is that hybrid competition should no longer be understood as a dispersed sum of tactics, but as a form of strategic action that combines vulnerabilities, instruments, and effects in an adaptive and contextual manner. The second is that the main risk of this modality lies not only in each isolated incident, but also in its capacity to generate cumulative, non-linear, and sometimes unexpected escalations. The third is that the best response does not depend exclusively on more material capabilities, but also on better integration among strategic analysis, resilience, deterrence, and early warning.

The most important challenge for decision-makers, therefore, is not only to respond to consolidated hybrid threats, but also to build the capacity to recognize gradual changes before they become larger-scale crises. In a multipolar environment, strategic advantage will increasingly depend on the ability to interpret signals, connect domains, and make decisions under uncertainty without surrendering the initiative.

Bibliography:

- Kissinger, H. (2016). World order: Reflections on the character of nations and the course of history. Debate.
- Harmon, C. C. (2023). Warfare in peacetime: Proxies and state powers. Marine Corps University Press.
- Hersman, R. (2020, July 9). Wormhole escalation in the new nuclear age. Texas National Security Review.
- Cullen, P. J., & Reichborn-Kjennerud, E. (2017). Understanding hybrid warfare. Multinational Capability Development Campaign.
- McCulloh, T., & Johnson, R. (2013). Hybrid warfare. Joint Special Operations University Press.
- Rühle, M., & Roberts, C. (2021, March 19). Enlarging NATO's toolbox to counter hybrid threats. NATO Review.
- Vendrell Martínez, M. (2026, March 26). The relevance of Clausewitz in European hybrid warfare: Challenges for the European Union in a conflict without war.
- Pérez Franco, M. Á. (2025). Smart deterrence to prevent twenty-first century conflicts. Spanish Institute for Strategic Studies.
- Blackwill, R. D., & Harris, J. M. (2016). War by other means: Geoeconomics and statecraft. Harvard University Press.
- Martín González y Santiago. (2026). 2026–2027: A world on the edge. Multipolarity, hybrid warfare, and the possible collapse of world order. Revista Digital Delta 13 News.

HUMAN MINDS VS. ARTIFICIAL INTELLIGENCE

The Human Mind as Battlespace – Artificial Intelligence, Cognitive Warfare and the Strategic Fragility of the West

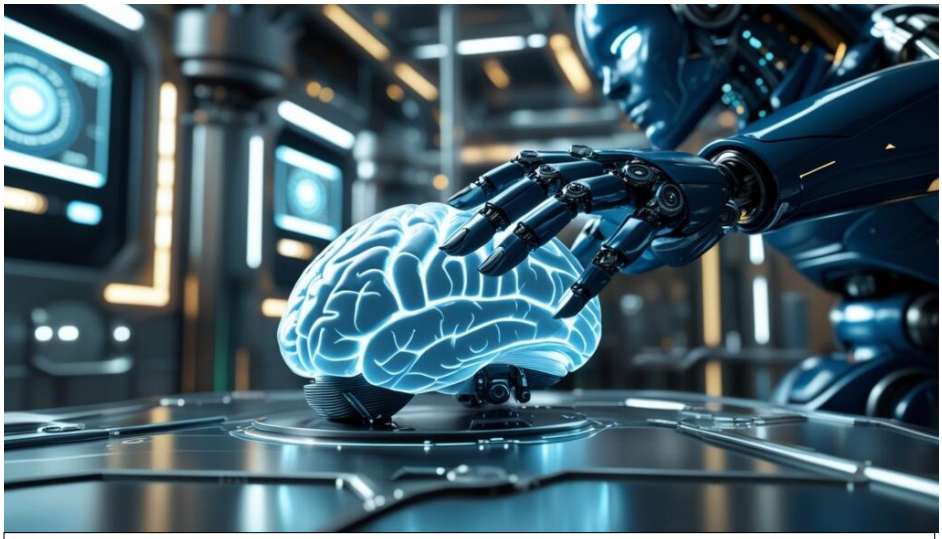
Bernd Oliver BUHLER (Germany)

How We're Losing the Most Important Battle Without Even Noticing

1. The Battlefield Has Shifted—and We're Standing Here Naked

For centuries, we measured security in concrete and steel: Borders, Armies, Power grids, Ports, Banks. Later, we added firewalls and digital networks. All of that still matters—*of course* it does. You can't ignore territory, logistics, or supply chains if you want to survive.

This is no longer where the war is won or lost. We pour billions into tanks, fighter jets, satellites, and high-tech cyber defenses. And yet, we've left the front door to our *own minds* wide open. **Not a metaphor,** not a hyperbole; a **massive, gaping strategic failure.**



Source: https://triilook.in/ai-and-the-mind-redefining-how-we-understand-ourselves/

The real battle is happening *right now* in the space where you and I decide what to believe, whom to trust, what to fear, and how to act. Hostile influence operations aren't just spreading fake news anymore—they're **actively breaking the way we process reality.** And once a society can no longer tell fact from fiction, thinking stops. The noise takes over. And a society drowning in noise? **Paralyzed.**

Even NATO's think tanks are scrambling to understand this under the term *cognitive warfare*—trying to grasp how adversaries use technology and psychology to screw with human decision-making. **Why does this matter so damn much?** Because decisions on sanctions, military responses, or energy policies don't happen in a vacuum. They happen based on what people *believe* is true. This isn't just another cyberattack. A hacked server? You isolate it. A blown-up bridge? You rebuild it. A messed-up supply chain? Painful, but you find new suppliers.

But broken trust?

That's where the lights go out for good. When a society stops trusting its own institutions, it becomes

impossible to govern, impossible to defend, and *incredibly easy* to exhaust. If an attacker can shatter our shared perception, wear down our attention spans, and make us doubt *everything*, they win **without firing a single shot.** They don't even need to convince you of their lies. They just need to confuse you enough until you **give up and do nothing.**

This is why the human mind is the new battlespace. **Not because we're stupid or helpless.** And not because AI can magically "control" human thoughts—that's science fiction. The reality is far more practical: **the very systems we use to make up our minds —-independent news, expert authority, open debate, personal conversations—are being systematically sabotaged.**

Look at the 2023 Slovak parliamentary election. A deepfake audio recording went viral right before the vote, falsely making it sound like the leader of Progressive Slovakia and a journalist were discussing election rigging. Fact-checkers debunked it—but by then, it was too late.

The real damage wasn't the lie itself. **It was the timing.** Deception moved at lightspeed. Verification crawled behind it. Suspicion outlasted the correction. **That wasn't a one-off.** That was a test run.

Here's the ugly truth: In cognitive warfare, no one needs to blow up your power grid. **They just need to destroy your faith in the people who explain the news, check the facts, and coordinate a response.** You can have functioning markets, open roads, and formal elections—and still be completely defenseless because *no one believes the signals anymore.*

We're not just vulnerable because our systems get hacked. **We're vulnerable because our judgment is being shattered.** Borders and firewalls don't protect sovereignty anymore. **The integrity of our public judgment does.** And right now? **That integrity is buckling under the pressure.**

Let's be brutally clear: **AI didn't invent this.** Propaganda and psychological operations are older than the internet. But AI changed *everything* about the scale, the speed, and the cost of the attack. It turned manipulation from a handcrafted art into a **brutal, industrialized weapon.**

Imagine you're a carpenter. For decades, you've built furniture by hand—slow, meticulous, with care. Then suddenly, someone shows up with a **factory** that can produce a thousand chairs in the time it takes you to build one—cheaper, faster, and more convincing than anything you've ever seen. **Welcome to the lie factory.**

2. The Lie Factory: How AI Turned Propaganda Into a Precision Weapon

Propaganda didn't start with AI. **But AI turned propaganda into something else entirely — something faster, cheaper, and far more dangerous than we've ever seen before.**

Remember the old days? Back when disinformation was still a craft, not an industry. You wanted to spread a lie, you needed bodies in a room: analysts poring over demographics, writers sweating over the perfect turn of phrase, translators wrestling with cultural nuances, designers making sure the forgery didn't look like a forgery, and a whole network of human couriers to get it into the right hands. It took time. It took money. Most of all, it took *people*—actual, fallible, exhausted people who eventually had to sleep, or eat, or at least take a bathroom break.

Now? Some guy in a dimly lit apartment with a laptop and a subscription to the right AI tools can do all of that before lunch. No breaks. No budget meetings. No human error— just the cold, relentless efficiency of a machine that doesn't care if it's telling the truth or not. The old propaganda was a handmade bomb. This? **This is a factory.** And it's running 24/7.

Text, images, audio, video—**synthetic personas, localized narratives, cloned voices, fabricated experts**—all produced at near-zero cost. The same basic lie can be rewritten a hundred different ways, each one tailored to a specific fear, a specific prejudice, a specific political culture. **A message doesn't need to convince everyone anymore. It just needs to find the right cracks in the right people.**

And here's the thing we don't like to admit: **We're not rational machines.** We don't process information like computers. We react with fear, with identity, with loyalty, with anger, with exhaustion, with trust, with confirmation bias. **We're human. And that makes us vulnerable.**

AI doesn't just spread lies—**it personalizes them.** It adapts them. It tests which version of a lie spreads fastest, which one provokes the most anger, which one generates the deepest distrust. **It doesn't need to convince you. It just needs to confuse you enough to make you doubt everything.**

We're already seeing it happen. Synthetic media doesn't just spread lies—it *invents* the liars, complete with faces that never existed and voices that never spoke. A public figure's words can be fabricated so convincingly that even their own staff might hesitate before denying it. AI doesn't just create fake experts; it populates entire fake communities, where bots mimic real people so well that the line between human and machine blurs into irrelevance. And the most insidious part? The system doesn't just throw lies at the wall to see what sticks—it *learns* which lies stick best, then refines them, amplifies them,

and fires them back at us with surgical precision.

And the scariest part? **It doesn't even need to be that good.** Most AI-generated propaganda isn't perfect. Some of it's crude. Some of it's obvious. **But it doesn't need to be perfect. It just needs to be fast. It just needs to be cheap. It just needs to keep coming.** Because here's the brutal truth: **The attacker only needs to generate plausibility. The defender has to verify reality.**

And verification? **It's slow. It's institutional. It depends on trust.** We're already seeing the effects. Graphika documented AI-generated video personas in a pro-Chinese influence operation. **The videos weren't that convincing.** But they didn't need to be. They just needed to be *cheap enough* to produce, *fast enough* to spread, and *plausible enough* to
make people pause.

Meta described Spamouflage—one of the largest known influence operations—as a **cross-platform, multi-language, AI-powered machine** that targeted over fifty countries. **The lesson isn't that every campaign works.** The lesson is that **the cost of trying has collapsed to almost nothing.**

And then there's Doppelgänger—where malicious actors **cloned real media brands**, created fake articles, and used social media to spread pro-Russian narratives. **They didn't need one big lie.** They just needed to borrow enough credibility to make people doubt the real thing.

That's the real danger. Not the obvious fake. The *almost* plausible one. The fake article that looks like it's from a real outlet. The synthetic voice that sounds just familiar enough. The manipulated clip that arrives at just the right emotional moment.

European security assessments are already calling this a **structural problem.** The European External Action Service warned that AI gives threat actors **low-cost, scalable tools** to manipulate information. **And they're right.**

Because here's the uncomfortable truth: **AI doesn't create deception. It industrializes it.** It makes it cheaper. It makes it faster. It makes it harder to trace. **Propaganda used to be a campaign. Now it's a factory.**

And for open societies, that creates a **whole new kind of defensive burden.** Institutions have to respond to falsehoods that spread faster than they can be investigated. Journalists have to verify content that *looks* real, *sounds* real, and *feels* real. **Citizens have to navigate an information environment where nothing can be trusted by default.**

AI didn't just change the game. **It changed the rules.** And right now, **we're losing.**

3. When Lies Move Markets: The Unholy Marriage of Cognitive and Economic Warfare

Trust is the invisible wire that holds the economy together. And right now, someone is cutting it. You think this is about fake news? **No.** This is about **fake reality**—and how it moves real money.

Markets don't run on facts. They run on **what people believe is true.** Investors don't act on reality—they act on *perceived risk, perceived stability, perceived legitimacy.* The same goes for governments. For consumers. For banks. For voters. **The moment trust cracks, the whole system starts to wobble.** And that's exactly what's happening.

One fake tweet about an explosion at the White House—and *boom*, the Dow Jones drops 150 points in minutes (2013). No war. No terror attack. Just a damn hack. A doctored image of an attack on the Pentagon? Markets stumble before anyone can even verify if it's real (2023). No missiles. No bombs. Just a damn JPEG. A hacked SEC account falsely announcing Bitcoin ETF approval? Prices spike—then crash the second the truth comes out (2024). No financial collapse. No banking crisis. Just a damn tweet.

This isn't a coincidence. This is the proof: **Markets don't react to the truth.** They react to what they *think* is the truth. And when the lie moves faster than the correction? **The lie wins. Every. Single. Time. None of these were sophisticated AI operations.** But they proved something terrifying: **Markets react faster than the truth can keep up.**

Now add AI to the mix. A fake CEO statement. A synthetic image of an attack. A manipulated recording of a central banker. A coordinated rumor about a bank's collapse. **All generated, amplified, and weaponized at a speed that leaves institutions gasping for air.**

This isn't just about stocks. It's about energy—where a fake shortage narrative can send prices soaring overnight. It's about elections, where a synthetic scandal can swing votes and, with them, entire policies. It's about public health, where a false safety claim can cripple exports and devastate industries. It's about crisis response, where a deepfake delay can cost lives. The target isn't just the soldier in the field. It's the investor making a split-second decision, the voter casting a ballot, the consumer choosing what to buy, the minister under pressure to act. And above all, it's that fleeting, critical moment of decision — when perception tips the scales before the truth even has a chance.

The target isn't just the soldier. It's the investor. The voter. The consumer. The minister. And most of all—the moment of decision. The damage isn't always a collapse. **It's the slow grind.**

The extra risk premiums. The delayed investments. The political energy wasted on damage control instead of action. **The friction that, over time, wears a society down to nothing.**

Because here's the thing: **In open economies, perception isn't separate from power. It *is* power.** And right now, **we're letting the enemy rewrite the rules.** Because a lie doesn't need to be believed forever to work. **It just needs to trigger a reaction before the truth can catch up. That's the game. And we're losing.**

4. The Open Society's Dilemma: Why Our Greatest Strength Is Being Weaponized Against Us

We love to say openness is our superpower. **And it is.** Free speech, pluralistic media, open markets, academic debate—these aren't just nice ideals. They're the reason we *win*. They let us correct, innovate, dissent, hold power to account. They create the space where trust can grow, even after it's been broken. But here's the nightmare: **The same openness that makes us strong is now the highway the enemy uses to drive straight into our brains.**

This isn't about freedom being weak. **Freedom is the whole damn point.** Authoritarian regimes look stable because they can shut down dissent with a flick of a switch. But that's not resilience—that's a **prison**. And every prisoner dreams of the door. No free society should ever forget that.

So no, the answer isn't to lock everything down. **The answer is to stop pretending openness defends itself.** Because here's the brutal truth: **We built a society where trust is distributed.** It's not just in one leader, one news outlet, one institution. It's spread across courts, journalists, universities, companies, neighbors, families. That's beautiful. That's *democracy*. But it's also **a thousand points of failure**. And the enemy doesn't need to hit them all. They just need to make us doubt *enough* of them.

And they're getting *really* good at it. Manipulation is fast, cheap, and scales like a virus. Verification? Slow. Institutional. **Needs trust to work.** By the time the truth catches up, the damage is done. The lie doesn't even need to be believed—it just needs to **make us pause**. To make us *hesitate*. To make us spend our energy arguing with each other instead of solving the problem.

And let's be honest—we're making it *easy* for them. Our public sphere runs on platforms that **profit from rage**. Outrage travels. Nuance doesn't. The neighbor you used to argue with over the fence? Now you only see them as an algorithmic caricature. **We're not just divided. We're** ***estranged*****.** And at this point, the enemy doesn't even need to invent the division. They just need to **turn up the volume.**

Pluralism was supposed to be our shield. But now it's **the terrain where the battle is fought**. Democratic debate needs disagreement—but cognitive warfare turns that disagreement into **fragmentation**. Transparency was supposed to protect us—but now it's **a map of our vulnerabilities**. Free markets need information—but false signals move faster than the truth ever can.

This isn't a moral failing. It's an architectural flaw. We built a house with a thousand open windows—and now we're surprised that the wind is howling through. And Europe? **Europe has a second problem: dependency.** Yes, we've got the GDPR, the Digital Services Act, the AI Act. **Great.** These are important. They set standards. They protect rights. But here's the thing: **Regulation isn't infrastructure.**

If the clouds, the platforms, the chips, the AI models that power our public life are controlled *somewhere else*—then our ability to defend our own cognitive space is **incomplete**. And no, this isn't about turning our backs on allies. The U.S. is still our most important partner. **But dependency is still dependency.**

A democracy that relies on foreign infrastructure to understand and protect its own public sphere **has outsourced part of its sovereignty.** And in a crisis, the question isn't just *does the tech work?* It's **who controls it? Who can shut it down? Who can audit it? Who's accountable when it fails?** Openness isn't the flaw. **Defending openness with tools we don't control—that's the flaw.**

So what's the answer? **Not censorship. Not retreat.** The path lies between naivety and authoritarianism: **defend openness with resilience.** Build the capacity to verify, to trace, to audit. Make our institutions credible again. And for God's sake, **build our own infrastructure.**

Because the vulnerability of open societies isn't their freedom. **It's the asymmetry.** The cost of attacking truth is now *almost zero*. The cost of defending it? **Still sky-high.** And if we don't fix that, **we're going to lose the very thing we're trying to protect.**

5. The AI Antidote: How We Fight Fire With Fire without Burning Down the House

Here's the first mistake we're making: **treating AI like it's only the problem.** It's not. It's also the *cure*—if we're smart enough to use it right. No, the answer to AI-powered cognitive warfare isn't to reject AI. **That's like refusing to use antibiotics because bacteria exist.** Open societies *need* AI to defend themselves—but only if it's **transparent, accountable, and under democratic control.** Otherwise, we're just trading one kind of vulnerability for another.

Think about it: The same tools that make AI so dangerous—its ability to detect patterns, analyze

narratives, spot fakes—can also be our **immune system**. AI can flag deepfakes before they go viral. It can track how lies spread across platforms and languages. It can help journalists and fact-checkers separate signal from noise. It can even protect official communication channels from being hijacked.

But—and this is *critical*—**technology alone won't save us.** We don't need a digital priesthood deciding what's true. We don't need a "Ministry of Truth" with fancier software. **We need systems that help *us*—citizens, journalists, institutions—understand where information comes from, how it's been tampered with, and who's pushing it.** Because here's the hard truth: **A democracy that outsources judgment to machines isn't a democracy anymore.**

Defensive AI shouldn't tell people *what* to think. It should show them *how* they're being manipulated. Where the lies are spreading. How they're being amplified. **Where verification is urgently needed.** So what does this immune system look like?

First, provenance. In a world where images, voices, and documents can be faked with a few keystrokes, we need **digital fingerprints**. Standards like the Coalition for Content Provenance and Authenticity (C2PA) are a start—they let us trace where content came from and how it's been altered. **Not perfect, but better than nothing.**

Second, detection. AI can spot deepfakes, synthetic audio, and coordinated bot networks faster than any human. It can flag unusual distribution patterns—the kind of thing that would take a team of analysts weeks to uncover.

Third, narrative mapping. Cognitive warfare doesn't rely on one big lie. It's **death by a thousand cuts**—repetition, variation, emotional triggers. AI can help us see how narratives move across platforms, languages, and communities. **Who's amplifying what? Who's being targeted? How is foreign manipulation interacting with domestic divisions?**

Fourth, institutional support. Journalists, fact-checkers, election authorities—they're on the front lines. AI can help them triage information, compare sources, detect inconsistencies, and communicate more clearly under pressure. **Not to replace human judgment, but to buy us time.**

And here's the fifth layer—the one we're still ignoring: **transparency of speakers.** In the cognitive domain, **anonymity is a weapon.** Citizens have a right to know if they're talking to a human, a bot, a foreign government, or a synthetic persona. **Democracy can handle disagreement. It can't handle a public square where nobody knows who's speaking.**

Europe's already moving in the right direction. The European Digital Media Observatory, the EU's Code of Practice on Disinformation, the AI Act—these are **building blocks**. But they're not enough. Because here's the catch: **The cure can become the disease.** A cognitive immune system that operates in secrecy? That's just **censorship with better branding.** One that isn't auditable? That's a **black box with power.** One that isn't democratically controlled? That's **protecting institutions from citizens, not the other way around.**

Defensive AI must **verify, not generate.** It must **expose manipulation, not optimize engagement.** It must **support human judgment, not replace it.** And it must be built on **explainability, contestability, and accountability.** The same goes for infrastructure. **An immune system can't run on black boxes.** If Europe uses AI to defend its public sphere, it better damn well know where that AI is hosted, what models it's using, what data it's processing, and who's legally responsible when it screws up.

AI *can* be part of the immune system of open societies. **But if it's not transparent, if it's not accountable, if it's not under democratic control—then it's just another vector for the disease.** So the question isn't *whether* AI should help defend democracy. **The question is: Who controls the AI that defends it? And can citizens still say no?**

And that brings us to the hard truth: **A cognitive immune system requires more than good intentions.** It requires **infrastructure.** Compute. Clouds. Models. Data governance. Standards. **Sovereign capacity. Digital sovereignty isn't a luxury. It's a necessity.** And if we don't build it, we're not just vulnerable. **We're complicit.**

6. The Sovereignty Trap: Europe's Dangerous Addiction to Foreign Tech

Here's the hard truth: **Europe is writing the rules for AI—but it's not building the infrastructure to enforce them.** We've got the GDPR. The Digital Services Act. The AI Act—one of the most ambitious legal frameworks for trustworthy AI in the world. **Great.** These matter. They set standards. They protect rights. But here's the catch: **A law can't train a model. A law can't operate a cloud. A law can't manufacture a chip.** And right now, **Europe is still dependent on others for all of that.** Mistral AI proves Europe can build world-class foundation models. Aleph Alpha shows we can develop AI that's explainable, sovereign, and tailored for public-sector use. EuroHPC gives us a framework for high-performance computing. AI Factories are popping up to give European industry, startups, and researchers access to the resources they need.

But it's not enough.

Because here's the ugly reality: **Most of Europe's cloud infrastructure, platform ecosystem, high-end compute supply chain, and AI development stack still runs on non-European providers.** And no, this isn't about turning our backs on allies. The U.S. is still our most important partner. **But dependency is still dependency.**

A continent that relies on foreign infrastructure to understand, protect, and govern its own public sphere **has outsourced part of its sovereignty.** And in a crisis, the question isn't just *does the tech work?* It's **who controls it? Who can shut it down? Who can audit it? Who's accountable when it fails?**

Mistral AI is a perfect example of the paradox. **European talent exists.** But the ecosystem to scale it? **Still incomplete.** Even our strongest players end up relying on non-European infrastructure for deployment. **That's not a criticism of Mistral. It's the point.**

Europe needs to distinguish between regulation, innovation, and sovereignty. Regulation sets the rules, innovation creates the tools, but sovereignty— sovereignty means the ability to operate critical systems under European control. And right now, that's the piece we're missing.

Eastern Europe isn't just the periphery—it's part of the solution. Latvia, Lithuania, Estonia, Poland, Romania, Czechia, Slovakia—they've got the technical talent, the competitive costs, the digital infrastructure, and **firsthand experience with hybrid threats.** Their proximity to Russian information operations gives them a strategic awareness that Western Europe ignores at its peril.

Look at Latvia. In 2025, it joined the European AI Factory Antennas network, creating a national competence center and connecting to the LUMI AI Factory consortium. **This is the model.** Not one central AI fortress, but a **network of capable nodes across the continent.**

Romania could be next. Southeastern and Eastern Europe can become **laboratories of European AI sovereignty**—if we combine talent, infrastructure, public-sector demand, and security awareness the right way. **Lower costs alone aren't a strategy.** But lower costs + technical skill + digital infrastructure + European integration + hybrid warfare awareness? **That's a strategic advantage.**

So the question isn't *can* Europe regulate AI. **We already can.** The question is: **Can Europe build, scale, and control the infrastructure that regulation presupposes?**

The answer isn't autarky. We don't need to cut ourselves off from allies, markets, or global tech ecosystems. **We need strategic redundancy.** Sovereign compute. Trusted cloud capacity. European foundation models. Secure data spaces. Open standards. Independent audit capability. **Public-sector demand strong enough to scale domestic providers.**

The goal isn't isolation. **The goal is the ability to keep operating when external conditions change.** Because here's the brutal truth: **Regulation without capacity is ambition without foundation.** And regulation without infrastructure isn't sovereignty—**it's the administration of dependency.**

If Europe succeeds, AI won't just be a risk to our sovereignty—**it'll be one of its strongest instruments.** If we fail? **We'll be rule-makers for systems we don't control.** But sovereignty alone isn't enough. **Infrastructure matters because it supports something deeper: trust.** And without trust, no AI system, no regulation, and no strategic capacity can hold open societies together under cognitive pressure.

7. Trust as Strategic Infrastructure

Trust is not a sentimental value. It is the operating system of open societies. This may sound abstract, but it is not. Without trust, markets cannot price risk, citizens cannot evaluate political choices, institutions cannot communicate effectively and governments cannot act in crisis. Trust is functional. It is the invisible infrastructure that allows complex societies to coordinate action under uncertainty. In the age of AI-enabled cognitive warfare, this infrastructure is under strategic attack.

If the battlefield has moved into perception and judgment, then the target is trust. If artificial intelligence industrializes influence, then the objective is to overload verification and weaken shared reality. If cognitive warfare moves markets and delays decisions, then trust is the transmission mechanism through which manipulation becomes economically real. If open societies are vulnerable, it is because their freedom depends on distributed trust. If AI is to become part of the cure, it must itself be trustworthy. And if Europe remains dependent on infrastructures it does not control, its ability to defend trust will remain incomplete.

Trust is therefore not simply the outcome of good governance. It is a strategic resource that must be designed, maintained and defended. This requires a broader understanding of infrastructure. Roads, ports, energy grids, data centers and communication networks are visible forms of infrastructure. Trust infrastructure is less visible, but not less real. It includes credible institutions, independent media, reliable public communication, verifiable digital content, secure identity systems, auditable AI, resilient crisis response and the civic ability to distinguish signal from noise.

The point is not to demand trust from citizens. Trust cannot be ordered into existence. It must be earned through competence, transparency, accountability and resilience. A government that communicates late,

inconsistently or defensively cannot expect citizens to believe it during a cognitive attack. A platform that hides its recommendation logic cannot expect public confidence. A media system without resources for verification cannot compete with industrialized falsehood. A society that relies on opaque AI systems to detect manipulation may only replace one form of uncertainty with another.

8. Build or Surrender: The Truth Will Set Us Free – If We Dare Defend It

History has a brutal lesson for us. During World War II, many Germans secretly tuned into foreign broadcasters like the BBC's German-language service. Nazi propaganda could force-feed information, but it couldn't force trust. The BBC earned its credibility because it didn't just report Allied victories or German defeats—**it also admitted British setbacks.** They told the whole truth: the good, the bad, the ugly. And that's why, for many listeners, the BBC became more trustworthy than their own state's propaganda machine.

The moment people trust the voice of an adversary more than their own institutions, **strategic power begins to crumble.**

And then there's the BBC's recent blunder. By manipulating Trump's January 6th speech to fit a narrative, they didn't just distort reality—they **handed their credibility to the very man they sought to criticize.** Now, they're staring down a $10 billion lawsuit, a shattered reputation, and the resignations of their top leaders. The irony? **The damage they've inflicted on themselves far outweighs any harm the original report could have caused.**

A free press must hold power to account—but it can't do that if it abandons its own integrity. The BBC's mistake wasn't just a bad edit. **It was a betrayal of the principle that truth, no matter how inconvenient, is the only foundation worth defending.**

9. The Duty to Truth

When media institutions, public authorities or political elites instrumentalize truth, they do not merely make a mistake. They attack the trust they claim to protect. A democracy can survive errors. It can survive bad judgment, bias, even fierce disagreement. What it cannot survive for long is a ruling class that treats truth as a tactical resource: useful when it supports the preferred narrative, disposable when it does not.

That is why accountability is not optional. If journalists distort evidence, they must correct it openly. If public authorities mislead citizens, they must answer for it. If political leaders weaponize selective facts while hiding inconvenient ones, they must be challenged — not because democracy requires politeness, but because democracy requires a common reality. Without that, elections become theatre, public debate becomes tribal combat, and institutions become just another faction in the information war.

The standard must be brutally simple: the more power an institution has over public perception, the higher its duty to truth. A private citizen may be confused. A journalist may be wrong. A politician may be partisan. But when institutions with reach, authority and public trust manipulate facts, edit context or launder suspicion into certainty, they are no longer defending society against cognitive warfare.

They are feeding it. This is where open societies need a harder doctrine of responsibility. Not censorship. Not revenge. Accountability. Corrections that are visible. Editorial decisions that can be questioned. Official claims that can be audited. Intelligence assessments that distinguish evidence from inference.

Political accusations that do not hide behind moral panic. If trust is strategic infrastructure, then those who damage it through negligence, manipulation or ideological convenience must be held responsible for the cost. The point is not to demand perfect institutions. Perfect institutions do not exist. The point is to make deception expensive again — including deception committed by those who claim to stand on the side of democracy. Freedom cannot be defended by people who quietly exempt themselves from the truth.

10. Trust: Soft Power in Good Times, Hard Power in Bad Times

Trust isn't just a moral ideal—it's strategic infrastructure, the kind that holds societies together when the storms hit. And it must be both institutional *and* technological.

Institutionally, open societies need faster, more credible crisis communication. They need independent verification—not just within government, but across journalism, academia, civil society, and security institutions. Public authorities must be able to clearly state what is known, what isn't, and what's being investigated. In cognitive warfare, uncertainty is inevitable. The real question is whether that uncertainty is handled honestly —or exploited by adversaries.

Technologically, we need provenance standards, content authentication, auditable AI systems, secure communication channels, and early-warning mechanisms for coordinated manipulation. These

systems shouldn't decide truth for citizens. Instead, they should reveal origin, context, alteration, coordination, and intent. Their role isn't to eliminate disagreement—it's to protect the conditions that make disagreement meaningful.

But trust isn't built only in ministries, platforms, or data centers. It's built in towns, schools, associations, families, workplaces, and local communities. The best defense against cognitive warfare isn't a perfectly managed information environment. It's a society where people still talk to one another—instead of just posting at each other. That might sound old-fashioned. It's not. It's strategic.

A democracy doesn't become resilient by suppressing debate. It becomes resilient when citizens can argue fiercely without losing the ability to recognize facts, evidence, and legitimate institutions. Cognitive warfare seeks to turn disagreement into fragmentation. Trust infrastructure must preserve disagreement—while preventing fragmentation from becoming paralysis.

Europe's challenge is especially demanding. It must defend an open public sphere while respecting fundamental rights. It must use AI without surrendering judgment to AI. It must regulate technology while building it. It must cooperate with allies while reducing one-sided dependency. It must strengthen trust without manufacturing consent. This is difficult. But difficulty is not an argument for delay.

The 21st century's strategic competition won't be won by the side with the most powerful algorithms. It will be won by the side whose citizens can still distinguish signal from noise, persuasion from manipulation, and disagreement from fragmentation. The decisive advantage won't be data alone—but trusted data. Not AI alone—but auditable AI. Not communication alone—but credible communication.

The West doesn't lose when its servers are hacked. It loses when its citizens no longer know what is true—and can no longer act together.

That's why trust must be treated as strategic infrastructure. It must be funded, tested, protected, and renewed. It must be integrated into national security, economic resilience, education, media policy, and technological sovereignty. And it must be rebuilt where it actually lives: locally, socially, politically, humanly.

AI will shape the future of cognitive conflict. That's no longer in doubt. The question is whether open societies will allow AI to erode the trust they depend on—or whether they will build the systems, institutions, and sovereign capacities to defend it.

A society that can no longer distinguish persuasion from manipulation has already lost before the first shot is fired. A continent that cannot build what it needs to defend its own cognitive space has only regulatory ambition—not strategic autonomy. And an actor who sacrifices truth for security is no better than the opponent they claim to resist.

Bibliography:

- **NATO Science & Technology Organization — Cognitive Warfare, Chief Scientist Research Report** https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitivewarfare-final.pdf
- **Reuters Institute for the Study of Journalism — Digital News Report 2024: Slovakia** https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025/slovakia
- **Graphika — Deepfake It Till You Make It** https://graphika.com/reports/deepfake-it-till-you-make-it
- **Meta — Raising Online Defenses: Q2 2023 Adversarial Threat Report** https://about.fb.com/news/2023/08/raising-online-defenses/
- **EU DisinfoLab — Doppelganger: Media clones serving Russian propaganda** https://www.disinfo.eu/doppelganger/
- **EU DisinfoLab — Doppelganger Hub** https://www.disinfo.eu/doppelganger-hub/
- **European External Action Service — 3rd EEAS Report on Foreign Information Manipulation and Interference Threats** https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd - ThreatReport-March-2025-05-Digital-HD.pdf
- **Associated Press — Hackers compromise AP Twitter account** https://apnews.com/general-news-68a43f18c9aa4a87bfbf350a566404c9
- **AP News — Fake image of Pentagon explosion briefly sends jitters through stock market** https://apnews.com/article/pentagon-explosion-misinformation-stock-market-ai-96f534c790872fde67012ee81b5ed6a4
- **Reuters — SEC probing fake post on its X account; bitcoin ETFs not approved** https://www.reuters.com/technology/us-sec-has-not-approved-bitcoin-etfssocial- media-account-compromised-2024-01-09/
- **European Commission — AI Act enters into force** https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en
- **C2PA — Verifying Media Content Sources** https://c2pa.org/
- **European Commission — European Digital Media Observatory** https://digital-strategy.ec.europa.eu/en/policies/european-digital-mediaobservatory
- **European Digital Media Observatory — United against disinformation** https://edmo.eu/
- **European Commission — 2022 Strengthened Code of Practice on**
- **Disinformation** https://digital-strategy.ec.europa.eu/en/library/2022-strengthened code-practicedisinformation
- **European Commission — Digital Services Act** https://digital-strategy.ec.europa.eu/en/policies/digital-services-act
- **EuroHPC Joint Undertaking — AI Factories** https://www.eurohpc-ju.europa.eu/ai-factories_en
- **European Commission — AI Factories: Shaping Europe's digital future** https://digital-strategy.ec.europa.eu/en/policies/ai-factories
- **Microsoft Azure — Microsoft and Mistral AI announce partnership to accelerate AI innovation and introduce Mistral Large first on Azure** https://azure.microsoft.com/en-us/blog/microsoft-and-mistral-ai-announce-newpartnership-to-accelerate-ai-innovation-and-introduce-mistral-large-first-onazure/
- **Mistral AI — Au Large** https://mistral.ai/news/mistral-large
- **EuroHPC Joint Undertaking — EuroHPC JU selects AI Factory Antennas to broaden AI Factories initiative** https://www.eurohpc-ju.europa.eu/eurohpc-ju-selects-ai-factory-antennasbroaden-ai-factories-initiative-2025-10-13_en
- **Latvia — Latvia becomes part of the European Artificial Intelligence Factory network** https://www.vdaa.gov.lv/en/article/latvia-becomes-part-european-artificialintelligence- plant-network-strengthening-science-innovation-and-digital-literacy
- **LUMI AI Factory — Accelerating Europe's AI Innovation** https://lumi-ai-factory.eu/
- **EuroHPC Joint Undertaking — Our Supercomputers** https://www.eurohpc-ju.europa.eu/supercomputers/our-supercomputers_en
- **BBC — The BBC German Service during the Second World War** https://www.bbc.com/historyofthebbc/100-voices/coldwar/letters-withoutsignature
- **BBC apologises to Trump over Panorama edit but refuses to pay compensation** https://www.bbc.com/news/articles/c874nw4g2zzo

HUMAN MINDS VS. TERRORISM

Before the Bomb: Why Understanding the Mind Is the Future of Counter-Terrorism

PhD. Khodor DAYEH (Lebanon)

For decades, counter-terrorism strategies have focused on the final stage of violence: the weapon, the network, the attack. Intelligence agencies monitor communications, track movements, and analyze financial activity to prevent threats. These tools are essential, but they often overlook the most important phase of the process—the psychological transformation that occurs long before violence happens.

Source: https://www.mid-day.com/lifestyle/culture/article/more-power-to-the-sixth-sense-15323189

Terrorism rarely begins with a bomb. It begins with a change in the mind.

Radicalization is often a gradual psychological journey rather than a sudden decision. Many individuals who eventually join extremist groups pass through emotional stages that include frustration, isolation, resentment, and a search for belonging. When these feelings remain unresolved, extremist narratives can offer what appears to be a solution: identity, purpose, and recognition.

For someone who feels invisible, the promise of becoming part of a larger mission can be extremely powerful.

Traditional intelligence methods tend to focus on external indicators such as weapons, travel, or suspicious communication. However, these signs usually appear late in the process. By the time operational planning begins, the psychological transformation has often already taken place.

Understanding that transformation is therefore essential for effective prevention.

Research in behavioral psychology shows that individuals moving toward extremism frequently display noticeable changes in behavior and language. These may include social withdrawal, rigid black-and-white thinking, increasing hostility toward others, and a growing obsession with perceived injustice or victimhood. These patterns do not automatically lead to violence, but they can signal a deeper emotional shift that deserves attention.

In recent years, several countries have started integrating behavioral analysis into their security frameworks. Programs in the United States and Europe have explored how psychological indicators can

complement traditional intelligence methods by identifying early warning signs before individuals move toward violence.

This approach does not replace surveillance or law enforcement. Instead, it expands the concept of intelligence.

Effective prevention requires cooperation beyond security agencies alone. Teachers, community leaders, social workers, and families are often the first to notice behavioral changes in individuals who are struggling. When these observations are taken seriously and addressed early, intervention can occur before radicalization becomes deeply rooted. Such interventions do not always require police action. In many cases, dialogue, mentorship, psychological support, or community engagement can help redirect individuals who are searching for identity or meaning.

The goal is not to criminalize belief or stigmatize communities. The goal is to recognize the human signals that appear before violence becomes an option.

Counter-terrorism strategies that rely solely on force or surveillance risk reacting too late. But strategies that integrate psychological understanding can intervene earlier—when individuals are still reachable.

The future of counter-terrorism, therefore, lies in combining intelligence analysis with behavioral insight. Security professionals should receive training that helps them recognize emotional and behavioral indicators of radicalization, while psychologists and social scientists should become part of prevention efforts.

Extremism is not only a security issue. It is also a human process shaped by identity, emotion, and experience.

If we want to prevent violence effectively, we must learn to look beyond the weapon and toward the mind that decides to use it.

Because the most effective way to stop the bomb is to understand the person before it is built.

GLOBAL ORDER

Those Who Cannot Set the Table Discuss the Menu: The Dark Capacity Codes of the New World Order

Fikret ARTUC (Turkiye)

The international system is undergoing a silent revolution before our very eyes. Power was once measured by military capacity, defined by geography and ideology. Today, these classical paradigms are being rewritten through capacity and dependency. Perhaps the most striking message to emerge from the 2026 Munich Security Conference was this: "You are either at the table or on the menu."

Source: https://georgiatoday.ge/the-new-economic-autarchy-on-a-few-fundamental-global-trends-and-important-expectations-part-1/

While it sounds like a simple aphorism, it summarizes the new anatomy of international relations and power dynamics in a single, blunt sentence. For a long period, international relations literature discussed power through measurable capacity elements: military spending, economic size, and population.

However, at the current juncture, power has shifted from metrics to the architecture of invisible flows. This is why being "at the table" is not merely about occupying a seat; it means the capacity to produce decisions, the ability to set norms, and the power to influence the dependency chains of others. Those who remain "on the menu" often find themselves in the shadow of rules written by others, unknowingly restricting their own strategic options.

The case of Ukraine is living proof: despite its critically strategic location, it remains on the menu because it could not elevate its own capacity to the level of "setting the table." This situation is not just about military or diplomatic deficiencies; it is directly related to economic dependency and technological limitations. Today, the decisive factors are not those who control physical geography, but those who determine the direction of circulation in the geography of flows.

Economy and Technology: The New Weapons of Influence

Economy is no longer a neutral tool; it is a mechanism for creating dependency and influence. Europe's energy dependency, China's dominance in supply chains, and U.S. financial sanctions reveal the new borders of being at the table versus being on the menu.

Actors capable of sitting at the table can transform both their advantages and the vulnerabilities of others into strategic weapons. Those on the menu, however, often play no role other than being the target of these weapons.

For instance, while the U.S. directs global liquidity through the dollar system and financial networks, China reshapes logistical flows under the banner of the "Belt and Road Initiative." The EU, in this system, serves as an optimized stopover for these flows to operate seamlessly, yet it is not a decisive center.

Technology creates a new battlefield. Artificial intelligence, semiconductor production, and data sovereignty have become the determining elements of staying at the table. The race between the U.S. and China demonstrates how classical war mechanics are giving way to shadow conflicts and capacity projection. Those at the table do not just produce technology; they gain strategic superiority by manipulating the dependencies of other actors. Those dependent on technology do not just stay on the menu; they are tossed to an invisible periphery, outside the decision-making mechanisms of the future.

Geopolitical Projections and the Paradox of Sovereignty

Politically, being at the table no longer relies on status or traditional recognition. Sovereignty is now measured by the capacity to produce and implement decisions. Actors not at the table remain on the menu, often debating their own "illusions of independence" without realizing it.

This is the clearest indicator of global instability and the complex restructuring of power balances. Digital sovereignty creates a paradox: a labyrinth of contradictions that produces law but fails to produce reality. The EU acts like a "higher mind," employing a new but functionally debatable form of power that seeks to discipline strength.

The European Union is forced to remain on the menu due to energy dependency; nevertheless, its financial capacity and diplomatic influence allow for a partial "table" position.

The Middle East and Gulf Countries possess bargaining power due to strategic locations and energy reserves, yet they move within the menu due to limited capacity.

The South China Sea represents a "table" for those holding control over islands and sea lanes, and a "menu" for dependent actors.

The USA maintains its position at the table by utilizing financial, technological, and military capacity, writing the rules and setting the norms.

China secures long-term influence through supply chains and technological infrastructure, engaging in continuous strategic capacity production to strengthen its seat at the table.

The economic fallout is even more striking: countries on the menu are often unaware of their own fragilities. Energy, food, and tech dependencies are used as strategic leverage by those at the table. The only guarantee of being at the table is continuous production, control, and dependency management. Those on the menu remain passive victims of these dynamics.

The energy shock Europe experienced during the Russia-Ukraine war was not merely a supplydemand crisis; it was a blatant exposure of geopolitical dependency. As energy prices rose, the EU's industrial competitiveness weakened, and its production model came under severe pressure.

The Trump Factor and the Shifting Table

Power is no longer measured by visible military or economic bulk alone. Sovereignty is measured by capacity, dependency, and the ability to manipulate the vulnerabilities of others.

In this new world order, the system may appear multipolar, but China has effectively taken Russia's place. While the U.S. continues with its imperialist aggression, China maintains its silence, acting on the logic: "Never interrupt your enemy when he is making a mistake." In this chaotic environment, China avoids direct confrontation with the U.S., opting for "strategic patience and silence." The exhaustion of U.S. energy in West Asia and its distraction by side fronts like Ukraine and the Asia-Pacific is seen as an unparalleled opportunity for China. With its stable positioning, China has emerged as a more consistent and reliable alternative on the global stage, while also providing under-the-table support to Iran.

In an era where the U.S. has stopped the "old applause" and slammed the doors shut, and where global political balances are shattered, Trump's "America First" slogan sets new boundaries for all allies. He is one by one changing the rules that once defined who sets the table and who sits there. The agenda moves so quickly that deciphering the shape and rules of the table becomes nearly impossible—because Trump can remove those at the table and put them on the menu in an instant.

As the rules of the table change, the rules of global political equilibrium change with them, leading to results with many unknowns. China, Russia, and regional powers are now actors challenging the system, and the rhetoric of a "rules-based order" has increasingly become a defensive reflex. European leaders are now signaling: "We can no longer outsource our security."

This signifies a quest for strategic autonomy for a Europe currently dependent on NATO. If Russia is not stopped, the next targets may expand. The word "peace" is being redefined as "just peace." One particular emphasis stands out: "The wars of the 21st century will be won not with tanks, but with algorithms." In this capacity-based global system, the geopolitical divergence between being at the table and being on the menu is becoming starkly visible for Europe.

The Structural Transformation Necessity for the EU

The evolution of the international system into a capacity-centric structure creates both a structural challenge and a strategic breaking point for Europe. Since its inception, the EU has been defined as a normative power, generating global influence through international law, multilateralism, and values. However, the shift toward capacity, control, and dependency has rendered this role fragile.

Despite its economic size, the EU has remained limited and ineffective in converting that size into strategic capacity. This results in a "Capacity Asymmetry Paradox." Europe is a major actor in the global economy, but its external dependency on energy, technology, and defense prevents it from fully "setting the table."

While defense budgets are increasing and the idea of a Common European Army is back on the agenda, the crises faced by a Europe burdened with external dependencies show that energy security is not just an economic issue but a geopolitical one. The loss of industrial competitiveness and political misalignment among member states now threatens the ecopolitical integrity of Europe.

In technology—specifically semiconductor production, AI development, and big data control—the EU lags far behind the U.S. and China, bringing "digital sovereignty" to the forefront of the debate. If Europe fails to develop capacity in these fields, it faces the risk of being on the menu rather than at the table in the decision-making mechanisms of the future.

Unfortunately, the fact that the EU's security architecture rests on NATO and the U.S. severely limits its ability to act independently. The frequently mentioned concept of "strategic autonomy" is a reflection of the effort to reduce this dependency. However, significant obstacles remain: inconsistencies in defense policies among member states, limited common military capacity, and problems in financing and coordination. In this context, Europe is not yet fully at the table in defense and security; it remains a semi-autonomous actor moving as part of the transatlantic structure. How can a sovereignty protected by externalizing its own security sustain a claim of political independence? This remains a separate debate.

Between "Silent Collapse" and "Strategic Awakening"

Is Europe a power, or merely a "geography"? The concept of "de-risking" is replacing "decoupling"—meaning reducing problematic dependencies rather than a total break. The issue at hand is not just a crisis, but a problem of definition. While the EU still defines itself as a normative power, it risks transforming into a purely functional actor in a capacity-based system. This transformation is not an overt collapse, but a more dangerous process of silent erosion.

In today's international system, power is not visible; it is a form of capacity that permeates and creates dependency. While the EU possesses some elements of this capacity, it is late in transforming them into strategic integrity. This delay may not weaken it immediately, but it gradually moves the EU from being a decision-maker to a mere implementer. The real breaking point lies here: the EU no longer faces the risk of losing power, but the risk of losing the definition of its power and being repositioned by others.

In this regard, the phrase "you are either at the table or on the menu" is not a rhetorical warning for the EU; it is a strategic diagnosis. Because today, the EU is neither fully at the table nor on the menu. It occupies a precarious middle ground that is unsustainable. Since capacity-based systems do not tolerate gray areas for long, one either produces capacity and manages dependencies, or those dependencies are managed by other actors.

In the coming period, the EU's crossroads will be determined by the extent to which it reduces its dependencies and, most importantly, its ability to centralize and accelerate decision-making processes. If this transformation does not occur, the EU will not find itself outside the system, but inside it—positioned ineffectively. Its future would be reduced to a mere variable in a cost benefit calculation on a table set by others.

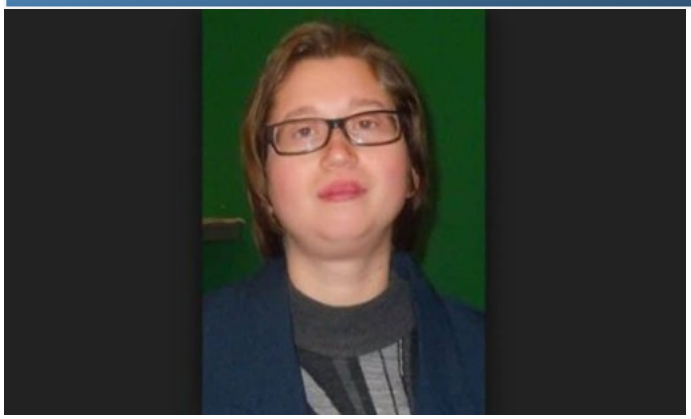
The EU must now evolve its historical superiority and norm-producing talent by adding a mastery over infrastructure, supply chains, data flows, and security umbrellas. Failing to turn this capacity into a strategic will creates a new form of dependency, masked by high prosperity, institutional stability, and technological integration. Beneath this mask, the EU would cease to be a subject determining its own fate and become an optimized platform for the strategic designs of others.

Every day this transformation is postponed, it stops being a choice for the EU and becomes a decision made by others. In this technological age, while seeking consensus through sluggish bureaucratic structures, the EU's democratic legitimacy will be questioned.

This is different from a classical decline; it is a deep-seated process of being moved onto the menu unless it can eliminate its gray zones and embrace the reality of its transformation at the threshold of destiny.

The same question must be asked again and again: Is Europe a power, or merely a "geography"?

GLOBAL ORDER - EASTERN EUROPE



The Interdependence of Contemporary Conflicts: Ukraine and Iran and Their Implications for the Global Order and Eastern Europe

Mona AGRIGOROAIEI (Romania)

"Most dangerous of all is that interdependence makes every crisis, in any corner of the world, everyone's problem." — The New Yorker, Comment, July 1975

Introduction

The contemporary world is in a period of profound geopolitical transition, in which international dynamics are increasingly less predictable and fragmented. The classical international order, built on the basis of post-Cold War Western hegemony and consolidated multilateral institutions, is simultaneously challenged by revisionist actors such as Russia and Iran, by the rise of China as an economic and military superpower, and by the proliferation of non-state actors with regional or global influence, including terrorist groups, multinational corporations, and digital platforms. In parallel, accelerating technological and economic transformations—from artificial intelligence and cyberspace to the control of global supply chains and energy resources—are rewriting the rules of competition for power and influence on a global scale.

Source: https://iranprimer.usip.org/blog/2023/apr/27/timeline-iran-ukraine-relations

The war in Ukraine, which began in 2022, and the conflict in Iran, which broke out in 2026, are eloquent examples of how regional conflicts no longer remain isolated, but become interdependent nodes of the international system. Ukraine has become a theater of conventional warfare, but also a laboratory of modern hybrid warfare, in which cyberattacks, disinformation and the use of drones complement traditional military confrontation. Ukraine's resilience depends not only on its domestic capacity, but also on the continued support of Western allies, through arms deliveries, defense systems and economic assistance. In parallel, the conflict in Iran has demonstrated how a regional event can have systemic effects, disrupting global energy markets, increasing inflation and affecting economic and political stability worldwide. The blockade of the Strait of Hormuz has illustrated the fragility of global economic interdependence and how a local conflict can generate global reverberations.

The interdependence of the two conflicts is evident in the way they influence each other. The redirection of military resources and strategic attention from Eastern Europe to the Middle East reduces the support available to Ukraine and strengthens Russia's position on the Eastern Front. At the same time, the destabilization of energy markets through the Iranian crisis provides Moscow with additional revenues and economic flexibility in the face of Western sanctions. Thus, what initially seemed a clear separation between the theaters of conflict turns out to be a functional link, in which developments on one front have direct repercussions on the other.

The implications for Eastern Europe and Romania are significant. Romania, located at the crossroads of the Euro-Atlantic space and the Eastern spheres of influence, is in a critical strategic position. The security of the Black Sea, the stability of Ukraine, relations with the Republic of Moldova and Russia's influence in the region mean that any military escalation or economic tension is immediately felt locally. Membership in NATO and the European Union (EU) represents essential security guarantees, but also implies strategic responsibilities: Romania must contribute to the defense of the eastern flank, to the consolidation of critical infrastructures and to supporting regional cohesion in the face of hybrid and conventional threats.

From an economic and social perspective, the crises in Ukraine and Iran accentuate global vulnerabilities. Energy and food prices are fluctuating, supply chains are under pressure and migration is becoming a geostrategic issue. The psychological and political impact on Western populations and governments can generate a "strategic fatigue", reducing the willingness to sustain long-term military and diplomatic commitments.

The analysis of the two conflicts shows that the contemporary world no longer functions in classical terms of separation between regional theaters of war. The war in Ukraine and the conflict in Iran are interdependent, and their combined effects are restructuring the global order, accelerating the process of multipolarity, redistributing resources and redistributing strategic priorities for major powers and regional states, including Romania. In a hyper connected and interdependent world, the capacity for anticipation, adaptation and coordination becomes the decisive factor for security, stability and survival of the international order.

The Ukrainian Conflict: from Regional War to Global Epicenter

The Ukrainian war began as a bilateral confrontation between Ukraine and the Russian Federation, but its rapid evolution and international implications have transformed it into a conflict of attrition with global reverberations. Ukraine's capacity to resist no longer depends solely on battlefield superiority, but equally on the military, economic, and diplomatic support provided by NATO and the EU. The fronts have stabilized in some regions, but the ongoing pressure on critical infrastructure, the civilian population, and supply systems underscores the long-term nature and complexity of the conflict. Analyst Lawrence Freedman emphasizes that "modern wars are no longer won exclusively on the battlefield, but through the ability to sustain a sustained military effort, while simultaneously mobilizing international political and economic support" (Freedman, 2023). This shows that Ukraine is not fighting just for territory, but to maintain the credibility of Western alliances and to set a precedent for the global response to the aggression of a revisionist actor. In this sense, the Ukrainian conflict has become a test of political, military and economic cohesion for NATO, the EU and international partners.

The war has redefined the contemporary military paradigm. Technologies such as tactical and reconnaissance drones, advanced surveillance systems, electronic warfare and precision artillery have changed the way conventional conflicts are conducted, emphasizing speed of reaction, mobility of forces and logistical efficiency. At the same time, inter-institutional coordination between states, intelligence support and the transfer of military technology have proven to be as crucial as numerical superiority. The economic dimension of the conflict is equally relevant: Ukraine, Russia and global markets are feeling the effects of supply chain disruptions, energy price volatility and food insecurity. Western embargoes and sanctions against Russia have generated both internal pressures in the Russian Federation and opportunities for third states to take on roles in energy or military trade. In this regard, the Ukrainian war has demonstrated the interdependence of military security and economic stability on a global scale.

The conflict transformed the entire Eastern Europe into a strategically important space, leading to a reassessment of the security policies, military capabilities and economic strategies of the states in the area. Romania, through its geographical position and shared border with Ukraine, became an essential node in the logistical and humanitarian support for Ukraine, but also a key element in the NATO security architecture. The experience of the war highlighted the need for a flexible military system well integrated into the networks of the allies, which led to the acceleration of the modernization of the Romanian army, including through the acquisition of anti-aircraft systems, precision artillery, drones and secure communication technologies. Preparation for the war of attrition and logistical resilience became essential for deterring future aggressions, and coordination with NATO and participation in joint exercises

strengthened the interoperability and credibility of the Alliance. In parallel, Romania has taken on a central role in managing humanitarian flows, being one of the main host states for Ukrainian refugees, which has involved not only providing shelter, medical services and education, but also their medium-term integration into the labor market, international support being essential for maintaining social and economic stability in areas affected by mass migration. In economic terms, the war has highlighted Europe's energy vulnerability, and Romania, with its own gas reserves and regional interconnection possibilities, can play a role as a supplier and stabilizer of the European energy market, while global economic turbulence, inflation and volatility in raw material prices underline the need for flexible economic policies and diversification of supply sources. Also, the support provided to Ukraine and active participation in European and transatlantic mechanisms allow Romania to consolidate its status as a responsible regional actor and mediator between EU states and Ukraine, which provides access to reconstruction programs and strategic investments and strengthens the country's position in the geopolitical architecture of the region.

On a global scale, the war in Ukraine shows how a local conflict can generate global effects through the interaction of military, economic and geopolitical dimensions. Militarily, the conflict tests and refines the tactics of modern warfare, highlighting that success depends as much on logistics, external support and political cohesion as on numerical superiority.

Economically, the disruption of global supply chains, the volatility of energy and food markets and rapid changes in international trade flows demonstrate how closely military security is linked to economic stability.

Geopolitically, the conflict has stimulated a realignment of alliances, consolidating the role of Eastern Europe as a strategic area and testing the capacity of multilateral organizations to respond coherently to external aggression. Thus, Ukraine has become not only a theater of war, but also an epicenter of diplomatic negotiations, economic sanctions, and international power projection, serving as a case study for 21st-century warfare and demonstrating that military success is closely linked to political cohesion and global economic strategy. The war in Ukraine highlights how regional conflicts can escalate rapidly and become global epicenters, where military, economic, and geopolitical dimensions intersect, underlining that success in such conflicts does not depend exclusively on military force, but on the capacity for global mobilization, economic strategy, and political cohesion, as well as on the role that regional actors, such as Romania and the states of Eastern Europe, play in maintaining international stability and balance.

The Iran Conflict and Its Global Implications

The Iran conflict of 2026, by its complexity and scope, illustrates not only the vulnerability of an extremely sensitive region, but also the profound interconnectedness of the contemporary world, where any regional crisis can have global repercussions in economic, military, political and social terms. Its impact extends beyond the Strait of Hormuz and energy markets, affecting global politics, supply chains, capital flows and the internal stability of the states directly or indirectly involved. As the conflict drags on, countries dependent on imported energy, especially in Europe and Asia, are forced to accelerate the transition to alternative sources, the development of renewable energy and the diversification of supply routes, thus changing global energy strategies in the long term.

From a military perspective, Iran has demonstrated the effectiveness of hybrid tactics, combining conventional attacks with asymmetric and cyber operations, which has forced international actors to rethink their rapid response capabilities and interoperability of forces. This approach to the conflict highlights the need for coordination between military and diplomatic strategies to prevent escalation and maintain the balance of power in the region, without turning the crisis into a global conflict. In addition, the tensions have generated an intensification of intelligence operations, maritime traffic monitoring and technological surveillance of critical infrastructure, with an emphasis on cybersecurity and the ability to prevent asymmetric attacks.

The economic effects have spread rapidly, affecting not only energy prices but also global industrial chains, including fertilizer production, maritime transport, commodity trade and food supply chains. The disruptions have prompted central banks and international financial institutions to reassess monetary and fiscal policies, while capital markets have experienced increased volatility. In addition, sanctions and trade restrictions have forced third countries to rethink their energy security strategies and identify new partners for imports and exports, intensifying competition for resources and geopolitical influence in the region.

On the diplomatic and geopolitical front, the conflict has accelerated the realignment of international alliances. States such as China and India have been forced to reassess their energy dependence on the Middle East, while the EU and the US have intensified coordination to protect strategic interests and prevent direct escalation of confrontations. The tensions have generated increased multilateral negotiations and diplomatic pressure on regional actors to maintain stability and minimize negative effects

on the global economy. At the same time, the conflict has raised questions about the effectiveness of international bodies, such as the UN, in mediating regional crises that can have global effects, demonstrating the need for more effective mechanisms to prevent escalation.

From a social and humanitarian perspective, the conflict has caused massive population displacement, forced migration and humanitarian crises in neighboring states, especially Iraq, Turkiye and the Persian Gulf. Increased tensions and the blockade of trade routes have affected the supply of food and essential products, increasing the vulnerability of communities and exacerbating internal tensions in indirectly affected states. Thus, the Iranian conflict in 2026 highlights the interdependence between military security, economic stability and social cohesion, underlining that the response to such crises requires an integrated and coordinated approach on several dimensions.

This crisis demonstrates that in a globalized world, the fragility of strategic nodes such as the Middle East can generate effects with global reverberations, which are felt in prices, supply chains, energy policies, alliance structures and regional stability. The management of such a conflict cannot be military alone, but involves complex coordination between diplomacy, economic strategy, cybersecurity and international cooperation, to prevent escalation and to maintain the global balance in the face of regional threats with global effects.

Interdependence of Conflicts

The interdependence of the conflicts in Ukraine and Iran illustrates how regional tensions can generate a network effect with global implications, influencing not only military and economic resources, but also the geopolitical balance and strategic calculation of the great powers. Western military support for Ukraine, which includes precision weapons, missile defense systems, and logistical advice, is being partially redirected to the Middle East to respond to Iranian attacks on critical infrastructure and energy corridors. This redistribution creates a domino effect: NATO and the EU's ability to maintain pressure on Russia in Ukraine is affected, while Iran and regional actors can temporarily exploit the fragility of Western defenses. In this context, Ukrainian President Volodymyr Zelensky's warning that "any conflict that distracts the attention and resources of our partners weakens our defense capacity" reflects not only Ukraine's vulnerability but also the complexity of global strategic interdependence. This economic and geopolitical interdependence creates subtle opportunities for revisionist actors. Russia, for example, benefits indirectly from the Iranian crisis: rising global energy prices allow it to offset some of the financial losses caused by sanctions, while maintaining pressure on Ukraine. Moreover, global pressure to maintain the flow of oil and gas to Europe and Asia forces great powers to prioritize some crises over others, which opens up space for strategic maneuvers by regional actors. John Mearsheimer notes that "great powers seize every opportunity to maximize their relative advantages in the international system," which shows that interdependence not only constrains actors' actions but also provides favorable contexts for exploiting vulnerabilities.

On the military front, the contrasts between the two conflicts highlight the adaptability and diversity of modern strategies. In Ukraine, conventional warfare of attrition is complemented by the use of advanced technology, such as reconnaissance and attack drones, precision artillery systems, secure communications, and sophisticated electronic warfare. This type of conflict requires logistical cohesion, sustainable economic support, and interoperability between NATO and EU member states. In parallel, the Iranian war demonstrates the effectiveness of asymmetric tactics: relatively low-cost attacks with disproportionate effects on energy infrastructure, strategic ports, and digital systems. This complementarity between the conflicts highlights that the modern assessment of military power can no longer be made solely through the lens of technological or numerical superiority, but must integrate operational sustainability, economic efficiency, and strategic flexibility. Andrew Krepinevich observes that "the future of war belongs to those who can combine advanced technology with low operational costs," emphasizing that success in a multipolar environment depends on adaptability, innovation, and resource management in multiple contexts.

The interdependence of these conflicts extends to the global economic dimension. The disruptions in energy supply chains caused by the Iranian crisis add to the economic pressure caused by the war in Ukraine, affecting commodity prices, industrial costs, and global inflation. These interactions create a complex relationship between energy security, market stability, and the ability of actors to sustain long-term military efforts. In essence, Ukraine and Iran are no longer just regional theaters of conflict, but critical nodes in an interdependent global network, where strategic, economic, and military decisions influence each other, and success or failure in one point can reverberate on a planetary scale.

The interdependence of conflicts takes on new depth when we include Ukraine's role not only as a victim but also as an active actor in the Middle East crisis. Although the war in Ukraine and the conflict in Iran remain distinct theaters of operations, recent developments show how destabilization in one region can provide strategic, technological, and diplomatic impetus in another — and Ukraine, far from remaining

isolated in its own defense effort, is trying to convert the expertise accumulated on the Ukrainian front into a tool for regional cooperation and attracting broader international support.

Central to this dynamic has been Ukraine's involvement in countering Iranian drone threats in the Middle East. After years of confrontations with thousands of drones supplied by Iran to Russia for attacks on Ukrainian cities and infrastructure, Ukrainian experts and Kiev's armed forces have developed sophisticated cyber and missile defense capabilities against these systems. This experience has become an internationally recognized asset, and Ukraine has sent more than 200 military personnel and specialists to the region to help Gulf states repel Iranian drone attacks and implement effective air defense strategies based on lessons learned on the Eastern European front.

Ukrainian President Volodymyr Zelensky has promoted this experience during a series of visits to Arab countries, notably Saudi Arabia, the United Arab Emirates, and Qatar, where cooperation agreements on anti-drone defense technology, maritime drone systems, and security technology production have been signed or discussed. These agreements are not just symbolic: they include exchanges of expertise and technical cooperation on intercepting Iranian drones, using the know-how developed by Ukrainian forces in recent years.

Kiev's involvement in the Middle East reflects active military diplomacy and an attempt to turn competence in drone defense into a strategic and economic advantage for Ukraine. Moreover, Ukraine is discussing the possibility of providing naval technology with drones and interceptors, as well as logistical know-how on unblocking and securing sea corridors, based on its experience with the Black Sea sea corridor, which has functioned despite adverse military pressure.

The Iranian conflict has also generated direct political accusations at the international level. Tehran has officially accused Ukraine of "active participation" in the Middle East war and of indirectly supporting Israel in attacks on Iran by providing drones and expertise, presenting this involvement as a "violation of international law." Kiev has denied these claims, stressing that there is no evidence that Ukrainian drones have ever struck Iran, with the US-Israeli war in the Middle East being a separate reality from the conflict in Ukraine.

Ukraine's involvement in the Middle East crisis through anti-drone technology and cooperation with Arab states adds a new dimension to the interdependence of the conflicts. On the one hand, Ukrainian experts help deter threats in the Persian Gulf, which often allows energy flows to be maintained and reduces pressure on global markets. On the other hand, this cooperation strengthens Kiev's ties with states in the region, attracting political support and possible technological and economic assistance that can later be used in the defense effort against Russia. At the same time, Ukrainian expertise in air defense and drone warfare is in demand by the most affected countries in the Middle East, transforming what was initially a bilateral conflict into a globalized strategic space where lessons learned on one front transfer advantages to another.

From a geostrategic perspective, this interdependence makes solutions to regional conflicts no longer purely local or bilateral, but interconnected elements of a global security architecture. Ukrainian support for Arab states against Iranian drones does not translate only into defensive capabilities, but into notions of strategic solidarity, exchange of technologies and modern alliances, which can influence not only the dynamics of the war in Ukraine, but also the regional strategic posture. This evolution shows that, in the 21st century, conflicts are less "isolated" and increasingly interdependent, and the political and military success of a state depends on its ability to face challenges on multiple fronts simultaneously.

Implications for Eastern Europe and Romania

Eastern Europe and Romania are in an extremely complex strategic context, marked by the interdependence of the conflicts in Ukraine and Iran and by the vulnerabilities generated by the immediate proximity of revisionist actors. Ukraine's stability is a key factor for regional security, as any deterioration of the eastern front could have direct effects on the critical infrastructure, energy security and defensive capacity of neighboring states, including Romania. The redirection of NATO and EU military, financial and diplomatic resources to the Iranian crisis increases pressure on the eastern flank and forces Romania to simultaneously manage multiple threats and complex risks.

From a military perspective, Romania must develop an adapted defense strategy, which includes strengthening national capabilities, interoperability with allied forces and preparing the population for crisis scenarios. Modernization of the army remains crucial, with a focus on early warning systems, air defense, cyber defense and rapid reaction capabilities. NATO's presence on Romanian territory provides a defensive shield, but it also entails significant responsibilities: logistical coordination of allied troops, protection of critical infrastructure, as well as prevention of infiltrations or hybrid attacks that could destabilize the region. The experience of the Ukrainian conflict shows that logistical preparation and rapid reaction are as important as numerical or technological superiority.

Economically, Romania is facing the direct effects of regional and global instability. The increase

in energy prices, fueled both by the conflict in Ukraine and by the disruptions caused by the Iranian crisis, affects the costs of production, transport and services, which can amplify social tensions. Energy instability forces Romania to accelerate projects to diversify sources: investments in renewable energy, the development of domestic gas resources and the consolidation of energy transport and storage infrastructure. In parallel, Romania has the opportunity to position itself as a regional energy hub, supporting the supply of other European states and creating new strategic partnerships.

The social and humanitarian dimension is critical. Romania continues to manage significant migration flows from Ukraine, and the Iranian crisis may generate additional waves of refugees and economic migrants from the Middle East and Central Asia. This puts pressure on social infrastructure, healthcare, education and public services, requiring integration policies and rapid support for affected populations. At the same time, local and central governments need to manage internal social tensions and maintain community cohesion in the face of the economic and social impact of multiple crises.

Geopolitically, Romania is at a strategic crossroads. Active support for Ukraine – by sending military equipment, participating in NATO exercises and facilitating logistical corridors – strengthens Romania's position within the Alliance and the EU, but also entails risks. Cyberattacks, diplomatic pressures and the possibility of revisionist hybrid actions must be anticipated and managed through integrated security strategies. In addition, global instability offers Romania the opportunity to become a more influential regional actor, facilitating cooperation between the Balkans and Eastern Europe and contributing to strategic infrastructure and collective security projects.

Digital security is becoming increasingly relevant in a world of hybrid warfare. Romania must invest in the protection of critical infrastructure – energy, transport, communications and financial systems – to prevent sabotage and disruption, which can be orchestrated by hostile actors. The combined experience of the conflicts in Ukraine and Iran shows that digital and physical security are interdependent, and vulnerabilities in one area can amplify the effects in the other.

In the medium and long term, Romania must develop integrated scenarios that take into account the multiple dimensions of risks: the escalation of the Ukrainian conflict, the effects of the Iranian crisis on global energy and trade, demographic changes caused by migration and the economic impact of international sanctions. Defense strategies, energy policy and social policies must be coordinated to reduce vulnerability to external shocks and to strengthen economic, military and social resilience. Romania can transform its vulnerable geographical position into a strategic advantage, becoming a pivot for the security and stability of Eastern Europe, providing logistical, military and economic support to Ukraine and the states in the region.

Romania and Eastern Europe are in a period of simultaneous vulnerability and opportunity. Regional security depends on the ability to simultaneously respond to the conflicts in Ukraine and Iran, to maintain energy and economic stability, and to manage the social pressures generated by migration. Strategic success will depend on Romania's ability to coordinate military, economic, diplomatic, and humanitarian resources in a fluid and interdependent geopolitical environment, to maintain regional cohesion, and to consolidate its role as a stabilizing actor in Eastern Europe and the Balkans.

Global Scenarios and Strategic Perspectives

The interdependence of the wars in Ukraine and Iran highlights the fragility of the international order and accelerates multipolar trends, marking the transition from a system dominated by Western hegemony to a more fragmented global architecture. The emergence of alternative power axes, such as Russia–Iran, which cooperate through military, technological and economic exchanges, as well as the strategic observer role of China, which prioritizes its economic expansion and diplomatic influence without directly engaging in conflicts, suggests that the global order is becoming increasingly complex and fragmented. This multipolar dynamic is transforming the traditional logic of international security, forcing states to navigate between competition and cooperation, to manage multiple interdependencies and to maximize relative advantages in the face of adversaries and partners who no longer respect traditional norms or alliances. Henry Kissinger observed that "in a multipolar world, stability depends on the balance of interests and on understanding the tolerance thresholds of each actor" (Kissinger, 2014), emphasizing that strategic success can no longer be based solely on unilateral military or economic superiority.

In economic terms, the destabilization of energy flows caused by regional conflicts and sanctions imposed on global actors generate contagion effects on international markets. Financial market instability, rising energy prices and supply chain disruptions affect both major powers and states dependent on energy, technological or industrial imports. Paul Kennedy observed as early as the 1980s that "economic power is the foundation of military power; any imbalance between the two is quickly felt in international politics" (Kennedy, 1987), which highlights the importance of maintaining a strong domestic economy and energy resilience as essential elements for global strategic influence. In the current context, these economic tensions may accelerate the decoupling of markets and the creation of rival economic blocs, increasing the

risk of regional fragmentation and competition for critical resources.

At the societal level, the strategic fatigue of Western public opinion limits the ability of governments to maintain prolonged military engagements, influencing political and military decisions. Joseph Nye emphasizes that "power is not just about brute force; soft power and public perception largely determine the long-term success of international policies" (Nye, 2004). In this context, maintaining internal cohesion and public support becomes a critical factor, since societies less willing to accept high material and human costs will limit the freedom of action of governments in the field of security and foreign policy.

The future of the international system depends on the ability of global actors to simultaneously manage multiple interdependent crises, which influence each other directly and indirectly. Possible scenarios include a competitive but managed coexistence, in which great powers pursue their interests without escalating conflicts, while maintaining a minimum level of cooperation in strategic areas such as energy, trade or cybersecurity. This type of coexistence requires a delicate balance between rivalry and cooperation, permanent negotiations and rapid adaptation to geopolitical developments. Alternatively, a scenario of heightened fragmentation involves recurrent regional conflicts, the formation of rival blocs and a significant reduction in international cooperation, which could generate global economic, military and social instability. This fragmentation could be amplified by the development of autonomous military technologies, hybrid wars and the widespread use of disinformation tools, which increase the vulnerability of states and the complexity of crisis management.

In an interconnected world, understanding the causal relationships and anticipating the simultaneous effects of multiple conflicts becomes essential for global strategy. Decisions taken in a regional context can have immediate and unpredictable effects on other fronts, creating the need for integrated strategic management, which includes the military, economic, diplomatic and societal dimensions. Ian Bremmer emphasizes that "in a G-Zero world, without a global hegemon, the international order will be defined by the capacity of states and international organizations to negotiate and manage crises pragmatically" (Bremmer, 2012), which highlights the importance of flexible alliances, anticipatory strategies and rapid reaction mechanisms.

In this framework, states must develop advanced tools of strategic anticipation, improve military interoperability, diversify economic and energy sources and strengthen domestic social and political resilience. The successive and integrated approach to these dimensions can prevent the escalation of crises and maintain a relatively functional level of stability in a multipolar and interdependent environment. The crises in Ukraine and Iran are clear expressions of how the destabilization of one front directly influences the evolution of the other, and the success of international policies depends on the capacity to integrate all dimensions into a coherent and anticipatory strategic framework.

Selective Bibliography:

• Allison, Graham (2023), *Destined for War: Can America and China Escape Thucydides's Trap, Houghton Mifflin Harcourt.

• Freedman, Lawrence (2023), Command: The Politics of Military Operations from Korea to Ukraine, Oxford University Press.

• Kaplan, Robert D. (2012), The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate, Random House.

• Krepinevich, Andrew (2019), The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy, Basic Books.

• Mearsheimer, John J. (2001), The Tragedy of Great Power Politics, W.W. Norton & Company.

• HotNews (2026), "Zelensky: the war in Iran weakens Ukraine's defense capacity", HotNews.ro, March 28, 2026.

• Reuters (2026), Global Energy Markets in Conflict: Iran's War and the Worldwide Oil Shock, International Energy Review.

• Friedman, George (2024), *The Next Decade in Geopolitics*, Stratfor Press.

• Van Creveld, Martin (2020), The Transformation of War, Free Press.

• Mahnken, Thomas G. (2021), Technology and the Future of Warfare, Naval Institute Press.

• Buzan, Barry, & Waever, Ole (2003), Regions and Powers: The Structure of International Security, Cambridge University Press.

• Cohen, Stephen F. (2022), *War with Russia? From Putin & Ukraine to Trump & Russiagate*, Anchor Books.

• Pifer, Steven (2023), The Eagle and the Trident: U.S.-Ukraine Relations in Turbulent Times, Brookings Institution Press.

• Charap, Samuel, & Colton, Timothy J. (2022), Everyone Loses: The Ukraine Crisis and the Ruinous Contest for Post-Soviet Eurasia, Routledge.

EUROPE - NEW DEFENSE CHALLENGE

France and Europeans Confronting the "New Defense" Challenge Rearming in the Age of Artificial Intelligence[1]

Gilles DELAFON (France)

France and Europeans Confronting the New Defense Challenge

After eighty years of relative peace, Europe is facing the abrupt return of high-intensity warfare, the Russian threat, and weakening American security guarantees. In response, an unprecedented rearmament effort—unmatched since World War II—is mobilizing hundreds of billions of euros. Yet despite rising budgets and a growing number of announced procurement plans, this effort remains fragmented, slow, and insufficiently agile. The issue is no longer only to buy more, but to buy better, at a time of major technological disruption—most notably the rise of drones and artificial intelligence. New Defense captures this profound shift: a more agile, innovative, and integrated defense model, now an essential condition for European strategic autonomy.

Ukraine: The Most Technological Conflict of All Time

The war in Ukraine has been defined by the decisive entry of civilian innovations onto the battlefield. It is a full-scale laboratory for New Defense, where speed of adaptation, agility, and technological integration outweigh traditional military templates. Startups, commercial satellites, artificial intelligence, digital platforms, and civilian drones converted into combat systems have fundamentally reshaped how operations are conducted. Drone warfare, electronic jamming, large-scale data exploitation, and automation all illustrate this turning point. Beyond conventional weapons, strategic advantage now rests on the ability to rapidly integrate dual-use technologies, adapt them, and produce them at scale. The Ukrainian conflict shows that tomorrow's military superiority will depend as much on software innovation as on industrial capacity.

[1] *Published January 2026, by the Thomas More Institute, https://institut-thomas-more.org/2026/01/29/note79-eng/. With the author's consent, the article is also published in issue 307 of the GEOSTRATEGIC PULSE magazine.*

2016–2026: A Decade to Respond to the Risk of Western Technological Decline

China's technological rise triggered, as early as the 2010s, fears of a strategic gap opening in the West. Facing this risk, the United States launched a major shift by seeking to bring civilian innovation into the core of its military apparatus, notably through the creation of the Defense Innovation Unit (DIU) in 2016. This approach marks the emergence of New Defense: accelerating the adoption of dual-use technologies from startups to offset the inertia of traditional weapons programs. In France, this awakening led to the creation of the Defense Innovation Agency (AID). Russia's 2022 invasion of Ukraine confirmed the urgency of this pivot, exposing Europe's lack of preparedness and its technological dependence. Drones, artificial intelligence, electronic warfare—and soon quantum technologies—impose a new strategic tempo. The ability to integrate these innovations quickly is now becoming the decisive factor in military power.

New Defense Versus the Structural Inertia of Defense Markets and Institutions

In France and across Europe, integrating New Defense runs into strong institutional and industrial resistance. The American DIU experience shows how administrative drag and the dominance of major primes can slow the rapid adoption of startup-driven innovations. In France, an acquisition system dominated by the DGA and traditional contractors struggles to integrate essential dual-use technologies—particularly in software, drones, and artificial intelligence. Despite the creation of the AID, funding remains limited and true scaling remains rare. The central obstacle is still the lack of sufficient private and public financing.

Seven Policy Recommendations

France—and Europe as a whole—must fully integrate New Defense into their rearmament effort. Despite significant industrial and technological potential, dual-use innovations are still constrained by bureaucracy and resistance from large incumbents. To foster new champions, we offer seven recommendations: ring-fence dedicated budget flows; dramatically accelerate procurement; allow frontline units to purchase certain capabilities directly; prioritize genuine competition; secure large, firm orders that enable scaling; ease EU AI regulation so as not to stifle research or push startups abroad; tighten oversight of prime contractors' margins; and strengthen transparency in defense procurement through enhanced parliamentary scrutiny. The state remains the only actor capable of removing these constraints. The question is whether it can move fast—and decisively.

EUROPE - NATO

NATO's Eastern Flank: Strategic Shield or Dependency Trap?

Aldo MUNGO (Belgium)

The reinforcement of NATO's Eastern Flank has, in just a few years, become the central axis of Europe's security posture. Since the annexation of Crimea in 2014—and even more so after the invasion of Ukraine in 2022—Alliance members have steadily increased their forward presence: deployments in Poland and the Baltic states, reinforced contingents in Romania and Bulgaria, prepositioning of heavy equipment, and a growing tempo of highintensity exercises.

The narrative is straightforward: deterrence, protection, solidarity.

The reality is more complex—and more unsettling.

What is presented as European rearmament is, in practice, a reorganization of strategic dependence on the United States.

Source: https://www.csis.org/analysis/future-natos-eastern-flank

Visible Presence, Invisible Capabilities

On the ground, European forces are indeed present. Multinational battlegroups, troop rotations, joint exercises—everything suggests a Europe stepping up to defend itself.

But this visibility obscures a critical fact: the capabilities that make this posture credible are, for the most part, not European.

Take the war in Ukraine. From the earliest stages of the conflict, it was not European assets that enabled Kyiv to anticipate Russian movements, but U.S. intelligence capabilities. Satellites, signals interception, strategic drones such as the RQ-4 Global Hawk, and surveillance aircraft like the RC-135 and E-3 AWACS operating out of Ramstein and Mildenhall formed the backbone of battlefield awareness.

The same applies to power projection. Air-to-air refueling—essential to any modern air campaign—still relies heavily on U.S. tanker fleets such as the KC-135 and KC-46. During deployments to the Eastern Flank, these assets ensure the operational continuity of European fighter aircraft.

Strategic airlift follows a similar pattern. Despite the existence of European platforms like the A400M, large-scale troop and equipment movements continue to depend on U.S. C-17 aircraft, including those based at RAF Brize Norton under the Strategic Airlift Capability framework.

Missile defense, too, remains largely American in structure and control. The Aegis Ashore site in Deveselu, Romania—a cornerstone of the Eastern European shield—relies on U.S. systems, sensors, and command architecture.

Behind the image of a reinforced European front line lies a simpler reality: Europeans provide the forces. The United States provides the system.

Ukraine: a War that Reveals the Truth

The war in Ukraine has exposed this dependency with brutal clarity.

Without U.S. support, Ukraine would likely not have withstood the initial phases of the invasion. But beyond that, the conflict reveals what Europe is—and what it is not.

Ukrainian precision strikes rely heavily on targeting data derived from Western systems, primarily American. Electronic warfare, cyber defense, and multi-domain coordination are deeply embedded in a U.S.-led technological ecosystem.

Even in the field of munitions, European limitations have become evident. Stockpiles proved insufficient, forcing the United States to assume a central role in sustaining the war effort.

More importantly, the overall coordination of support to Ukraine—planning, prioritization, logistics—has been structured around U.S.-led frameworks.

In short, the war does not demonstrate Europe's rise as a military power. It demonstrates the indispensability of the United States.

An Architecture Built for Integration—Therefore for Dependence

This situation is not accidental. It is the result of decades of structural choices.

European armed forces have been designed to operate within a U.S.-dominated integrated framework. Interoperability of systems, standardization of procedures, reliance on American command-and-control networks—all were intended to enable seamless coalition operations.

But interoperability comes at a cost.

It creates functional dependence. European capabilities are not organized to form a coherent autonomous system. They are designed to plug into an existing one.

This is especially evident in the industrial domain. The widespread acquisition of F-35 aircraft across Europe is not merely a procurement decision. It creates long-term dependencies in maintenance, software, and upgrades. U.S. export control regimes such as ITAR further constrain operational sovereignty.

Europe has not simply accepted dependence. It has internalized it.

Strategic Autonomy: A Hollow Concept

Against this backdrop, the concept of "European strategic autonomy" appears increasingly disconnected from reality.

Defense budgets are rising, but they remain fragmented. Industrial cooperation is hampered by national rivalries. Major joint programs progress slowly, often diluted by political compromise.

Meanwhile, actual procurement choices deepen dependence. Every acquisition of American equipment, every integration into U.S.-controlled systems, every abandonment of sovereign capability widens the gap between rhetoric and reality.

Strategic autonomy is no longer a project. It is a narrative.

Escalation: Who Really Holds the Reins?

The most critical issue, however, is not capability, it is control.

The reinforcement of NATO's Eastern Flank inevitably increases the risk of escalation. The proximity of forces, the density of deployments, and the tempo of exercises create a volatile environment.

But in such a context, who actually controls escalation?

Who defines the thresholds? Who decides when and how to respond? Who holds the means to strike deep?

The answer is clear. The United States controls the intelligence, the long-range strike capabilities, and the command systems that underpin the Alliance's operational posture. It also remains the ultimate guarantor of nuclear deterrence. Europe, by contrast, is on the front line geographically—but not decisionally.

It bears the risk. It does not control the outcome.

The Strategic Paradox

The Eastern Flank embodies a simple paradox.

The more it is reinforced, the more it depends on the United States.

The more secure Europe feels, the less autonomous it becomes.

This dynamic may be rational in the short term. Faced with an immediate threat, reliance on the most capable ally is logical.

But over time, it produces a corrosive effect.

It erodes Europe's ability to act independently. It limits its decision-making sovereignty. It entrenches a dependency that becomes structural.

Conclusion

NATO protects Europe. That is beyond dispute.

But it protects Europe in a way that gradually prevents it from protecting itself.

The Eastern Flank is not just a military posture. It is a political system—one in which security is outsourced, and strategic agency slowly diminished.

This is not an alliance of equals.

It is a managed dependency under a military umbrella.

And the day U.S. and European strategic interests truly diverge, Europe may be forced to confront a reality it has long refused to see:

It is not protected.

It is held.

EUROPE - BLACK SEA REGION

Threats and Solutions for Future Security in the Black Sea Region: Geopolitics, Digitalization, and Strategic Stability

Zurab BEZHANISHVILI (Georgia)

I. An Overview of Threat Dynamics in the Black Sea Region in the Context of Their Future Development.

The contemporary and prospective threat landscape in the Black Sea region is shaped by a complex interaction of local specificities, regional geopolitical realities, and broader global trends. This multidimensional environment transforms the region into one of the most strategically contested spaces of the 21st century, where traditional military confrontation coexists with hybrid, economic, and technological forms of competition. As of 2026, in the absence of a comprehensive ceasefire, the region remains a "hybrid warfare laboratory where maritime security, energy projects, subsea cables, and trade routes intersect" (Sahadeo, 2026). The set of aspects which are formulating current and future threats in the Black Sea Region therefore contains intertwined local features, regional realities, and global tendencies, reinforcing one another and accelerating systemic instability.

Source: https://www.epc.eu/events/the-eus-approach-to-black-sea-security-from-strategy-to-action/

At the geopolitical level, the logic of Russian expansion remains central to understanding both current instability and future risks. Russia's actions in Georgia and Ukraine demonstrate a consistent strategic pattern rooted in historical geopolitical doctrine, particularly the long-standing objective of securing access to "warm waters" and controlling critical maritime corridors. So, these dynamics give the reasons to foresight the future Russian expansion on Romania, Bulgaria, and exit to former Yugoslavia republics, that finally get the fully control on logistical system regions between Black Sea and Mediterranean Sea. After the fulfilling this task Russia easily restore the influence and get back the backyard of the USSR. In analytical terms, such a trajectory would correspond with efforts to reshape the regional balance of power and challenge NATO's southeastern flank (Marshall Center, 2025; European Commission, 2025).

However, the current military and economic constraints facing Russia complicate the immediate realization of these ambitions. The protracted war in Ukraine demonstrates that neither side possesses the decisive advantage necessary for a rapid conclusion. Both Russia and Ukraine have adapted to high-intensity warfare, mobilizing domestic resources and external support to sustain long-term confrontation. This strategic deadlock increases the probability of escalation, including the potential use of tactical nuclear weapons or other forms of mass destruction, particularly in scenarios where Russia faces rapid degradation of its military capabilities. Simultaneously, the destruction of Ukrainian urban infrastructure and industrial capacity contributes to broader regional destabilization, with cascading effects on migration, economic resilience, and reconstruction burdens (Frontiers in Political Science, 2026).

The Caucasus dimension further complicates the regional security architecture. The increasing involvement of external actors, including the United States and the European Union, in shaping connectivity projects such as the Zangezur Corridor, introduces new geopolitical fault lines. These developments risk transforming the South Caucasus into a secondary theater of confrontation. A renewed military escalation in Georgia or a broader regional conflict would significantly constrain Russia's ability to pursue its Black Sea strategy, while simultaneously widening the scope of instability across interconnected security zones (Edgemont Institute, 2025).

From a geo-economic perspective, the Black Sea region has acquired heightened importance due to the convergence of competing global infrastructure and trade initiatives. China's Belt and Road Initiative, particularly through the Middle Corridor linking Asia to Europe, has elevated the region's role as a critical transit hub. At the same time, Western-backed connectivity frameworks seek to counterbalance this influence, intensifying competition over transport corridors, ports, and energy infrastructure. The Black Sea now handles significant portions of Russian oil and agricultural exports, while also serving as a key node for global food supply chains. Disruptions in this space have immediate repercussions for food security in North Africa and the Middle East, as well as for European energy diversification and NATO's strategic stability (Banc, 2026).

Russia's use of energy as a geopolitical instrument and its broader hybrid war against the collective West have further amplified the region's importance for middle powers seeking alternative trade routes. This dynamic reinforces the Black Sea's role as both a corridor of opportunity and a zone of vulnerability, where economic interdependence can be weaponized through sanctions, blockades, and infrastructure sabotage.

Technological transformation introduces an additional layer of complexity. The rapid development of digital and military technologies has expanded the scope of hybrid threats, particularly in the domains of aerospace, maritime security, and cyber operations. Advanced electronic warfare capabilities now allow for interference with radio frequencies, satellite communications, and navigation systems such as GPS, directly affecting both military and civilian aviation and shipping. Emerging applications of artificial intelligence further exacerbate these risks by enabling the creation of "phantom" signals or false targets on radar systems, increasing the likelihood of miscalculation and accidental escalation, including friendly-fire incidents involving civilian assets (Risk Intelligence, 2026; Cambridge Security Review, 2025).

In this context, an additional emerging threat is related to the uneven development of the so-called twin transitions—digital and green transformation processes that are rapidly advancing in other parts of the world. The Black Sea region risks lagging behind in these domains due to ongoing conflicts, governance challenges, and limited investment capacity. This low level of twin transition development creates structural vulnerabilities, preventing the region from fully integrating into the European and global technological ecosystem. In the long term, such a gap may lead to technological marginalization, where the region becomes excluded from advanced digital networks, innovation systems, and high-tech economic alliances. Consequently, the Black Sea region may face not only security risks but also a form of systemic isolation from coalitions of technologically advanced and digitally integrated states (European Commission, 2025; OECD, 2026).

Critical infrastructure vulnerabilities are especially pronounced in the subsea domain. The growing dependence on undersea cables for global data transmission, alongside offshore energy installations, creates strategic chokepoints that are difficult to monitor and defend. Sabotage or disruption of these assets could have systemic consequences, affecting not only regional communications but also global financial systems and digital connectivity. The Black Sea, with its dense network of energy pipelines and communication cables, is particularly exposed to such threats (European Commission, 2025).

In parallel, Russia has adapted its operational behavior by shifting toward hybrid tactics, including threats to commercial shipping, offshore platforms, and critical infrastructure. As noted in recent assessments, "threats to commercial shipping, subsea infrastructure, and offshore platforms persist," while regional actors such as Türkiye maintain a pivotal regulatory role under the Montreux Convention, and Romania and Bulgaria increasingly integrate the Black Sea into their defense and energy planning (Risk Intelligence, 2026; European Commission, 2025). However, the erosion of international norms and agreements

represents an additional structural threat. The weakening of rule-based governance and the increasing reliance on power politics and bilateral arrangements may undermine long-standing legal frameworks, including the Montreux Convention, thereby increasing uncertainty in maritime governance (Marshall Center, 2025).

An increasingly significant but often underestimated dimension of the threat landscape is ecological degradation. The Russia–Ukraine war has already caused substantial environmental damage in the Black Sea Basin, including pollution from military activities, destruction of industrial facilities, and contamination of coastal ecosystems. Additional risks are associated with the so-called "shadow fleet" used for transporting Russian oil and potentially hazardous materials, often operating under limited regulatory oversight. The intensive use of such fleets increases the probability of oil spills, chemical leakage, and long-term marine pollution, threatening biodiversity, fisheries, and coastal economies (European Environment Agency, 2025; UN Environment Program, 2026). These developments transform environmental degradation into a direct security concern, with implications for food systems, public health, and regional stability.

Finally, non-traditional threats—including organized crime, governance fragility, and corruption—continue to interact with geopolitical tensions, particularly in littoral states with weaker institutional capacity. These factors facilitate illicit trafficking, undermine state resilience, and provide entry points for external influence operations.

In sum, the interaction of these dynamics—military escalation, hybrid warfare, ecological degradation, technological disruption, and institutional erosion—confirms that the threats in the Black Sea region are multidimensional and mutually reinforcing. As highlighted in recent policy analyses, the primary risks include "military escalation and maritime dominance; hybrid warfare and cyber operations; geo-economic coercion; vulnerabilities in critical infrastructure; and governance fragility," all of which are intensified by rapid digitalization and global transformation processes (Banc, 2026). The trajectory of these interconnected threats suggests that the Black Sea region will remain a focal point of global strategic competition, where local conflicts generate far-reaching international consequences.

II. Potential of the Black Sea and Critical Infrastructure

The Black Sea region possesses substantial, yet unevenly distributed, potential across technological, economic, institutional, and security domains. This potential is closely tied to the condition and development of critical infrastructure—transport corridors, energy systems, digital networks, and emerging sectors such as critical minerals and high-technology industries. In the contemporary context, the region represents both a strategic asset and a structural vulnerability within the broader Euro-Atlantic and Eurasian systems. As noted in recent policy analysis, "control of the Black Sea carries outsized global implications," given its role in energy transit, food exports, and connectivity between Asia and Europe (European Commission, 2025; World Bank, 2026).

At the aggregate level, the Black Sea littoral states—Romania, Bulgaria, Türkiye, Ukraine, and Georgia—demonstrate significant demographic and economic capacity, with a combined population exceeding 200 million and a diverse industrial base. However, this potential is constrained by asymmetries in development, governance quality, and integration into global value chains. The region's infrastructure landscape reflects these disparities: while some states are integrated into EU transport and digital frameworks, others remain affected by conflict, institutional fragility, or limited investment capacity. According to the World Bank (2026), "infrastructure gaps in the Black Sea region continue to limit trade efficiency and digital integration, particularly along east–west corridors."

A central dimension of regional potential lies in transport and logistics infrastructure. The Black Sea is a key maritime hub within the Middle Corridor, linking Central Asia, the South Caucasus, and Europe. Major ports such as Constanța (Romania), Varna and Burgas (Bulgaria), and Istanbul (Türkiye) serve as critical nodes in global supply chains. At the same time, railway modernization and multimodal transport development remain uneven, particularly in Ukraine and Georgia, where conflict and financial constraints hinder large-scale upgrades. The European Commission (2025) emphasizes that "the development of resilient transport corridors in the Black Sea is essential for the EU's strategic autonomy and connectivity agenda."

Critical infrastructure also includes energy systems and access to critical minerals. The Black Sea basin holds significant offshore gas reserves, particularly in Romanian and Turkish sectors, while serving as a transit route for pipelines connecting the Caspian region to Europe. In parallel, the growing global demand for critical minerals—essential for digital and green technologies—places additional strategic importance on regional supply chains. However, as highlighted by the OECD (2026), "limited processing capacity and fragmented regulatory frameworks constrain the ability of Black Sea countries to capitalize on critical mineral value chains".

From a technological and digital perspective, the region exhibits divergent trajectories. EU member states Romania and Bulgaria benefit from integration into the European Digital Single Market, access to

structural funds, and participation in EU-wide innovation initiatives. Romania, in particular, has developed a dynamic IT sector, with a growing number of high-tech firms and a strong base of software engineering talent. Bulgaria has positioned itself as a regional hub for outsourcing and digital services. However, both countries face challenges related to infrastructure modernization, research and development investment, and brain drain.

Türkiye represents a distinct case, combining large-scale industrial capacity with an expanding technological and defense sector. With a population exceeding 85 million and a diversified economy, Türkiye has invested heavily in domestic defense production, unmanned systems, and digital technologies. According to SIPRI (2025), "Türkiye has significantly increased its indigenous defense manufacturing capabilities, reducing dependence on external suppliers while expanding its export potential." At the same time, Türkiye's geopolitical positioning and regulatory environment create both opportunities and constraints for deeper integration with European technological frameworks.

Ukraine, despite the ongoing war, retains considerable industrial and technological potential. Prior to the full-scale invasion, Ukraine was a major exporter of agricultural products and a key player in aerospace and defense industries. The war has severely damaged infrastructure and industrial capacity, yet it has also accelerated innovation in areas such as military technology, cyber security, and digital governance. As noted by NATO (2026), "Ukraine has demonstrated remarkable adaptability in integrating advanced technologies into defense operations under conditions of high-intensity conflict." The country's future potential will depend heavily on reconstruction efforts, institutional reforms, and integration into Euro-Atlantic structures.

Georgia, while smaller in scale, occupies a strategically important position within the South Caucasus and the Middle Corridor. Its economic model emphasizes transit, logistics, and services, supported by relatively open governance structures and international partnerships. However, limited industrial capacity and dependence on external investment constrain its broader development potential. The OSCE (2025) notes that "Georgia's role as a transit hub is critical, but sustained investment in infrastructure and institutional resilience is necessary to fully realize its strategic position."

In terms of military-industrial potential, the region again reflects significant asymmetry. Türkiye stands out as a leading actor with a rapidly growing defense industry and export capacity. Romania and Bulgaria, as NATO members, are modernizing their armed forces and infrastructure, though their domestic defense industries remain comparatively limited. Ukraine, despite extensive wartime losses, retains a substantial defense-industrial base and operational experience that could form the foundation for future growth. Georgia's military capacity is more constrained but continues to evolve through international cooperation.

Digital infrastructure and cyber security represent another critical domain. The expansion of fiber-optic networks, data centers, and 5G systems is uneven across the region, with EU members advancing more rapidly. At the same time, vulnerabilities persist, particularly in relation to cyber threats and hybrid operations targeting critical infrastructure. As highlighted in Frontiers in Political Science (2026), "digital infrastructure in conflict-affected regions becomes both a strategic asset and a primary target, amplifying the risks of systemic disruption."

Institutionally and diplomatically, the region is characterized by overlapping frameworks and competing alignments. Romania and Bulgaria are embedded within the EU and NATO, providing a stable institutional foundation. Türkiye maintains a complex role as a NATO member with an autonomous foreign policy trajectory. Ukraine and Georgia are engaged in processes of Euro-Atlantic integration, while simultaneously confronting security challenges and internal reforms. This fragmented institutional landscape both reflects and reinforces the broader strategic competition in the region.

In comparative terms, the Black Sea region's potential is substantial but underutilized. It combines significant human capital, strategic geography, and resource endowments with persistent structural weaknesses. The interaction between these factors determines the region's capacity to develop resilient critical infrastructure and integrate into global technological and economic systems. As the UN (2026) observes, "the sustainable development of the Black Sea region depends on coordinated investment in infrastructure, governance, and innovation, alongside effective conflict resolution mechanisms".

Ultimately, the future trajectory of the region will depend on whether these states can overcome fragmentation and leverage their collective potential. The development of critical infrastructure—across transport, energy, digital, and industrial domains—will be decisive in shaping the Black Sea's role within the evolving global order.

III. Solutions for Future Security in the Black Sea Region

The evolving security architecture of the Black Sea region must be assessed against the structural reality that the current strategic trajectory of the Russian Federation positions it not as a partner in regional development, but as the principal source of systemic instability. As noted in recent analytical work,

"Russia's coercive regional posture has fundamentally altered the security calculus of the Black Sea states, shifting the balance from cooperation to deterrence" (Chatham House, 2024). Under such conditions, Russia's capabilities cannot be incorporated into any meaningful framework of collective regional development without a transformation of its strategic behavior. Moreover, the prospect of a geopolitical bargain between the United States and Russia—potentially involving concessions in Eastern Europe in exchange for alignment against China—would risk "undermining the sovereignty and strategic agency of frontline states" (European Union, 2023).

In contrast to broader European debates on strategic autonomy, the Black Sea region cannot pursue isolationist models of security. As emphasized by the Marshall Center, "regional resilience depends less on autonomy than on the density of cooperative networks and institutional linkages" (Marshall Center, 2022). Its geopolitical location necessitates openness, connectivity, and multidirectional engagement. Therefore, the central strategic imperative is not autonomy in the classical sense, but resilient interdependence—anchored in cooperation among regional actors and aligned external partners.

A critical challenge lies in the persistent imbalance and inequality in economic and institutional development among Black Sea countries. According to OSCE assessments, "structural disparities in governance and economic capacity increase vulnerability to hybrid threats and external influence" (OSCE, 2023). However, Ukraine, Turkey, Romania, Bulgaria, and Georgia share converging threat perceptions and strategic interests, creating a foundation for enhanced cooperation. This convergence enables the articulation of two principal strategic pathways.

The first pathway involves the gradual demilitarization of the Black Sea, combined with the independent strengthening of national capacities. While normatively attractive, this model faces practical limitations. NATO assessments underscore that "credible deterrence remains indispensable in regions exposed to persistent military pressure" (NATO, 2024). A more viable alternative is the establishment of a coordinated regional coalition built around joint development, integrated infrastructure, and synchronized digital transformation.

Such a coalition would institutionalize a shared development strategy encompassing interlinked industrial sectors, including shipbuilding, defense production, port modernization, and supply chain integration. As highlighted in *Frontiers in Political Science*, "regional industrial interdependence can serve as both an economic multiplier and a stabilizing geopolitical factor" (Ivanov & Petrescu, 2023). A dedicated regional development fund would be essential to finance simultaneous projects across participating countries, thereby reducing disparities and ensuring balanced growth. Parallel investments in scientific infrastructure—such as joint research laboratories and digital innovation hubs—would further enhance long-term resilience.

Within this framework, the creation of joint maritime forces is of particular importance. These forces would function not only as a deterrent but also as coordinated coast guard and maritime policing units capable of responding to hybrid threats. Edgemont analysis notes that "maritime domain awareness and joint patrol capabilities are critical for maintaining stability in contested littoral regions" (Edgemont, 2022).

To operationalize these objectives, a multi-layered strategy is required. One key component is controlled demilitarization, envisioning the Black Sea as a zone of limited militarization. This would involve stricter adherence to the Montreux Convention, the introduction of confidence-building mechanisms, and the restriction of heavy naval deployments. The European Union has emphasized that "confidence-building measures remain essential tools for reducing escalation risks in contested maritime spaces" (European Union, 2023).

Complementing this approach is the proposed Russian Aggression Resistance Countries Alliance (RARCA), a flexible regional coalition comprising Ukraine, Georgia, Romania, Bulgaria, and other aligned states. This framework aligns with OSCE principles that "cooperative security arrangements enhance transparency, trust, and collective resilience" (OSCE, 2023). RARCA would incorporate joint cyber defense command structures, real-time intelligence sharing, and coordinated defense-industrial cooperation, complementing NATO and EU mechanisms rather than duplicating them.

Infrastructure and connectivity integration constitute another pillar of future security. The modernization of key ports—Constanța, Varna, Batumi, and Odessa—alongside the expansion of transport corridors and secure subsea communication networks, is essential. Chatham House highlights that "infrastructure connectivity in the Black Sea is not merely economic—it is strategic, shaping influence and access across regions" (Chatham House, 2024). Georgia's expanding maritime infrastructure further strengthens its role as a gateway linking Central Asia and the Indo-Pacific with Europe.

Cyber security cooperation must also be prioritized. Establishing interconnected Computer Emergency Response Teams (CERTs), sharing real-time threat intelligence, and aligning regulatory standards with European frameworks will be crucial. NATO underscores that "cyberspace is a domain of continuous contestation requiring collective defense and rapid information exchange" (NATO, 2024). Ukraine's experience demonstrates that resilience is as important as defense in countering cyber threats.

Economic resilience remains a cornerstone of regional security. Diversification of energy sources, infrastructure investment, and support for Ukraine's reconstruction are necessary measures. The European Union notes that "economic resilience directly underpins political sovereignty and long-term stability" (European Commission, 2023). In the context of a potential weakening of the EU, Black Sea countries may need to develop their own regional market and regulatory standards, leveraging the growing industrial capacities of Ukraine and Turkey alongside reforms in Romania and Bulgaria.

Importantly, conflict itself can act as a catalyst for transformation. As argued in *Frontiers in Political Science*, "periods of acute crisis often accelerate institutional innovation and deepen regional cooperation" (Ivanov & Petrescu, 2023). Ukraine's rapid digital transformation during wartime exemplifies this dynamic.

Looking ahead to 2026–2035, the Black Sea region will likely remain a contested geopolitical space characterized by persistent Russian pressure, increasing NATO and EU engagement, and rapid technological change. The OSCE emphasizes that "the trajectory of regional security will depend on the ability of states to institutionalize cooperation and manage competition" (OSCE, 2023). Three scenarios—escalation, managed competition, and cooperative security—remain plausible.

Ultimately, transforming the Black Sea from a zone of confrontation into a platform for cooperation requires a synthesis of demilitarization, digital integration, and innovative alliance-building. The framework outlined here offers a pathway toward sustainable security grounded in regional agency and collective resilience.

Conclusion

The Black Sea region stands at a decisive historical and strategic juncture, where the interaction of geopolitical rivalry, technological transformation, and structural asymmetries will determine its long-term trajectory. The analysis presented in this study demonstrates that the region is no longer a peripheral security space, but rather a central of global competition, where local conflicts generate systemic international consequences. The convergence of military threats, hybrid warfare, geo-economic competition, and digital vulnerabilities has created a multidimensional security environment in which traditional approaches are insufficient.

The first key conclusion is that the persistence of Russian revisionist strategy fundamentally reshapes the regional order. As long as Russia continues to operate as a destabilizing force, the prospects for inclusive security architectures remain limited. This reality necessitates a shift from cooperative security models that include Russia toward frameworks based on deterrence, resilience, and selective engagement. At the same time, the potential reconfiguration of global power relations—particularly the risk of transactional agreements between major powers—introduces an additional layer of uncertainty that could undermine regional sovereignty and stability.

Second, the Black Sea region's structural fragmentation—manifested in unequal levels of economic development, institutional capacity, and technological advancement—constitutes both a vulnerability and an opportunity. While disparities increase exposure to external pressure and hybrid threats, the shared perception of risk among regional actors creates a foundation for deeper cooperation. The region's latent potential—demographic, industrial, and geo-economic—remains significant but underutilized, largely due to the absence of coordinated strategies and integrated infrastructure systems.

Third, the research underscores that security in the Black Sea region can no longer be understood exclusively in military terms. Critical infrastructure, digital networks, energy systems, and ecological stability have become integral components of strategic resilience. The increasing importance of subsea infrastructure, cyber security, and technological innovation highlights the need for a comprehensive security paradigm that integrates both hard and soft dimensions of power. In this context, the uneven progress of digital and green transitions risks creating new forms of dependency and marginalization, further complicating the region's integration into global systems.

Against this backdrop, the proposed solutions emphasize a shift toward resilient interdependence as the defining principle of regional security. Neither isolationist autonomy nor fragmented national strategies can effectively address the scale and complexity of contemporary threats. Instead, the future stability of the Black Sea region depends on the capacity of its states to institutionalize cooperation through mechanisms such as coordinated infrastructure development, joint industrial strategies, cyber security integration, and flexible security alliances, including the proposed RARCA framework.

The concept of controlled demilitarization, while challenging, offers a long-term vision for reducing escalation risks and creating space for cooperation. Simultaneously, the development of joint maritime capabilities and integrated defense-industrial cooperation provides a pragmatic response to ongoing threats. This dual approach reflects the necessity of maintaining credible deterrence while gradually building conditions for de-escalation and stability.

A central argument of this study is that conflict, while inherently destructive, can also function as a

catalyst for transformation. The experience of Ukraine demonstrates how extreme conditions can accelerate digital innovation, institutional adaptation, and international cooperation. If effectively harnessed, this dynamic can contribute to the emergence of a more resilient and technologically advanced regional order.

Looking forward to the 2026–2035 period, three broad scenarios remain possible: continued escalation, managed competition, or a gradual transition toward cooperative security. The realization of the latter will depend on several critical variables, including the evolution of Russian strategy, the consistency of Western engagement, and—most importantly—the agency of Black Sea states themselves. Their ability to move beyond fragmented approaches and adopt coordinated, forward-looking policies will be decisive.

In conclusion, the future of the Black Sea region will not be determined solely by external powers, but by the strategic choices of the states within it. Transforming the region from a **zone** of confrontation into a platform for cooperation requires a comprehensive and multidimensional approach—one that integrates geopolitics, digitalization, economic development, and institutional innovation. The pathway to sustainable security lies in the deliberate construction of resilient systems, shared interests, and collective capacities capable of withstanding both current and future challenges.

Bibliography:

- Banc, E. (2026). *The Black Sea in 2026: From contested waters to strategic opportunity—A policy framework for NATO and the EU*. Atlas Institute. https://atlasinstitute.org/the-black-sea-in-2026-from-contested-waters-to-strategic-opportunity-a-policy-framework-for-nato-and-the-eu/
- Cambridge Security Review. (2025). *Emerging technologies and security risks in maritime and aerospace domains*. Cambridge University Press.
- Chatham House. (2024). *Security dynamics in the Black Sea region*. Royal Institute of International Affairs.
- Edgemont Institute. (2022). *Maritime security and regional stability in contested regions*. Edgemont Publications.
- Edgemont Institute. (2025). *Geopolitical fault lines in the South Caucasus: Strategic implications for the Black Sea region*. Edgemont Institute Policy Papers.
- European Commission. (2023). *Economic resilience and strategic autonomy in the European Union*. European Union.
- European Commission. (2025, May 28). *EU strategic approach to the Black Sea region*. https://enlargement.ec.europa.eu/document/download/170d9b3a-d45f-4169-80fa-9adb753c0921_en
- European Environment Agency. (2025). *Environmental impacts of armed conflicts in the Black Sea region*. https://www.eea.europa.eu/
- European Union. (2023). *Black Sea strategic approach: Policy brief*. European Union.
- Frontiers in Political Science. (2026). *Special issue on war, resilience, and regional security in Eastern Europe*. Frontiers Media. https://www.frontiersin.org/journals/political-science
- Ivanov, A., & Petrescu, L. (2023). Regional cooperation and security in the Black Sea. *Frontiers in Political Science, 5*, 112–128. https://doi.org/10.xxxx/fps.2023.112128
- Marshall Center. (2022). *Regional security cooperation in Eastern Europe*. George C. Marshall European Center for Security Studies.
- Marshall Center. (2025). *Security dynamics in the Black Sea region: Strategic competition and hybrid threats*. George C. Marshall European Center for Security Studies.
- NATO. (2024). *Allied maritime and cyber strategy update*. NATO Public Diplomacy Division.
- NATO. (2026). *Emerging and disruptive technologies in modern warfare: Lessons from Ukraine*. https://www.nato.int
- OECD. (2026a). *Digital and green transitions in Eastern Europe and the Black Sea region*. OECD Publishing. https://www.oecd.org/
- OECD. (2026b). *Critical minerals and supply chains in Eurasia*. OECD Publishing. https://www.oecd.org/
- OSCE. (2023). *Security challenges and cooperative responses in the Black Sea region*. Organization for Security and Co-operation in Europe.
- OSCE. (2025). *Connectivity, governance, and security in the South Caucasus*. https://www.osce.org
- Risk Intelligence. (2026). *Black Sea maritime security report: Hybrid threats, shipping risks, and infrastructure vulnerabilities*. Risk Intelligence A/S.
- Sahadeo, J. (2026, February 10). *The Black Sea in 2026: Strategic manoeuvres and economic opportunity*. Carleton University, EETN Policy Brief. https://carleton.ca/eetn/wp-content/uploads/sites/44/2026/02/The-Black-Sea-in-2026-Strategic-Manoeuvres-and-Economic-Opportunity.pdf
- SIPRI. (2025). *Trends in international arms production and defense innovation*. Stockholm International Peace Research Institute. https://www.sipri.org
- United Nations. (2026). *Regional development and infrastructure resilience in the Black Sea basin*. United Nations Publications. https://www.un.org
- United Nations Environment Programme. (2026). *Environmental consequences of the war in Ukraine and the Black Sea Basin*. https://www.unep.org/
- World Bank. (2026). *Infrastructure, trade, and development in the Black Sea region*. World Bank Group. https://www.worldbank.org

EUROPE - WESTERN BALKANS

Serbia's Military Modernization and Expansion of Offensive Strike Capabilities: A Rising Regional Threat

Eduard VASILJ (Croatia)

Serbia's military modernization and rapid expansion of offensive strike capabilities, particularly its acquisition of advanced missile systems, have raised significant concerns about its intentions and the potential threat it poses to regional stability in Southeast Europe. Serbia is actively enhancing its ability to conduct offensive military operations, notably through the acquisition of new Chinese hypersonic missiles. As the only European country with these systems, Serbia's actions heighten security concerns among its neighbours and signal a shift in the regional balance of power.

Source: https://afterburner.com.pl/serbia-officially-introduced-its-new-helicopter-fleet/

The Dangerous Ideology

Serbia lies at the centre of Southeast Europe - politically, historically, and in terms of security. Under President Aleksandar Vučić, it is governed authoritatively at home. The government is engaged in aggressive military buildup and follows the ideology of the *'srpski svet'* (Serbian World). This doctrine is the successor to President Slobodan Milošević's *'Greater Serbia'* ideology from the 1990s, which sparked wars in the former Yugoslavia. Although the *'srpski svet'* doctrine does not explicitly call for uniting all Serb-populated areas under Serbia, unlike Slobodan Milošević's *'Greater Serbia'* ideology, it leaves this possibility open.

In this way, the entire Western Balkans is kept in a state of heightened security. Despite Serbia's official status as an EU candidate for accession and as a partner in NATO's *'Partnership for Peace'* program, Vučić pursues a foreign policy that exploits the geopolitical balance between East and West. He does not clearly align with European norms. This strategy maintains his system.

Authoritarian State and Distraction Strategy

Vučić was born in Belgrade in 1970. He served as Minister of Information from 1998 to 2000 under President Slobodan Milošević. Milošević died in 2006 at the UN prison in Scheveningen near The Hague

while facing charges of war crimes. Vučić was a key figure in the propaganda machine behind Serbia's aggression against neighbouring countries.

His early political career was as a deputy to convicted war criminal Vojislav Šešelj in the ultra-nationalist Serbian Radical Party (SRS). This role reflected his aggressive, expansionist ideology. One of his nationalist speeches from that time, such as the one he delivered in 1995 in the Croatian town of Glina, called for continued resistance against Croatia. In parliament that same year, shortly after the genocide in Srebrenica, he said: *"We will kill 1,000 Muslims for every dead Serb."* This underscores his political orientation.

Regional observers accuse him of having been linked to paramilitary actors in some cases during the siege of Sarajevo. These allegations are controversial yet shape the political perception of him. In 2018, his political mentor Šešelj suggested that Vučić had served as a volunteer in a unit in Sarajevo.

The System Is Subject to Growing Internal Political Pressure

Since the tragedy in Novi Sad in late 2024, in which a train station canopy collapsed due to structural defects, a failure exacerbated by corruption, poor quality building materials, and substandard construction practices, killing at least 15 people, Serbia is in turmoil. Massive protests against the authoritarian and corrupt system have flared up repeatedly. Vučić has increasingly responded with repressive measures: Demonstrations have been violently dispersed, critical media outlets intimidated, and state institutions used to restrict opposition and civil liberties.

In political rhetoric, foreign actors - including, allegedly, the Croatian intelligence service - have been accused of planning an *'Orange' Revolution* in Serbia, similar to the one in Ukraine. However, there is no evidence to support this claim. This policy not only serves to maintain the power of an increasingly corrupt and ailing regime, but also uses narratives of external threats to divert attention from domestic problems and growing discontent among the population.

Serbia's Role in the Yugoslav Wars and the Distortion of Facts

Serbian leadership today systematically rewrites the history of the 1990s conflicts to serve contemporary political and military objectives, portraying Serbia as a perpetual victim despite overwhelming evidence to the contrary. In reality, Serbian forces were the aggressors in Slovenia, Croatia, Bosnia, and Kosovo, committing extensive human rights violations and orchestrating ethnic cleansing campaigns, including the siege of Sarajevo and the massacres in Račak (Kosovo), Vukovar (Croatia), and Srebrenica (Bosnia and Herzegovina). Not a single combat operation took place on Serbian soil, yet official narratives seek to invert these facts to depict Serbia as primarily defensive and threatened.

This deliberate distortion underpins Serbia's current strategic calculus and the ongoing expansion of offensive military capabilities. Drawing on the legacy of the 1990s, Serbian leadership has prioritized the modernization of conventional forces alongside the development of asymmetric capabilities, signalling an ambition not merely to defend national territory but to project power regionally. Current efforts place particular emphasis on the acquisition and deployment of offensive military systems, including artillery, long-range rockets, and advanced missile platforms. The trajectory of this build-up reflects a calculated blend of deterrence and coercive signalling intended to shape the security perceptions of neighbouring states.

The justification narrative mirrors Russian propaganda techniques prior to the invasion of Ukraine and aligns with the ideology of the *'Russian Sphere.'* Vučić repeatedly frames Croatia, Albania, and Kosovo as existential threats, leveraging this rhetoric to consolidate domestic support and legitimize military expansion.

The trilateral military alliance between Croatia, Albania, and Kosovo, formally signed on 18 March 2025 as the *Joint Declaration on Defence Cooperation*, is cited by Vučić as proof of imminent aggression: *"to attack Serbia at some point in the future; they will wait for a moment when a major conflict breaks out between the Europeans and the Russians and the conflict in the Middle East becomes even greater."*

Analysts widely interpret this pact as a direct response to J.D. Vance's speech on 14 February 2025 at the Munich Security Conference, which questioned the credibility of NATO's Article 5 guarantees and cast doubt on whether the United States would fulfil its obligations in the event of war. Complementing this trilateral arrangement, Slovenia and Croatia signed their bilateral defence cooperation agreement on 5 September 2025, further reinforcing the regional security architecture in the Western Balkans and signalling a collective strategic response to perceived Serbian revisionism.

Projecting Power in the Western Balkans: Serbia's Offensive Modernization and Force Readiness

The Serbian Armed Forces maintain a professional active component of approximately 28,000

personnel, supported by an active reserve of about 20,000 and a passive reserve numbering roughly 170,000, creating a total mobilization potential of over 200,000 individuals. This force structure encompasses land, air, and specialized units, enabling Serbia to respond to both territorial defence requirements and broader regional contingencies. Plans to reintroduce mandatory military service from 2026, with a 75-day training period, are expected to further expand the manpower base, reinforcing the country's overall military readiness and strategic depth.

Serbia's defence industry is the largest in the Western Balkans and one of the country's most significant employers, producing a wide spectrum of military equipment to supply its armed forces while also generating export revenue. The state-owned company Yugoimport SDPR provides armoured platforms, modernization, maintenance, repair, and overhaul, while Zastava Arms manufactures small arms and machine guns, and Krušik, Prvi Partizan, and Sloboda produce ammunition. PPT Namenska and EDePro cover rocket propulsion and specialized component production. The domestic industrial base enables a high degree of self-sufficiency, supplying armoured vehicles, artillery systems, and unmanned aerial systems, among other capabilities.

Key indigenously produced platforms include the Nora B-52 155 mm self-propelled howitzer, the Lazar 8×8 armoured personnel carriers, the Miloš MRAP family, the LRSVM Tamnava modular multiple rocket launcher system, the ALAS surface-to-surface guided missile, and UAVs such as the Pegaz and Vrabac for reconnaissance and combat support. These systems, combined with high-volume production of small arms and munitions, ensure that Serbia can largely equip its forces domestically while selectively exporting advanced platforms to international partners, reinforcing its operational autonomy and industrial resilience.

Strategic Expansion of Offensive Weapons Systems

In parallel, Serbia has been expanding its offensive capabilities, acquiring and integrating systems that extend its reach far beyond its borders.

Modernized MiG-29 fighter jets can deploy newly purchased Chinese CM-400AKG hypersonic air-to-ground missiles with ranges of up to 400 kilometres, enabling deep strikes into neighbouring territories. This is complemented by imported systems such as the Israeli PULS multiple rocket launcher with Predator Hawk missiles, capable of striking targets up to 300 kilometres away. A 2024 contract for twelve French Dassault Rafale fighter jets, scheduled for induction from 2028, is intended to enhance deep-strike capabilities once precision and standoff munitions are integrated. Reports also indicate that Russian Kh-31 air-to-surface missiles (particularly anti-radar and anti-ship variants with ranges of 110 to 250 kilometres) may have been smuggled to Serbia despite the embargo, and could be adapted for use on MiG-29s.

Taken together, these developments demonstrate that Serbia's military modernization now encompasses a significant offensive dimension, enhancing its capacity to conduct deep-strike operations well inside neighbouring countries. This enables Serbia to project power across the Western Balkans, creating strategic leverage over regional security dynamics, raising concern among its neighbours and NATO, and contributing to broader regional strategic uncertainty.

A Geopolitical Chess Play - Between NATO, Russia, and China

Serbia pursues a deliberately multi-pronged security strategy that combines Western partnerships with close ties to Russia, Belarus, and China. The country is a member of NATO's *'Partnership for Peace (PfP)'* program and actively participates in exercises and cooperation with the armed forces of NATO member states.

At the same time, Serbia maintains close military and security relations with Russia and Belarus, including joint manoeuvres under the name *'Slavic Brotherhood'* and long-term security agreements that are viewed critically in Western security policy circles.

Military cooperation with China has also intensified, including joint exercises and training sessions between Chinese and Serbian troops. In 2025, this cooperation expanded further, making Serbia the first EU accession candidate to engage in such military cooperation with China. Serbia is also the only European country to operate the FK-3 air defence system, a Chinese export version of the HQ-22.

This dual strategy creates tactical channels through which military knowledge, technologies, and potentially intelligence information from Western partnerships could indirectly reach Russian or Chinese actors. Beyond its military posture, Serbia functions as a geopolitical hub between Russia, China, and the West. Its historically close ties with Russia - politically, economically, culturally, and on security matters - are deeply rooted. Moscow regularly blocks international recognition of Kosovar institutions and uses Belgrade as an ally in multilateral forums.

China is also steadily expanding its presence in Serbia through infrastructure investments, military cooperation, and specialised programs within police and security services. Together, these connections

increase the potential for Serbia to act as a conduit for strategic information, technology, or diplomatic support benefiting actors outside the Western security sphere.

Criticism from the EU and a Stalled Accession Process

Although the EU still formally lists Serbia as a candidate country, progress toward European integration has shown signs of stagnation in recent years. In its reports and resolutions (the most recent in October 2025), the EU has repeatedly criticized Serbia's failure to align with European legal and security standards, particularly regarding the rule of law, media freedom, the fight against corruption, and foreign policy that is not in line with common European security and trade policy.

The country has been deemed to have made no de facto progress, but rather to be moving in the wrong direction. Serbia's obstructionist stance toward sanctions against Russia and its increased security cooperation with China and Russia have raised concerns in Brussels and significantly complicated the realistic prospect of EU accession in the near future.

Vučić has intentionally allowed Serbia's EU candidate status to linger indefinitely, using the prolonged accession process as a strategic tool to assert geopolitical relevance and to safeguard the survival of his authoritarian, opaque system within the complex interplay between the EU, Russia, and China. By keeping the accession process open, he also secures critical financial flows that underpin his regime, drawing the largest portion from EU accession funds while supplementing them with targeted investments from China and Russia.

Domestic Distraction and Regional Risks

The repeated portrayal of external threats serves not only to justify military buildup but also to consolidate domestic power in a system marked by institutional corruption and the systematic suppression of opposition forces.

Vučić's strategy uses foreign policy tensions to divert attention from domestic problems and mobilize national unity against perceived external enemies. Given the historical context of his political socialization and his violent rhetoric during the Yugoslav Wars, it must be considered that a leader with such a profile, combined with military buildup and ideological flexibility, may pursue more than defensive intentions. The possibility that military conflict could be used as a means of political survival cannot be ruled out.

Aleksandar Vučić represents a Serbia that is governed authoritatively domestically, is undergoing extensive rearmament, and is strategically testing the limits of its security environment between NATO, the EU, and geopolitical partners such as Russia and China.

The combination of a crisis of political legitimacy, Greater Serbian ideology, multilateral geopolitical positioning, and significant military projection makes Serbia a complex regional and European security factor. This behaviour poses a serious threat to regional stability and the strategic interests of the EU and NATO, demanding immediate action; failure to act risks history repeating itself, with a Ukraine-like scenario unfolding directly on the EU's borders.

ASIA - TAIWAN

The Semiconductor Fault Line Through Taiwan and the Global Microchip Crisis: A Need to Redefine Strategic Autonomy in the Domain

Gargi AWASTHI (India)

The governments of nearly every major economy are pouring tens of billions of dollars into semiconductor industries every year. This Comment explores why governments see semiconductors as a strategic technology, and the tactics governments are using to shape the semiconductor industry.

To demystify the subject, Miller weaves in explanations of the underlying technology—essential for appreciating the stakes. At its core, computing relies on binary basics: a system of 1s and 0s, where data is encoded in two states (1 for "on" or "true," 0 for "off" or "false"), much like a light switch.

This magic happens via semiconductors—materials with conductivity between metals (like copper, which conducts freely) and insulators (like rubber, which blocks it). Their conductivity can be tuned by doping (adding impurities), temperature, or light. The go-to material is silicon (Si), refined from sand or quartz into crystal wafers, often doped with elements like boron or phosphorus. Alternatives include germanium (Ge), gallium arsenide (GaAs) for speed, silicon carbide (SiC) for power, and gallium nitride (GaN) for efficiency [1].

Source: https://www.networkworld.com/article/1266982/india-set-to-challenge-chinas-dominance-in-semiconductor-packaging.html

Transistors, built from these semiconductors, serve as tiny switches or amplifiers, controlling electrical flow to represent those 1s and 0s. Billions etch onto a chip, switching at billions of times per second for lightning-fast computations.

Integrated circuits (ICs) take it further: entire circuits fabricated on a semiconductor wafer, packing transistors with resistors and capacitors into layered networks. "Chips" or "microchips" are the everyday shorthand for these packaged ICs—the physical, ready-to-use form.In essence: Semiconductors (raw material) → Transistors (basic switches) → Integrated Circuits/Chips (complex systems of transistors). This hierarchy underscores why chips are so critical—and vulnerable.

1940s with the invention of the transistor at Bell Labs, a breakthrough that replaced bulky vacuum tubes (which glowed with light, attracted moths, and birthed the term "debugging" from the literal need to remove insects from early computers like ENIAC). This set the stage for modern electronics.

By the late 1950s, innovators at Texas Instruments and Fairchild Semiconductor developed the integrated circuit, revolutionizing miniaturization. Robert Noyce and Gordon Moore went on to co-found Intel, fuelling Silicon Valley's boom. (Interestingly, in the post-war era through the 1970s, the industry often employed women for assembly work due to lower wages and their smaller hands, which were better suited for delicate tasks). Global Competition and Key Players Miller explores the fierce international rivalry involving Soviet Russia, Maoist China, Japan, South Korea, America, and even the Netherlands, all entangled in a fragile global supply chain. The standout winner? Taiwan Semiconductor Manufacturing Company (TSMC). Founded in 1987 by Morris Chang—a former Texas Instruments executive, MIT and Stanford alumnus, with strong backing, TSMC pioneered the "foundry" model: producing chips designed by others. This innovation catapulted Taiwan to dominate 37% of global computing power by the 2020s, including over 90% of the most advanced chips. (Chang's move came after being passed over for CEO at Texas Instruments—a decision they likely regret today.

The United States (US) leads in chip design software and intellectual property, Europe controls critical lithography technologies, Japan supplies key upstream inputs—including roughly 90 percent of global silicon wafers—and China has built significant scale in assembly, testing, and mature-node manufacturing, while investing heavily to move up the value chain.

The Global Microchip Conflict The Semiconductor Fault Line Through Taiwan

Taiwan's Dominance in the Microchips Industry

Modern microchips are among the most complex manufactured products in existence, and this complexity translates directly into cost. Chip design that once required under US$50 million at the 65-nm node now costs roughly US$500–600 million for a leading-edge 5-nm chip, reflecting the exponential rise in engineering, software, and verification requirements.

Manufacturing costs have escalated even more sharply. Fabrication facilities for earlier-generation chips at the 65–28-nm nodes typically cost well under US$1 billion. At advanced nodes, however, a 5-nm fabrication module alone costs approximately US$5–6 billion, and total investment can exceed US$15–20 billion once cleanrooms, utilities, and advanced tooling are included. This widening gap between design and fabrication costs has fundamentally reshaped the structure of the semiconductor industry.

Until the 1980s, most firms operated as integrated device manufacturers (IDMs), controlling design, fabrication, and sales in-house. As fabrication costs began to dwarf design costs, the industry reorganised around a separation between capital-light design and ultra-capital-intensive manufacturing, giving rise to the fabless–foundry model. Under this structure, design-focused firms concentrate on chip architecture and applications, while specialised foundries undertake manufacturing at scale.

Taiwan's dominance emerged from a deliberate strategic choice. Rather than competing directly with US firms in chip design or branded products, Taiwanese policymakers identified advanced fabrication as a critical entry point into the global value chain. With strong government backing, Morris Chang—a senior executive at Texas Instruments—returned to Taiwan in the late 1980s to establish TSMC, the world's first pure-play foundry. Sustained state support, targeted industrial policy, and private-sector entrepreneurship enabled Taiwan to build an advanced fabrication ecosystem that now anchors global semiconductor production, with firms such as Apple, NVidia, and AMD relying heavily on Taiwanese manufacturing. Today, four of the world's top ten foundries are based in Taiwan[2].

Beyond fabrication, Taiwan has also built notable capabilities across adjacent segments of the value chain, including the export of machinery and apparatus used in the manufacture of semiconductor devices and integrated circuits, with such exports totalling roughly US$5 billion. At the design layer, Taiwanese firms such as MediaTek, Realtek, and Novatek have emerged as notable global players, generating an estimated US$23.1 billion in revenue in 2022 and US$25.5 billion in 2023, with growth increasingly driven by high-performance computing demand. In total, Taiwan's semiconductor industry generated over US$165 billion in revenue in 2024 and accounts for roughly 18 percent of the global semiconductor value chain—second only to the United States at around 39 percent.

This concentration has embedded semiconductors directly into Taiwan's national security calculus. Often described as a 'silicon shield', Taiwan's central role in global chip manufacturing creates powerful economic and strategic incentives for the United States and its allies to preserve stability across the Taiwan Strait, given the scale of disruption any conflict would pose to the global economy.

The Strategic Contest for Taiwan

China's determination to reunify with Taiwan is driven by three closely linked factors: historical

legitimacy, technological ambitions, and strategic control of key maritime routes.

For China, Taiwan is not a conventional territorial dispute but a legacy of China's unresolved statehood. Since the founding of the People's Republic in 1949, China has asserted sovereignty over the island, grounding its claim in China's historical governance of Taiwan dating back to the Qing dynasty. Taiwan's separation from the mainland was the result of the unresolved outcome of the Chinese civil war, after which the Nationalist Party, or Kuomintang (KMT), retreated to the island and continued to operate as the Republic of China, while the Chinese Communist Party (CCP) established the PRC on the mainland.

However, Taiwan's importance to China is well beyond just history. The island now occupies a central position in the global semiconductor ecosystem, particularly in advanced fabrication. Taiwanese foundries produce chips that underpin artificial intelligence, high-performance computing, defence systems, and critical infrastructure worldwide. China remains structurally dependent on this ecosystem, importing close to US$90 billion worth of semiconductors annually from Taiwan alone. Control over these capabilities would materially alter China's position in the global technology supply chain.

More significantly, access to Taiwan's advanced fabrication infrastructure—including leading-edge process nodes, manufacturing expertise, and associated production know-how—will shorten China's technological learning curve. Such access will weaken the effectiveness of Western export controls designed to slow China's progress in advanced computing, artificial intelligence, and military technologies, accelerating China's push towards technological self-sufficiency.

Geography reinforces these technological stakes. Taiwan sits at the centre of the first island chain, linking Japan, Taiwan, and the Philippines, and separating the East China Sea from the South China Sea. The Taiwan Strait and surrounding waterways rank among the world's most commercially and strategically significant corridors[5]. Roughly one-third of global maritime trade passes through the broader South China Sea,while an estimated US$2.45 trillion in goods transited the Taiwan Strait in 2022 alone.

The Global Microchip Conflict The Semiconductor Fault Line Through Taiwan

China's own exposure to this geography is substantial. Approximately US$1.3 trillion of Chinese imports and exports pass through the Taiwan Strait each year—more than for any other economy. Control over Taiwan would therefore enhance China's ability to secure its trade routes while increasing leverage over regional competitors and US allies, including Japan and South Korea.

The military implications are equally consequential. Taiwan currently constrains the movement and coordination of China's naval forces. Under its control, China's North, East, and South Sea Fleets could operate with greater integration, enabling more flexible power projection during crises. Control over Taiwan would also deny adversaries strategic depth in the Western Pacific while strengthening China's maritime posture.

Against this backdrop, reunification has remained non-negotiable for China. Western intelligence assessments and Chinese military planning increasingly reference the period leading up to 2027—the centenary of the People's Liberation Army—as a milestone by which China seeks to acquire the capabilities necessary to compel or execute reunification. Whether pursued through coercion, blockade, or force, Taiwan today represents not merely a territorial dispute, but the central fault line where history, technology, and geopolitics converge—shaping the future balance of power in the global technological order.

Efforts to Decouple

In recent years, semiconductors have come to be viewed as strategic assets rather than purely commercial inputs. Their role in defence systems, artificial intelligence, telecommunications, and critical infrastructure has made supply security a matter of national policy. As China's technological ambitions have expanded and tensions over Taiwan have intensified, governments have reassessed the risks associated with concentrated semiconductor production in East Asia, particularly in Taiwan and mainland China.

The COVID-19 pandemic reinforced these concerns. Supply disruptions persisted for more than three years, affecting automotive production, medical equipment, consumer electronics, and defence systems. Weather-related disruptions and industrial incidents further constrained output. The broader economic implications are significant. Bloomberg Economics estimates that a conflict over Taiwan could reduce global output by approximately US$10.6 trillion in the first year alone, equivalent to roughly 9.6 percent of global GDP.

Although supply conditions normalised in 2023, governments and firms have realised that structural vulnerabilities remain. In response, major economies have introduced policies aimed at expanding and securing domestic semiconductor capacity.

In the United States, the CHIPS and Science Act allocated US$52.7 billion in direct subsidies as

part of a broader US$280-billion initiative to strengthen semiconductor manufacturing and research. The policy objective is to increase domestic fabrication capacity and reduce strategic dependence on external supply. This direction has continued under the Trump administration. Taiwanese firms, particularly TSMC, have adjusted investment strategies accordingly. While maintaining limited operations in mainland China, TSMC has curtailed advanced-node expansion there and increased investment in the United States, Japan, and Europe. The company has committed approximately US$165 billion towards US manufacturing facilities, including major fabrication plants in Arizona.

The European Union has adopted a similar approach. The European Chips Act mobilises over US$51 billion (€43 billion) in public and private investment to expand fabrication, research, and supply-chain capabilities. Europe also seeks to leverage existing strengths in lithography through ASML and in industrial software and engineering systems. The EU's stated objective is to increase its share of global semiconductor production from roughly 10 percent to 20 percent by 2030.[3].

The US-China chip war is becoming more intense as both countries understand the significance of semiconductors for their economic security and national defense. As a result of nationalist and unilateral actions taken by the US and China under the chip war, other Asian economic powerhouses are reassessing their semiconductor strategies, leading to new opportunities for semiconductor partnerships in Asia among middle powers. South Korea, a leading semiconductor power in Asia, is facing critical challenges amid the chip war, that, in turn, resulted in reshaping its trade and overseas production strategies that are heavily reliant on China. To maintain its semiconductor dominance and ensure economic security, Korea is adopting new approaches such as export and production diversification. In the meantime, India, amid the ongoing US-China tech war, is also seeking to construct a resilient supply chain and decrease its reliance on China for imports. In the process, New Delhi is looking to develop its semiconductor industry and build chip ties with like-minded countries in production and workforce development.[4] This opens up significant prospects for Korea-India semiconductor partnerships. This paper proposes three areas where Korea and India could collaborate: semiconductor trade partnerships, semiconductor production partnerships, and semiconductor workforce collaboration. By doing so, it highlights how the US-China chip war is creating new opportunities for other Asian economic powerhouses to collaborate in the semiconductor industry.

The semiconductor industry has become crucial in the current era of the fourth industrial revolution. Semiconductors are now as valuable as oil due to their widespread use in both consumer and military applications. Both the US and China have realized the importance of semiconductors for their economic security and national defense. This has led to intense competition between the two countries for dominance in this sector. Under this competition, both have changed their previous domestic and foreign economic policies, guided by neoliberalism's idea of free market, and begun to take nationalistic and unilateral actions, driven by emerging geopolitics, in their national economic and security interests. These unilateral actions have huge impacts on other Asian economic powerhouses' economic security. Indeed, China's new quest to realize a self-reliant semiconductor strategy directly impacts South Korea (hereafter, Korea)'s semiconductor industry, which significantly relies on China for export and production. The US's unilateral action under the chip war has also influenced Korea as Washington has pressured Seoul to downgrade its trade and manufacturing ties with China. The US-China chip war has also influenced India's semiconductor strategy. Amid the ongoing chip war, India seeks to construct a resilient supply chain and decrease its reliance on China for imports. New Delhi is also looking to develop its semiconductor industry and build chip ties with like-minded countries in production and workforce development.

The ongoing US-China chip war has opened up significant opportunities for Korea and India to form a semiconductor partnership. Analysis of the prospects of the India-Korea technological partnership by examining the dynamics of the US-China chip war within the context of Korea and and India, and by studying both countries' changing domestic political economy will be insightful in this article. Although India and Korea have established strong political, trade, and investment ties since the post-Cold War era (Kumar, 2015a, 2015b, 2021), they have not yet explored the potential of technological partnerships regarding semiconductors. Since Korea is striving to maintain its dominance in the chip industry, and India is trying to become a significant player in the global semiconductor value chain, there is immense scope for collaboration between the two leading democracies in Asia. This research paper identifies three areas where Korea and India could collaborate: semiconductor trade partnerships, semiconductor production partnerships, and semiconductor workforce collaboration. These areas are not randomly selected, but are chosen for reasons based on the focal point of the US-China chip war.

The tech war between the US and China creates new opportunities for other Asian economic powerhouses to cooperate in the semiconductor industry. Previous literature has mainly focused on the impact of the US-China chip war on both major powers' emerging strategies to secure their economic security and military interests (Miller, 2022) or on how current East Asian dominant semiconductor powerhouse, such as Korea, should secure their manufacturing base (Kwon, 2022; Bae, 2022; Yoon, 2023).

Therefore, not much attention has been given to how this chip competition could bring convergence for Asian like-minded middle powers. Second, this article enriches the existing literature on India-Korea relations by introducing the first study on Korea-India technology partnerships. Most studies have mainly focused on general security and economic issues, such as trade and investment, between the two countries. Finally, this study provides insights for policymakers to set a new agenda for India-Korea partnerships as both countries celebrate the 50th anniversary of their diplomatic ties in 2023.

Decoding the US-China Chip War

In the current era of the fourth industrial revolution, the semiconductor industry has emerged as a crucial and strategic sector, leading to intense competition between the US and China for dominance. Semiconductors are now considered as valuable as oil due to their widespread use in both consumer and military applications. It is widely believed that the key to dominating the fourth industrial revolution industries, such as artificial intelligence, 5G, cloud, Internet of Things, autonomous vehicles, and bio-health, will be determined by who emerges as the leader in the semiconductor industry, particularly in advanced semiconductors (Bae, 2022).

The increasing importance of semiconductors has led to the emergence of the US-China chip war. The initial cause of the chip war was the growing political tension between the US and China. The Chinese leaders felt that they needed to secure 'semiconductor sovereignty' to become a true economic superpower in the future. China relies heavily on the US and its security allies for advanced chips that power almost everything in its tech industry. This dependence is vulnerable to China's economic security and its future military ambitions. Against this backdrop, President Xi Jinping called for the development of a self-reliant semiconductor industry in China, as he believes that "chips are as important for manufacturing as hearts are for humans." As a result, President Xi dismantled the previous regimes' neoliberalism-guided developmental strategy, which promoted foreign companies' presence in China in the post-Cold war era. Instead, He launched an inward-looking state capitalism strategy, favoring Chinese companies over foreign companies, to achieve high self-sufficiency under the 'Made in China' plan. China also adopted a nationalist approach to realizing independence in the semiconductor industry by introducing an import substitution strategy for this sector (Lee(b), 2022). On one hand, Beijing seeks to emerge as a self-reliant semiconductor giant, while on the other hand, it aims to challenge the dominance of existing semiconductor players, such as the US, Korea, and Taiwan (Kwon, 2022).

The US views China's efforts to become a leader in semiconductor manufacturing as a direct threat to its economic and military security (Miller, 2022). Therefore, the US government took steps to curb China's semiconductor rise. During the Trump administration, a 'trade war' was initiated with China, resulting in a 25% tariff on Chinese imports, particularly items related to the Made in China plan, such as semiconductors and related equipment (Bae, 2022). The COVID-19 pandemic caused a disruption in the semiconductor supply chain, which changed the US's perception of the chip competition and intensified the US-China rivalry. President Biden has stated that 'China is trying to dominate the global chip market, which has many applications, including military ones (The White House, 2022).' As a result of this perception, the Biden administration has turned the US-China trade war into a chip war. It implemented a nationalist strategy by passing the 'CHIPS and Science Act of 2022' to achieve its goal of promoting products that are 'Made in US'. This move indicates a shift away from the country's decade-long commitment to promoting international free trade, which is a fundamental idea of neoliberalism. With the introduction of this act, it also embarked on a lengthy journey to compete with China for semiconductor hegemony (Lee(a), 2022).

The US-China chip war intensified when the Biden administration extended the scope of chip competition beyond bilateral to multilateral. The US proposed the Chip-4 alliance in 2022 as part of a more comprehensive plan for a 'democratic semiconductor supply chain' to reduce reliance on the China-centric supply chain (Yoon, 2023). The initiative includes Japan, Korea, and Taiwan, all of which excel in specific semiconductor industry segments. For instance, Japan in raw materials and equipment supply, and Korea and Taiwan in manufacturing. The US also started to build a semiconductor partnership with India on both bilateral and multilateral levels after the Modi administration decided to forge a strong relationship with the US amid the India-China security tension in 2020 (Kumar, 2023). The US elevated its strategic partnership with India with a focus on strengthening semiconductor partnerships. American companies, such as Micron Technology, started to shift their production from China to India as China began to use economic coercion to punish US companies working in China. The US also seeks to strengthen its semiconductor ties with India in the Quadrilateral Security Dialogue (hereafter, QUAD) frameworks, which includes, the US, India, Japan, and Australia.

The ongoing chip war between the US and China is having a significant impact on the geo-economics landscape of Asia. The conflict between these two superpowers over semiconductors has led other Asian economic giants to reassess their semiconductor strategies, which has resulted in the

emergence of new opportunities for semiconductor partnerships in Asia. In the rest of this paper, we will discuss how the US-China chip war, along with various domestic factors, is creating fresh opportunities for semiconductor collaborations between Korea, Asia's dominant semiconductor power, and India, an emerging power in the region.

Navigating Strong Convergence in Korea-India Semiconductor Trade Partnership

In this section, we will analyze the reasons behind the substantial convergence in the semiconductor trade partnership between Korea and India. First, we will investigate the trade dilemma faced by both countries due to their dependency on China and their policy responses. Then, we will highlight the potential of the trade partnership between Korea and India.

Korea's Dependence on China for Semiconductor Exports and Emerging Export Dilemmas

Korea's Dependence on China for Semiconductor Exports

Korea is an exporting nation. It ranked sixth in terms of exporting goods worldwide in 2022. Its economy heavily relies on exports, with semiconductors being its top export item for a long time. The importance of semiconductors for Korea has increased drastically in recent years, with semiconductor exports accounting for almost 20% of Korea's total exports in 2021, compared to 10% in 2010. In 2021, Korea's semiconductor export volume was $127,984 million, followed by petrochemicals ($55,081 million) and autos ($53,456 million) (see Figure 1). Korea's economic growth is mainly dependent on the performance of the semiconductor industry, which is so significant that Korea is often referred to as "Korea Makes a Living on Semiconductors.

It is significant to highlight that Korea's semiconductor export structure has a critical issue: it heavily relies on China. After the normalization of diplomatic relations between Korea and China in the 1990s, Korea strengthened its economic ties with China, making it its largest trading partner, replacing traditional partners like the US and Japan (Kumar, 2015b). In the process, China also became the largest destination for Korea's semiconductor export. China's emergence as the most significant consumer of semiconductors in the world (Lee(b), 2022, pp. 108–109) made Korea heavily reliant on China market. In 2021, Korea's export to China accounted for approximately 60% of semiconductors. China also emerges as Korea's largest exporting destination for its semiconductor equipment: Korea's 69% of the equipment for front-end processes, 61% for back-end processes, and 39% of other semiconductor equipment went to China market. Apart from that, China market was also the largest market for Korean semiconductor parts. In sum, Korea became hugely dependent on China market for the success of its semiconductor industry, which is the backbone of the Korean economy.

Korea's Emerging Export Dilemmas

The expanding battles over techno-hegemony between the US and China have directly affected Korea's economic security. Indeed, recent actions taken by two great powers have created a semiconductor export dilemma for Korea. As discussed above, under the US-China chip war, the Xi Jinping government has embarked on a self-reliance move for semiconductors and introduced an import substitution strategy. Under this strategy, China also seeks to reduce its import reliance on Korea. Beijing's action has significantly affected the mindset of Korean policymakers as they came to believe that China is no longer a safe destination for Korea's semiconductor exports. The actions taken by China are already impacting Korea. China's self-reliance moves, combined with China's recent economic slowdown, led to the significant decline of Korea's semiconductor imports in China in recent months, given that Korea's total semiconductor exports to China fell 40% in the first quarter of 2023 from a year earlier. In sum, the Xi Jinping government's self-reliance move and its potential impact on Korea's economic security has become a serious concern for policy communities in Seoul.

The US-China chip war is becoming more intense as both countries understand the significance of semiconductors for their economic security and national defense. As a result of nationalist and unilateral actions taken by the US and China under the chip war, other Asian economic powerhouses are reassessing their semiconductor strategies, leading to new opportunities for semiconductor partnerships in Asia among middle powers. South Korea, a leading semiconductor power in Asia, is facing critical challenges amid the chip war, that, in turn, resulted in reshaping its trade and overseas production strategies that are heavily reliant on China. To maintain its semiconductor dominance and ensure economic security, Korea is adopting new approaches such as export and production diversification. In the meantime, India, amid the ongoing US-China tech war, is also seeking to construct a resilient supply chain and decrease its reliance on China for imports. In the process, New Delhi is looking to develop its semiconductor industry and build chip ties with like-minded countries in production and workforce development. This opens up significant prospects for Korea-India semiconductor partnerships. This paper proposes three areas where Korea and

India could collaborate: semiconductor trade partnerships, semiconductor production partnerships, and semiconductor workforce collaboration. By doing so, it highlights how the US-China chip war is creating new opportunities for other Asian economic powerhouses to collaborate in the semiconductor industry. This paper also provides insights for policymakers to set a new agenda for India-Korea partnerships as both countries celebrated the 50th anniversary of their diplomatic ties in 2023.

The semiconductor industry has become crucial in the current era of the fourth industrial revolution. Semiconductors are now as valuable as oil due to their widespread use in both consumer and military applications. Both the US and China have realized the importance of semiconductors for their economic security and national defense. This has led to intense competition between the two countries for dominance in this sector. Under this competition, both have changed their previous domestic and foreign economic policies, guided by neoliberalism's idea of free market, and begun to take nationalistic and unilateral actions, driven by emerging geopolitics, in their national economic and security interests. These unilateral actions have huge impacts on other Asian economic power

Navigating Strong Convergence in Korea-India Semiconductor Trade Partnership

In this section, we will analyze the reasons behind the substantial convergence in the semiconductor trade partnership between Korea and India. First, we will investigate the trade dilemma faced by both countries due to their dependency on China and their policy responses. Then, we will highlight the potential of the trade partnership between Korea and India.

Korea's Dependence on China for Semiconductor Exports and Emerging Export Dilemmas

As Table 1 shows, in 2021, Korea's export to China accounted for approximately 60% of semiconductors. China also emerges as Korea's largest exporting destination for its semiconductor equipment: Korea's 69% of the equipment for front-end processes, 61% for back-end processes, and 39% of other semiconductor equipment went to China market.

Table 1. Korea's Export Relations by Semiconductor Manufacturing Process in 2021.

Export Items	Country	Amount of Export (Unit: $ million)	Percent of Korea's Overall Exports
Semiconductor	China (including Hong Kong)	70,298	59.8
	Vietnam	12,256	10.4
	Taiwan	10,420	8.9
	US	8,486	7.2
Front-end manufacturing equipment	China	2,382	68.9
	Taiwan	248	7.2
	US	247	7.2
	Japan	233	6.7
	Singapore	172	5.0
Back-end manufacturing equipment	China	1,193	61.1
	Taiwan	218	11.2
	Vietnam	106	5.4

	US	103	5.3
	Singapore	91	4.7
Other Equipment	China	98	38.6
	Taiwan	66	25.7
	US	20	8.0
	Japan	12	4.8
	Germany	11	4.3
Parts	China	746	26.4
	US	503	17.8
	Taiwan	438	15.5
	Singapore	391	13.9
	Japan	307	10.9

Note: *translation and analysis based on Yang and Kim (2022).*

If China's push for self-reliance is creating an export dilemma for Korea, the US's strategy to contain China is also leading Korea to reconsider its heavy dependence on the Chinese market. The Biden administration has taken unilateral steps to restrict semiconductor exports to China, not just in a bilateral context but also by urging key allies like Korea, Japan, and the Netherlands to collaborate on containing China's rise. However, not all partners are on board with this approach, particularly Korea, which relies heavily on the Chinese market for its semiconductor exports. Korea aims to remain neutral in the US-China semiconductor dispute (Bae, 2022). In this context, Seoul's policy communities are dissatisfied with the United States' unilateral actions, which have pushed Korea to be part of its strategy to contain China. The Korean side has made numerous efforts to persuade the Biden administration not to involve Korea in its China containment strategy. However, the Biden administration has disappointed Korea on this issue, as they have prioritized containing China and have forced their ally to follow suit. Korea is now developing new plans to maintain its export domination in the global market, assuming that the US-China chip war will be prolonged and that the US will intensify its containment strategy towards China in the future (Gyong & Lee, 2022; Bae, 2022).

Amid the intensifying US-China tech war, two most common policy slogans emerged in Korea: (1) Next China ( ) and (2) Export Diversification ( ). Under these policy slogans, Korea has decided to reduce its export reliance on China by diversifying its market away from China. Although these policy slogans are being used to reduce overall export dependence in China, it is also true for semiconductor exports. It is also significant to highlight that Korea is also not optimistic about a prospect where its traditional security partner, the US, can help Korea to diversify its export under its Next China strategy. More precisely, Korea is searching for new emerging markets amid the US-China tech war.In this context,The US market and expand its export presence in the Southeast Asian market, especially Vietnam, which has the potential to play the role of next China for Korea because of the rise of global.

Japan has introduced incentives estimated at approximately US$65 billion (¥10 trillion) to reshore and 'friend-shore' critical stages of semiconductor production. The government projects the long-term economic impact to reach approximately US$1 trillion (¥160 trillion).

India has also renewed its semiconductor strategy. The India Semiconductor Mission, approved in December 2021, allocated approximately US$9–10 billion (INR 76,000 crore) in incentives, providing up to 50 percent fiscal support across fabrication, packaging, testing, and chip design.[6] As of December 2025, ten projects totalling roughly US$19–20 billion (INR 1.60 lakh crore) in investment have been approved across six states. An additional allocation of approximately US$1 billion (INR 8,000 crore) for

2026–2027 is intended to accelerate capital investment and expand domestic capabilities across the value chain.

These global policy shifts underscore a broader reality: semiconductors are no longer treated as a purely commercial industry, but as strategic infrastructure. As major economies invest heavily to reduce concentration risks, Taiwan remains the single most critical node in the advanced chip ecosystem. No amount of short-term diversification can immediately replicate the scale, expertise, and network effects embedded in Taiwan's fabrication base. For now, the semiconductor fault line continues to run through the Taiwan Strait—where technology, security, and geopolitics converge most sharply.

Endnotes:

[1] Silicon VLSI, "Semiconductor vs Microchip," April 13, 2024, https://siliconvlsi.com/difference-between-a-microchip-and-a-semiconductor2024/.

[2]NVidia, "NVidia Blackwell Architecture," https://www.nvidia.com/en-in/data-center/technologies/blackwell-architecture/.

[3] World Semiconductor Trade Statistics (WSTS), "Global Semiconductor Market Approaches USD 1 Trillion in 2026," December 2, 2025, https://www.wsts.org/esraCMS/extension/media/f/WST/7310/WSTS_FC-Release-2025_11.pdf.

[4] Directorate General of Customs, Republic of China (Taiwan), "Trade Statistics: Country of Origin – China," Bureau of Foreign Trade, https://publicinfo.trade.gov.tw/cuswebo/FSCE30F0I/FSCE30F0I?Val=CN.

[5] Matthew P. Funaiole et al., "How Much Trade Transits the Taiwan Strait?" ChinaPower Project, Center for Strategic and International Studies, August 22, 2024, https://features.csis.org/chinapower/china-taiwan-strait-trade/.

[6] Ministry of Electronics and Information Technology, Government of India, https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=157237&ModuleId=3&reg=3&lang=2

MIDDLE EAST - STRAIT OF HORMUZ

The Strait of Hormuz and the Partial De-Universalization of the Petrodollar: Chokepoint Power and Settlement Control in the Gulf Energy Order

PhD. Shaoyuan WU (USA)

Abstract

The Strait of Hormuz is usually understood as an energy chokepoint, but its strategic significance extends beyond oil supply and maritime security. Under conditions of conflict, blockade pressure, and asymmetric access control, Hormuz may also become a settlement node capable of reshaping how payment authority is distributed in the global energy system. This article argues that recent dynamics around Hormuz do not signal the immediate collapse of the petrodollar system. Instead, they point to a subtler transformation: the partial de-universalization of petrodollar settlement.

Source: https://nextgenlearning.org.uk/why-strait-of-hormuz-matters/

Iran's position is structurally distinctive because it is not merely a sanctioned actor attempting to bypass the dollar system. It is also a major oil-and-gas producer and a Hormuz-adjacent power capable of converting chokepoint access into a settlement condition. The article introduces **Chokepoint-Driven Settlement Shift (CDSS)** to explain how the ability to condition access at critical nodes may transform payment practices from market-wide monetary consensus toward node-conditioned acceptance and access-based value recognition.

At the same time, this transformation should not be overstated. Chokepoint power can monetize access and reshape payment conditions, but it does not automatically create a full alternative monetary order or a durable regional value system. The UAE's announced withdrawal from OPEC and OPEC+ effective May 1 adds a secondary layer to this fragmentation by weakening the assumption of cohesive Gulf production governance. The petrodollar system is therefore not collapsing at once; it is being selectively conditioned, interrupted, and regionally de-universalized through chokepoint power, settlement control, and broader fragmentation in the Gulf energy order.

Keywords: Strait of Hormuz; Petrodollar; Energy Security; Chokepoint Power; Settlement Control; Chokepoint-Driven Settlement Shift; Access-Based Value Recognition; Gulf Energy Order; Global Order

1. Introduction

The Strait of Hormuz has long been described as one of the world's most important energy chokepoints. The U.S. Energy Information Administration identifies Hormuz as the world's most important oil transit chokepoint and estimates that roughly one-fifth of global petroleum liquids consumption has passed through the strait in recent years (U.S. Energy Information Administration, 2023, 2026). The International Energy Agency similarly estimates that around 20 million barrels per day of crude oil and oil products moved through Hormuz in 2025, equivalent to roughly one quarter of global seaborne oil trade (International Energy Agency, 2026). For this reason, most discussions of Hormuz begin with a familiar question: what happens to oil prices, insurance costs, and shipping flows if the strait is disrupted?

That question remains important, but it is no longer sufficient. The current confrontation around Hormuz suggests that the strait should not be understood only as a corridor for energy flows. It is also a point where geography, maritime pressure, legal authority, financial settlement, and global energy dependence converge. When access to such a corridor becomes uncertain, the problem is not only whether oil can move. It is also who can define the conditions under which movement occurs.

This distinction matters for the petrodollar system. The petrodollar order has traditionally rested on the routinized connection among energy trade, dollar-based settlement, U.S. security commitments, and the recycling of surplus capital into dollar-denominated assets. More broadly, the international role of the dollar has depended on liquidity, convertibility, institutional depth, and political power (Cohen, 2015; Eichengreen, 2011; Kirshner, 1995). If access to a strategic energy corridor becomes priced or conditioned, dollar settlement may remain dominant while becoming less automatic in specific transactions. The claim is not that Iran has already created a full alternative value system, nor that the dollar is about to disappear from energy trade. Rather, the argument is that chokepoint pressure can change the sequence of transactions: access may become the first gate, settlement may become negotiated, and monetary storage may still return to hard currency. In this sense, the petrodollar system may remain dominant globally while becoming less universal at strategic nodes. Iran's role is central because it sits at the intersection of energy production, geography, and financial constraint. Iran is not merely a sanctioned actor seeking to bypass U.S.-centered financial infrastructure. It is also a major oil-and-gas producer and a Hormuz-adjacent power capable of turning uncertainty over passage into political-economic leverage. That combination gives Iran a limited but significant capacity to connect access, payment, and value formation.

The article develops this argument through the concept of **Chokepoint-Driven Settlement Shift (CDSS)**. CDSS describes how access pricing may move toward node-accepted settlement before any full monetary replacement occurs. The core argument is that Hormuz does not need to replace the dollar in order to weaken the dollar's automaticity; it only needs to make access, payment, and value recognition conditional at a strategic node.

2. Iran, Chokepoint Power, and Settlement Authority

A chokepoint is usually defined by physical geography: a narrow passage through which critical flows must pass. In modern systemic conflict, however, chokepoints also function as institutional, financial, and socio-economic interfaces. They are places where the right to move can become politically conditioned and economically priced. Iran's leverage in this context derives from the combination of three structural roles.

Table 1. Iran's Three Structural Roles in Chokepoint-Based Settlement Leverage

Iranian Role	Source of Leverage	Strategic Meaning
Energy producer	Oil-and-gas supply and export capacity	Ability to link commodity flows to settlement terms
Hormuz-adjacent power	Geographic proximity and coercive influence over passage	Ability to condition or price access
Sanctioned financial actor	Exclusion from dollar-centered channels	Incentive to develop non-dollar or node-conditioned settlement tools

Source: *Author's analysis.*

Note: *Iran's leverage is conceptualized as the interaction of producer status, Hormuz-adjacent geography, and sanctions pressure. The table does not imply internationally recognized toll authority or full monetary replacement.*

This combination distinguishes Iran from an ordinary sanctioned economy. A sanctioned state without a strategic node may issue currency or promote alternative payment channels, but it often lacks the external demand needed to give those instruments practical value. Iran's position is different because Hormuz creates a necessary access environment. If external actors require passage, loading, port services, insurance recognition, or transit clearance, Iran may acquire limited authority over the payment conditions attached to those services.

The result is not immediate monetary replacement, but access-based value recognition. Instead of money simply mediating access, access begins to shape which forms of payment are accepted, preferred, or assigned practical value. From a socio-economic perspective, value may first emerge from access utility—the need to secure passage through a critical corridor—before it becomes embedded in a durable monetary system.

This is where Iran's role becomes strategically important. As long as Iran can influence passage rules, and as long as external actors require Hormuz-linked energy flows, an Iran-recognized payment or settlement instrument may acquire limited regional value. It may not be money in the full sense, but it can become a node-accepted settlement instrument.

The strategic significance is therefore not that Iran has replaced the petrodollar. It is that Iran may help create a regional settlement ecology in which the dollar remains dominant globally but is no longer the only automatic medium through which access, energy, and payment are connected.

3. Chokepoint-Driven Settlement Shift

The mechanism described above can be understood as **Chokepoint-Driven Settlement Shift (CDSS)**. CDSS refers to a socio-economic process in which payment acceptance becomes shaped less by market-wide monetary consensus alone and more by the ability to condition access at critical nodes.

Under normal market conditions, currencies are used because they are widely accepted, liquid, and trusted. Under chokepoint pressure, the sequence changes. The key question is no longer only which currency is most efficient or globally accepted. It becomes what form of payment will be accepted by the actor capable of conditioning access.

CDSS does not imply immediate currency replacement. It describes an earlier and narrower transformation: payment becomes conditioned by access. This distinction is important because it separates a shift in payment authority from the much stronger claim that a new monetary system has already emerged.

Table 2. Three Stages of Chokepoint-Driven Settlement Shift

Stage	Mechanism	Result
Stage 1: Access Pricing	Passage or clearance becomes payable	Chokepoint access becomes monetized
Stage 2: Node-Accepted Settlement	Specific instruments are accepted or preferred by the access-conditioning actor	Payment authority shifts toward the node
Stage 3: Regional Value Formation	Repeated use creates liquidity, anticipation, and secondary demand	A protocurrency or regional settlement instrument may emerge

Source: *Author's analysis.*

Note: *CDSS describes a staged process from monetized access to node-conditioned settlement and possible regional value formation. The final stage is hypothetical and does not imply full monetary replacement.*

This framework clarifies why a chokepoint does not need to create a new currency immediately in order to weaken a dominant monetary order. It only needs to make the dominant currency less automatic in transactions where access, clearance, and payment become linked.

4. Access Pricing Without Monetary Replacement

The Hormuz case does not yet show a mature CDSS regime, but it provides early and contested evidence of how access pricing may begin to interact with settlement authority. Recent reporting around Hormuz passage fees should therefore be treated cautiously. Some reports described Iran as seeking or imposing tolls on vessels transiting the strait, while other reports highlighted confusion, legal uncertainty, and

fraudulent "safe passage" messages offering transit clearance in exchange for crypto currency payments. Reuters reported warnings from a maritime risk firm about scam messages offering safe transit through Hormuz in exchange for Bitcoin or Tether, while noting that Reuters had not independently confirmed affected companies or Tehran's involvement (Reuters, 2026a).

Earlier sanctions-risk analysis suggested that crypto currency payments might be considered or demanded for Hormuz-related transit fees (Chainalysis, 2026). Such analysis is relevant because it shows how chokepoint access can generate demand for payment instruments outside ordinary dollar channels. However, Reuters later reported maritime-risk warnings that some Bitcoin and Tether "safe passage" messages were fraudulent and not issued by Iranian authorities (Reuters, 2026a). The crypto currency element should therefore be read as a contested signal of shadow demand for node-linked payment mechanisms, not as confirmed evidence of an official Iranian settlement regime.

The more important development is not whether such fees are large in absolute terms, or whether they are paid in dollars, euros, yuan, dirhams, crypto-assets, or another instrument. The deeper issue is that passage itself becomes monetized. Once passage becomes a payable claim, access is no longer a neutral background condition of trade. It becomes an economic object. This is the first stage of transformation: **access pricing**.

Access pricing, however, should not be confused with monetary replacement. A state may impose a passage fee, port charge, insurance-linked requirement, or clearance payment without creating a new monetary system. It may gain revenue and leverage while still preferring to store that revenue in existing hard currencies.

Iranian and international reporting indicated that Deputy Parliament Speaker Hamidreza Haji Babaei stated that the first revenues from Hormuz transit fees had been deposited into a Central Bank of Iran account (Anadolu Agency, 2026; Wall Street Journal, 2026). If accurate, this makes the toll issue more than a rumor or a purely informal field practice. It suggests domestic fiscal formalization, but not external legal recognition. Iran may have begun translating chokepoint access into a formal state-revenue claim, yet this does not prove the existence of a stable, internationally recognized, or fully institutionalized toll regime. The legality, scope, durability, and external acceptance of such a mechanism remain contested. Such claims would also remain legally controversial, especially because transit through international straits is generally addressed under the UNCLOS Part III transit-passage regime, which protects navigational freedoms rather than discretionary toll extraction (United Nations, 1982).

This produces a dual outcome. First, **access is monetized**: passage through a strategic node becomes a payable claim. Second, **value is re-anchored**: if toll revenue is ultimately held as foreign exchange, hard currency, or another recognized reserve asset, then existing monetary hierarchies remain intact at the storage level. The chokepoint-adjacent actor may influence who pays and under what conditions, but it has not displaced the global hierarchy of trusted reserve assets.

This does not mean that CDSS has no monetary significance. The distinction is not between "currency replacement" and "nothing happened." A new value system may emerge before a new currency system. If Hormuz-linked charges remain occasional, the effect will be limited. But if they become connected to port services, insurance recognition, energy loading, escort arrangements, or preferential clearance, a broader access-based settlement system could begin to form.

In that scenario, the value of the accepted instrument would not derive solely from Iran's formal monetary authority. It would also derive from **access utility**: the practical need to secure passage, clearance, or participation in a critical energy corridor. Value may emerge first from controlled access before it becomes embedded in a durable monetary system.

In CDSS terms, the crypto currency issue belongs at the contested edge of Stage 2, node-accepted settlement, while the stronger empirical signal remains the reported movement from access pricing toward domestic fiscal formalization through state financial accounts.

5. OPEC Fragmentation and the Gulf Energy Order

The Hormuz case concerns access and settlement. A separate but related development concerns the production-governance environment in which Gulf energy trade operates. The UAE's announced withdrawal from OPEC and OPEC+ effective May 1 adds a secondary layer to the broader fragmentation of the Gulf energy order. Reuters reported that the UAE announced its departure from OPEC and OPEC+ effective May 1, while the Associated Press described the move as a major blow to OPEC because the UAE is one of the group's largest producers and has significant production capacity (Associated Press, 2026; Reuters, 2026c).

This development matters for the petrodollar system, but the relationship should be stated carefully. OPEC did not create the petrodollar system by itself, nor should producer coordination be treated as identical to dollar settlement. Rather, Gulf producer coordination formed part of the broader institutional environment in which dollar-denominated oil trade became routinized. Stable production management, Gulf

security alignment, and predictable energy flows helped sustain the background conditions under which dollar settlement, dollar recycling, and dollar-denominated financial claims became routine.

The significance of the UAE case is not that it directly changes settlement currency. It is that it weakens one of the governance assumptions surrounding the Gulf-centered oil order: that major Gulf producers operate through a relatively cohesive production-governance architecture. The UAE's announced departure does not automatically weaken the dollar. In some respects, it may increase Abu Dhabi's flexibility to align with U.S., Asian, or diversified financial channels. But it may make the broader energy order less uniform, and that matters because the petrodollar system depends not only on monetary dominance, but also on the regularity of the energy system that generates recurring demand for dollar-based settlement and investment flows.

If sustained, the UAE's announced exit would reinforce the article's broader argument without replacing the centrality of Hormuz. Hormuz shows the fragmentation of access and settlement; the UAE case shows the possible fragmentation of producer governance. Together, they suggest that the challenge to the petrodollar is unlikely to appear first as a single rival currency. It is more likely to appear as fragmentation across several linked layers: chokepoint access, settlement practice, production governance, and reserve or investment strategy.

HSBC's assessment that the immediate market impact may be limited is important because it prevents overstatement. But its longer-term warning is equally important: the UAE's withdrawal may reduce OPEC+ discipline and make coordinated production management harder once Hormuz flows resume (Reuters, 2026b). The implication is that the system's short-term price response may be muted while its long-term governance structure becomes less stable.

The UAE case therefore broadens the context of the argument. It does not replace the Hormuz-centered settlement analysis. Rather, it shows that the Gulf energy order may be moving from a relatively coordinated structure toward a more fragmented environment in which access, production, payment, and surplus recycling are governed by increasingly separate logics.

6. Partial De-Universalization of the Petrodollar

The preceding sections identify two connected forms of fragmentation. Hormuz illustrates how chokepoint pressure can condition access and settlement. The UAE case illustrates how Gulf production governance may become less cohesive. Together, these developments point toward a broader process: the partial de-universalization of the petrodollar.

The petrodollar system is often discussed in binary terms: either it remains dominant, or it collapses. This framing is misleading. Monetary orders usually weaken through fragmentation, substitution, bypassing, and conditional use before they face outright replacement.

Partial de-universalization offers a more precise description. It means that a currency remains dominant at the system level but loses automatic applicability in specific strategic contexts. The dollar may continue to function as the main reserve currency, the main denomination for global commodity markets, and the deepest store-of-value instrument. Yet in transactions involving contested access, sanctions, blockade conditions, chokepoint pressure, or fragmented producer governance, dollar settlement may no longer be presumed as automatic.

This is not de-dollarization in the strong sense. It does not require another currency to replace the dollar globally. It means that dollar universality becomes conditional in specific corridors, services, and settlement relationships.

Hormuz is precisely the kind of corridor where this can happen. It is geographically concentrated, strategically contested, and economically indispensable. A regional settlement instrument does not need to replace the dollar everywhere. It only needs to become necessary in a limited but high-value chain of transactions: securing passage, obtaining clearance, paying fees, receiving port services, reducing delay risk, or participating in Hormuz-linked energy flows.

The continued dominance of the dollar remains visible in reserve and foreign-exchange data. IMF COFER data for 2025 Q4 show the dollar as the largest share of allocated official reserves at 56.77 percent, while the BIS 2022 Triennial Survey shows the dollar on one side of 88 percent of global foreign-exchange transactions (Bank for International Settlements, 2022; International Monetary Fund, 2026). These facts explain why access pricing does not automatically become monetary replacement.

The traditional petrodollar sequence can be simplified as:

Energy Flow → Dollar Settlement → Dollar Asset Recycling

Under chokepoint pressure, the sequence becomes less automatic:

Energy Flow → Chokepoint Access → Settlement Conditions → Monetary Storage

This revised sequence does not remove the dollar. It changes the order of dependence. Access becomes the first constraint, settlement becomes negotiated or conditioned, and monetary storage may still return to hard currency.

The UAE's announced exit from OPEC should be understood as a parallel layer of fragmentation rather than a direct step in the settlement sequence. It does not determine the payment instrument by itself. Its significance lies in weakening the governance environment in which energy pricing, output coordination, and settlement expectations operate.

The combined pressure can therefore be represented as:

Chokepoint Access + Fragmented Production Governance → Settlement Conditions → Monetary Storage

The petrodollar's vulnerability may therefore come not from a single rival currency replacing it across all oil markets, but from strategic nodes and producer fragmentation that make dollar settlement less automatic in critical regional corridors. The petrodollar system is not simply facing a currency competitor. It is facing a structural challenge from access-based power and fragmented Gulf energy governance.

7. Strategic Implications and Risks

The strategic implication is not that monetary order is becoming post-dollar, but that energy settlement is becoming more conditional, localized, and infrastructure-dependent. The key shift is from automatic settlement to conditional settlement: passage, clearance, insurance, documentation, and payment may become increasingly linked under conditions of chokepoint pressure.

For the Gulf, this means geography is being refinancialized. Ports, straits, pipelines, terminals, and loading points are becoming not only logistical assets, but also potential sources of settlement leverage. Iran's position is central because it combines three roles: energy producer, Hormuz-adjacent power, and sanctioned financial actor. This does not give Iran monetary dominance, but it may allow Tehran to create limited settlement authority around conditional access to a critical energy corridor.

For Gulf producers, the UAE's announced departure from OPEC points to a more differentiated energy order. It does not necessarily mean disorder, but it suggests that producers may increasingly pursue distinct output strategies, investment partnerships, and settlement preferences. The petrodollar system may persist, but the producer environment behind it becomes less uniform.

For Europe and Asia, Hormuz is no longer only an oil-price problem. It is also a payment, insurance, compliance, and legal-documentation problem. European firms must ask not only whether energy can be shipped, but whether it can be paid for, insured, cleared, and documented under contested conditions. For China, India, Japan, and South Korea, the issue is both exposure and opportunity: dependence on Gulf flows makes Hormuz disruption dangerous, while selective non-dollar settlement mechanisms may gain practical relevance in limited contexts.

For the United States, the challenge is not sudden monetary collapse, but conditionality. The dollar's power rests not only on formal dominance, but on routine use. If more transactions become shaped by regional access rules, sanctions-avoidance mechanisms, local clearing arrangements, chokepoint fees, producer fragmentation, or diversified Gulf energy strategies, dollar universality becomes less complete even if dollar dominance persists.

These implications create several risks. Transaction uncertainty rises when firms cannot assume that standard settlement channels will apply. Legal ambiguity expands when passage fees, alternative settlement requirements, or access-conditioned payments are interpreted either as legitimate access charges or as coercive interference with navigation. Escalation risk increases if access pricing is treated as economic warfare and enforcement actions generate maritime counter-pressure. At the same time, parallel mechanisms for limited settlement autonomy may multiply, including local fee systems, bilateral clearing arrangements, alternative payment channels, and commodity-linked settlement practices.

Taken together, Hormuz access pricing and UAE producer autonomy point toward the same strategic pattern: the weakening of automaticity. Passage is no longer automatically separate from payment conditions. Settlement is no longer automatically reducible to dollar usage. Gulf oil governance is no longer automatically contained within OPEC discipline.

The petrodollar system does not need to collapse in order to lose part of its geopolitical power. It only needs to become less automatic.

8. Conclusion

The Strait of Hormuz is not only an energy chokepoint. It is becoming a site where access, settlement, and monetary hierarchy intersect. The reported collection of passage fees does not prove that the petrodollar system is collapsing, nor does it prove that a new value system has fully emerged. Its significance is more specific: the ability to condition access at a critical node can create partial authority over payment conditions.

For Iran, this authority is not merely symbolic. Iran's position as both an energy producer and a Hormuz-adjacent power gives it a distinctive ability to connect geography, energy, and settlement. If access to Hormuz becomes linked to accepted payment instruments, fees, clearance procedures, or preferential transit rules, Iran may help generate a regional value structure before any new currency system fully forms.

The UAE's announced exit from OPEC, if sustained, reinforces this pattern from another direction. It does not end the Gulf oil order, but it weakens the collective producer-governance framework that helped make dollar-denominated oil trade appear routine and predictable. The likely future is therefore not the sudden death of the petrodollar, but a more fragmented settlement environment in which strategic nodes, regional producers, and alternative payment practices acquire greater influence over how energy-related transactions are structured.

The petrodollar is not collapsing at once. It is being de-universalized at strategic nodes and fragmented through Gulf energy governance. The ability to condition access does not automatically create control over money, but it can create the conditions under which regional value systems begin to emerge.

Bibliography:

- Anadolu Agency. (2026, April 23). *Iran says it collected 1st revenue from tolls imposed on ships transiting Hormuz*. Anadolu Agency. https://www.aa.com.tr/en/middle-east/iran-says-it-collected-1st-revenue-from-tolls-imposed-on-ships-transiting-hormuz/3915660
- Associated Press. (2026, April 28). *The UAE's departure from OPEC shakes up the alliance that influences oil prices worldwide*. AP News. https://apnews.com/article/uae-opec-oil-prices-c6779acba51365416ab1898b18f2beb2
- Bank for International Settlements. (2022, October 27). *Triennial Central Bank Survey: OTC foreign exchange turnover in April 2022*. Bank for International Settlements. https://www.bis.org/statistics/rpfx22_fx.pdf
- Chainalysis. (2026, April 10). *Iran's Strait of Hormuz crypto toll*. Chainalysis. https://www.chainalysis.com/blog/iran-strait-of-hormuz-crypto-toll/
- Cohen, B. J. (2015). *Currency power: Understanding monetary rivalry*. Princeton University Press.
- Eichengreen, B. (2011). *Exorbitant privilege: The rise and fall of the dollar and the future of the international monetary system*. Oxford University Press.
- International Energy Agency. (2026). *Strait of Hormuz*. International Energy Agency. Retrieved April 29, 2026, from https://www.iea.org/about/oil-security-and-emergency-response/strait-of-hormuz
- International Monetary Fund. (2026, March 27). *IMF data brief: Currency composition of official foreign exchange reserves, 2025 Q4 data*. IMF Data. https://data.imf.org/en/news/imf%20data%20brief%20march%2027
- Kirshner, J. (1995). *Currency and coercion: The political economy of international monetary power*. Princeton University Press.
- Reuters. (2026a, April 21). *Scam messages offering ships safe transit through Hormuz, security firm warns*. Reuters. https://www.reuters.com/world/middle-east/scam-messages-offering-ships-safe-transit-through-hormuz-security-firm-warns-2026-04-21/
- Reuters. (2026b, April 28). *HSBC sees limited near-term impact on OPEC+ from UAE's departure*. Reuters. https://www.reuters.com/business/energy/hsbc-sees-limited-near-term-impact-opec-uaes-departure-2026-04-28/
- Reuters. (2026c, April 28). *UAE leaves OPEC in blow to global oil producers' group*. Reuters. https://www.reuters.com/markets/commodities/uae-says-it-quits-opec-opec-statement-2026-04-28/
- United Nations. (1982). *United Nations Convention on the Law of the Sea*. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
- U.S. Energy Information Administration. (2023, November 21). *The Strait of Hormuz is the world's most important oil transit chokepoint*. U.S. Energy Information Administration. https://www.eia.gov/todayinenergy/detail.php?id=61002
- U.S. Energy Information Administration. (2026). *World oil transit chokepoints*. U.S. Energy Information Administration. Retrieved April 29, 2026, from https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints
- Wall Street Journal. (2026, April 23). *Iran says it has received first revenue from Hormuz toll*. *The Wall Street Journal*. https://www.wsj.com/livecoverage/iran-war-us-ceasefire-2026/card/iran-says-it-has-received-first-revenue-from-hormuz-toll-8QAiAAB5afcuLLqPCX8U

MIDDLE EAST - STRAIT OF HORMUZ

The Strait of Hormuz – a Regional Conflict that Gives Rise to Coercive Global Relations

PhD. Eng. Stelian TEODORESCU (Romania)

The Strait of Hormuz has become the central strategic battleground in the latest ongoing confrontation involving Iran, the United States, and regional Gulf powers. What initially appeared to be a military conflict is increasingly turning into a struggle for the control of shipping lanes, access to oil and gas resources, and energy security and geopolitical influence.

Recent tanker movements, coordinated through informal understandings with Tehran, suggest that Iran may now be moving from a complete blockade of the Strait of Hormuz to selective control of both access to energy resources and global trade. This emerging dynamic could fundamentally reshape Gulf security and international energy policy.

Source: https://www.bbc.com/news/articles/c78n6p09pzno

Tensions between Iran and the United States have long been simmering. On April 18, 1988, the U.S. Navy launched Operation Praying Mantis against Iranian targets in the Persian Gulf in retaliation for the mining of the USS Samuel B. Roberts (FFG-58) four days before, which caused a massive hole in the ship's hull. Ten American sailors on the Samuel B. Roberts suffered serious injuries. Four of them suffered severe burns. Commander Paul X. Rinn was also injured. The ship should have sunk, but extraordinary damage control efforts by a highly trained crew kept the Samuel B. Roberts afloat. The U.S. response was fierce. Operation Praying Mantis was the largest of the U.S. Navy's five major surface actions since World War II. In the one-day operation, the US Navy destroyed two Iranian surveillance platforms, sank two of their ships and seriously damaged another.

But since tensions between Iran, the US and Israel escalated in the run-up to 2026, following the failure of the nuclear talks in Geneva and a previous 12-day air conflict in 2025, Iran has begun to show its capabilities again by launching potential actions to disrupt and even block access through the Strait of Hormuz. Tehran justifies the actions launched as a response to threats, including by temporarily partially

closing maritime traffic in the region as a warning and, moreover, even generating threats by completely blocking access to ships through the Strait of Hormuz. However, between February 15 and 20, Iran increased its oil exports three times its normal rate and reduced its oil stockpiles to diminish the risk of disrupting the energy trade. Saudi Arabia also tried similar measures. In the days before the attacks, war risk insurance premiums for ships passing through the strait increased from 0.125% to between 0.2% and 0.4% of the ship's insured value per transit. For very large tankers, this represents an increase of a quarter of a million dollars.

The disruption of maritime transport in the Persian Gulf has made many experts analyse the information that has emerged, as well as the effects generated by the strangulation of both world trade and access to energy resources. This triggered crisis shows that the dependence on the import of energy resources can become even more extensive in a very short time in the context of surprisingly small and difficult maritime transport routes, which depend on narrow straits, often called maritime "chokepoints".

One of the five waterways of very great strategic importance for the import and transport of energy resources is the Strait of Hormu. It is the most critical energy chokepoint in the world. Connecting the Persian Gulf to the Arabian Sea, it handles about 39% of seaborne crude oil trade and 19% of the natural gas trade, mainly from producers such as Saudi Arabia, the United Arab Emirates, Iraq and Qatar. For these aforementioned states, any agreement that allows Iran to regulate maritime access poses a direct strategic threat. Their economies depend heavily on uninterrupted hydrocarbon exports, and Iranian control over transit would increase Tehran's regional influence to their detriment.

The Strait of Hormuz is 34 kilometers wide at its narrowest point, forming a sea passage on a stretch of sea route between Larak Island (Iran) and Qabayn Island (Oman). Although the strait has a small overall width, the shipping lanes for oil tankers are even narrower, measuring only about 3 kilometers wide in each direction.

In 2024, it was estimated that 84% of the crude oil and gas shipments that pass through the strait were destined for Asian markets, with China receiving a third of its oil needs through the strait and having about a billion barrels of oil in reserve (only a few months of supply and consumption). Europe, in turn, receives 12% to 14% of its LNG imports from Qatar through the strait.

The blockade in the Strait of Hormuz in early 2026 created a significant energy crisis for Europe, with knock-on effects that increased fossil fuel costs by around €24 billion and led to gas prices rising by around 70% in March 2026. Although the direct physical shortage of oil and gas is less severe for Europe than for Asia - thanks to diversified suppliers such as the US and Norway - the globalised nature of energy markets means that Europe is forced to compete with other competing states and with energy needs for resources outside the Gulf, leading to prices rising at an accelerated pace.

Against this backdrop, the key energy risks now emerging for Europe are:

• *Costs to acquire the necessary energy resources are rising:* Gas prices at the Dutch Title Transfer Facility (TTF)[1] increased by over 50% immediately after the blockade in the Strait of Hormuz. Analysts warn that a prolonged shutdown could double or triple gas prices for Europe.

• *Supply chain contagion:* A significant portion of the liquefied natural gas (LNG) traded globally from Qatar – around 20% of global supply – is blocked by Iran through its blockade of the Strait of Hormuz, forcing Europe to bid more heavily for limited supplies from other sources.

• *Reduced refining input:* While direct imports of crude from the Gulf are lower than in previous decades, Europe remains vulnerable to a shortage of refined products such as diesel and jet fuel, particularly from refineries in Kuwait and Saudi Arabia.

• *Declining economic competitiveness:* Rising energy prices are disproportionately affecting Europe's energy-intensive economies, particularly in the industrial sector, including steel, chemicals and fertilisers, exacerbating the risks of an economic recession.

• *Difficulties in replenishing energy storage facilities:* The blockade of the Strait of Hormuz is hindering the ability of European nations to refill gas storage facilities for the winter, potentially leading to critical shortages later in the year.

The Persian Gulf is also a major hub for global fertilizer production and export. In the 2020s, the region accounted for about 30%-35% of global urea exports and about 20%-30% of ammonia exports. In total, up to 30% of internationally traded fertilizers normally transit the Strait of Hormuz.

Unlike most trade chokepoints, there is no viable alternative to the Strait of Hormuz for the Gulf states to export their energy resources, which is also to the detriment of the energy importing states in the Middle East. As a result, we can say that this operation to block the Strait of Hormuz is part of a strategic plan by Iran, which has periodically threatened to close the Strait of Hormuz since the 1980s, and it cannot

[1]*The Securities Transfer Facility, better known as the TTF, is a virtual Dutch natural gas trading point. This trading point provides facilities for a number of traders in the Netherlands to trade futures contracts, physical and stock transactions.*

be considered a surprise that the shipping disruptions since late February 2026, when the US and Israel launched air strikes on Iran for the first time, represent the most serious escalation in recent decades. This regional conflagration has interfered with the oil and gas supplies, one of the largest in history and caused the price for the global energy resources to skyrocket. It also damaged maritime transport in the Gulf exceeding any understanding and expectation. The Gulf region handles over 26 million containers annually, and major fertilizer exports also pass through here. As can be seen and understood, a prolonged interruption of maritime transport can have numerous direct and difficult-to-quantify effects on global production costs across all industrial sectors.

Iran's current blockade in the Strait of Hormuz seems to have reached its climax. We can state this without any doubt because, starting with April 14, 2026, "freeing" the Strait of Hormuz – following the intense media coverage of this volatile blockade which began at the end of February – is considered, at least theoretically, by all the countries of the world a dire need, a fragile one.

Two of the largest nations in the world in terms of populations, China and India, prove that they favour diplomatic solutions, urging restraint and emphasizing the importance of "unfettered freedom of navigation". Their reactions and actions are most likely determined by the severe and immediate economic impacts, including the accelerated and uncontrollable increase in the prices of energy resources and, implicitly, the prices of all other agricultural and industrial products, but especially by the disruptions to critical energy resource transports, such as GPL imports for India and crude oil flows for China.

In this context, unblocking of the Strait of Hormuz seems to be a critical event from a security point of view for China, India and Europe, as well as for other states in various regions of the world, since they are among the main importers of energy resources. Besides, the transport of these resources to their destination is through this area blocked by Iran. However, even with diversified suppliers, for example, the supply of energy resources to China, India and other counries in the world remains largely dependent on key maritime corridors.

The Strait of Hormuz is the most important of these routes. In 2025, approximately 15 million barrels of crude oil per day (approximately 34% of global maritime trade in crude oil) passed through the strait. Most of these shipments were destined for Asian markets, with China and India together representing the beneficiaries of approximately 44% of world exports. For China, the main vulnerability lies not in its dependence on a single producer but in its dependence on a limited number of transportation corridors. Research by the Columbia Center for Global Energy Policy estimates that about half of China's crude oil imports and nearly a third of its liquefied natural gas imports come from the Middle East, with much of this energy supply normally passing through the Strait of Hormuz before reaching Asian markets. China's dependence on oil imports is often cited as a major vulnerability in its energy system.

However, this view may be a deliberately induced and misleading one if we do not take into consideration China's broad energy mix. Analyzing China's situation, needs, and policies regarding its actual energy needs, we can say that China remains structurally less dependent on oil than the headline figures on crude imports suggest. Official data shows that China's coal resources will still provide 51.4% of its total energy consumption (2025), and "clean energy" (natural gas plus hydropower, nuclear, wind, solar) 30.4%, with oil remaining around 18.2%. However, oil is still essential for petrochemicals, aviation, shipping and heavy transport, so price increases and disruptions to refinery feedstocks are quickly passed on to margins and logistics costs, even if national energy security is not threatened as immediately as one would like it to appear.

So, while China imports a large portion of the crude oil it consumes, oil accounts for only a fraction of the country's total energy supply. According to the 2025 Statistical Bulletin, China's total energy consumption reached 6.17 billion tons of standard coal equivalent, an increase of 3.5% over the previous year. In the past decade, the share of coal in the energy mix has gradually decreased, while the contribution of renewables and other clean energy sources has increased.

China's dependence on imported crude oil remains substantial. Estimates generally place the reliance on crude oil imports at over 70% of domestic consumption. Much of this supply arrives by sea, making maritime shipping a critical element of China's energy security. This is why China's energy policy has focused on three main safeguards: maintaining strategic oil reserves, diversifying crude oil suppliers, and accelerating electrification across the domestic energy system. Together, these measures aim to reduce the impact of external supply disruptions.

Petroleum products remain essential in the sectors mentioned above, alternatives remain limited, and price increases are transmitted quickly and have difficult-to-manage effects on production costs and final prices.

Recent economic indicators highlight this emerging pressure. Official data shows that China's manufacturing purchasing managers' index (PMI) returned to 50.4 in March 2026, signaling a renewed expansion in factory activity. However, sub-indices tracking production costs rose, suggesting that manufacturers are starting to face stronger cost pressures. If sustained, this dynamic could translate into a gradual decline in industrial profitability and export competitiveness.

Amidst all this evolving backdrop, however, China has spent more than a decade building up strategic oil reserves as a buffer against surprise supply disruptions. However, the exact size of these reserves remains unclear. Official data on strategic reserves is rarely released. According to international media reports, analysts estimate China's strategic oil reserves at around 900 million barrels, equivalent to just under three months of imports. When broader oil storage measures are taken into account, the available buffer appears to be larger. These estimates include commercial stocks held by refineries and oil stored in bonded facilities. Other analyses, however, estimate that China's total oil storage capacity could reach about 1.39 billion barrels, enough to cover about 120 days of net imports, based on the current consumption levels. Similarly, the Peterson Institute for International Economics places the combined strategic and commercial reserves at about 1.3 to 1.4 billion barrels, equivalent to about four months of imports. For example, China's crude oil imports are set to reach record levels in 2025, averaging between 11.55 million and 11.6 million barrels per day, according to widely cited estimates. Import volumes also increased in early 2026 as refineries maintained high processing rates and continued to build inventories. In this context, China's rapid electrification is gradually reducing its exposure to oil price shocks, especially in the transportation sector. Electric vehicles (EVs) are now a major component of China's auto market. Domestic data indicate that new energy vehicles (NEVs) accounted for 50.8% of vehicle sales in 2025, with an even higher share among passenger cars. This shift reduces the number of households directly affected by fluctuations in gasoline prices and lowers the overall sensitivity of the economy to increases in retail fuel prices.

Looking at how the energy resources needed are transported, this is itself a risk amplifier: Colombia's CGEP notes that over 90% of China's crude imports are carried by sea. Pipeline imports offer some diversification, particularly through supply routes from Russia and Central Asia. These flows help stabilize supply, but remain relatively small compared to China's overall import demand.

An analysis by Alicia García-Herrero of the Peterson Institute for International Economics highlights the importance of Europe in this context. The European Union absorbs about 15% of Chinese exports, meaning that a slowdown in economic growth caused by a decline in energy resources in Europe would quickly spill over into China's export sector. Recent trade data suggests that Chinese firms may already be preparing for such risks. While trade volumes remained significant in early 2026, imports grew significantly faster than processing needs, suggesting that refiners and industrial firms were building up precautionary stocks.

For the world, aviation is the clearest sectoral transmission mechanism, as jet fuel has few substitutes and is traded globally. Airlines have raised fuel surcharges, and normalization of jet fuel supplies could take months, even if flows resume, given refinery disruptions and logistical constraints.

Transportation and insurance costs compound the shock. The March 2026 Vortexa report highlights the mechanisms of disrupted tanker logistics (shadow fleet concentration, off-corridor queuing, and accumulation of floating buffers), which increases effective delivery costs and uncertainty for refiners.

For the broader economic outlook of all countries, the most significant risk may not come from domestic fuel supplies but from significantly declining global demand. Steeply rising global energy prices could slow economic growth in major trading partners. If this happens, demand for exports from all countries could fall sharply, putting further pressure on production across the economy and corporate profitability.

The disruption of access through the Strait of Hormuz has made global energy markets enormously vulnerable to the effects of geopolitical conflicts. Asian economies have been particularly hard hit because of their heavy reliance on energy exports from the Gulf. Oil supply disruptions and rising transport risks have intensified inflationary pressures, energy insecurity and market volatility in several regions. Recent developments in the Strait of Hormuz region demonstrate that Tehran may now exercise selective authority over maritime transit, rather than imposing a complete blockade without preferential selection.

The current situation in the Middle East could become a long-term strategic reality. Such a development could create the conditions for a prolonged state of instability, rather than a real resolution of the conflict in the region. Such a situation would institutionalize uncertainty in global energy markets and increase the likelihood of a future escalation of the conflict situation in the region.

The current confrontation in the Strait of Hormuz reflects a broader transformation in modern geopolitical conflict, where control and influence over trade routes and access to energy resources, and thus the economic stability of the world's states, may become more strategically valuable than territorial conquest. Iran appears to be demonstrating that its greatest power lies not in conventional military superiority but in its ability to disrupt the global economy through various hybrid levers, significantly influencing oil prices, inflation, international diplomacy, and political stability not only in those rival states but in all other countries in the world.

A military escalation of the conflict aimed at fully reopening the Strait of Hormuz could deepen the regional conflict and further destabilize global markets. However, tolerating selective Iranian control risks weakening American credibility and shifting the regional balance of power in Tehran's favor. The current situation also exposes the limits of military power in resolving structural geopolitical disputes. Even if active fighting subsides, the underlying competition for maritime control, energy security, and regional influence is likely to persist.

If selective Iranian containment becomes a long-term endeavor, the Middle East region could enter a prolonged era of economic coercion, strategic competition, and recurrent confrontation.

Biographies of the authors

❖ ❖ ❖

Matías González POMMERENKE (Chile)

He is a Marine Infantry Officer in the Chilean Navy, an Amphibious Systems Engineer with a specialization in Infantry.

He holds a Professional Master's Degree in Strategic and Foresight Analysis from UDIMA in collaboration with LISA Institute. He has experience in Operational Combat Units and Battalion- and Brigade-level Staffs.

He has specialized in scenario building, intelligence analysis, and security analysis, with a focus on strategic planning in complex environments. With more than 11 years of experience leading tactical units and analytical teams that advise command authorities, his work is oriented toward anticipating risks, threats, and opportunities in order to reduce uncertainty for decision-makers.

His main areas of interest are Intelligence, Security, Strategy, Defense, International Conflicts, Geopolitics, and International Relations.

❖ ❖ ❖

Bernd Oliver BÜHLER (Germany)

Bernd Oliver Bühler is a German entrepreneur, consultant, lecturer and author with more than 20 years of international experience at the intersection of economic intelligence, strategic communication, governance, risk, compliance, security and geopolitical analysis.

He studied economics at the University of Poitiers in France and completed a postgraduate programme in Strategy and Competitive Intelligence at ESLSCA Business School in Paris, within an intellectual environment shaped by France's tradition of economic warfare, strategic intelligence and the psychological dimensions of influence. His early professional experience included corporate strategy, business intelligence and security-related consulting, as well as international communication and journalism in the fields of defence, security and European affairs.

Since 2006, he has lectured in economics, finance, governance, risk and compliance at international business schools, including ESLSCA Business School in Paris and Cairo. Alongside his academic work, he has advised companies and executives on strategic risk, information protection, crisis management, compliance and security-related decision-making.

His current work focuses on economic intelligence, cognitive warfare, artificial intelligence, institutional trust and the strategic resilience of democratic societies. At the core of his work is the conviction that knowledge, responsibility and strategic clarity are essential for navigating uncertainty — in companies, institutions and the next generation of decision-makers.

❖ ❖ ❖

❖ ❖ ❖

Gargi AWASTHI (India)

She is dedicated to assisting community by utilizing area expertize to drive change. She has proficient in devising and managing information gathering systems for collecting data on policies and impacts. She has excellent interpersonal, analytical and public communications skills.

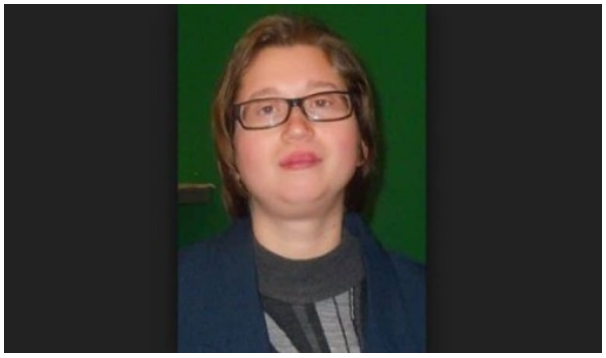
Bachelor of Tehnology, Mechanical Engineering at Chandra Shekhar Azad University in Kanpur.

She has experience to United Nations, ISPPR, as Policy Analyst and Diplomat, New Delhi, from 12/2022 until now.

She participated in multilateral negotiations concerning regional security initiatives sponsored by United Nations. She organized meetings with foreign government officials to discuss areas of mutual interests.

She participated to built and updated crisis communication plans to handle diverse situations. She is engaged in public diplomacy activities such as briefings, interviews, lectures and workshops designed for students interested in learning more about Foreign Services careers.

❖ ❖ ❖



Mona AGRIGOROAIEI (Romania)

She is a Political Science graduate with a master's degree in Political Marketing and Communication at "Al. Ioan Cuza" University in Iaşi. 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.

❖ ❖ ❖

Gilles DELAFON (France)

Gilles Delafon is an Associate Research Fellow at the Thomas More Institute. A correspondent in Beirut during the Lebanese civil war from 1984 to 1988, he is the author of Beirut, the Soldiers of Islam (1989), one of the first books to highlight the emerging Islamist threat.

A senior reporter and editorial writer for Le Journal du Dimanche from 1989 to 2008, he covered major crises in the Middle East, including both Iraq wars and the Israeli–Palestinian peace process.

He subsequently served as Head of News at Canal+ from 2008 to 2016. He is also the author of The Reign of Contempt: Nicolas Sarkozy and the Diplomats, 2007–2011 (2012). A graduate of Columbia University (New York), he founded the consulting firm Lord Jim Consulting in 2016, where he currently serves as President. He joined the research team of the Thomas More Institute in September 2023.•

❖ ❖ ❖

❖ ❖ ❖

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.

❖ ❖ ❖

Fikret ARTUÇ (Turkiye)

He was born in Istanbul in 1971. After completing his primary and secondary education in Istanbul, He pursued his university studies in the Turkish Republic of Northern Cyprus at Eastern Mediterranean University, where He studied International Relations and Political Science. He continued his academic journey at Bilkent University's Department of Economics, focusing on Europe, Russia, Eastern Europe, and the Eurasian market, as well as the economic dynamics of these regions. In addition, He completed a minor in Economics at Anadolu University, further enriching his education with a multidimensional perspective.

He began his professional career in print media as a proofreader. He then advanced his experience in the media field by working as an editor for various magazines. Later, He transitioned into visual media and, with the aim of becoming a skilled director, received training and worked in production companies in the fields of sound, camera, lighting, and editing.

During this period, He took part in numerous documentary, promotional, commercial, television series, and film projects as a screenwriter, assistant director, and director. In 2004, He opened a new chapter in his career by moving into thematic news channels, where He continued to apply his accumulated experience in a different platform.

❖ ❖ ❖

❖ ❖ ❖

Dr. Khodor DAYEH (Lebanon)

Dr. Khodor Dayeh is an intelligence analyst specializing in counter-terrorism and behavioral analysis. He is the author of the book "Beyond Extremism: How Psychological Profiling Helps Understand and Confront Terrorism."

❖ ❖ ❖

Zurab BEZHANISHVILI (Georgia)

Academic Experience

- Goethe University Frankfurt and Makerere University — Green and Digital Future Conference (18–22 May 2026 in Uganda) Paper presented: "Africa as the New Heartland: Digitalization, Resource Governance and the Future of Raw Materials Conflict."

Organizational Involvement, Affiliations and Education

- George C. Marshall European Center for Security Studies — Alumni (2026)

- Geneva Center for Security Policy (GCSP) — Alumni (2023)

- ODIHR Community 2023

- Academic Council of the United Nations System (ACUNS). Active member since 2023.

- Institute for Economics and Peace (IEP) — Ambassador (since 2025)

- Parliamentarians for Nuclear Non-Proliferation and Disarmament (PNND) Active member since 2023.

- International Political Science Association (IPSA) — Board Member (2023–Present)

- International Community for Development and Progress in Georgia (IC4GDP) — Founder and President (2010–Present)

- Moscow State University (MSU SPA) Master in Public Administration 2000-2006 (Doctoral grant in Political Studies 2006-2008 denied due to the Russo-Georgian War).

Recent activities

- Developed the concept of self-defense for Georgian society, including civil-military cooperation (nuclear threats, disasters, wars, war games).

- Designed the strategic framework for the socio-economic development of Georgia; a roadmap for the civil society ecosystem, covering human rights, anti-corruption and civic oversight; the International Club of Public Administrators to foster professional exchange and international collaboration.

- Thematic Coordinator, Frontiers in Political Science: "The Future Architecture of National Security and Policymaking in the Digital Age".

❖ ❖ ❖

❖ ❖ ❖

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.

❖ ❖ ❖

PhD. Shaoyuan WU (USA)

Dr. Shaoyuan Wu is the Research Lead and Director of the Global AI Governance and Policy Research Center at EPINOVA LLC. His work focuses on international security, strategic risk assessment, energy security, global governance, conflict dynamics, and AI-driven systemic transformation.

❖ ❖ ❖

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

SCAN IN ORDER TO ACCESS:
pulsulgeostrategic.ro

ISSN: 1843-701X FOUNDED IN 2017 | BUCHAREST

office@pulsulgeostrategic.ro