Volume 17 | Spring 2026

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
NATO Strategic Communications Centre of Excellence

Volume 17 | Spring 2026

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
NATO Strategic Communications Centre of Excellence

ISSN 2500-9486 (online)
ISSN 2500-9478 (print)
DOI 10.30966/2018.RIGA.17
Defence Strategic Communications

Defence Strategic Communications is an international peer-reviewed academic journal. The journal is a project of the NATO Strategic Communications Centre of Excellence (NATO StratCom COE). It is produced for scholars, policy makers, and practitioners around the world.

NATO Strategic Communications Centre of Excellence
Riga, Kalnciema iela 11b, Latvia, LV1048, www.stratcomcoe.org

Contents

Foreword

What a relief to know that oases of calm endure in a world of turbulence and turmoil. Peterhouse is the oldest and smallest college in Cambridge. In late April the university town retains its tranquillity touched by the diffident sunshine of early summer. Quiet reflection comes easily to the college, as indeed it has for seven centuries. Unsurprisingly, a colloquium of thinkers from around the world, not just scholars, chose this moment and place to imagine what might follow the much heralded demise of the international liberal order.

The first dialogue of the Knowledge Economy Transition by 2045 (KE2045) was convened at Peterhouse to consider how society should address the vacuum of big storytelling or metanarratives so absent from current public debate. Given that in any big story must sit a big idea. Yet as the group's orchestrator, Professor Malik Āl Dahlan, later observed, 'strategic communication was what allowed the recognition of rupture to become a threshold rather than remain a slogan: it gave the room a register through which the rupture could be carried forward as work rather than as commentary'.[1]

Conversation came to circle a central proposition: 'to design the political economy of a legitimate knowledge economy transition by 2045, through which a legitimate settlement in turn can be shaped'.[2] Legitimacy was considered the determinant of what would constitute a legitimate (gold to oil, 1971) or illegitimate (Washington Consensus, 1990s) transition from one stage of history to another. 'The political economy of recognition is the architecture by which that legitimacy is built.'[3] And that translates to finding an equitable distribution of resources and benefits between people and generations, preserving human dignity in a dehumanising

1 Growth Follows Recognition: The Road to Redemption—The Political Economy of a Legitimate Knowledge Economy Transition—the 2045 Paradigm (forthcoming), Quraysh.com.

2 Ibid., Opening Threshold.

3 Ibid.

DOI 10.30966/2018.RIGA.17.1

world of AI and emerging technologies, safeguarding natural assets for their own sake not simply as subservience to economic necessity.

Readers of this journal will be aware that the field of strategic communications, among its defining criteria, includes long-term (no less *longue durée*) and high-level storytelling. It's fundamentally about shifting and shaping significant discourses in society. It promotes a vision and ambition to create better societies in the future. And it roots itself in the values of freedom and choice of liberal democracy now struggling to retain its primacy in international politics. So it's normative, not simply instrumentalist communications.

Strategic communications is a concept that has been enthusiastically adopted by the NATO alliance of thirty-two nation states. Other governments have subsequently embraced the term, if not the thinking. As for storytelling in a turbulent, uncertain, and unpredictable world, NATO's narrative imagination is sadly constrained by what it sees as an existential confrontation between democracy and autocracy in geopolitics. Focusing on the day to day as national governments stagger from one perceived crisis to the next.

Pre-emption is consistently superseded by reaction. Pandemics, climate change, mass migration, and more equitable economic models are no longer foregrounded in conversation as states focus on a growing number of wars and economic recession amid transactional coping policies. The world is caught up in a vortex of securitisation and militarisation. Cast our minds back a few years and NATO was weighing other if not bigger concerns due to their interrelatedness for the evolution of the security environment. Undeniably viewed through a lens of threats and vulnerabilities, these reached beyond the battlefield into other areas of social and economic life. With an eye to 2043, the drivers of change were understood to be 'climate change, resource scarcity, disruptive technology development, securitization of economics, human networks

DOI 10.30966/2018.RIGA.17.1

empowered, the exploitation of the global commons and an international order in transition'.[4]

Not to downplay the accretion of influence that is emanating from authoritarian regimes, the political-military alliance sought a wide picture of understanding. If autocracy is making a siren appeal to a simpler way of life, a retreat from contradictions, then there must be substance in any alternative democratic offering, not simply sloganeering. And intent, not promise. Regrettably, the field of vision seems to be narrowing by the day.

The need to fill the vacuum of storytelling as grand strategy is not new. Winston Churchill described Europe in the aftermath of World War II as 'a rubble heap, a charnel house, a breeding ground of pestilence and hate'. While Dean Acheson spoke of his fellow politicians' 'misconceptions of the state of the world around us'.[5]

Acheson recalled: 'Only slowly did it dawn upon us that the whole world structure and order that we had inherited from the nineteenth century was gone and that the struggle to replace it would be directed from two bitterly opposed and ideologically irreconcilable power centers.'[6]

Many would suggest that we face a similar challenge today. Except today's threats come from the collapse in self-confidence of liberal democracy anchored in persistent failure to deliver on historic promises, while facing the growing appeal of populist and authoritarian governance beyond and in the West.

Equally, the return of Great Power assertiveness and sphere-of-influence geopolitics are dismantling international law, fanning the flames of securitisation and militarisation. And significantly, political elites are struggling to understand societal transformation driven by Artificial Intelligence and neural microtargeting. These are designed and owned as autocratic command-and-control technologies and ultimately businesses,

4 NATO Allied Command Transformation, *Strategic Foresight Analysis*, 2023, p. 13.

5 Dean Acheson, *Present at the Creation* (New York: W.W. Norton, 1988).

6 Ibid.

DOI 10.30966/2018.RIGA.17.1

and are increasingly being woven into the processes of state bureaucracies. Yet governments still talk of them as if they were exclusively tools. How myopic this may yet prove to be is underlined by NATO StratCom COE's convening of international futurists and technologists: 'Neuro-warfare is emerging, requiring urgent attention,' the authors warn. 'This convergence of human and machine surpasses artificial intelligence to become a neurotechnological revolution with profound implications for democracy and the information environment. Predicting human consciousness and interpreting neural data are not theoretical, they already exist.'[7]

Dynamic technologies are reshaping the information environment in which we live and through which ontologically we make sense of the world. In a technological landscape of algorithmic reach and microtargeting, what does it mean to be an individual—what is identity? And if knowledge can be shredded and reconstituted in an instant, how should consensus and collective memory be created? Soon, what will it mean to be human?

These drivers demand innovative storytelling—grand plans captured in big visions that anchor strategy and the perception of progress. In the twenty-first century we are ill-served by a twentieth-century lexicon. We lack the words to describe events unfolding before our eyes.

In 1947 imaginative measures followed the Bretton Woods initiatives aimed at preventing a replay of the disastrous trade wars, economic depression, totalitarianism, and societal upheavals of the 1930s.

The Marshall Plan was perhaps the greatest public diplomacy effort of the last century. The US committed 5 per cent of its GDP to the reconstruction of an exhausted and bankrupt Europe in the face of what the diplomat George Kennan saw as the relentless drive of Soviet Communism to absorb the European continent. In a tone not unfamiliar to contemporary audiences, Kennan's Long Telegram (cable 511 at

7 Neville Bolt and Elina Lange-Ionatamishvili, *The NextGen Information Environment* (Riga: NATO StratCom COE, 2026), p. 12.

DOI 10.30966/2018.RIGA.17.1

5540 words) sent in 1946 from Moscow, or his 'X' article published the following year in *Foreign Affairs*, had foreseen and forewarned against a Soviet ambition barely acknowledged in Washington political circles.[8] But how to respond? Kennan's words hummed on the wires:

> We must formulate and put forward for other nations a much more positive and constructive picture of sort of world we would like to see than we have put forward in past. […] Finally we must have courage and self-confidence to cling to our own methods and conceptions of human society. After [all], the greatest danger that can befall us in coping with this problem of Soviet communism, is that we shall allow ourselves to become like those with whom we are coping.[9]

Subsequently, Harry S. Truman's top-down project would prove visionary, driven nonetheless in the face of resistance from Congress.[10] Yet the president was not alone.

Independently a bottom-up or middle-up project was pursued by thirty-six economists, historians, and philosophers who met up at the Mont Pèlerin conference, in a hotel overlooking Lake Geneva, that would subsequently become the Mont Pelerin Society. Imagined by Austrian economist Friedrich Hayek, it aimed to fill a discursive vacuum via a refreshed interpretation of liberalism connecting market freedoms to individual freedoms. And as a way of keeping Europe both democratic and capitalist. And at peace.

What became after several twists and turns neoliberal economics would sweep the world in thirty years. From research and policy thinking in the 1950s and 1960s that built bridges to Wall Street, to the controversial laboratories of economic theory in Chile and Argentina in the 1970s,

8 Frank Costigliola, *Kennan: A Life between Worlds* (Princeton: Princeton University Press, 2023).

9 Kennan to Secretary of State, 861.00/2 - 2246: Telegram, 22 February 1946, https://nsarchive2.gwu.edu/coldwar/documents/episode-1/kennan.htm.

10 Benn Steil, *The Marshall Plan: Dawn of the Cold War* (New York: Simon & Schuster, 2018).

DOI 10.30966/2018.RIGA.17.1

through the 1980s reforms of Reagan and Thatcher, to the present day, it became one of the great projects of discourse creation and dissemination. That said, neoliberalism has been and continues to be heavily condemned for the creative destruction it has visited on states.[11]

Setting ethical and ideological concerns to one side for a moment, it's as a communications project that neoliberalism bears objective consideration. As an ambition that sought to present a worldview, a way of delivering it as realisable policy-set, and with an appeal to the 'invisible lines' in public discourse. Namely, to those traces of ideas and conversations present in the public imagination that could be joined up and targeted to meet the challenges of the day.

Like it or loathe it, here was an attempt at the kind of big thinking that today's generation of international political leaders is struggling to imagine. Save perhaps for China with its state capitalism and technological surveillance society, and its vision of an alternative sovereign order to the one dominated by the US since 1945.

As lofty as Hayek's ambitions were, the prosaic realities of finding benefactors to pay for flights and hotels with minimal strings attached required patient negotiation and navigation from the outset. A familiar picture to many academics today. Success is only judged in hindsight and never comes with guarantees. But a ten-day conference of presentations and periods of reflective conversation tackled topics as diverse as '*free*' enterprise and competitive order; the future of Germany; modern historiography and political education; problems and chances of European federation; and liberalism and Christianity. Years later, its legacy would come to shape a proposition around 'market deregulation, state decentralization, and reduced state intervention into economic affairs in general'.[12]

11 Bruce Caldwell, *Mont Pèlerin, 1947* (Hoover Institution Press, 2022).

12 Ibid.

Read the Mont Pèlerin conference transcripts, and it's noticeable how its participants were looking to create an enduring organisation but one with clear research questions: to explain to others the moral and economic causes of the crisis; to redefine how totalitarian and liberal systems function; to re-establish the rule of law; to prevent the misuse of history that advances creeds hostile to liberty; to create international order to safeguard peace and liberty; and to establish harmonious international economic relations.[13]

And with a clear commitment: 'The group […] seeks to establish no meticulous and hampering orthodoxy. It aligns itself with no particular party. Its object is solely, by facilitating the exchange of views among minds inspired by certain ideals and broad conceptions held in common, to contribute to the preservation and improvement of the free society.'[14]

There is a clear resonance with what took place at Peterhouse in Cambridge in 2026. What many see today is a need to address the all-important gap in public discourse. If the twentieth-century liberal order has indeed broken down irreversibly, or at least is mutating to a different form, what system should replace it in the twenty-first? And what should become the bedrock of transition? KE2045 tapped into a crisis of legitimacy in its plea to recognise the need for epochal change. Significantly, strategic communications can be viewed as an intersection between two axes of tension. One axis represents a tension between authority (holding power) and legitimacy (moral right to hold power) and the second a tension between persuasion and coercion.[15] At the heart of this form of political communications sits a societal negotiation that creates a consensus around a mobilising idea. Legitimacy here must infuse the fabric of politics, while authenticity is required for those politics to be persuasive, to ring true. Successful scripts are intrinsically authentic. William Goldman, that doyen of Hollywood screenwriters, observed

13 Ibid.

14 Ibid.

15 Neville Bolt, Martha Stolze, Leonie Haiden, and Jente Althuis, *Understanding Strategic Communications,* Terminology Working Group Publication 3 (Riga: NATO StratCom COE, 2023), p. 19; see Bolt's Paradigm.

DOI 10.30966/2018.RIGA.17.1

that a bad movie could be made from a good script, but a good movie rarely follows from a bad script.[16]

At a moment of rupture, we should recall that strategic communications sets out pre-emptively to shape the story of the day after tomorrow. This arises not from incrementally tweaking or even turbo-charging the past. Rather, from imagining the unimaginable and painting a picture, telling a story that societies want to embrace. And making both relevant to their everyday lives and aspirations for the future of their children and grandchildren.

First that means joining the dots, creating a coherent picture, without which no cohesive framework of analysis is possible. And without that conceptual framework, there can be no persuasive storytelling. But storytelling in the absence of substance will not convince anyone. Shaping the way we tell stories depends on the architecture of an idea and its ability to engage with the aesthetics of politics. We are reminded that President John F. Kennedy's Berlin speech in 1963 mentioned 'freedom' or 'free' fifteen times in 674 words. In his inaugural speech he had used 'free', 'freedom', and 'liberty' ten times in 1400 words.[17] Yet each moment aimed at more than rhetorical appeal. Freedom was to be a metaphor for a constructed reality, both architect and architecture of a new world.

In this issue of *Defence Strategic Communications* a variety of perspectives explore how to make sense of a disruption that is upending our customary worldviews. Malik Āl Dahlan highlights the collapse of international law under wanton assault from the projection of raw power—the realism of geopolitics and geoeconomics. If freedom emerged as the keyword to meet the mid-twentieth-century rupture that would inspire the Mont Pèlerin gathering, then for Dahlan legitimacy becomes the rallying point for intellectual and spiritual renewal in 2026. Roland Benedikter plots an array of current tensions among a variety of factors and actors in his attempt to join up the dots. That entails, he says, creating an inter- and

16 William Goldman, *Adventures in the Screen Trade* (Abacus, 1996).

17 Louis Menand, *The Free World* (London: 4th Estate, 2021), p. 334.

DOI 10.30966/2018.RIGA.17.1

transdisciplinary view to embrace the most prevalent trans-sectoral key dialectics, shifts, and trajectories if we are to anticipate the future of the security environment.

Timo Lenk and Julian Neylan look to the last two decades to trace the ways actors understood the adoption of FIMI (Foreign Information Manipulation and Interference) against the backdrop of dynamic geopolitical developments and institutional imperatives. Their chronicle talks to some of the key players who shaped the concept in response to growing and systematic state disinformation from foreign and domestic influences. Chiyuki Aoi et al. argue that diplomatic efforts and commitments to create cooperative relations between Europe and Indo-Pacific countries in countering foreign information manipulation have so far failed to bear fruit. Rhetorical alignment has struggled to deliver operational cooperation, suggesting a fundamental failure by European states to understand Indo-Pacific contexts.

Meanwhile, Natalya Kovaleva reveals how US–Belarus diplomatic relations have become dominated by phased releases of Belarus pro-democracy activists and human rights prisoners in return for payment from the US. Negotiations in the last two years have secured the release of 500 Belarusians, with another 900 still behind bars. Are humanitarian ambitions and their honourable outcomes being compromised by the Minsk government's new-found income stream? While on the fiftieth anniversary of the movie *All the President's Men* Paul Bell raises the dilemma of the journalist as objective witness. 'To be properly objective', he says, 'is not to be disengaged, it is the opposite.' Journalism has changed in Bell's long and rich career. Partisanship versus objectivity: where today is the dividing line? As each week brings new threats to liberal democracy, Mitch Ilbury asks what the Greek philosopher Plato would have made of it all. A political order straining under its own internal contradictions might not have appeared so alien to him. Far from tyranny being an external invader, he would have appreciated that it lurks latent in all systems of governance.

DOI 10.30966/2018.RIGA.17.1

Maria Golubeva designs wargame scenarios. Against the backdrop of a fracturing liberal order, she highlights the ambiguity of rationale in the ways hybrid actors seek to disrupt the political status quo. By not automatically attributing geopolitical intent, wargames, she argues, can offer more nuanced analytical insight. Finally, the children's construction toy LEGO has become a global commercial success in recent decades. However, perhaps the company business plan never foresaw its emergence as an actor in the geopolitical sphere. Louis Brooke and Sophia Krauel reveal what democratic states might yet learn from Iran's experience of depicting LEGO characters in its information output during the current war with the US.

We wish you a stimulating read.

Dr Neville Bolt

Editor-in-Chief

Spring 2026

How the Term FIMI Took Shape: Told by Those Involved

Timo Lenk and Julian Neylan

Keywords—*Foreign Information Manipulation and Interference, FIMI, EEAS, disinformation, institutionalism, sensemaking, strategic communication, strategic communications*

About the Author
Timo Lenk is Associate Fellow at TU Dortmund University and postdoc researcher in the Horizon Europe project ADAC.iO. His research interests are in strategic communications, disinformation, and the public sphere.[1]

Julian Neylan is Dissemination and Defence Lead at the DISARM Foundation, London, and Training Programme Lead with Alliance4Europe. His research interests are in disinformation, cyber security, and public health.

Abstract
Foreign Information Manipulation and Interference is shaping the EU's response to disinformation and foreign influence operations. However, the concept did not emerge overnight. It took shape in a particular time period and under specific geopolitical conditions, accompanied by key geopolitical events. While general accounts have traced the adoption of the FIMI concept on the basis of policy documents and other official sources, this article examines the adoption process from the perspective of individuals who were involved in it at the time. Based on a sample of selected interviewees and adopting an organisational theory perspective, the article demonstrates how actors understood the adoption

1 Timo Lenk (corresponding author), TU Dortmund University, Emil-Figge-Straße 50, 44227 Dortmund, Germany, +49 231 755 6534, Timo.lenk@tu-dortmund.de.

DOI 10.30966/2018.RIGA.17.2

of FIMI against the backdrop of dynamic geopolitical developments and institutional imperatives.

Introduction

In the long history of war propaganda,[2] foreign attempts to shape information for political ends are not new, but the concept of Foreign Information Manipulation and Interference (FIMI) to describe such threats to the information environment is a recent development. Prompted by concerns in Western democracies over foreign disinformation that surged after events like Russia's 2014 annexation of Crimea and meddling in the 2016 US elections, there were calls to better define and counter foreign influence in the digital information space.[3] Within the European union the issue of what was termed 'foreign digital interference' was mandated to be addressed by the European External Action Service (EEAS) by 2019 amid various incidents and investigative reports.[4] Experts and policymakers alike recognised that the existing terminology including *fake news* or the general term *disinformation* were insufficient to capture the evolving scope and multidimensionality of influence campaigns that often involve more than just false content.[5] Existing definitions were frequently borrowed from Russian concepts such as *informatsionnoye protivoborstvo* (IPb), translating as *information confrontation*, or *dezinformatsiya*—disinformation.[6] Terms like *information*

2 Propaganda is understood here as communication activities aimed at influencing the beliefs and behaviours of target audiences in line with the propagandist's agenda, often seeking to sow discord and enmity without audiences being aware of the manipulation. *War propaganda* refers to such efforts accompanying kinetic operations during wartime. Dror Walter and Yotam Ophir, 'Trolls without Borders: A Comparative Analysis of Six Foreign Countries' Online Propaganda Campaigns', *Human Communication Research* 49 Nº 4 (2023): 421–32, https://doi.org/10.1093/hcr/hqad022.

3 Lucas Proto, Paula Lamoso-González, and Luis Bouza García, 'The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight', *Media and Communication* 13 (2025), https://doi.org/10.17645/mac.9474.

4 Nicolas Hénin, *FIMI: Towards a European Redefinition of Foreign Interference*, EU DisinfoLab, 2023, https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf [accessed 27 February 2026].

5 Ibid.

6 Michelle Grisé et al., 'Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation', *RAND*, 2022, https://www.rand.org/pubs/research_reports/RRA198-8.html. Deen Freelon and Chris Wells, 'Disinformation as Political Communication', *Political Communication* 37 Nº 2 (2020): 145–56, https://doi.org/10.1080/10584609.2020.1723755.

warfare or *information operations* captured parts of the problem but were not serviceable for defining the mandate of the EEAS. The latter therefore commissioned research to further develop the conceptual framework. Notably, James Pamment established a hierarchy starting from misinformation, going up to disinformation,[7] then influence operations, and finally foreign influence as the most severe level.[8] While this hierarchy places an emphasis on foreign influence activities, the term *FIMI* itself was adopted by the EEAS in the early 2020s to capture state-sponsored manipulation activities, making a shift from focusing on just false content to a broader spectrum of patterns of malign behaviour, as well as on the specific actors.[9] At the time, US government agencies and intelligence organisations used a similar term, 'Foreign Malign Influence', to characterise the problem,[10] while the UK and Australia used the term 'foreign interference'.[11] FIMI conceptually builds on (historical) propaganda and disinformation terminology but reframes these concepts into a modern context of digital information spaces, emphasising coordinated foreign campaigns purported by EU institutions to threaten democratic processes.

While the context and sequence of events that led to the emergence and adoption of the FIMI concept have already been mapped out, for example

7 There are at least two approaches to defining the relationship between mis- and disinformation. One distinguishes them as separate categories: misinformation refers to the unintentional spread of inaccurate information, while disinformation involves the intentional dissemination of false information to deceive. The alternative approach adopted here understands misinformation as an overarching concept encompassing inaccurate or misleading information regardless of intent, with disinformation as a subcategory referring to goal-directed manipulation. Michael Hameleers et al., 'Mistake or Manipulation? Conceptualizing Perceived Mis- and Disinformation among News Consumers in 10 European Countries', *Communication Research* 49 № 7 (2021): 919–41, https://doi.org/10.1177/00936502219977l9.

8 James Pamment, 'The EU's Role in the Fight against Disinformation: Developing Policy Interventions for the 2020s', *Carnegie Endowment for International Peace*, 2020, https://carnegieendowment.org/research/2020/09/the-eus-role-in-the-fight-against-disinformation-developing-policy-interventions-for-the-2020s.

9 Raquel Miguel, 'Decoding FIMI: A Complex Interrelation with Disinformation', *Project Athena*, 2025, https://project-athena.eu/decoding-fimi-a-complex-interrelation-with-disinformation/ [accessed 27 February 2026].

10 '50 U.S. Code § 3059 - Foreign Malign Influence Center', *LII / Legal Information Institute,* https://www.law.cornell.edu/uscode/text/50/3059#e_2.

11 Home Office, 'Foreign Interference: National Security Bill Factsheet', *GOV.UK,* updated 24 June 2025, https://www.gov.uk/government/publications/national-security-bill-factsheets/foreign-interference-national-security-bill-factsheet [accessed 13 April 2026].

DOI 10.30966/2018.RIGA.17.2

by Proto et al.,[12] in great detail, the authors know of no account which specifically focuses on the perspectives of the people directly involved in or closely following its development and implementation at the time. This paper addresses this gap by giving voice to individuals who played a role in shaping and adopting the concept. Two theoretical lenses from organisation theory, institutionalism and sensemaking, are employed to frame and contextualise the adoption of the FIMI concept. While an institutional lens helps explain the role of environmental pressures in the organisational adoption of change,[13] a sensemaking perspective sheds light on how individual actors interpret ambiguous circumstances and transform them into coherent understandings that inform and guide action.[14] Jensen et al. argue that institutional concepts alone cannot explain how organisational actors make sense of and adopt change, and call for complementing an institutional perspective with sensemaking to analyse how individual actors' interpretations shape adoption processes, linking micro and macro levels of analysis.[15] Since the FIMI concept is new and academic literature on its adoption is sparse, applying this integrated lens constitutes a novel contribution: it illuminates how the EU's adoption of FIMI was shaped by both institutional pressures and the sensemaking of individuals and organisations who framed and operationalised the concept.

The article is structured as follows. The next section briefly recapitulates key events in the adoption process of FIMI. This part relies to a significant extent on grey literature, including policy documents, strategy papers, and official reports, which is a valuable source of information, especially in emerging research fields.[16] This is followed by a description of the

12 Proto et al., *'EU's FIMI Turn'*.

13 Mats Alvesson and Anna Jonsson, 'Organizational Dischronization: On Meaning and Meaninglessness, Sensemaking and Nonsensemaking', *Journal of Management Studies* 59 Nº 3 (2021): 724–54, https://doi.org/10.1111/joms.12790.

14 Karl E. Weick, Kathleen M. Sutcliffe, and David Obstfeld, 'Organizing and the Process of Sensemaking', *Organization Science* 16 Nº 4 (2005): 409–21, https://doi.org/10.1287/orsc.1050.0133.

15 Tina Blegind Jensen, Annemette Kjærgaard, and Per Svejvig, 'Using Institutional Theory with Sensemaking Theory: A Case Study of Information System Implementation in Healthcare', *Journal of Information Technology* 24 Nº 4 (2009): 343–53, https://doi.org/10.1057/jit.2009.11.

16 Eduardo Noronha, João Varela Da Costa, and Miguel Mira Da Silva, 'A Multivocal Grey Literature Review on Fake News and Risk Management', *Discover Computing* 29 Nº 1 (2026), https://doi.org/10.1007/s10791-025-09902-w.

DOI 10.30966/2018.RIGA.17.2

theoretical framework utilised to interpret the accounts of the experts interviewed for this article from an organisational perspective, and then an outline of the methodological approach. The paper then moves on to the interviewees' perspectives, with a particular emphasis on identifying shared explanations for the adoption of the FIMI concept, followed by a brief conclusion. The focus of the analysis is hermeneutic and exploratory in nature, with the aim of gaining a deeper understanding of the interviewees' perspectives on the reasons behind the adoption of FIMI.

A Brief History of the FIMI Concept from a General Account

In recent years democracies have grown increasingly concerned about hostile disinformation and influence operations. The EU has responded by coining and adopting the concept of FIMI to describe a broad range of coordinated foreign influence activities targeting the information space. FIMI refers to a 'mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes'.[17] Described as 'manipulative in character',[18] FIMI shifts the focus from the truthfulness of content to a broader range of deceptive behaviours.

Initially the EU's approach to information influence treated disinformation as a core problem, based on a widely shared academic consensus that the massive spread of false information online could destabilise democratic discourse and with that the integrity of democratic processes.[19] However, multiple overlapping terms circulated, including misinformation, disinformation, propaganda, and coordinated inauthentic behaviour,

17 European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats. Exposing the Architecture of FIMI Operations*, 2025, https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf [accessed 27 February 2026].

18 Ibid.

19 Stephan Lewandowsky et al., 'Misinformation and the Epistemic Integrity of Democracy', *Current Opinion in Psychology* 54 (2023): 101711, https://doi.org/10.1016/j.copsyc.2023.101711.

DOI 10.30966/2018.RIGA.17.2

each capturing a different part of the problem.[20] EU institutions lacked a unified concept tailored to the EEAS's specific mandate to counter foreign authoritarian influence in European public discourse.[21] The EEAS commissioned research that came to the conclusion that the EU should reframe the problem as one of foreign interference conducted in a coordinated manner rather than false information circulating online.[22] This reframing would allow treating information manipulation as a security threat. The result was the development of the concept of FIMI.[23] By focusing on manipulative behaviours including but not limited to the spread of false information, such as the use of fake personas, the coordinated amplification of content, and, more recently, AI-enabled techniques, the FIMI concept is designed to encompass the full spectrum of modern information threats while sidestepping definitional debates related to terms like *disinformation* and *fake news*. The scope of FIMI was deliberately limited to foreign actors engaging in concrete, definable harms, thereby protecting the EEAS from accusations of silencing domestic criticisms or legitimate concerns raised by citizens. This aspect became increasingly important with the growing politicisation of the terms *fake news* and *disinformation*, which were instrumentalised by influential political actors to denigrate other political actors.[24] At the same time, from a legal perspective, political actions against misinformation constitute a balancing act between addressing false and harmful communication and protecting freedom of expression. State interventions targeting false or misleading information must remain consistent with the protection of fundamental rights.[25] Against this backdrop, a central element in

20 European Union Agency for Cybersecurity and European External Action Service, 'Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape | ENISA', 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape [accessed 27 February 2026].

21 Julian Neylan, 'Module What Is FIMI?', *Saufex Blog,* 19 October 2024, https://saufex.eu/post/What-is-FIMI [accessed 27 February 2026].

22 Proto et al., *'EU's FIMI Turn'*.

23 Ibid.

24 Michael Hameleers, 'The (Un)Intended Consequences of Emphasizing the Threats of Mis- and Disinformation', *Media and Communication* 11 Nº 2 (2023), https://doi.org/10.17645/mac.v11i2.6301.

25 Marko Milanovic and Philippa Webb, 'False Speech', in *Freedom of Speech in International Law,* ed. Amal Clooney and David Neuberger (2024; online edn, Oxford Law Pro), pp. 220–76, https://doi.org/10.1093/law/9780198899372.003.0004.

the creation of FIMI was creating a space for the EEAS to operate that would not encroach upon domestic free speech.

The official adoption of FIMI began in 2021.[26] The term 'foreign information manipulation and interference' (though not yet labelled with the acronym) appears in a joint communication by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament and the Council on 'The EU strategy for cooperation in the Indo-Pacific' in September 2021.[27] Under the headline 'New Security Challenges' the document states, 'The EU will help combat foreign information manipulation and interference by state and non-state actors in the Indo-Pacific region through new tools aimed at identifying, analysing, assessing, countering and imposing costs on information manipulation.'[28] The term made a previous appearance (also without the acronym) in a US–EU Summit Statement in June 2021, in which both sides committed to countering hybrid threats as part of a revitalised transatlantic partnership.[29] As of January 2026, the document is no longer available on the official White House website.

In 2022 'foreign information manipulation and interference'[30] became a key concept in a dedicated section on 'Hybrid threats, cyber diplomacy and foreign information manipulation and interference' in the EEAS's Strategic Communication Division's 'Strategic Compass for Security and Defence'.[31] In late 2022 the European Union Agency for Cybersecurity (ENISA) and the EEAS dedicated a joint report on the 'threat landscape' associated with Foreign Information Manipulation and Interference,

26 Proto et al., 'EU's FIMI Turn'.

27 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council. The EU Strategy for Cooperation in the Indo-Pacific,* 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021JC0024 [accessed 27 February 2026].

28 Ibid.

29 Proto et al., *'EU's FIMI Turn'*.

30 European External Action Service, 'A Strategic Compass for Security and Defence', *EEAS,* 2022, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en [accessed 27 February 2026].

31 Ibid.

DOI 10.30966/2018.RIGA.17.2

placing the concept at the centre of analysis.[32] The 2022 report further characterises FIMI, now used as an acronym, in relation to mis- and disinformation, operationalises the concept, for example in terms of victims, threat actors, and severity, and establishes links between FIMI and cybersecurity threats. Since 2023 the EEAS has published an annual report on FIMI threats to discuss current developments and the latest findings, including the 2023,[33] 2024,[34] and 2025[35] reports.

Theoretical Framework

From the preceding discussion, the adoption of FIMI can be understood as a response to make sense of and institutionalise the handling of ambiguous threats. As noted above, the diverse and vaguely defined terminology surrounding perceived threats to the integrity of information spaces, sometimes collectively and equally vaguely referred to as 'information disorders',[36] proved increasingly insufficient to account for the diversity of information manipulation (which is considered part of the broader term 'hybrid threats'),[37] the exact mechanisms utilised, and the potential harms. At the same time the lack of a clear definition drew decision-makers into more politicised terrain as there were genuine concerns that attempts to mitigate information disorders would be used to silence dissenting opinions. The adoption of the FIMI concept can be seen as a response

32 European Union Agency for Cybersecurity and European External Action Service, 'Foreign Information Manipulation Interference'.

33 European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a Framework for Networked Defence*, 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf [accessed 27 February 2026].

34 European External Action Service, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence,* 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf [accessed 27 February 2026].

35 European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats. Exposing the Architecture of FIMI Operations,* 2025, https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf [accessed 27 February 2026].

36 Anton Liagusha and Dmytro Iarovyi, 'Memes, Freedom, and Resilience to Information Disorders: Information Warfare between Democracies and Autocracies', in *Social Sciences & Humanities Open* 11 (2024): 101247, https://doi.org/10.1016/j.ssaho.2024.101247.

37 Home Office, 'Foreign Interference: National Security Bill Factsheet'.

to the need for a clearer understanding of the threat landscape and as an effort to avoid the pitfalls of an increasingly politicised debate surrounding these issues, while enabling the development of a well-defined political mandate to address it. The perception of a need and the subsequent steps taken to develop a clear structure for an ambiguous problem can be better understood by drawing on two long-standing theoretical concepts from organisational theory, institutionalism and sensemaking.

Introduced by Karl Weick,[38] sensemaking, as an organisational theory, describes the process by which the members of organisations give meaning to their collective experiences, especially in the face of novel circumstances and ill-defined problems.[39] Central to institutional theories is that organisations (must) respond to pressures from their environments, which are referred to as 'organisational fields', to maintain their legitimacy and to preserve their capacity for action.[40] With regard to the broader paradigm of institutionalism, the present article focuses on the strand of institutional theory discussed within organisational research.[41] This focus on an organisational perspective follows from the circumstance that FIMI is adopted and enacted by organisations, particularly EU agencies, government agencies, and civil society organisations.

Defining institutions as systems of rules, beliefs, and expectations, there is a clear link between organisational adaptation to environmental requirements and interactive sensemaking processes.[42] It seems reasonable to assume that this link is recursive, as the perception and interpretation of external pressures and needs determine how organisations respond to these challenges. In this regard the present article assumes a mutually interdependent relationship between actors and their sensemaking processes (agents), on the one hand, and their institutional contexts

38 Karl E. Weick, *Sensemaking in Organizations* (Thousand Oaks, CA: SAGE, 1995).

39 Weick et al., *'Organizing and the Process of Sensemaking'*.

40 Alvesson and Jonsson, *'Organizational Dischronization'*.

41 Olivier Berthod, 'Institutional Theory of Organizations', in *Global Encyclopedia of Public Administration, Public Policy, and Governance,* ed. Ali Farazmand (Cham: Springer, 2016), pp. 1–5, https://doi.org/10.1007/978-3-319-31816-5_63-1.

42 Michael Smets, Tim Morris, and Royston Greenwood, 'From Practice to Field: A Multilevel Model of Practice-Driven Institutional Change', *Academy of Management Journal* 55 Nº 4 (2012): 877–904, https://doi.org/10.5465/amj.2010.0013.

DOI 10.30966/2018.RIGA.17.2

(structures), on the other: individuals make sense of and act within structures that they, in turn, shape through their behaviour. Against this background, the article examines the adoption of FIMI at the organisational meso-level, set against geopolitical macro-contexts, through the lens of the micro-level perspectives of the actors involved. The debate, rooted in the tradition of organisational research, as to what extent the adaptation to environmental pressures is merely ceremonial and to a lesser extent reflected in action[43] will not be explored further here. The key argument is that organisations must respond to emerging requirements and challenges posed by their environments, and that this response is driven by individuals making sense of the uncertain and ambiguous conditions faced by their organisations, for example, political institutions and government agencies, or the people these organisations represent, for example, the populations of European states.[44]

EU institutions faced an increasingly uncertain threat environment when it came to information threats due to shifting geopolitical realities since the mid 2010s, as Russia's information warfare targeting became more aggressive particularly after its annexation of Crimea and the start of the Ukraine conflict in 2014.[45] As a response the European Council, after a March 2015 meeting, declared that it condemned the illegal annexation of Crimea and 'stressed the need to challenge Russia's ongoing disinformation campaigns'.[46] Following this, significant institutional steps were the launch of the East StratCom Task Force and the EUvsDisinfo database.[47] However, even at this stage, the issue was difficult to grasp due to the breadth of Russian activities under its 'active measures' regime. This

43 John W. Meyer and Brian Rowan, 'Institutionalised Organizations: Formal Structure as Myth and Ceremony', *American Journal of Sociology* 83 Nº 2 (1977): 340–63.

44 Alvesson and Jonsson, *'Organizational Dischronization'*. Jensen et al., *'Using Institutional Theory'*.

45 Michal Bokša, *Russian Information Warfare in Central and Eastern Europe: Strategies, Impact, Countermeasures* (German Marshall Fund of the United States, 2019), https://www.gmfus.org/sites/default/files/Russia disinformation CEE - June 4.pdf [accessed 27 February 2026]. Alexander Lanoszka, 'Disinformation in International Politics', *European Journal of International Security* 4 Nº 2 (2019): 227–48, https://doi.org/10.1017/eis.2019.6.

46 European Council, *European Council Meeting (19 and 20 March 2015)—Conclusions (EUCO 11/15),* 2015, https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf [accessed 27 February 2026].

47 Elsa Hedling, 'Transforming Practices of Diplomacy: The European External Action Service and Digital Disinformation', *International Affairs* 97 Nº 3 (2021): 841–59, https://doi.org/10.1093/ia/iiab035. Proto et al., *'EU's FIMI Turn'*.

DOI 10.30966/2018.RIGA.17.2

included the expansion of the global reach of propaganda outlets such as RT and Sputnik, which disseminated demonstrably false information; the intensification of Russian state-linked social media activities, including the hiring of freelance social media armies; the forging of documents; and a range of other measures.[48] This spectrum of activities could not be adequately captured with the term disinformation, which was both conceptually imprecise and perceived as politically charged.[49]

Against this background, the perspectives of individuals directly involved in or closely connected to the adoption of the FIMI concept are particularly insightful. Compared to previous accounts, the great strength of the sensemaking approach adopted here lies in its ability to surface actors' individual readings of the problem and the political constraints they perceived, going beyond official documents that smooth over events through retrospective rationalisation. The accounts given by the interviewed actors should therefore not be read as comprehensive descriptions, but as individually situated interpretations and assessments of key events.

Methodology

To capture the perspectives of these contemporary witnesses, semi-structured qualitative expert interviews were conducted with individuals directly or indirectly involved in the development and adoption of the FIMI concept. The study follows an explanatory and hermeneutic approach aimed at understanding the adoption process and does not claim completeness in expert selection. Following a quasi-ethnographic approach, access to the field was established through a primary contact within the Counter Disinformation Network (CDN), initiated by the non-profit organisation Alliance4Europe. The CDN connects researchers, analysts, journalists, and other experts working on and countering

48 Lanoszka, '*Disinformation in International Politics*'.

49 Jana Laura Egelhofer et al., 'Populist Attitudes and Politicians' Disinformation Accusations: Effects on Perceptions of Media and Politicians', Journal of Communication 72 Nº 6 (2022): 619–32, https://doi.org/10.1093/joc/jqac031.

DOI 10.30966/2018.RIGA.17.2

disinformation. We interviewed key figures in the EEAS involved in the creation of the term and external experts and practitioners who played a role in its development and adoption (*n*=5). Including external experts and practitioners was also important, as the term has since become widely used beyond the EEAS, including among members of civil society. Additionally, interviewees were asked at the end of each interview to recommend further relevant contacts, following a chain-referral sampling approach that is also common in ethnographic sampling methodology.[50]

The interview guide was designed for a duration of 20–30 minutes and comprised four thematic blocks, structured according to a narrative logic intended to encourage extended responses. First, participants were invited to describe their personal role in the development and adoption of the FIMI concept. Second, they were asked to characterise FIMI from their point of view and highlight aspects they considered particularly important. The third block consisted of follow-up questions to deepen or expand on previous responses, including why the concept was adopted by the EEAS, what had changed since its introduction, how FIMI had influenced practical responses to influence operations, and how this had affected the participants' own professional work. The fourth block invited personal assessments of potential weaknesses in the concept or its implementation. Participants were then given the opportunity to add further comments and to suggest additional relevant interview partners. In line with the logic of semi-structured interviews, the course of the interview was slightly adapted where this supported the natural flow of the conversation.

All interviews were conducted and recorded digitally via Zoom. Prior to the interviews, participants received a consent form by email outlining the purpose of the research. During debriefing, participants were thanked for their time and informed that they could contact the responsible researcher at any point with questions or concerns and withdraw their approval. All participants gave their consent for their full names to

50 Manisha Pahwa, Alice Cavanagh, and Meredith Vanstone, 'Key Informants in Applied Qualitative Health Research', *Qualitative Health Research* 33 Nº 14 (2023): 1251–61, https://doi.org/10.1177/10497323231198796.

be attributed to their respective quotations. The approach taken in presenting the results in the following section is to give the interviewed experts as much space as possible to speak in their own words, adding only brief contextualisation and summaries in order to provide a direct insight into the motivations and decisions surrounding the introduction of the FIMI concept.

The views expressed by the interviewees do not represent those of the authors of this research, nor do they necessarily constitute a comprehensive account of all relevant events and contexts, but rather they reflect what these individuals recall as key developments and aspects from their personal and professional perspectives.

A History of the FIMI Concept Told by Those Involved

FIMI as a term and concept was not introduced and adopted overnight. Lutz Güllner, former head of the External Action Service's Strategic Communication Division who had a managing role during the FIMI adoption process, describes the evolving institutional framework around strategic communications and countering disinformation as follows:

> So my own role was relatively prominent in this, because I used to be the head of unit in the External Action Service that was in charge of originally strategic communications, and within this strategic communications division in 2016, the little cell of the East StratCom Task Force was placed, in a slightly separate entity, but within the division, which then evolved relatively rapidly, in particular, in 2018 and 2019, into a much bigger operation, into a more complicated structure, and led, in 2019, actually to a reorganisation of the strategic communications division and to the creation of a new division, which was exclusively looking at […]

DOI 10.30966/2018.RIGA.17.2

> information manipulation and […] the Strategic Communication Task Forces, basically dealing with FIMI. (Lutz Güllner)

With regard to the shift from the concept of disinformation to that of FIMI, which was closely tied to this process of restructuring and expanding organisational structures, the interviewees describe a preparatory period, like an orientation phase, during which EU actors increasingly felt that the existing approach to addressing what they called *disinformation* no longer sufficed to respond to the evolving threat landscape, while at the same time no alternative framework was yet readily available. James Pamment, professor at Lund University, who was commissioned by the EEAS StratCom division to author the *Future Threats, Future Solutions* series[51] in 2020, and was at the time a researcher at the Carnegie Endowment for International Peace, recalls:

> So, in 2015, EUvsDisinfo and the East StratCom Task Force were created, and around about 2017, maybe even 2016, very, very early on, I had contact with one of the members, and they came to visit me in Lund for a workshop that I was holding. And that was the first time I really sort of understood the EEAS's role in all this. It was still very new at that time under Mogherini. And then I got tasked in 2017 with preparing for the Swedish elections that would come in 2018, and I did […] national guidelines for how the public sector should handle election interference. And then straight after that, I did something for the UK, which was following up on the Skripal poisoning [in Salisbury].[52] And it was basically because they like the sort of Swedish approach that we've done in that handbook, they requested that I investigate basically lessons learned from all the

51 Pamment, *'EU's Role in the Fight against Disinformation'*.

52 Michael Farrell, 'Assassination and Poisoning', in *Criminology of Poisoning Contexts* (Palgrave Macmillan, 2020), pp. 69–92, https://doi.org/10.1007/978-3-030-40830-5_4.

different organisations that had handled the Skripal poisoning. So, I did that, and the output, in the end, became the UK's guidelines called RESIST.[53] And […] when I'd done this, the EEAS was obviously very interested in these two pieces of work, and they asked me to help them kind of develop the next stage of their work […]. [T]he East StratCom Task Force was already up and established. EUvsDisinfo was established. This would have been 2019 when the Code of Practice[54] was already up and running. They were talking about the Democracy Action Plan[55] and developing that. And they commissioned me basically to write a non-paper for them, which was supposed to kind of bring the best practices from Sweden, the UK and from other countries that I've been working with, put it in the context of the EU level, and kind of help them basically influence the European Democracy Action Plan process. So that came out in three reports published by Carnegie, and those were, to my understanding, the sort of foundation of what became the FIMI idea. (James Pamment)

53 The RESIST framework was developed in 2018 by James Pamment to 'support communicators in reducing the impact of manipulated, false, and misleading information on wider society and national interests': UK Government Communication Service, *RESIST 3: Building Resilience to Information Threats* (London: GCS, 2025) https://www.communications.gov.uk/publications/resist-3-building-resilience-to-information-threats [accessed 13 April 2026]. Its development coincided with the FCO's Counter Disinformation and Media Development Programme, which was 'designed to protect national security by countering disinformation directed at the UK and its Allies from Russia'; the Salisbury attack was cited as a key example of this threat: Sir Alan Duncan, Written Answer to Parliamentary Question 198813, tabled by Chris Williamson, 10 December 2018 https://questions-statements.parliament.uk/written-questions/detail/2018-12-04/198813 [accessed 13 April 2026]; UK Government Communication Service, 'RESIST Counter-Disinformation Toolkit Launched Today', 10 April 2019, https://webarchive.nationalarchives.gov.uk/ukgwa/20200203103626/https://gcs.civilservice.gov.uk/news/resist-counter-disinformation-toolkit-launched-today/ [accessed 27 February 2026].

54 European Commission, *2018 Code of Practice on Disinformation,* 2022, https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation [accessed 27 February 2026].

55 European Commission, 'European Democracy Action Plan: Making EU Democracies Stronger', 3 December 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250 [accessed 27 February 2026].

DOI 10.30966/2018.RIGA.17.2

This quote describes a characteristic phase in organisational change in which processes of restructuring and reorientation unfold in real time, even though the desired end state has not yet been fully defined or clearly articulated by the actors involved. In such phases actors seek to fill the emerging 'sensemaking gaps'[56] in interaction with others:

> I was in Brussels at the time; I was talking to everybody I could. […] [W]e knew […] that disinformation couldn't carry the policy any more. You know, we called it disinformation, and we all knew that it meant something else in reality. (James Pamment)

In this context the commissioning of academic experts can be understood as an institutionalised search for so-called sensegiving resources, which, as an extension of sensemaking theory, refers to the provision of intentional support from an external source to the organic sensemaking process.[57] In this way academic expertise can assist in the (re)construction of meaning and provide guidance towards a preferred reinterpretation of a given situation or problem, particularly in the complex (geo)political environment surrounding foreign influence.

There was a growing consensus among policymakers and experts that the concept of disinformation had reached its analytical limits as a way of describing the problem. At the same time, however, there was not yet a clear trajectory for FIMI to emerge as the central concept it would later become within the EEAS:

> During that time, I also worked closely with the Commission and with the Parliament, and it was a lot of kind of just aligning the way everybody was thinking. […] I never in any way suggested that it

56 Robert Kihlberg and Ola Lindberg, 'Reflexive Sensegiving: An Open-Ended Process of Influencing the Sensemaking of Others during Organizational Change', *European Management Journal* 39 № 4 (2020): 476–86, https://doi.org/10.1016/j.emj.2020.10.007.

57 Ibid.

DOI 10.30966/2018.RIGA.17.2

> should be called FIMI, but we did talk a lot about how you kind of control the concept and how you define it. (James Pamment)

This overarching search for a new approach that James Pamment describes is also reflected in the following quotes. Anneli Ahonen, former head of the East StratCom Task Force at the EEAS, recalls how the perspective on disinformation as a phenomenon started to widen in the late 2010s and early 2020s along with the publication of key policy documents that James Pamment had also mentioned:

> So, I worked at the External Action Service in the East StratCom Task Force from 2017 until 2021. […] And then I was a couple of years the head of the team at the end of the time. And when I was working in Brussels, disinformation was the concept and the word that was used. So, it was the time when this whole EU's countering disinformation work only was starting, and it got built up and the StratCom Task Force was the first thing that was established as a result of Russia's aggression in Ukraine and illegal annexation of Crimea to counter pro-Kremlin disinformation. So that was the kind of the main concept back then. And then there were kind of the first steps in EU's policy development around this. So, there was the 2018 Action Plan against disinformation.[58] And then by the end of the time, when I was in Brussels, the EU developed the policy further, and there was the European Democracy Action Plan.[59] And there you can see how this kind of […] more nuanced way of describing the threat and the problem started appearing. (Anneli Ahonen)

58 European Commission, *2018 Code of Practice on Disinformation*.

59 European Commission, 'European Democracy Action Plan'.

DOI 10.30966/2018.RIGA.17.2

Omri Preiss, managing director at Alliance4Europe, civil society partner in the EEAS-linked FIMI-ISAC network, recalls this orientation phase from a methodological perspective a bit later in the adoption process:

> So, our involvement as Alliance4Europe was very much on the methodology side. […] And we wanted to help civil society campaigners understand the digital media environment around them, understanding kind of how different disinformation narratives were playing out. […] And we saw that there was not a common understanding in the space about how different actors should work with one another. […] Do we have common criteria, and so on. And so, we saw that there was a bigger problem to solve there. And then, as we were looking at how to solve this, we came across a group of cyber security experts that […] had developed this thing called AMITT, which was essentially drawing on cyber security methods, MITRE ATT&CK, the tactics framework in cyber security that is sort of the lingua franca in breaking down cyberattack operations, and they had applied this to the information space as sort of an open-source collaborative effort. […] [It] was in 2021 that we started talking to them. We saw there was interest in developing a community-led open-source framework for disinformation tactics and disinformation behaviours for FIMI, essentially for FIMI behaviours, and that also fits within the ABCDE framework that James Pamment had proposed. […] We worked with partners, rebranded AMITT as DISARM, and together with partners we established the DISARM Foundation and developed a few iterations of the DISARM Framework, which then quite a few different governments and institutions took up and started using. (Omri Preiss)

DOI 10.30966/2018.RIGA.17.2

The realisation by the actors involved that the concept of disinformation could no longer adequately capture the threat landscape within the information environment unfolded over a period of several years. In retrospect the actors associate this development with key geopolitical events, including Russia's annexation of Crimea 2014, the Covid pandemic from 2020, and Russia's full-scale invasion of Ukraine, but also more general developments like an increasing awareness of the importance of social media in the information environment and the emergence of artificial intelligence:

> From 2014 onwards, it was clear that there is an increased level of Russian what was called disinformation at that time. And a lot of the member states, in particular from Eastern and Central Europe, but also from Northern Europe, were extremely concerned about this and voiced it also very clearly. […] The high representative at that time, Federica Mogherini, set up a very dedicated team dealing with this, and it was very much focused on Russian disinformation, and that was the birthplace of the East StratCom Task Force. […] And what happened then was that this issue of disinformation became a much more pressing political issue, first of all, because Russia and its proxies became […] more active on many different channels. It was, of course, also the further expansion of social media, […] the technical possibilities also of using different technical means for disinformation, [and] the first steps of artificial intelligence. So, I think, in the course of 2018 it became very clear that there is a massive issue that needs to be addressed. […] The most important feature of all this development was the fact that in this time, in 2019, and at the very latest in 2020, when Covid started, the term disinformation […] became a term that was very difficult to

DOI 10.30966/2018.RIGA.17.2

> operationalise politically, because it became more and more a political term, as had been the fake news term beforehand. […] And if I look back, it was unclear whether it covers external or internal actors. It was unclear whether it covers true or false narratives. So, is it a fact-checking exercise? Is it something else? It was unclear about key features of it; the technical elements were not specified. So, very, very quickly, this disinformation term became something that you could not work with any more, politically and operationally. And that was the birth. (Lutz Güllner)

To account for the complexity of the evolving situation identified during the sensemaking process, a multifaceted concept emerged in the course of the institutionalisation of FIMI, incorporating several dimensions. Based on a breakdown of the FIMI acronym, specific decisions made during this process can be reconstructed. Lutz Güllner illustrates the political and institutional considerations surrounding the adoption of FIMI by examining the individual elements of the acronym in turn:

> [T]he term […] consists of four words, foreign, information, manipulation, and interference. So, first information manipulation, because we wanted to get away from the normative approach to disinformation—what people like, what they don't like, what is accepted, what is not accepted—but to get into the activity of things, and that is the manipulative activity in the information space. […] We also, as a foreign service, did not want to focus on domestic issues in particular. What we know in many countries, this domestic dimension became more and more problematic, an issue in itself, also something that needed to be dealt with. But our mandate and our approach was really about external actors using information manipulation for a specific purpose.

DOI 10.30966/2018.RIGA.17.2

> So that's where the 'F' came from. And last but not least, the [second] 'I' of FIMI, the interference […]. Many of the actors that use information manipulation are not just doing it to manipulate the information for its own sake. They pursue an aim. They pursue an objective, which we would call now a hybrid threat, for example, or a hybrid campaign, you know. So, new security-related kind of issues which are not using military or traditional kinetic forms. (Lutz Güllner)

According to this, central to the shift towards FIMI was a shift of the analytical focus from false content to manipulative behaviours, such as the coordinated dissemination of narratives that extended beyond individual authentic user activity. This aspect is also emphasised by the other interviewees:

> We used a lot of material that was being produced at the time, for example, from Professor Pamment from Lund University, who […] published the ABCDE model, although the ABC model is most important. So, to identify disinformation, you have three characters. You have the A, the actor, you have the B, the behaviour, and C, the content. And the disinformation is only one element, the C, the content. That's where you can see kind of what is being said. But we felt the FIMI term was much better to capture also the A and the B, and the most important element being the B, the behaviour, the manipulative behaviour. And then we developed it further. […] So, the entire exercise was done to move away from a more philosophical, unclearly defined debate to something that is much more precise in its identification, […] and with a very clear focus on having a more objective framework to do this. (Lutz Güllner)

DOI 10.30966/2018.RIGA.17.2

I believe that the EEAS kind of saw that there would be a need to focus more on behaviours and describing more and analysing more the behavioural aspects of the threat. And maybe it was seen as that disinformation is kind of a content-based concept. (Anneli Ahonen)

Essentially the novelty of it was at the time a focus on the manipulative behaviours and tactics, as opposed to previously on fact checking and narratives. So earlier iterations of trying to deal with the […] influence operation problem that we have, at first the EU thought this is about the facts. You know, there are lies being told, and if we just correct the facts, then we will solve the problem. And then that didn't work. And then they went, it's not just the facts, it's also the narrative. It's the story that's being told, and the story is wrong, and if we just kind of try and shape the narrative, or do something to the narrative, that will be the way to go. And then FIMI was about the tactics. It's about the behaviour that's being used to manipulate. So, it's not about the content as such. It's a series of manipulative behaviours. (Omri Preiss)

The initial idea was to get from narratives to behaviours. So, getting from a narrative-based methodology to a behaviour-based methodology. […] The problem with narrative-based methodologies is that there is no table of narratives. Every organisation has its own set of narratives […]. So, if we don't have a whole body of narratives, we don't have a standardised setup, so we don't have numbers, we don't have normal counteraction policies. So, the idea was, with the help of an NGO, Alliance4Europe, […] and the DISARM Framework, to create a behaviour-based methodology

DOI 10.30966/2018.RIGA.17.2

> where everybody can have the same standards, and we can put everything into a database. (Antoine de Gunzbourg: contracted to operationalise the FIMI concept and to develop open-source-intelligence-based methodologies for the detection of FIMI activities, he describes himself as extremely critical of the FIMI concept.)

From these accounts it becomes clear that there were several reasons associated with this shift from content or narratives towards behaviours that is reflected in the term *FIMI*, which stresses manipulation and interference rather than disinformation. Two reasons emerge as particularly significant in this context. First, from a technical and operational standpoint, moving from narratives to behaviours made it possible to define and standardise manipulative phenomena more precisely, thereby enabling a more concrete and structured response. This is also reflected in a conceptual convergence with cybersecurity and hybrid warfare, as well as in efforts to adopt the corresponding standardised terminology:

> So, there was a bit of a feeling that, you know, either we kind of move closer to cyber or we move closer to hybrid […]. And I think, adding interference to it was really the way of just sort of saying, you know, yeah, it's part hybrid. (James Pamment)

> It became clear that communication is only one element of our response strategy. […] In the end we moved away from this very singular focus on 'this is just a communication issue' to 'this is a vector of a hybrid threat as well and needs to be countered also as a hybrid threat'. […] I think that is really the crucial element. (Lutz Güllner)

Second, from a legal and also a discursive standpoint, this shift allowed a move away from politically charged discussions around free speech and

DOI 10.30966/2018.RIGA.17.2

censorship allegations that are associated with the term *disinformation*, which had evolved into a politically charged term.

This second reason is also related to another important decision, the focus on foreign activities as opposed to harmful activities originating in domestic political information spaces within the EU, as Omri Preiss stresses:

> So, there is a reality of FIMI out there, and there is an administrative need to distinguish between foreign and domestic […] But at the same time, […] [i]t's a transnational cross-border issue. So, these FIMI operations, they don't operate in a vacuum. They operate by engaging with local media, national media, national debates, with the support of domestic actors, national actors, politicians, etc., which means that there is a real sort of interplay between FIMI and DIMI, or domestic information manipulation and interference and FIMI […] I mean, not without reason, but governments are very hesitant to apply an internal security lens to information manipulation, basically, because of the freedom of speech concern that exists. And of course, I mean, don't take me out of context here, it is very, very important to protect freedom of speech, of course. But the thing is that there is no freedom of speech problem because we're not actually talking about curtailing any speech, like this whole idea that there is somehow a dichotomy between handling FIMI or handling disinformation and limiting free speech is just a complete fabrication […] because when we talk about dealing with FIMI we're not talking about taking down any opinion or free speech of any citizens. You know we're not talking about closing down a newsletter or newspaper. We're not talking about like taking down your neighbour's posts because they posted

DOI 10.30966/2018.RIGA.17.2

> Covid disinformation or something. We're talking about inauthentic behaviour. We're talking about actors pretending to be things that they are not. We're talking about intentional weaponised manipulation. So, it's not a question of freedom of speech. It's a question of information warfare, and you're not addressing anyone's actual speech or actual opinions. You're addressing a bot farm or a troll farm; it's just manifestly not the same thing. (Omri Preiss)

The EEAS was aware that this distinction between foreign and domestic actors and their activities did not adequately reflect the complexity of online communication environments, but that this decision was grounded in political and operational considerations:

> So, an increasingly blurred line between external and internal, I think, would be another difficulty anyway, but these were never kind of things that we said we can solve with this. It was more to put things in a much clearer policy framework that we can actually operationalise, that can be politically explained. (Lutz Güllner)

Two other aspects are related to the decision to include 'foreign' in the conceptualisation of FIMI. First, defining information manipulation and interference as an external threat placed FIMI directly within the EEAS's sphere of responsibility, aligning it with its mandate, as previously noted from the interview with Lutz Güllner:

> We also, as a foreign service, did not want to focus on domestic issues in particular. What we know in many countries, this domestic dimension became more and more problematic, an issue in itself, also something that needed to be dealt with. But our mandate and our approach was really about external actors using information manipulation for a specific purpose. (Lutz Güllner)

DOI 10.30966/2018.RIGA.17.2

> [A]lso, this distinction between foreign and internal enables foreign ministries and the EEAS as an agent, an entity that's supposed to deal with foreign stuff, to take the lead on it. And it sort of administratively enables a division of labour between what happens internally, which will be dealt with by the Justice Ministry and the media regulators and so on, and what happens externally, which will be dealt with by the Foreign Ministry and external threats. (Omri Preiss)

Second, the shift from narratives to behaviours, following the example of cybersecurity, and especially adding the element of interference to the FIMI definition, enabled the infliction of political sanctions on entities conducting influence campaigns:

> They'd seen the cyber sanctions regime, and they sort of had this ambition of raising […] disinformation to that level where you could have sanctions related to disinformation. And I think in the end the reason they chose FIMI was because that could more easily support the sanctions regime than just disinformation. (James Pamment)

> There is some kind of new sanction regime again, […] like on hybrid threats […] and cyber. (Anneli Ahonen)

> What did start happening is sanctioning threat actors, so where there has actually been an attribution of the actors that are driving these FIMI operations. Then the Council […] actually sanctions them, and that means that they are effectively geo-blocked in the EU and their content becomes illegal content and the platforms need to take it down. So that then gives you a really powerful tool to actually start breaking apart these influence operations. (Omri Preiss)

> [Y]ou need to work with sanctions. We have many examples where it worked. Think about March 2022, when the Commission president suggested to put FIMI actors or disinformation actors or propagandists […] on the sanctions list of the European Union.[60] That was a very strong signal. And that was exactly kind of what was intended, but that only worked in this very clear situation of war and peace, of destabilisation, of having a legal framework underneath. (Lutz Güllner)

While these quotes describe manifest consequences of the implementation of FIMI, there is also an agreement among the interviewed experts that adopting the concept did not fundamentally alter the underlying threat perception, as there already had been a strong problem awareness before, which initially sparked the search for a new framework:

> Well, we always said the FIMI concept is just a concept. It's just a way to understand the threat, and it tries to capture a […] very complex phenomenon, which is, of course, accelerated, you know, by the digitalisation of our communications and the possibilities to manipulate. (Lutz Güllner)

> I think the definitions are important. And it's very good to try to achieve a situation where we speak in a common language, and we know what each other mean[s] with it, but I don't think it fundamentally changes our perception of the foreign threat actors. (Anneli Ahonen)

60 European Council, 'Russia's Military Aggression against Ukraine: Council Imposes Sanctions on 26 Persons and One Entity', 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/02/28/russia-s-military-aggression-against-ukraine-council-imposes-sanctions-on-26-persons-and-one-entity [accessed 27 February 2026].

DOI 10.30966/2018.RIGA.17.2

Rather, in line with a sensemaking perspective, the reframing of the issue enabled actors to shift perspectives and situate the problem within a broader and more complex context of hybrid threats, thereby acting as a catalyst for the institutionalisation of countermeasures. It was a process of developing a mutual understanding between different actors and a political approach to align counter-disinformation activities with the mandate of the EEAS, exclude the sensitive issue of domestic political discourse, and enable sanctions against foreign actors interfering with domestic political processes.

At the same time the adoption process sparked a series of research and development projects resulting in frameworks and tools to operationalise the analysis of FIMI activities:

> I think what got done is there was a whole wave of actually developing methodology around FIMI. The EEAS played a thought leadership role in this. They really pushed the boat out and with the FIMI toolbox and adopting DISARM. […] And suddenly you had a whole set of tools that analysts could use to say, Okay, this is an influence operation, and these are the tactics, […]. And then you could actually do attribution. And you could say, we believe, we think that this is probably like a set of Russian actors, etc. […] But then you've done so much methodological work, and you've done so much analysis, that the question is, what do you actually do with it? And a lot of the time you don't do enough. We're in a completely different place now than we were maybe three or four years ago, but the problem is also a lot more severe, like so we have much better tools now to deal with the issue, but it's also become that much bigger problem. (Omri Preiss)

DOI 10.30966/2018.RIGA.17.2

In this regard there is a consensus among the interviewees that further work needs to be done to sharpen the contours of the approach and further concretise the associated methodology. For example, James Pamment comments on a need to sharpen the conceptual relationship between FIMI and the closely related fields and concepts of cybersecurity and hybrid warfare:

> We want the cyber sanctions regime, but we don't want to get just swallowed up by cyber. We want to be close to hybrid […] but hybrid is kind of everything and nothing. So where do we sit? And in the end, I think the decision was, more or less, we want to keep information for ourselves. We want to make sure that it's kind of ring-fenced and protected. (James Pamment)

What is described here is a balancing act between aligning FIMI with already existing concepts and the political imperative to preserve clear competencies and a well-defined mandate. This conceptual relationship, which remains somewhat ambiguous, is also reflected in areas where the interviewees highlight the need for further refinement of the operationalisation:

> If they would have asked me about building the actual term, […] if I'd known then what I know now, I would have probably said to build in something that links it more clearly to those other subjects, so that there is a hierarchy and a clear kind of position for information within those other problems. Because I think that's still the kind of crux of the issue that we have now, and why most of our methods aren't very successful, why there's a little confusion around what we're doing. (James Pamment)

In addition to what James Pamment describes as the vague (horizontal) positioning and weighting of information within a conceptual landscape

DOI 10.30966/2018.RIGA.17.2

spanning fields such as cybersecurity and concepts such as hybrid warfare, another issue can be identified in a (vertical) gap between the political responsibility for attribution and on-the-ground analysis. Antoine de Gunzbourg attributes this to uncertainties surrounding attribution, which is essential for classifying an information manipulation incident as foreign:

> So, when they called me, they already had set up the FIMI notion as a notion. And it was, so I understood, agreed upon by all the member states, and they were really happy about that, like it was a big victory to agree all the European states to come up with a notion. And I was tasked with inventing methodologies, open-source intelligence, or methodologies for the analysts to detect FIMI incidents. So, we had to invent what was an incident to develop OSINT methodologies and to invent what was FIMI on the operational level, so for the analyst on the ground to detect FIMI. So, it was theorised from like above, and my job was to try to invent methodologies for the analyst to detect it. And this is how I became really critical of this notion, because I realised it was an impossible task, because FIMI is, how can I say this, it is a way for policymakers to not make any political decision. So, in disinformation, we have this problem of attribution—how do we attribute? How do we attribute an information operation? How do we attribute disinformation; and with FIMI, as I managed to understand [it] while trying to do this job, the analyst can only go to a 90 per cent certainty in any like OSINT job or the best analysis that you could do, you can do a 90 per cent certainty. (Antoine de Gunzbourg)

The attribution problem that is described in this quote refers to a degree of uncertainty in such cases where there is no unequivocal evidence

regarding the responsible actor behind manipulative activities or their affiliation with a previously attributed campaign. In such situations a *cui bono* assessment in the geopolitical dimension may become necessary. This, in turn, raises the question of responsibility for attribution: according to de Gunzbourg, attribution is a political responsibility that cannot and should not be delegated to researchers and analysts.

Interestingly the quote draws attention to a circumstance in the adoption history of FIMI that may have contributed to the emergence of this dilemma: the seemingly delayed practical operationalisation of FIMI following its initial conceptualisation at a more abstract political level, where the considerations outlined above appear to have been particularly influential. While this development has been shaped by the described institutional imperatives, it may also have constrained the relationship between analytical practice and attribution, the latter of which always carries a political dimension. Against this backdrop, the tension between analysis and attribution is likely to require more sustained and systematic discussion in the future.

Conclusion

From the perspective of the interviewees, the adoption of the FIMI concept by the EEAS and other European institutions has not been completed and probably never will be. In contrast the complexity of the information environment with its ever-shifting infrastructural and geopolitical contexts, as well as evolving information operations, requires constant conceptual advancements and redefinitions of the threat that is to be addressed. Other terms have emerged to define variations of the problem, including 'illicit influence operations'[61] to characterise the grey legality of such campaigns, 'hostile information campaigns' as used by

61 Carl Miller, 'Directing Responses against Illicit Influence Operations (D-RAIL)', *EU DisinfoLab*, 19 August 2024, https://www.disinfo.eu/publications/directing-responses-against-illicit-influence-operations-d-rail.

DOI 10.30966/2018.RIGA.17.2

Singapore,[62] and 'technologically enabled manipulation', which emphasises the technological dimension of manipulation rather than questions of veracity.[63] The utility of these terms depends on the exact scope of the problem being addressed and the context in which they are employed.

From talking to experts involved in the development of the FIMI concept at different stages and levels of responsibilities, its adoption served two main purposes that can be contextualised using sensemaking and institutional perspectives. First, adopting the framing of FIMI and the focus on Russia, a selection based on the EEAS's mandate and strategic priorities,[64] supported sensemaking processes related to the problem of coordinated disinformation in times of increasing geopolitical challenges and shifting technological parameters, helping to navigate the threat landscape and creating mutual understanding between different actors.

Second, by reframing disinformation as information manipulation and external interference conducted by autocratic regimes, the EEAS could align the problem with its mandate, which relates to foreign activities. In other words, this shift allowed the EEAS to connect the problem to its institutional identity in external action and security and translate it into the institutional logic of the EEAS. In sensemaking terms this can be seen as a process of rationalising the combating of disinformation as part of the EEAS's normal role defending EU values from foreign threats. This confirms the analysis of Proto et al. that the EEAS has succeeded in 'shaping both policy and public perception in a way that aligns with its mandate and expertise'.[65]

The adopted lenses from organisational theory prove highly suitable for tracing the adoption process of FIMI. The interviews conducted with a small but highly heterogeneous sample of experts reveal a broadly

62 SG101, 'Hostile Information Campaigns and Foreign Interference', last updated 6 October 2025, https://www.sg101.gov.sg/defence-and-security/current-threats/hics-and-foreign-interference [accessed 13 April 2026].

63 Julian Neylan et al., 'Managing Threats from Emerging Technologies in Emergency Contexts', *Journal of Emergency Management* (forthcoming).

64 Hénin, *FIMI: Towards a European Redefinition of Foreign Interference.*

65 Proto et al., *'EU's FIMI Turn'*, p. 3.

shared understanding of this adoption process, while also pointing to a range of aspects and critical debates that warrant further exploration. At the political level this includes, for example, the question of how shifting geopolitical conditions, particularly the transition towards a more multipolar world, may entail a reorientation of a concept that has thus far focused predominantly on Russia.[66]

Moreover, a critical debate has emerged around the question of who bears responsibility for attribution and how political actors navigate potential tensions arising in diplomatic contexts. Finally, as also highlighted in the interviews, there is the question of whether and how rapidly evolving technological conditions, particularly with regard to artificial intelligence, should be incorporated into FIMI in future iterations of the concept and its methodology; the processes of sensemaking and institutionalisation remain ongoing.

Bibliography

'50 U.S. Code § 3059 - Foreign Malign Influence Center', *LII / Legal Information Institute,* https://www.law.cornell.edu/uscode/text/50/3059#e_2.

Alvesson, Mats, and Anna Jonsson, 'Organizational Dischronization: On Meaning and Meaninglessness, Sensemaking and Nonsensemaking', *Journal of Management Studies* 59 Nº 3 (2021): 724–54, https://doi.org/10.1111/joms.12790.

Berthod, Olivier, 'Institutional Theory of Organizations', in *Global Encyclopedia of Public Administration, Public Policy, and Governance,* ed. Ali Farazmand (Cham: Springer, 2016), pp. 1–5, https://doi.org/10.1007/978-3-319-31816-5_63-1.

Bokša, Michal, *Russian Information Warfare in Central and Eastern Europe: Strategies, Impact, Countermeasures* (German Marshall Fund of the United States, 2019), https://www.gmfus.org/sites/default/files/Russia disinformation CEE - June 4.pdf [accessed 27 February 2026].

Duncan, Sir Alan, Written Answer to Parliamentary Question 198813, tabled by Chris Williamson, 10 December 2018, https://questions-statements.parliament.uk/written-questions/detail/2018-12-04/198813 [accessed 13 April 2026].

Egelhofer, Jana Laura, Ming Boyer, Sophie Lecheler, and Loes Aaldering, 'Populist Attitudes and Politicians' Disinformation Accusations: Effects on Perceptions of Media and Politicians', *Journal of Communication*, 72 Nº 6 (2022): 619–32, https://doi.org/10.1093/joc/jqac031.

European Commission, *2018 Code of Practice on Disinformation,* 2022, https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation [accessed 27 February 2026].

European Commission, 'European Democracy Action Plan: Making EU Democracies Stronger', 3 December 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250 [accessed 27 February 2026].

66 Hénin, *FIMI: Towards a European Redefinition of Foreign Interference.*

DOI 10.30966/2018.RIGA.17.2

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council. The EU Strategy for Cooperation in the Indo-Pacific,* 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021JC0024.

European Council, *European Council Meeting (19 and 20 March 2015)—Conclusions (EUCO 11/15),* 2015, https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf [accessed 27 February 2026].

European Council, 'Russia's Military Aggression against Ukraine: Council Imposes Sanctions on 26 Persons and One Entity', 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/02/28/russia-s-military-aggression-against-ukraine-council-imposes-sanctions-on-26-persons-and-one-entity [accessed 27 February 2026].

European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a Framework for Networked Defence,* 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf [accessed 27 February 2026].

European External Action Service, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence,* 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf [accessed 27 February 2026].

European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats. Exposing the Architecture of FIMI Operations,* 2025, https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf [accessed 27 February 2026].

European External Action Service, 'A Strategic Compass for Security and Defence', *EEAS*, 2022, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en [accessed 27 February 2026].

European Union Agency for Cybersecurity and European External Action Service, *Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape*, 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape [accessed 27 February 2026].

Farrell, Michael, 'Assassination and Poisoning', in *Criminology of Poisoning Contexts* (Palgrave Macmillan, 2020), pp. 69–92, https://doi.org/10.1007/978-3-030-40830-5_4.

Freelon, Deen, and Chris Wells, 'Disinformation as Political Communication', Political Communication 37 Nº 2 (2020): 145–56, https://doi.org/10.1080/10584609.2020.1723755.

Grisé, Michelle, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, 'Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation', *RAND,* 2022, https://www.rand.org/pubs/research_reports/RRA198-8.html.

Hameleers, Michael, 'The (Un)Intended Consequences of Emphasizing the Threats of Mis- and Disinformation', *Media and Communication* 11 Nº 2 (2023), https://doi.org/10.17645/mac.v11i2.6301.

Hameleers, Michael, Anna Brosius, Franziska Marquart, Andreas C. Goldberg, Erika Van Elsas, and Claes H. De Vreese, 'Mistake or Manipulation? Conceptualizing Perceived Mis- and Disinformation among News Consumers in 10 European Countries', *Communication Research* 49 Nº 7 (2021): 919–41, https://doi.org/10.1177/0093650221997719.

Hedling, Elsa, 'Transforming Practices of Diplomacy: The European External Action Service and Digital Disinformation', *International Affairs* 97 Nº 3 (2021): 841–59, https://doi.org/10.1093/ia/iiab035.

Hénin, Nicolas, *FIMI: Towards a European Redefinition of Foreign Interference,* EU DisinfoLab, 2023, https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf [accessed 27 February 2026].

Home Office, 'Foreign Interference: National Security Bill Factsheet', *GOV.UK,* updated 24 June 2025, https://www.gov.uk/government/publications/national-security-bill-factsheets/foreign-interference-national-security-bill-factsheet [accessed 13 April 2026].

Jensen, Tina Blegind, Annemette Kjærgaard, and Per Svejvig, 'Using Institutional Theory with Sensemaking Theory: A Case Study of Information System Implementation in Healthcare', *Journal of Information Technology* 24 Nº 4 (2009): 343–53, https://doi.org/10.1057/jit.2009.11.

Kihlberg, Robert, and Ola Lindberg, 'Reflexive Sensegiving: An Open-Ended Process of Influencing the Sensemaking of Others during Organizational Change', *European Management Journal* 39 Nº 4 (2020): 476–86, https://doi.org/10.1016/j.emj.2020.10.007.

Lanoszka, Alexander, 'Disinformation in International Politics', *European Journal of International Security* 4 Nº 2 (2019): 227–48, https://doi.org/10.1017/eis.2019.6.

Lewandowsky, Stephan, Ullrich K.H. Ecker, John Cook, Sander Van Der Linden, Jon Roozenbeek, and Naomi Oreskes, 'Misinformation and the Epistemic Integrity of Democracy', *Current Opinion in Psychology*, 54 (2023): 101711, https://doi.org/10.1016/j.copsyc.2023.101711.

Liagusha, Anton, and Dmytro Iarovyi, 'Memes, Freedom, and Resilience to Information Disorders: Information Warfare between Democracies and Autocracies', *Social Sciences & Humanities Open* 11 (2024): 101247, https://doi.org/10.1016/j.ssaho.2024.101247.

Meyer, John W., and Brian Rowan, 'Institutionalised Organizations: Formal Structure as Myth and Ceremony', *American Journal of Sociology* 83 Nº 2 (1977): 340–63.

Miguel, Raquel, 'Decoding FIMI: A Complex Interrelation with Disinformation', *Project Athena*, 2025, https://project-athena.eu/decoding-fimi-a-complex-interrelation-with-disinformation [accessed 27 February 2026].

Milanovic, Marko, and Philippa Webb, 'False Speech', in *Freedom of Speech in International Law*, ed. Amal Clooney and David Neuberger (2024; online edn, Oxford Law Pro), pp. 220–76, https://doi.org/10.1093/law/9780198899372.003.0004.

Miller, Carl, 'Directing Responses against Illicit Influence Operations (D-RAIL)', *EU DisinfoLab,* 19 August 2024, https://www.disinfo.eu/publications/directing-responses-against-illicit-influence-operations-d-rail.

Neylan, Julian, 'Module What Is FIMI?', *Saufex Blog*, 19 October 2024, https://saufex.eu/post/What-is-FIMI [accessed 27 February 2026].

Neylan, Julian, Sonny Patel, Timo Lenk, and Timothy B. Erickson, 'Managing Threats from Emerging Technologies in Emergency Contexts', *Journal of Emergency Management* (forthcoming).

Noronha, Eduardo, João Varela Da Costa, and Miguel Mira Da Silva, 'A Multivocal Grey Literature Review on Fake News and Risk Management', *Discover Computing* 29 Nº 1 (2026), https://doi.org/10.1007/s10791-025-09902-w.

Pahwa, Manisha, Alice Cavanagh, and Meredith Vanstone, 'Key Informants in Applied Qualitative Health Research', *Qualitative Health Research* 33 Nº 14 (2023): 1251–61, https://doi.org/10.1177/10497323231198796.

Pamment, James, 'The EU's Role in the Fight against Disinformation: Developing Policy Interventions for the 2020s', *Carnegie Endowment for International Peace*, 2020, https://carnegieendowment.org/research/2020/09/the-eus-role-in-the-fight-against-disinformation-developing-policy-interventions-for-the-2020s.

Proto, Lucas, Paula Lamoso-González, and Luis Bouza García, 'The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight', *Media and Communication* 13 (2025), https://doi.org/10.17645/mac.9474.

SG101, 'Hostile Information Campaigns and Foreign Interference', last updated 6 October 2025, https://www.sg101.gov.sg/defence-and-security/current-threats/hics-and-foreign-interference [accessed 13 April 2026].

DOI 10.30966/2018.RIGA.17.2

Smets, Michael, Tim Morris, and Royston Greenwood, 'From Practice to Field: A Multilevel Model of Practice-Driven Institutional Change', *Academy of Management Journal* 55 № 4 (2012): 877–904, https://doi.org/10.5465/amj.2010.0013.

UK Government Communication Service, *RESIST 3: Building Resilience to Information Threats* (London: GCS, 2025), https://www.communications.gov.uk/publications/resist-3-building-resilience-to-information-threats [accessed 13 April 2026].

UK Government Communication Service, 'RESIST Counter-Disinformation Toolkit Launched Today', 10 April 2019, https://webarchive.nationalarchives.gov.uk/ukgwa/20200203103626/https://gcs.civilservice.gov.uk/news/resist-counter-disinformation-toolkit-launched-today [accessed 27 February 2026].

Walter, Dror, and Yotam Ophir, 'Trolls without Borders: A Comparative Analysis of Six Foreign Countries' Online Propaganda Campaigns', *Human Communication Research* 49 № 4 (2023): 421–32, https://doi.org/10.1093/hcr/hqad022.

Weick, Karl E., *Sensemaking in Organizations* (Thousand Oaks, CA: SAGE, 1995).

Weick, Karl E., Kathleen M. Sutcliffe, and David Obstfeld, 'Organizing and the Process of Sensemaking', *Organization Science* 16 № 4 (2005): 409–21, https://doi.org/10.1287/orsc.1050.0133.

From Declarations to Practice? Institutional Constraints on Europe–IP4 Cooperation against Foreign Information Manipulation

By Chiyuki Aoi, Paul Bacon, Shinae Lee, Corey Wallace, and Aurelio Insisa

Keywords—*information manipulation, foreign information manipulation and interference, interference, strategic communication, strategic communications, middle powers, Indo-Pacific, IP4*

About the Author
Chiyuki Aoi is Professor of International Security at the University of Tokyo, where she directs the Strategic Communications Education and Research Unit (SCERU).

Paul Bacon is Professor of International Relations in the Faculty of International Research and Education at Waseda University, Tokyo.

Shinae Lee is a Research Fellow in the National Security and Japan–US Program at the Sasakawa Peace Foundation and a Fellow at the Strategic Communications Education and Research Unit (SCERU).

Corey Wallace is Associate Professor of Kanagawa University, Yokohama, Japan, and a Fellow at the Strategic Communications Education and Research Unit (SCERU).

DOI 10.30966/2018.RIGA.17.3

Aurelio Insisa is Senior Analyst at MERICS (Mercator Institute for China Studies), Berlin.

Abstract
This article explains why dense diplomatic commitments to cooperate against information manipulation have so far produced limited practical collaboration between Europe and key Indo-Pacific democracies. Focusing on the IP4 (Japan, South Korea, Australia, New Zealand), it shows how EU–IP4 partnerships, G7 mechanisms, and a now stalled US agenda have generated extensive rhetorical alignment on counter-information manipulation, while leaving operational cooperation still largely unaddressed. The analysis argues that this gap reflects enduring misalignments in institutional architectures, technical capacities, and political-bureaucratic cultures, rather than merely time lags or a lack of political will. Drawing on country case studies and Euro-Atlantic experience with centres of excellence, the article proposes a layered, research-driven approach that embeds counter-information manipulation in a broader strategic communications framework and privileges minilateral formats, especially among the IP4, as the most viable pathway from declaratory intent to durable, cross-regional practice.

Introduction

In recent years there has been a visible proliferation of initiatives in which socalled 'like-minded' middle powers in Europe and the Indo-Pacific pledge to collaborate on countering information manipulation—what the European Union (EU) terms Foreign Information Manipulation and Interference (FIMI)—even as the United States has effectively exited the counter-disinformation regime it once led. There is now ample diplomatic evidence of this trend. The EU–Japan Security and Defence Partnership (2024) explicitly prioritises counter-FIMI cooperation; the EU–Republic of Korea Security and Defence Partnership (2024) elevates cyber, hybrid, and FIMI-related collaboration in the broader EU–ROK strategic relationship; and the Australia–EU Security and Defence

DOI 10.30966/2018.RIGA.17.3

Partnership (2026) identifies hybrid threats and FIMI as key pillars of their security dialogue. New Zealand is in the process of negotiating a similar agreement, and all four IP4 countries participate to varying degrees in multilateral mechanisms such as the G7 Rapid Response Mechanism and NATO's flagship cooperation with the IP4. The NATO-IP4 framework explicitly includes 'countering disinformation', and, taken together, these mechanisms create a web of rhetorical and diplomatic commitments to counter-FIMI cooperation.

At first glance these developments might suggest the emergence of a robust, cross-regional architecture for practically oriented collaboration among the IP4 (Australia, New Zealand, South Korea, and Japan) and their European partners. This article, however, starts from a more cautious premise. It argues that the current pattern of cooperation is marked by a widening gap between diplomatic declarations and practical implementation, and that this gap is unlikely to close simply with the passage of time. While it is reasonable to acknowledge that countering FIMI and other intricate forms of manipulation demands sophisticated capabilities and dense governmental as well as societal institutions—and that some of the present limitations in outcomes might be interpreted as a temporary time lag—the research conducted for this paper suggests the presence of more enduring obstacles. Unless underlying conditions are addressed, cooperation that is repeatedly affirmed at the diplomatic level is likely to remain slow or continue to be deferred.

The core contention is that these obstacles are rooted less in an absence of political will or shared diagnosis of threats than in the divergence of relevant institutions and policy frameworks across the IP4. IP4 governments routinely signal willingness to work with European and North American partners, but several structural factors systematically hinder deeper collaboration: divergent strategic priorities and threat perceptions; differing institutional architectures, including cultural factors; and uneven technical capacities. Together these factors create persistent barriers to translating political commitments into operational cooperation. Even where high-level decisions or joint statements exist, the underlying

DOI 10.30966/2018.RIGA.17.3

bureaucratic structures and culture, coordination mechanisms, and technical communities remain poorly aligned, impeding the development of shared procedures, platforms, or frameworks for action. The result is an uneven and fragmented pattern of activity in which formal agreements proliferate while practical collaboration remains underdeveloped.

It should also be noted that there are marked differences in how capable these nations are in managing relations with external powers on such issues. Australia, by virtue of its higher technical proficiency and its participation in arrangements such as Five Eyes, AUKUS, and other frameworks with Europe and the US, is a considerably more capable actor in managing information manipulation and interference, while New Zealand, in a very different strategic setting, nevertheless possesses stronger counter-disinformation capabilities than most Asian states. Yet some of the same underlying conditions—divergent strategic priorities and threat perceptions, and the preference to address information challenges primarily in established bilateral relationships with the very 'adversaries' engaged in FIMI—remain common features across the IP4, further constraining the scope for deeper cooperation.

The Euro-Atlantic and Indo-Pacific contexts are linked by a common pattern of foreign information manipulation, with Russia (primarily in Europe) and the People's Republic of China (PRC, primarily in the IndoPacific) targeting allied democracies and seeking to weaken confidence in Western security arrangements, including NATO and US-led alliances in the Indo-Pacific. Yet momentum to construct broader international cooperation has slowed since the change of administration in Washington, and emerging EU-led platforms have not overcome the frictions generated by misaligned institutions and capacities. Existing frameworks—ranging from the EU–IP4 security and defence partnerships that reference FIMI to multilateral mechanisms such as the G7 Rapid Response Mechanism (RRM) and NATO's flagship cooperation with the IP4, which includes a strand on counter-disinformation—remain largely externally driven and have not yet fostered dense, operational linkages across the Indo-Pacific.

DOI 10.30966/2018.RIGA.17.3

Against this backdrop, the article does not advance a normative position that prescribes new institutional architectures, including a collective security arrangement which has historically not taken root in the Indo-Pacific and remains highly unlikely to do so in the foreseeable future (although a later section briefly considers the feasibility of minilateral and pragmatic forms of collaborations in limited, specific areas). Rather, it uses the IP4 cases to pose a more specific question: why have an expanding set of diplomatic commitments to counter-information manipulation cooperation, and a shared recognition of common threats, translated into relatively little sustained, practically oriented collaboration, even in trilateral or minilateral format? In this paper the IP4 countries were selected for closer examination because they represent the Indo-Pacific's democratic and relatively stable middle powers, forming a 'second-tier' frontline to the PRC's manipulative activities in the region; they are thus qualitatively distinct from Taiwan, which belongs to a Sinophone sphere with far denser historical, social, and informational ties to the PRC. The argument advanced is that diverse domestic institutional settings, including bureaucratic-political culture, and technical capabilities in the Indo-Pacific create a persistent mismatch with Euro-Atlantic approaches, limiting the ability of existing agreements to generate practical, durable cooperation on information manipulation. These internal and institutional factors, more than the absence of political will, explain why the current web of cross-regional commitments remains largely symbolic and why, without targeted institutional adaptation, the promised evolution from diplomatic intent to pragmatic collaboration is likely to continue to be deferred.

Presentation of this evidence proceeds in three sections. The first section outlines the Indo-Pacific information environment, based on existing qualitative studies and opensource research, providing the foundation for expectations for plausible middlepower responses in the region in light of the preceding theoretical discussion. The second section, and the original contribution of this paper, analyses how key Indo-Pacific democracies—Japan, South Korea, Australia, and New Zealand—have responded to information manipulation in their respective regions, examining both policy choices and institutional arrangements. This section offers

DOI 10.30966/2018.RIGA.17.3

explanations for why cross-regional middle-power cooperation on information manipulation has so far remained under-institutionalised, focusing on external threat perceptions and internal institutional and technical factors, including political-bureaucratic/academic culture.[1]

Third, this paper considers practical ways out of the current impasse by advancing a layered approach to overcoming the obstacles to cooperation, one that essentially draws upon practical minilateral-based collaboration in specific, limited areas. This diagnosis partially draws from research into European experiences with established relevant centres of excellence (namely, NATO StratCom COE and the European Hybrid Centre). This section further reflects critically on how the absence of a longterm strategic projection of shared European and Indo-Pacific values can be understood as a byproduct of the EU's predominantly reactive, tactically focused approach to FIMI which consists of essentially subversive yet tactical practices by adversaries. It argues for the construction of an agreed policy framework for strategic communications that links Europe's and the Indo-Pacific's long-term visions and common values, and then identifies concrete areas for practical cooperation, including counter-FIMI, at operational and tactical levels. The conclusion synthesises these observations and argues that, if effective collaboration is to be sustained amid intense great-power competition, such strategic vision-building must come first, followed by a step-by-step deepening of collaborative, practical ventures.

Definitions of key terms

Before proceeding, this paper clarifies its use of core terms, since even in the Euro-Atlantic context defining and structuring relevant terminology remains contested. There is, to date, no unified effort to coordinate concepts across key organisations such as NATO and the EU, which have not converged on a common vocabulary.

1 Research informing this section was partly supported by the JSPS KAKENHI Grant Number 23K25483, 'Comparative Policy and Institutions: Strategic Communications and Foreign Information Manipulation', Principal Investigator: Chiyuki Aoi, 2023–26.

DOI 10.30966/2018.RIGA.17.3

The paper follows the EU's notion of FIMI as a behaviour-based concept: patterns of coordinated, often non-illegal behaviour by state or non-state actors that can undermine democratic values, procedures, and political processes, with emphasis placed on observable tactics, techniques, and procedures rather than on 'false' or 'harmful' content alone.[2] This approach also underpins the EU's comparatively greater willingness than many Indo-Pacific states to attribute such operations publicly to Russia and, to a lesser degree, China.[3]

The term 'state threat' is used here for behaviour-based information threats and associated influence activities that can be attributed to particular state actors, aligning with this shift from content- to behaviour-focused analysis.

In line with NATO usage, the paper understands strategic communications as a holistic and values- and interests-based approach that 'encompasses everything an actor does to achieve objectives in a contested environment', geared towards longterm shaping and shifting of dominant discourses in society through words, actions, images, and symbols. The NATO approach to strategic communications is explicitly rooted in liberal values and fundamental freedoms, consistent with the Alliance's mission under the Washington Treaty to protect democracy, individual liberty, and the rule of law in member states. Within this framework, strategic communications is conceived as a longterm effort to align words and deeds in order to shape perceptions and behaviour in support of Allied objectives, rather than as a reactive approach.[4]

2 European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats* (Brussels: EEAS, 7 February 2023), glossary.

3 Ibid., and EEAS, 'Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)', 17 March 2026, https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en.

4 Neville Bolt et al., *Understanding Strategic Communications,* Terminology Working Group Publication No. 3 (Riga: NATO Strategic Communications Centre of Excellence, 2023). *Allied Joint Doctrine for Strategic Communications (AJP10),* 2023.

DOI 10.30966/2018.RIGA.17.3

Characteristics of the Indo-Pacific Theatre: Nature of State Threats

This section situates the IndoPacific middle powers in a wider comparative context by contrasting their information environments. It highlights a feature crucial for understanding the Indo-Pacific strategic theatre: the nature of state threats, dominated by the PRC and complemented by emerging Russian activities. This will be further contextualised in later sections by the analysis of threat perceptions and institutional structures.

The Indo-Pacific strategic theatre: PRC-driven manipulation and emerging Russian influences

In the Indo-Pacific the primary state threat in information manipulation is the PRC, with early signs that Russia is preparing for enhanced activities in selected theatres. Other long-term players in the region include North Korea and to a lesser extent Iran. China's rise as an economic and military power under Xi Jinping has been accompanied by a global expansion of capabilities in the information domain, broadening the scale, reach, and sophistication of its manipulation practices. In a communist partystate such as the PRC—whose political system retains key features of its Leninist heritage, particularly the conception of the party as a vanguard—propaganda (*xuanchuan*) is better understood as 'a collection of practices through which the Party-State exercises power in relation to the public articulation of discourses',[5] rather than as the simple dissemination of false or distorted information. As a result, 'propaganda work' (*xuanchuan gongzuo*) primarily concerns the dissemination of state-approved content tasked with providing the public with an 'orthodox' understanding of events and a form of continuing ideological education.[6]

5 Kingsley Edney, *The Globalization of Chinese Propaganda: International Power and Domestic Cohesion* (Palgrave MacMillan, 2014), p. 8.

6 Clyde Yicheng Wang, 'The Ideology Is Blowing in the Wind: Managing Orthodoxy and Popularity in China's Propaganda', *Political Communication* 41 № 3 (2024): 435–60.

DOI 10.30966/2018.RIGA.17.3

Externally, 'foreign-facing' propaganda (*duiwai xuanchuan*) not only disseminates party-approved information to shape the 'correct' understanding of the nation to foreign audiences, but also functions as a 'system-of-systems' (*tixi*),[7] anchored in the Central Leading Group for Propaganda, Ideology, and Culture, the Propaganda Department (known as the 'Publicity Department' in the West), and the Office for External Propaganda of the Propaganda Department (known as the State Council Information Office—SCIO). In the Indo-Pacific context, external crises and disputes have repeatedly triggered this system to engage in more overt and sometimes covert information manipulation. At the height of the Senkaku/Diaoyu Islands dispute with Japan in 2012–14, China's manipulation of information revolved mainly around arguments sustaining the country's territorial claims over the islands (e.g. 'geographical proximity', 'map-based evidence', and 'historical jurisdiction').[8]

Later the more aggressive 'wolf warrior' diplomacy of 2017–23 highlighted Beijing's willingness to take reputational risks as it defended its positions on issues such as Xinjiang, Hong Kong, and Covid-19. The confrontational style of political communication adopted by Chinese actors during the Senkaku/Diaoyu dispute was more widely embraced between 2017 and 2018 as Xi Jinping further consolidated his personal power.[9] In wolf warrior diplomacy, information manipulation was a tool to deflect and rebut criticism targeting Beijing's actions with a dual audience: externally it sought to contest unfavourable narratives and project resolve, while domestically it helped to channel nationalist sentiment and pre-empt or deflect criticism at home. Further, Chinese manipulation targeting foreign audiences shifted from an original focus on legacy media (newspapers, magazines, TV, and radio channels, as well as the online websites related to

7 Jeffrey Engstrom, *System Confrontation and System Destruction Warfare: How the People's Liberation Army Seeks to Wage Modern Warfare* (RAND, 2018), pp. 2–3.

8 People's Republic of China, State Council Information Office, *Diaoyu Dao, an Inherent Territory of China*, September 2012.

9 Peter Martin, *China's Civilian Army: The Making of Wolf Warrior Diplomacy* (Oxford University Press, 2021), p. 211–15.

DOI 10.30966/2018.RIGA.17.3

such media) to a strong focus on building a diffuse social media presence on Western platforms, particularly Twitter (now X).[10]

Nowhere are these dynamics more visible than with regard to Taiwan, which occupies a unique position in PRC thinking as both a 'core interest' and as a democracy where the information space is highly exposed to mainland manipulation through the Chinese language. Chinese information manipulation intensified around the 2018 local elections in Taiwan, when troll factories and coordinated inauthentic behaviour were used to disguise favoured candidates and microtarget demographics (narrow audience segments selected on the basis of data-driven sentiment analysis of their attitudes and concerns), with the Beijing PLA's Base 311 widely cited as a key actor. These techniques expanded in Taiwan's 2020 presidential and 2022 local elections and culminated in the 2024 general election, when artificial intelligence (AI) generated or doctored audio and video featured prominently in attacks on candidates opposed to unification, with narratives seeded by sock-puppet accounts and subsequently amplified by mainstream media and political figures.[11] Such campaigns have been closely intertwined with other forms of (particularly economic) coercion, making it difficult to disentangle the specific causal impact of information manipulation from parallel tools of influence.

Experiences in Taiwan and Hong Kong have informed Chinese approaches elsewhere in the region. As PRC actors refine techniques and test them on these 'core' interests, they adapt lessons to the multiple 'frontlines' that extend from US allies such as Japan, South Korea, Australia, and New Zealand to Southeast Asian states and Pacific Island countries. Although the modalities and intensity of manipulation vary across these contexts, they are connected by a strategic objective: to weaken or neutralise US presence and influence in the Indo-Pacific and, over the longer term,

10 Zhao Alexandre Huang and Rui Wang, 'Building a Network to "Tell China Stories Well": Chinese Diplomatic Communication Strategies on Twitter', *International Journal of Communication* 13 (2019): 2984–3007.

11 Chen-Ling Hung et al., *AI Disinformation and Taiwan's Responses during the 2024 Presidential Elections* (Taiwan Communication Association and Thomson Foundation, 2024).

DOI 10.30966/2018.RIGA.17.3

to underpin a Sino-centric global order. In this logic, information manipulation is the preferred method of the PRC to achieve that purpose.

In the Indo-Pacific, PRC information operations have targeted middle powers' strategic communications and associated connectivities. One of the central targets has been Japan's 'Free and Open Indo-Pacific' (FOIP) vision that forms discourses on alliance and minilateral associations. For example, China frames FOIP and related minilateral and alliance structures as US-driven containment, promoting instead narratives of Chinese economic connectivity and development.[12] These narratives circulate through official media, state-affiliated social media accounts, and coordinated or sympathetic Japanese-language networks, often exploiting flashpoints such as the Fukushima ALPS water release.

Russian information operations targeting FOIP also exist, albeit on a more limited scale. They are more explicitly tied to Ukraine, to delegitimate Japanese and associated Western support for it. State media and affiliated accounts further question Western unity, highlight NATO and AUKUS as destabilising, and cast Japan's alignment with the G7 and its Western partners in a negative light. Russian and Chinese activities against FOIP converge in practice by repeatedly amplifying overlapping anti-FOIP and anti-Western frames to create a 'net information effect'.[13]

Conceptually the Indo-Pacific information environment can thus be understood as a contested space where multiple strategic discourses—liberal, rules-based visions such as FOIP, and authoritarian, sovereignty-centric alternatives—compete.[14] Within that space, PRC and Russian-linked actors mobilise overlapping ecosystems of state media, diplomatic accounts, proxy outlets, and inauthentic personas to amplify grievances, delegitimate Western associations, and normalise their own alternative frames.

12 Chiyuki Aoi, Martin Innes, Emma Martin, and Tara Flores, 'Japan's "Free and Open Indo-Pacific" and Russian and Chinese Information Influence', *Defence Strategic Communications* 16 (Autumn 2025): 175–222.

13 Ibid.

14 Chiyuki Aoi, 'The Indo-Pacific, Geopolitics and Strategic Communications: The Construction of the Indo-Pacific', *Defence Strategic Communications* 14 (Spring 2024).

DOI 10.30966/2018.RIGA.17.3

Gaps in the Existing Regional Architecture against Information Manipulation

Despite the ongoing and region-wide information manipulation challenge originating in the PRC—and, to a lesser degree, Russia, and in the case of South Korea, North Korea—counter-manipulation capabilities vary considerably or exist in disparate forms among the IP4 and lag behind in certain areas. Several factors explain this uneven and uncoordinated state of regional counter-information manipulation capabilities. One cluster of explanations relates to external structural conditions—the background institutional environment, notably the absence of a common regional security framework, and divergent strategic perceptions and priorities. Another cluster comprises internal institutional, technical, and political-bureaucratic and academic cultural constraints, all of which are path-dependent in nature. These are examined in turn below. Overall the analysis suggests that although external conditions help set the broad direction of policymaking, the more salient explanatory factors lie in internal institutional conditions. Against a backdrop of information threats that link the Indo-Pacific and the Euro-Atlantic, Indo-Pacific partner states could in principle benefit from closer collaboration with European counterparts, even in the relative absence of US leadership in this policy area. Yet, in practice, state responses are mediated—and at times effectively overridden—by domestic institutional configurations and policymaking cultures.[15]

Institutional scarcity and fragmented architectures

A defining characteristic of the Indo-Pacific theatre is the lack of a region-wide multilateral institutional setting, which makes the region potentially more vulnerable to hostile information manipulation. Asian alliances with the US are traditionally organised on a 'hub and spokes' basis, and while recently trilateral and minilateral networks have spread, they

15 Gideon Rose, 'Neoclassical Realism and Theories of Foreign Policy', *World Politics* 51 Nº 1 (1998): 144–72; Randall L. Schweller, 'Unanswered Threats: A Neoclassical Realist Theory of Underbalancing', *International Security 29* Nº 2 (2004): 159–201.

DOI 10.30966/2018.RIGA.17.3

are without treaty or normative obligations.[16] The lack of multilateral institutions in the Indo-Pacific contrasts with the situation in Europe, where there are dense layers of these, including regional alliances and organisations, of which NATO's commitment to Article 5 of the North Atlantic Treaty spelling out the collective defence obligations of all members is the clearest example.

From the perspective of Indo-Pacific middle powers, this institutional landscape where there is no overarching security architecture binding them to a common normative framework seems to present constraints in the domain of information threats as well. The lack of dense regional architecture makes it harder for Indo-Pacific middle powers to develop a common situational awareness regarding the nature of information threats, standardise terminology to describe the nature of threats, or scale up successful national practices across borders on countering information manipulation.

While 'minilateral' arrangements have proliferated in the region, such institutions have not yet been leveraged to establish a shared framework for countering information manipulation, except in the trilateral context involving the US, Japan, and South Korea, where they agreed at Camp David in 2023 to establish a trilateral political commitment to 'discuss ways to coordinate efforts to counter disinformation' as part of a broader security agenda.[17] While this remained at the level of general intent, in December 2023 Japan and the US bilaterally concluded a separate Memorandum of Cooperation on Countering Foreign Information Manipulation, which sets out a bilateral framework to improve their capacities to detect, analyse, and respond to FIMI and 'sets the direction for future collaboration' between the two governments.[18] While these

16 Victor D. Cha, 'Power Play: Origins of the U.S. Alliance System in Asia', *International Security* 34 Nº 3 (Winter 2009/10): 158–96.

17 U.S. Embassy and Consulates in Japan, *Fact Sheet: The Trilateral Leaders' Summit at Camp David*, 18 August 2023, https://jp.usembassy.gov/fact-sheet-trilateral-summit-at-camp-david [accessed on 27 April 2026].

18 Japan, Ministry of Foreign Affairs, 'The Signing of the US Japan Memorandum of Cooperation on Countering Foreign Information Manipulation', Press Release, 6 December 2023, https://www.mofa.go.jp/press/release/pressite_000001_00027.html [accessed 27 April 2026].

DOI 10.30966/2018.RIGA.17.3

commitments have not been publicly discontinued, however, there has been little discernible progress since President Trump took office, and the US has since disbanded the State Department's office responsible for programmes on counter-manipulation.

More recently, in their '2+2' consultations Japan and Australia have discussed enhancing cooperation 'on strategic communications, narratives and countering foreign information manipulation, including through developing our joint understanding of the impact of foreign state information manipulation, and discussing ways to support civil society, media and academia to build societal resilience', along with enhancing cybersecurity cooperation and information security cooperation.[19] In a separate context Japan has also signalled an intention to work with Pacific Island partners to build regional 'resilience' against cyberattacks, AI misuse, and disinformation.[20] These moves highlight the potential of such minilateral arrangements, but it is, at the time of writing (spring 2026), too soon to judge their trajectories; the way these arrangements are implemented may underscore the relative difficulty—compared with areas such as joint exercises or humanitarian assistance and disaster relief—of translating political intent on FIMI into fully operational agreements.

By contrast, over the past decade, European responses have been more rapid and significant than in the Indo-Pacific, and such efforts seem to have coalesced in dense institutional structures. The EU has developed a dedicated FIMI concept, built monitoring capacities, and established procedures for exposing FIMI incidents, while sponsoring specialised centres and projects. Increasingly the EU seems to have established a conceptual link between its counter-FIMI activities and the defence of democracy, a most recent expression of which is the EU Democracy

19 Japan, Ministry of Foreign Affairs, 'Eleventh Japan-Australia 2+2 Foreign and Defence Ministerial Consultations ("2+2")', 5 September 2024, https://www.mofa.go.jp/a_o/ocn/au/pageite_000001_00553.html.

20 Japan, Ministry of Defence, 'Keynote Address [by the Defence Minister Koizumi]: The Pacific—at the Center of Resilient Connectivity', 23 February 2026, https://www.mod.go.jp/en/article/2026/02/943b03d55e3e3b350e72c0a3ac7844810c2b3755.html#:~:text=1.,the%20"Ocean%20of%20peace.

DOI 10.30966/2018.RIGA.17.3

Shield.[21] For Europe the lack of comparable institutionalisation in the Indo-Pacific would mean that any attempt to build cross-regional cooperation on FIMI must contend not only with the specificities of PRC and Russian information strategies in the Indo-Pacific, but also with the institutional thinness of the regional order. Euro-Atlantic actors accustomed to operating in dense organisational settings will encounter partners whose responses are anchored in national bureaucracies and bilateral alliances with Washington, rather than robust regional platforms. In fact, since President Trump took office in 2025, Japan and South Korea, in particular, appear to have adopted a more cautious approach to counter-information manipulation, with the result that independent or collaborative activities in this area are less likely to be publicly emphasised than during the previous US administration.

Divergent threat perceptions and strategic priorities

Beyond the background structural conditions outlined above, the IP4 countries perceive information threats emanating from state actors differently, depending on historical background and geographical context, which results in divergent strategic priorities across the group. Regional threat perceptions also diverge from those prevailing in the Euro-Atlantic area.

In general, IP4 countries have had to contend with multiple, simultaneous 'frontlines' when devising policies and building readiness against information threats. In this study the term 'frontlines' is used as an analytical concept denoting how each government perceives and organises information threats, and does not imply that the governments themselves employ the term in official doctrine. Under such conditions, policies must be continually balanced and prioritised across these distinct frontlines.

21 European Commission, Press Release, 'European Democracy Shield and EU Strategy for Civil Society Pave the Way for Stronger and More Resilient Democracies', Brussels, 12 November 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2660.

DOI 10.30966/2018.RIGA.17.3

Australia's case illustrates this well. While the need to address a rapidly evolving information landscape is widely recognised by policymakers, experts, and stakeholders, Australian policymakers generally distinguish between the challenges of the domestic information environment and those of the broader Indo-Pacific information environment. While interconnections exist between the two—in terms of both the operating environment and the actors involved—the nature of each is understood to require substantially different policy responses, due to the different degrees of state capacity, political norms, and geopolitical stakes involved.

In Australia's own home-front information environment, both state threat actors and non-state threat actors are active in information manipulation. Australia first became concerned at information manipulation (in the post-Cold War era) in the context of counter-terrorism. The focus was on non-state actors. In the early 2010s the PRC and other state actors emerged as sources of cyberattacks or cyber insecurity and unwanted political influence (including elite capture) in initial discussions of foreign interference.[22] A major turning point came when, in 2017, on the basis of a finding that the Chinese Communist Party had spent a decade seeking to penetrate major political parties and influence policymaking,[23] Prime Minister Malcolm Turnbull launched a 'Counter Foreign Interference Strategy' as a new focus for national security.[24] The strategy focused on protecting democracy and boosting resilience through four central components—sunlight, enforcement, deterrence, and capability—backed by a rolling legislative programme on foreign interference and espionage. More institutional innovations followed to detect, disrupt, and deter illegal interference.

22 In the 2010s vigorous debate resulted in bans on Chinese vendors from Australia's national broadband (2013) and the 5G mobile networks (2018).

23 Chris Uhlmann and Caitlyn Gribbi, 'Malcolm Turnbull Orders Inquiry Following Revelations ASIO Warned Parties about Chinese Donations', *ABC*, 3 June 2017, https://www.abc.net.au/news/2017-06-06/turnbull-orders-inquiry-following-revelation-asio-warned-parties/8592308; John Garnaut, 'Testimony to US House Armed Services Committee', 21 March 2008, https://docs.house.gov/meetings/AS/AS00/20180321/108048/HHRG-115-AS00-Wstate-GarnautJ-20180321.pdf.

24 Malcolm Turnbull, 'Speech Introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017', 7 December 2017, https://www.malcolmturnbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an.

DOI 10.30966/2018.RIGA.17.3

The threat of the PRC and other state actors has since remained a staple of the discussion on foreign interference over the last decade. Economic coercion by the PRC in response to Australia's combative stance towards Chinese influences in the World Health Organisation during the Covid-19 pandemic, and information manipulation framing the Australian government as aggressive and Australian society as hostile to Chinese people, triggered further concern about FIMI threats in Australia.[25] Russia's status as a state threat actor in information manipulation became more salient following its invasion of Ukraine in 2022.

Disinformation is therefore rife on the home front, whether promoted by foreign state or nonstate actors, and intersecting with homegrown actors, with officials reporting increased misinformation on social media, especially during elections. Public debates surrounding changes in Australia's national security posture and its defence build-up, including Australian relations with allies and AUKUS arrangements, are also susceptible to foreign manipulation. An increase in engagement in debates about Australian foreign policy approaches by inauthentic, likely state-directed actors is notable with regard to Ukraine and the Hamas–Israel conflicts.

Beyond the Australian information environment, Canberra's most immediate areas of importance are the Southeast Asian and Pacific frontlines, primarily due to their potential capacity to impact the fight against foreign interference and information manipulation. Importantly these two information environments differ markedly and therefore require tailored approaches, so that they will align with Australia's pre-existing initiatives in overseas development assistance, cybersecurity, defence and maritime security engagement, and transnational crime.

Rapid change in the online environment and weak state capacity to govern such rapid change is characteristic of the Pacific frontline. The completion of submarine cable projects and telecommunications infrastructure

25 Marise Payne, 'Australia and the World in the Time of COVID-19', Speech, National Security College, Australian National University, 16 June 2020, https://www.foreignminister.gov.au/minister/marise-payne/speech/australia-and-world-time-covid-19.

DOI 10.30966/2018.RIGA.17.3

investment by regional and international organisations drove a surge in social media uptake between 2017 and 2020, prompting the Pacific to become one of the most connected places in the world in terms of social media usage.[26] Weaker traditions of legacy media institutions in these countries, however, mean fewer countervailing sources of information. Institutional capacity and legal tools or 'regulatory confidence' in addressing malign information operations, or simple misinformation, are often weaker.

In regard to the Southeast Asian frontline, in turn, Australia has a distinct interest in greater transparency and, where appropriate, consolidation of democratic resilience. It has hence indicated a willingness to support capacity building for information resilience, recognising that Southeast Asian nations face both state and non-state actors attempting to influence their information environments. Other vulnerabilities throughout Southeast Asia include the exacerbation of political differences through information operations that create bias in societal debates on national security matters concerning Canberra, namely, South China Sea maritime issues, AUKUS, and Taiwan.[27]

In the case of New Zealand, Wellington lacks the capacity to shape the wider Indo-Pacific information environment, but it has a direct interest in foreign interference and disinformation in the Pacific. In 2023 the country's first ever national security strategy (*Secure Together*) identified twelve distinct core separate national security issues, including Pacific resilience and security, disinformation, and foreign interference and espionage.[28] As *Secure Together* makes clear, 'New Zealand's national security is intertwined with the security, stability, and resilience of the Pacific region.'[29] The contribution to social, cultural, and economic life of Pacific peoples through fluid migration patterns makes New Zealand

26 Meg Tapia, 'The Pacific disinformation playbook', *The Interpreter*, 27 November 2024, https://www.lowyinstitute.org/the-interpreter/pacific-disinformation-playbook.

27 Interview with researchers from the Australian Strategic Policy Institute (ASPI), 14 December 2024.

28 New Zealand, 'Aotearoa's National Security Strategy: Secure Together Tō Tātou Korowai Manaaki', August 2023, https://www.dpmc.govt.nz/publications/aotearoas-national-security-strategy-secure-together-tatou-korowai-manaaki.

29 Ibid., p. 26.

DOI 10.30966/2018.RIGA.17.3

a 'Pacific nation' in terms of shared interests. In fact the Pacific and New Zealand information environments can be considered liminal rather than distinct spaces, given the broader strategic narrative that New Zealand is 'both in, and of, the Pacific Islands'.[30]

New Zealand has therefore situated itself in the 'ecosystem' of Pacific resilience based on a 'Pacific-centric view of our collective interests'.[31] Wellington has invested resources in a positive agenda for promoting authentic, Pacific-created media content and institutions in both the Pacific and New Zealand, rather than adopting a combative approach to disinformation. Furthermore, New Zealand engages in media capacity-building support in the Pacific to shape the information environment, and, like Australia, has funded studio equipment and upgrades and provides training for local technicians and journalists as well as content creators. Wellington also provides technical aid (like Australia) to help Pacific nations build computer emergency response teams as part of its own evolving cybersecurity strategy. This capability helps track the origins of disinformation campaigns to state-sponsored actors and protects election processes, which are considered critical infrastructure.

While these initiatives are not explicitly positioned in the ambit of a government-led Pacific counter-disinformation strategy, the potential impact on the information environment in the Pacific is not lost on New Zealand politicians and officials.[32] The ultimate goal of these 'positive' initiatives in the Pacific information space was 'to build and support an empowered, resilient and sustainable Pacific broadcasting community which supports informed, open and democratic societies, and regional cohesion'.[33] This aligns with New Zealand's more civil

30 Henrietta McNeill, 'New Zealand's Statecraft "in and of the Pacific"', in J. Wallis, H. McNeill, M. Rose, and A. Tidwell (eds), *Power and Influence in the Pacific Islands: Understanding Statecraftiness* (Routledge, 2024), p. 151.

31 New Zealand, 'New Zealand's Pacific Engagement: From Reset to Resilience', Cabinet Paper, Proactive Release, 11 November 2021, https://www.mfat.govt.nz/assets/Cabinet-papers/Cab-Paper-NZ-Pacific-Engagement-From-Reset-to-Resilience.pdf.

32 Winston Peters, 'New Zealand Announces $10m Pacific Broadcasting Expansion, Support for Pacific Journalism', *Beehive.govt.nz*, 4 September 2018, https://www.beehive.govt.nz/release/new-zealand-announces-10m-pacific-broadcasting-expansion-support-pacific-journalism.

33 Winston Peters, 'Celebrating the 10th Anniversary of Pasifika TV', *Beehive.govt.nz*, 12 March 2026, https://www.beehive.govt.nz/speech/celebrating-10th-anniversary-pasifika-tv.

DOI 10.30966/2018.RIGA.17.3

society focused approach which puts the state in the background at home to deal with disinformation as a national security issue distinct from foreign interference and espionage (although all are consciously connected to 'resilience'). However, there are long-standing worries in New Zealand that policy implementation in areas such as climate change, disaster response, and political stability and election integrity, which strongly overlap with New Zealand's official development assistance and Pacific priorities,[34] will be negatively impacted by misinformation and disinformation.

Beyond the Pacific, New Zealand is considerably less involved than Australia in information-resilience efforts in Southeast Asia, despite recognising the region's importance for its security and trade. By contrast, Wellington is highly attentive to Australia's information environment, because New Zealand's wider security and foreign policy depend heavily on its only treaty ally, close societal ties, and continued access to Five Eyes cooperation. Any attempt to drive a wedge between Australia and New Zealand, or serious degradation of Australia's information space, would therefore have significant consequences for New Zealand.

At home, when disinformation overlaps with potential violent extremism or election interference, New Zealand's institutions have stronger tools and can require the removal of harmful content. Since 2023, 'election protocols' have required the government to adopt a more proactive, multi-agency posture to detect and counter disinformation and foreign interference while remaining politically neutral.[35] In major crises it can convene ODESC (Officials Committee for Domestic and External Security Coordination) to coordinate senior officials. In serious disinformation incidents during crises or elections, ODESC can activate legal levers such as the Crimes (Countering Foreign Interference) Act 2025, the Films, Videos, and Publications Classification Act 1993,

34 New Zealand's Pacific neighbours receive almost 60 per cent of its official development assistance funding. This number is closer to 40 per cent for Australia, although this is still Australia's largest regional contribution.

35 New Zealand, *Electoral Commission of New Zealand*, 'Election Protocols', 2023, https://elections.nz/guidance-and-rules/election-protocols.

DOI 10.30966/2018.RIGA.17.3

and the Harmful Digital Communications Act 2015, which together enable authorities to criminalise foreign interference, classify and block objectionable material, and order the takedown of content causing serious emotional distress, strengthening the focus of the Intelligence and Security Act 2017 on foreign interference and information manipulation.

Outside these more extreme scenarios, the New Zealand government defaults to a more passive, civil society and resilience focused approach to disinformation. In 2024, after a multi-year review of media regulation and proposals for a centralised online-safety regime, it effectively ruled out new legislation to directly regulate digital disinformation, and the Department of the Prime Minister and Cabinet endorsed a civil society report that recommended cautious government involvement. This reticence, in contrast to its firmer stance on foreign interference and espionage, reflects the view that, while disinformation warrants monitoring, a stronger centralised legislative response would be premature given New Zealanders' relatively high trust in government, media, and social institutions.[36]

South Korean perceptions of threat pertaining to information manipulation also identify multiple 'frontlines', albeit ones that are somewhat less clear-cut than those in the Oceania (Australia and New Zealand) case studies. A closely associated issue with multiple 'frontlines' is the complex interaction between foreign information manipulation and domestic discourses, suggesting the difficulty of applying the concept of FIMI, which assumes separation of foreign-sourced and domestic-sourced manipulation.

In South Korea the first frontline is facing the traditional adversary, North Korea, which is not only a conventional military threat, but also a persistent source of influence operations, including information manipulation, designed to exacerbate 'national division and socio-economic disruption', together with cyberattacks and heists targeting

36 New Zealand, DPMC, 'Multi-Stakeholder Group to Strengthen Resilience to Disinformation', 19 June 19, https://www.dpmc.govt.nz/our-programmes/national-security/strengthening-resilience-disinformation/multi-stakeholder-group-strengthen-resilience-disinformation.

DOI 10.30966/2018.RIGA.17.3

South Korean military, banking, and telecom networks.[37] Since 2023 Pyongyang has advanced the so-called 'hostile two-state policy', and appears to have shifted its influence operations towards systemic competition. In place of its earlier emphasis on the collapse of the South Korean regime and unification under its leadership, it has positioned itself in broader opposition to the US-led international order.[38]

Currently there is growing recognition in South Korea that China is a source of information manipulation threats, accompanied by widespread concern regarding malign political influence attributed to Beijing. The PRC has, in recent years, engaged in both overt and covert activities intended to influence South Korea's policymaking and public opinion. When Seoul decided to deploy the THAAD (Terminal High Altitude Area Defense) anti-ballistic missile system, Beijing responded through official statements and economic coercion, while Chinese patriotic hacktivists targeted the Lotte Group, which provided a golf course for the system's deployment, and South Korean government agency websites.[39]

South Korea's information space is unique among the IP4 in that a significant cohort of public opinion believes that the US or Japan is the source of information manipulation or disinformation.[40] Yet the most striking feature is how foreign information manipulation grew increasingly politicised in South Korean society as foreign information manipulation became integrated or used in domestic political discourses. An example is the administration of former President Yoon, whose declaration of martial law resulted in his impeachment. While in office Yoon took the unprecedented step of publicising an official report on

37 Republic of Korea, Office of National Security, *National Cybersecurity Strategy*, February 2024, p. 26, https://www.ncsc.go.kr:4018/ko/main/PageLink.html?token=MDEyMzQ1Njc4OWFiY2RlZrBvBnCd4cC_Aqu-HrYk1bj40bf53UCktx0S0UOFjLhu4da4JEysnhMG2KEmLDkdK1r5XRh8mf3uVEYp84lWk3nDC0V_akNmpFFHwsQOLQhJ.

38 Expert interview, 13 February 2026.

39 Jaewoo Choo, 불통의 중국몽 [The uncommunicative Chinese dream] (Inmoongonggan, 2024), pp. 99–135.

40 A recent opinion poll found that, when asked to name the two countries most likely to interfere in South Korean elections, respondents who placed China first or second comprised a combined 32.48 per cent, followed by North Korea at 29.23 per cent, the US at 23.10 per cent, and Japan at 10.30 per cent. Sunghack Lim, *Foreign Electoral Interference in South Korea: Public Perceptions and Current Landscape*, EAI Working Paper (Seoul: East Asia Institute, 2024).

DOI 10.30966/2018.RIGA.17.3

PRC influence activities in South Korea in 2023, produced by the National Cyber Security Center under the National Intelligence Service (NIS).[41] When he declared martial law at the end of 2024, he justified the order as a necessary measure to safeguard the country's liberal democracy from internal and external hybrid warfare threats—including disinformation campaigns and election interference—allegedly involving authoritarian regimes, namely North Korea and China, as well as purported collaboration with the South Korean opposition party.[42]

The Democratic Party rejected these claims, accused Yoon and his supporters of spreading disinformation and conspiracy theories, and launched the 'Democratic Police Station' asking the public to report suspected manipulation. After Lee Jae-myung became president in June 2025, the government shifted focus towards domestically generated manipulation, including hate speech and distorted information as threats to democracy,[43] as evidenced by the administration's particular concern about disinformation attributed to domestic right-wing extremism, including the amplification of anti-China sentiment.

This deepening political polarisation complicates the governance of foreign information influence. Information is increasingly evaluated through partisan lenses, with narratives aligned with one's political position framed as legitimate and opposing claims dismissed as 'disinformation'. Moreover, political divisions have made actors across the political spectrum more receptive to ideologically aligned narratives, further blurring the boundary between FIMI (foreign) and DIMI (domestic). This blurring presents a key analytical and policy challenge concerning FIMI, as noted in interviews conducted in Seoul. FIMI is often difficult to identify

41 Republic of Korea, National Cyber Security Center, 'China's Malign Activities by Exploiting "Fake News Websites"', 13 November 2023, pp. 6–8, https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=SecurityAdvice_main&nttId=88028&menuNo=020000&subMenuNo=020200&thirdMenuNo=#LINK [accessed December 2025; the link has since become unavailable].

42 Kwak Min-seo, [전문] 尹, 체포영장 집행 후 '국민께 드리는 글' 공개 [[Full text] Yoon releases 'Letter to the People' after execution of arrest warrant], *Yonhap News Agency*, 15 January 2025, https://web.archive.org/web/20250115100024/https://www.yna.co.kr/view/AKR20250115144300001.

43 Jihae Lee, 'President Lee Announces Crackdown on Hate Speech, Racism', *Korea.net*, 12 November 2025, https://www.korea.net/NewsFocus/policies/view?articleId=282088.

DOI 10.30966/2018.RIGA.17.3

because it aligns closely with pre-existing domestic beliefs, values, and narratives in South Korea.

In the case of Japan, it is difficult to identify clearly discernible 'frontlines' in dealing with information manipulation. Japan is primarily concerned about information operations of the PRC, although scholarly research suggests the presence of other state threats, albeit not to the same significant degree as the PRC's. Japan's information activities, including monitoring, analysis, and signalling, are clustered on the Indo-Pacific information environments around which there are strategic relations with the PRC—such as territorial disputes over Senkaku/Diaoyu—and discourses on Japan's FOIP vision.[44] Information activities also cluster around key theatres of strategic competition, including US–China rivalry and North Atlantic–Russia confrontation—for example, over Taiwan in the former case and over the war in Ukraine and Japan's support for Kyiv in the latter.

Japan's approach is also characterised by its weakness in dealing with threats to its own information space (the home front),[45] emanating from foreign or domestic malign or politically motivated actors, either state threat or non-state threat. This may reflect the disproportionate attention given to general misinformation (as opposed to disinformation or more behaviourally oriented FIMI traceable to foreign sources) by internal ministries, and divided bureaucratic responsibilities where foreign political-strategic and malign sources are the purview of the national security bureaucracy, as opposed to the Ministry of Internal Affairs and Communication (which deals with more general platform matters). This may partially be due to the weakening but prevalent perception, including among officials, that Japan's information space is both insular

44 For a comprehensive open-source intelligence analysis of the FOIP concept, see Aoi et al., 'Japan's "Free and Open Indo-Pacific"'.

45 See also Kyoko Kuwahara, 'Japan Must Reboot Its Disinformation Defences', *East Asia Forum*, 24 May 2025, https://eastasiaforum.org/2025/05/24/japan-must-reboot-its-disinformation-defences.

DOI 10.30966/2018.RIGA.17.3

and resilient vis-à-vis foreign manipulation, due to strong support given to baseline foreign and defence policies.[46]

Japan is a latecomer to counter-disinformation or information manipulation activities. The term FIMI has not been officially adopted to date. While historically focusing on strategic-level narratives, relying on the Indo-Pacific construct since former Prime Minister Abe promoted the concept in the mid 2000s, and the FOIP concept as a strategic narrative since 2017, Japan did not have a specific focus on detecting and countering information manipulation attacks.[47]

It was the 2022 strategic documents (comprising Japan's *National Security Strategy*, *National Defense Strategy* and *Defense Buildup Program*[48]) that identified 'information warfare' in the so-called 'cognitive domain, including the spread of disinformation'[49] or 'integrated information warfare with special regard to the cognitive dimension'[50] as a feature of the contemporary threat landscape, and mandated the Japanese government to develop capabilities for countering it. The same documents also stipulated a budget for counter-disinformation capacity building in the government, including a pledge to develop advanced intelligence and analytical systems using AI by 2027, a process which has since been accelerated by a year before the planned revision of the documents at the end of 2026.

46 Heather A. Conley et al., 'Countering Russian & Chinese Influence Activities', *Center for Strategic and International Studies*, 1 July 2020, https://www.csis.org/analysis/countering-russian-chinese-influence-activities-0; D. Stewart, *China's Influence in Japan: Everywhere yet Nowhere in Particular* (Washington, DC: Center for Strategic and International Studies (CSIS), Europe, Russia, and Eurasia Program/Southeast Asia Program, 2020). For more context, see Aoi et al., 'Japan's "Free and Open Indo-Pacific"'.

47 On the linkage between the Indo-Pacific, FOIP, and strategic communications, see Aoi, 'Indo-Pacific, Geopolitics and Strategic Communications'.

48 Japan, *National Security Strategy of Japan*, December 2022, https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf (English version); Japan, *National Defense Strategy*, 16 December 2022, https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf; Japan, Ministry of Defense, *Defense Build-Up Program*, 16 December 2022, https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf.

49 Japan, *National Security Strategy* of Japan, p. 27.

50 Japan, *National Defense Strategy*, p. 15.

DOI 10.30966/2018.RIGA.17.3

Hence, it is largely 'information warfare' in the cognitive domain and 'disinformation' that the government is mandated to counter, with these concepts described but not tightly defined in the documents. Japan's 2022 national security documents and subsequent official statements commit to defending a free and open international order grounded in universal values such as freedom, democracy, human rights, and the rule of law as core national interests, and they highlight information warfare, including the spread of disinformation, as a growing challenge for Japan's security and decision-making environment.[51] In Japan it is the National Security Secretariat that coordinates whole-of-government efforts at the level of the assistant chief cabinet secretary, in collaboration with the director of cabinet intelligence and director of cabinet public affairs. Under its coordination, each ministry has enhanced, to date, its own monitoring and analytical capabilities, as well as external communications against information manipulation. The Cabinet Public Affairs Office/ International Public Relations Office collaborates closely with the National Security Secretariat, the Ministry of Foreign Affairs, the Ministry of Defense, and other relevant ministries and agencies. It is currently the Cabinet Intelligence and Research Office (CIRO) Situation Center that collects, aggregates, and analyses publicly available information, including disinformation attempts, under the direction of the director of cabinet intelligence. As will be further discussed below, the current government plan is to overhaul Japan's fragmented intelligence system by creating a National Intelligence Council and a National Intelligence Directorate to coordinate and integrate collection and analytical functions that are now dispersed across multiple ministries and agencies.

Japan's current system for countering an 'information war' is organised through approaches to information threats that are not explicitly linked to specific actors or theatres, although government sources often describe multilayered challenges, including hybrid and informational ones,

51 Japan, *Defense Buildup Program*; Ministry of Defense, 'Integrated Information Warfare in the Three Security Documents', https://www.mod.go.jp/en/images/ed8cf86c9f9cad56f540d58d782f0e5dc50bc272.pdf; and Ministry of Foreign Affairs, *Diplomatic Bluebook 2024*, chs. 1 and 3 (sections on information warfare and strategic communications), https://www.mofa.go.jp/policy/other/bluebook/2024/pdf/pdfs/2024_all.pdf.

DOI 10.30966/2018.RIGA.17.3

posed by the PRC. Rather, judging from past practice,[52] Japan's approach to counter-manipulation tends to be tied to major foreign policy events where reputation needs to be protected.

Internal institutional factors and technical constraints

The principal constraints on inter-regional and intra-regional middle-power cooperation, however, are internally rather than externally induced, and they derive from path-dependent divergences in institutional design, technical capacity, and bureaucratic-political/academic culture that shape how information manipulation is monitored, interpreted, and disclosed. These divergences are also dependent upon the historical trajectories of particular states: they reflect the uneven evolution of domestic arrangements for information governance, as well as the absence of shared standards in the conduct and management of analysis, attribution, and publication across the IP4 and between the Euro-Atlantic area and the Indo-Pacific. They also point to asymmetries in technical capability, since identifying and communicating information manipulation require specialised analytic infrastructures, evidentiary practices, and discretionary judgement.

Lack of a regionally shared terminology, narrative, or metaphor to describe the threat of information manipulation

The analysis above indicates the general recognition that the PRC is commonly engaged in information manipulation aimed at undermining the region's collective ties to the US. Yet the analysis also indicates that nations adopt different framing and terminology for information manipulation and that there is no common term, narrative, or metaphor to describe the common *regional* experiences. The four countries (South Korea, New Zealand, Australia, and Japan) examined describe the

52 Japan, Ministry of Foreign Affairs, 'The Responses to Information Manipulation, including Spread of Disinformation', 4 December 2025, https://www.mofa.go.jp/policy/pagewe_000001_00052.html.

DOI 10.30966/2018.RIGA.17.3

information manipulation threats to their own country in varied terms without necessarily producing a common or conjoined perception of the threat environment in the broader Indo-Pacific context, which the PRC probably targets to disrupt democratic linkages. The general lack of willingness to attribute these manipulations publicly, as further discussed below, only makes it more difficult to adopt streamlined concepts on a national basis and to achieve international coordination of common narratives.

In terms of framing, in South Korea to date, foreign information manipulation, or FIMI, has not been formally defined or fully institutionalised in government practice and is typically subsumed under, or closely associated with, cybersecurity policy or intelligence/counter-intelligence, rather than being treated as a distinct policy category. This is a trend that can perhaps be attributed to the historical context of having North Korea as the main external foe, where the main domestic actors empowered to deal with analysis of security questions have been intelligence-related organisations—which do not necessarily enjoy popular trust. Under the former (and disgraced) Yoon administration, Chinese online 'commenting' operations—an oft-used Korean term denoting foreign information manipulation—were noted by the government and experts alike as threatening to exacerbate existing cultural, social, and ideological divisions and to undermine the nation's strategic alignment with the US and Japan. Under the current Lee administration, by contrast, there is a tendency not to pursue Chinese commenting operations as keenly as did the previous administration. Given the deep political divide between conservatives and the opposition, even attempts to acknowledge and attribute information manipulation tend to be politicised, as noted above.

Australia, on the other hand, has a policy of integrating information manipulation and counter-information manipulation in the cabinet-led StratCom framework. The government is clear about the use of terms to describe relevant information manipulation activities. It is also well aware of the identity of state and non-state threat actors. Yet the

DOI 10.30966/2018.RIGA.17.3

government as a matter of principle does not publicly name the PRC as an information manipulation actor. *The policy is to avoid making information manipulation an isolated issue, and to deal with it in the context of ongoing foreign or security policy.* Notably, Australia frames foreign influences in terms of both Australian and Indo-Pacific regional concerns. Australia perceives multiple frontlines where state threats and non-state information manipulation is concerned—domestically and in its immediate vicinity, such as Southeast Asia and the Southern Pacific Islands.

New Zealand, although allied with Australia, has distinct perceptions and definitions when it comes to 'disinformation' or foreign influences. In its case foreign interference pertains to many of the same issues as with Australia and is defined similarly. However, disinformation as a form of information manipulation is considered a national security issue distinct from foreign interference and espionage. Disinformation sits on its own alongside foreign interference, espionage, and counter-terrorism concerns as one of the twelve 'core national security issues'.

Also, the way New Zealand contextualises and defines its disinformation approach, as in Australia, is embedded in pre-existing or overall national security and development/official development assistance (ODA) frameworks. Specific legislative initiatives or new or repurposed government agencies or taskforces have not been explicitly directed towards 'shaping' the information environment to prevent disinformation. Rather, New Zealand's 'whole of society approach' to disinformation is civil society focused and more in line with the approach of the Pacific Islands Forum, a regional body which New Zealand helped establish, which today is focused on enhancing resilience through cooperation on sustainable development, climate change, security, and other shared priorities. Hence, both Australia and New Zealand exhibit a strong tendency to embed information resilience into their own national foreign and security policy, which is distinct from Europe's approach to FIMI.

Japan, on the other hand, does not officially use the term information manipulation or FIMI, but it generally locates disinformation and

DOI 10.30966/2018.RIGA.17.3

information manipulation related threats under 'information warfare in the cognitive domain, including disinformation' (*National Security Strategy*, 2022). The government is reviewing three strategic doctrines including the national security strategy later in 2026 and presumably all these frame issues are under review. The information manipulation threat is also located under the national security goals, which call for the maintenance of the rules-based order in the Indo-Pacific region. Japan is relatively silent on what it sees in terms of the PRC or other state threat actors' information manipulation activities, and how it characterises them. That policy, as well as analytical capabilities in this area, is yet to emerge and develop fully.

Another issue pertaining to the 2022 strategic documents is that by incorporating the language of 'information war' into doctrine, together with a range of aspects to be strengthened, the relationship with, and hierarchy among, all these new elements and strategic communications dating back to the mid 2000s became unclear, while Japanese grand strategy has remained focused on the Indo-Pacific vision.

Thus, the four countries variously describe and frame information manipulation threats as a matter of independent policy and analysis, without mention of the broader Indo-Pacific context where PRC attacks on democratic association are considered a common threat. Where a country does have an Indo-Pacific component in its information manipulation policy, such as Australia, it is not closely connected to other states' assessments in the Indo-Pacific region. Responses are also nationally oriented and currently not coordinated.

Lack of willingness to publicly attribute the source of information manipulation

One of the most striking features of information manipulation and counter-information manipulation in the region is that, in contrast to Europe, the US, or Canada, where 'exposure' (of predominantly Russian

DOI 10.30966/2018.RIGA.17.3

and to a lesser extent PRC information manipulation) is a near routine and often chosen practice, three of the countries examined—Australia, Japan, and South Korea—lack an express willingness to publicly attribute the source of the threat, especially when it is the PRC, in a routinised manner as part of a counter-information manipulation approach. Exceptions do exist. In South Korea, under the previous Yoon administration, the government released the NIS report on PRC manipulation. But that proactive approach appears to have been closely tied to Yoon's own political stance rather than institutionalised practice. The current Lee administration seems markedly less active on this issue.

This reluctance stems from a few factors. First, some governments in the region, namely Japan, Australia, and New Zealand, consider civil society in their nation to be highly resilient towards information manipulation. Under such circumstances, the governments consider public attribution at the highest levels of government to be sub-optimal, as it may cause overreaction among the public or unnecessary incitement in society.[53] Second, and equally important, is a reluctance to provoke state threat actor(s) out of concern for the possibility of even stronger actions that might exacerbate regional tension. Finally, public attribution may reduce the scope of actions that can be taken on the part of the government concerned, where the preference is to understand information manipulation attacks in context and to balance any counter-information manipulation actions with broader diplomatic and security agendas.

Canberra considers Australia to be relatively resilient towards information manipulation and argues that the nation has not been subjected to information manipulation on the level experienced by European nations and the US. Rather, it sees information manipulation as an ongoing threat that has to be dealt with in balance with the overall foreign policy and security context. Australia sees the threat landscape it faces along several 'frontlines', all of which create distinct contexts. Australia also sees different types of information manipulation threats when it looks

53 As discussed below, New Zealand has had a unique policy of routinely and publicly attributing sources of disinformation through transparency exercises by intelligence assessments since 2023, but not through a cabinet-centred process.

DOI 10.30966/2018.RIGA.17.3

beyond its vicinity (Southeast Asia and the Southern Pacific) into the alliance with the US and newer minilateral entities such as the Quad and AUKUS. There, the impetus is likely to be more straightforward exposure and counter-action against state threat actor(s), together with equally equipped actors such as the US.

Similarly the Japanese government considers the Japanese public to be highly resilient to Chinese information manipulation when it comes to foreign and security policy. Japan does not officially acknowledge the PRC as an information manipulation threat actor, although the government is well aware of such threats and does carefully monitor narratives that spread hostile images of Japan. Like Australia, Japan has had to contend with various coercive measures, including informational and economic ones, that Beijing has historically adopted. Like Australia, Japan has had a tendency to prefer case-by-case responses in the context of diplomacy at the time, where exposure or public attribution is more an exception than routine.

New Zealand, however, has a routine process of disclosing the primary source of foreign interference, including informational manipulation, in the context of foreign interference and espionage challenges (although these states are not explicitly framed as disinformation vectors). Namely, the New Zealand Security Intelligence Service (NZSIS) began publishing an annual unclassified threat assessment in 2023 as a response to recommendations following the 2019 Christchurch attack and to the need to be more transparent about national security forecast and assessment. In subsequent annual reports, PRC, Iranian, and Russian interference are highlighted, ranging from political and economic espionage to the informational. The 2024 report refers to a Chinese-language news media outlet suspected of coordinating PRC directions and amplifying PRC narratives, while signing content sharing agreements with organisations that also conform to the narratives.[54] The 2025 report also notes foreign interference being conducted in New Zealand by the PRC's United

54 New Zealand Security Intelligence Service, *New Zealand's Security Threat Environment 2024*, 2024, p. 23, https://www.nzsis.govt.nz/assets/NZSIS-Documents/New-Zealands-Security-Threat-Environment-2024.pdf.

DOI 10.30966/2018.RIGA.17.3

Front Work Department to build influence through co-optation. However, NZSIS makes it clear that its intelligence insights 'should not be considered a Government policy document', and frames them as a way to inform New Zealanders about national security threats, rather than as a prescriptive strategy.[55]

Therefore, there remains a general reluctance among the majority of the IP4 to directly 'name and shame', and there is no region-wide shared approach or framing to categorise attribution and public attribution matters.

Uneven capabilities at both governmental and civil society levels for gathering information and analysing ongoing or potential information manipulation threats

Although Beijing has long interfered in neighbouring countries, information manipulation as an explicitly defined policy domain is relatively new for most governments in the Indo-Pacific. For both governments and civil societies in the region, relevant monitoring and analytical capabilities, as well as policies to govern this area, remain at an early stage of development, with Australia standing out as by far the most advanced. Developments in this domain are heavily shaped by existing strategic (including intelligence), private sector, and academic cultures and practices, which in many cases are more likely to hinder than accelerate capacity growth, as argued below. The uneven development of information manipulation related analytical capabilities is another element that sharply distinguishes the Indo-Pacific from the Euro-Atlantic zone.

A major exception to this region-wide pattern is Australia, where both the government and civil society have comparatively well-developed capabilities to gather, analyse, and publish research on information manipulation. Major think tanks and academic centres focus on these matters, supported by an active press and media sector. The government

55 New Zealand Security Intelligence Service, *New Zealand's Security Threat Environment 2025*, 2025, https://www.nzsis.govt.nz/our-work/new-zealands-security-threat-environment/security-threat-environment-2025.

DOI 10.30966/2018.RIGA.17.3

itself—particularly its intelligence organisations—routinely analyses the information environment, using both quantitative and qualitative data. And methodological innovations are actively pursued across relevant agencies, driven by the Department of Home Affairs (re-established in 2017 in response to concerns about foreign interference), which works horizontally across government agencies and with civil society to combat FIMI. This complements the cabinet-centred focus facilitated by the Department of the Prime Minister and Cabinet, which vertically integrates and coordinates the national security architecture from the top. In New Zealand the corresponding department plays a similar role in national security coordination and possesses privileged insights on disinformation due to its oversight of the country's intelligence community. However, as noted above, New Zealand's Department of the Prime Minister and Cabinet appears to have taken a step back in favour of a civil society and resilience focused approach to disinformation and, by design, lacks the breadth of legislative tools that Australia has to tackle foreign interference and information manipulation. Nor does it have a home affairs ministry—although the size of the country also plays a major role in the latter choice.

Both Japan and South Korea are still in the process of developing analytical capabilities in this area, albeit with distinct challenges. In Japan quantitative and open-source research is becoming more prevalent, and a small number of reports using foreign-sourced technologies have been published primarily by private entities. For example, a Nikkei investigation drew on foreign-sourced analytics to examine PRC-linked social media manipulation in relation to Okinawa,[56] and a recent academic study employed open-source intelligence on PRC and Russian attacks on Japan's FOIP construct.[57] However, as noted, it is not standard practice for the Japanese government to publish its own-source intelligence or open-source analyses for the purpose of publicly attributing threats, and developments in Japanese private-sector industries regarding advanced data-collection and analysis technologies are likewise rarely disclosed in

56 Nihon Keizai Shimbun, 沖縄独立煽る偽情報拡散 [Spread of disinformation promoting independence of Okinawa], 3 October 2024, www.nikkei.com/telling/DGXZTS00012030S4A900C2000000.

57 Aoi et al., 'Japan's "Free and Open Indo-Pacific"'.

DOI 10.30966/2018.RIGA.17.3

detail to the public. Japan is not short of official or semi-official warnings concerning potential foreign information manipulation threats or, more generally, disinformation and misinformation, yet these warnings are often not substantiated by data-driven analysis of potential perpetrators. Overall, systematically developed quantitative and qualitative research on information manipulation remains limited, although it is slowly expanding. The relative weakness of civil society capabilities is likely to constrain the government's capacity to obtain the sophisticated understanding and analysis required in this domain.

In terms of analytical and intelligence capabilities, it is also worth noting that Japan is in the midst of a significant reorganisation of its central intelligence architecture. At the time of writing, the CIRO is to be upgraded into a National Intelligence Directorate, and its director elevated to a rank equivalent to the secretary general of the National Security Secretariat.[58] A government bill submitted to the Diet in March 2026 was approved by the House of Representatives on 23 April, establishing a ministerial-level National Intelligence Council, chaired by the prime minister, with the new directorate acting as its secretariat and 'control tower' for collecting and analysing information from across ministries and agencies, including on foreign espionage, election interference, and foreign influence operations such as disinformation. This marks a historic effort to streamline and strengthen Japan's central intelligence apparatus, with an initial emphasis on consolidating domestic security and counter-espionage functions, and a further build-out of external and foreign-intelligence roles envisaged thereafter. Although the bureau's detailed mandate and powers remain to be finalised, the creation of a national-level intelligence chief, elevated to a level comparable to the head of the National Security Secretariat, signals a shift towards a more integrated, strategic intelligence community, in contrast to the previously fragmented, ministry-based model.

58 Nihon Keizai Shimbun, 「国家情報局」にインテリジエンス機能集約　政府、法案を閣議決定 [Government approves bill to consolidate intelligence functions in a 'National Intelligence Directorate'], 13 March 2026, https://www.nikkei.com/article/DGXZQOUA1221K0S6A310C2000000.

DOI 10.30966/2018.RIGA.17.3

South Korea has a separate and distinct set of issues when it comes to developing information manipulation analysis and counter-information manipulation capabilities. To date, much of the capacity for analysing information manipulation has been concentrated in national intelligence entities, although there are signs of progress in civil society and academic analysis, including open-source work.[59] The major constraint in South Korea, however, remains political. Deep-seated distrust towards the intelligence community, particularly among liberal actors in part due to past interference in national elections by the NIS, has prompted some civil society groups and experts to argue that the government is not the ideal entity to be tasked with counter-manipulation mandates. They tend to assert that counter-FIMI should be left to civilian capabilities. This political context has constrained the NIS role in countering foreign influence, as reflected in the January 2024 transfer of counter-espionage investigative authority to the police, a reform introduced under the liberal Moon Jae-in administration. Furthermore, political division has often led to inconsistent government priorities in focus on and support for counter-information manipulation, limiting the development of related capabilities in civil society and academia, particularly given the close linkages between academia and government in South Korea through funding and policy networks.

Another example is that intensifying political polarisation and institutional stalemate makes South Korea particularly vulnerable to information manipulation and at the same time complicates the creation of durable, stable collaborative ties even with close allies and partners. To wit, the Indo-Pacific as a strategic construct—central for Japan, the US, and Australia—has been approached differently by successive Korean administrations, precluding a consistent policy framework. Growing awareness of threats originating in the PRC might be making the public more alert, but political divisions are inclined to delay the passage of necessary legislation, including laws that would clearly define the remit

59 Eunyoung Kim and Minwoo Yoon, 사이버 인지전의 새로운 양상: 한국 온라인 플랫폼 댓글 활동 분석연구 [Cyber cognitive warfare's new patterns: an analysis of comment activities on Korean online platforms], *Korean Journal of Public Safety and Criminal Justice Administration* 22 Nº 5 (2025): 91–108, https://doi.org/10.25023/kapsa.22.5.202512.91.

DOI 10.30966/2018.RIGA.17.3

of government authorities in analysing, attributing, and determining the legality of particular activities.

Information manipulation and counter-information manipulation capabilities sit at the intersection of AI, open-source, and classified data, and of qualitative and quantitative methods, and are inherently multidisciplinary. Above all, however, effective analysis and response require stable political will to keep potential and ongoing information manipulation campaigns sharply focused. These characteristics leave Indo-Pacific countries outside the close-knit Western security–defence–diplomatic networks (such as Five Eyes, AUKUS, and NATO) struggling to keep pace with the evolving threat. Regional cultures of research, information-sharing, and intelligence—marked by strong deference to authority and relatively static political economies—further slow the development of robust capabilities in this field.

Lack of a shared platform through which to pool information, analysis, and potentially data internationally on aspects of information manipulation and information resilience

The region is virtually devoid of processes or platforms through which information manipulation related analysis, lessons learned, and potentially data can be systematically shared among countries and with the wider public. Two features that often characterise information manipulation analysis—the covert nature (at least partially) of sources, and the technology-driven nature of both manipulation and countermeasures—tend to hinder information-sharing and cooperative research. In addition, issues related to foreign interference are still sensitive in the region, and some governments may be reluctant to discuss information manipulation in open fora. While it is unlikely that intelligence-sharing mechanisms comparable to Five Eyes (in which Australia and New Zealand participate) will emerge in the Indo-Pacific, it would be desirable to establish accessible and transparent mechanisms for sharing open-source research and analysis.

DOI 10.30966/2018.RIGA.17.3

By contrast, Europe's success in establishing COEs has built on the creation of platforms for sharing research and good practice, and this sharing has helped to mainstream and nurture related work across both governmental institutions and civil society in the Euro-Atlantic area and beyond. Whether the Indo-Pacific can create a similar trajectory is uncertain, but the development of a common platform—or interoperable networks—for sharing information, analysis, and methodologies would significantly benefit the region.

Lack of a coordinated operational approach to counter information manipulation when manipulation and interference are identified

Given the broader reluctance even to acknowledge or publicly attribute ongoing information manipulation campaigns, it is perhaps unsurprising that there is as yet no region-wide operational mechanism to discuss, share information on, or jointly diagnose and counter such activity, beyond participation in the G7 RRM or limited minilateral formats. It is not so self-evident that operational responses to specific manipulation campaigns must be handled through international bodies; given the reality of the tightly intertwined nature of information manipulation and interference with other areas of national security—from broader espionage and foreign influence campaigns to the concerned nation's development/ODA and security and defence policy—in practice, operational responsibility will probably remain with sovereign states.

Notwithstanding, a region-wide coordination process—centred on the voluntary sharing of research and analysis, mutual consultation on best practices and lessons learned in countering information manipulation, and, where politically feasible, discussion of possible joint responses—would be preferable to the current absence of any structured platform. This would be particularly relevant given that PRC-linked information manipulation targets the Indo-Pacific as a whole, even if individual campaigns are tailored to specific states or sub-regions.

DOI 10.30966/2018.RIGA.17.3

At the same time, the marked caution in much of the Indo-Pacific about formally attributing information manipulation activities suggests that any such mechanism would need a concept and operating approach that are different from existing European models, including FIMI toolboxes, especially regarding when and how to share information and which types of responses to explore collectively. Even so, once manipulation is identified, routine inter-regional dialogue on information manipulation issues and structured information-sharing, with a view to considering individual or, where appropriate, coordinated responses, could help underpin a more stable and resilient information environment in the region.

The Way Forward: Towards a Research-Driven Framework for Cross-Regional Cooperation

The analysis in this study suggests that the central challenge for cross- and intraregional cooperation on information manipulation in the Indo-Pacific is not a lack of formal diplomatic commitments, but the absence of shared concepts, analytical baselines, and institutionalised channels for sustained exchange. At present the region is characterised by divergent strategic priorities, heterogeneous institutional architectures, and uneven technical capacities, all of which inhibit the emergence of practical cooperation.

Against this backdrop an ambitious attempt to construct an immediately operational regional mechanism would be politically unrealistic, at least in the short term. A more feasible avenue lies in a research-driven framework that incrementally builds common understanding, shared language, and habits of collaboration, in which specific counter-information manipulation measures can later be embedded. Such a step, moreover, should develop a shared strategic communications concept/vision, based upon common discursive practices which enable and over time create an international environment that is amenable to realising both the interests and values of those countries and organisations which are engaged.

DOI 10.30966/2018.RIGA.17.3

Such a posture amounts to a shift in the current practice on the side of the European approach to FIMI. The predominantly tactical orientation of FIMI has produced important gains in the monitoring, attribution, and exposure of hostile information operations. Yet it has not always been accompanied by a clear articulation of longer-term strategic communications aims or of how day-to-day FIMI work contributes to broader political objectives. The Indo-Pacific landscape, by contrast, despite the existence of threats, is marked by a lack of regionally shared narratives and metaphors through which those threats are conceptualised.

The result is a double gap: Euro-Atlantic partners have developed elaborate FIMI toolkits but only a partial strategic frame, while Indo-Pacific partners have neither a common strategic communications vision nor a shared vocabulary for describing information manipulation. Any attempt to institutionalise cooperation that focuses narrowly on FIMI techniques without addressing these deeper discrepancies is likely to reproduce existing fragmentation rather than overcome it.

For this reason the most credible way forward is to deepen cooperation in phases, starting from research and analysis sharing and promotion. The creation of one or more minilateral groupings—it would be premature to create an Indo-Pacific-based centre of excellence modelled on European COEs—may be considered to serve as a research-promoting hub. A focus of initial research should be to generate shared terminology, typologies, and threat assessments that integrate European and Indo-Pacific perspectives on both state and nonstate information manipulation. This would involve systematic comparative research on threat actors, methods, target audiences, vulnerabilities, and their impacts; mapping of national institutional architectures and legal constraints; and the development of common methodological standards for identifying, analysing, and characterising information manipulation campaigns. In this sense, the core added value would be in helping reconstruct information manipulation as a subset of a broader, explicitly articulated strategic communications agenda, rather than treating it as an autonomous issue area.

DOI 10.30966/2018.RIGA.17.3

Minilateral groupings could also facilitate the co-production of conceptual tools: for example, regionally grounded notions of 'strategic equilibrium (or stability)', 'hostile influence', or 'defence and deterrence, including disruption' that are intelligible across Euro-Atlantic and Indo-Pacific contexts.

In a second phase, as trust and conceptual convergence deepen, the minilateral mechanisms could expand to include capacity building—just as some minilaterals already engage in capacity building on diverse topics. Topics should cover a broad range of activities and themes, and could include tailored education and training courses, secondments, joint methodological workshops, and tabletop or scenariobased exercises that test capabilities in various phases of information operations, as well as strategic communications.

Only in a later phase, and subject to clear political consent, would it be appropriate to consider modest operational functions, such as voluntary protocols for confidential information-sharing on major FIMI incidents, informal coordination of exposure and disruption campaigns, or aligned communications. Even then, such activities should remain firmly nested in a broader strategic communications framework that prioritises long-term discourse formation over short-term 'naming and shaming' effects.

This sequencing—from research and conceptual alignment, through capacity building, to limited operational support—reflects lessons drawn from Euro-Atlantic centres of excellence, which have generally been most effective where they have supported national and regional authorities and civil society actors with expertise, training, and methodological innovation, and simply offered platforms to publish, rather than attempting to substitute for political decision-making.

A further consideration is participation in and design of such minilateral endeavours. A flexible, research-centric network—rather than a rigid organisation with uniform obligations—would better accommodate differentiated roles and levels of engagement, increasing its compatibility

DOI 10.30966/2018.RIGA.17.3

with regional political and social realities and its ability to attract and retain a critical mass of participants.

Finally, embedding a stronger StratCom component into cross-regional cooperation has normative as well as functional significance. A research-driven approach that foregrounds strategic communications—understood as the coherent articulation of policy, values, and interests over time—can help ensure that technical FIMI measures remain accountable to democratic principles and do not drift into opaque and purely tactical and technical practices.

Conclusion

The analysis in this paper has shown that, despite increasingly dense rhetoric and formal commitments, cross-regional cooperation between European and Indo-Pacific middle powers, as well as among Indo-Pacific middle powers, on information manipulation and FIMI remains weakly institutionalised and operationalised. Rather than the simple functions of time lag or limited awareness, this shortfall reflects a combination of external factors, such as divergent threat environments, and internal factors, which this analysis has shown to be of greater salience, namely, asymmetries in institutional and technical capacity, and deeply rooted political-bureacratic and academic cultures that shape how different actors understand and prioritise information threats. These frictions have meant that frameworks largely initiated under US leadership, and more recently elaborated by the EU, have not to date translated into autonomous, horizontal patterns of coordination among middle powers themselves.

The comparison between the Euro-Atlantic and Indo-Pacific theatres underscores the extent to which institutional density and conceptual clarity matter. In Europe, Russian (and to a lesser extent Chinese) information operations have been recognised as a structural, long-term challenge, prompting the development of a dedicated FIMI concept,

DOI 10.30966/2018.RIGA.17.3

specialised monitoring capacities, and an emerging linkage between counter-FIMI efforts and the defence of democracy. By contrast, Indo-Pacific middle powers face a threat landscape dominated by the PRC, where information manipulation is tightly intertwined with economic coercion, legal warfare, and maritime and military pressure, yet must respond in a context of far thinner regional security architectures and more fragmented domestic arrangements. Under such conditions of scarcity, the withdrawal of the US from the counter-disinformation regime and the new administration's apparent hostility towards counter-manipulation efforts risk encouraging weaker allies to self-censor or downplay their own attempts to strengthen counter-manipulation measures. This asymmetry of institutions and concepts makes it difficult to transpose Euro-Atlantic approaches onto Indo-Pacific realities, or to build genuinely joint mechanisms that go beyond diplomatic declarations.

In the Indo-Pacific, the IP4 cases illustrate that internal constraints are more salient than external pressures. Australia has moved furthest towards building integrated capabilities across government and civil society, with New Zealand following with its focus on counter-disinformation, within a different frame. Meanwhile Japan and South Korea each struggle with distinctive constellations of challenges—from siloed bureaucracies and limited data-driven, open-source analytical ecosystems to politicised debates over the proper role of intelligence agencies in democratic societies. These domestic constraints complicate efforts to design and legitimise robust mandates for monitoring, attributing, and responding to foreign information manipulation, and they also limit the ability of these states to engage European actors as equal partners in a shared FIMI agenda. Where analytical and institutional capacities are weak or contested at home, cross-regional cooperation risks becoming symbolic rather than substantive.

At the same time, the strong emphasis on FIMI in the EU, while understandable given its exposure to Russian operations, carries the risk of anchoring cooperation in a predominantly tactical, reactive, and defensive posture. If counter-FIMI is not nested in a broader,

DOI 10.30966/2018.RIGA.17.3

value-based strategic communications framework, it may narrow rather than deepen the shared strategic horizon between European and Indo-Pacific partners. The absence of a clearly articulated, long-term vision of how European and Indo-Pacific middle powers wish to shape the information environment—and of how their respective values and interests can be projected coherently across regions—helps explain why even promising initiatives remain under-institutionalised and siloed. Efforts to expose, attribute, and sanction specific operations, while necessary, are unlikely to substitute for this missing higher-order alignment.

Against the backdrop of hegemonic retrenchment, both European and Indo-Pacific middle powers face a stark choice. They can continue to rely on fading patterns of US leadership and accept a largely reactive role in a contested information order, or they can assume greater responsibility for defining, resourcing, and sustaining their own cooperative architectures. The analysis here suggests that meaningful progress will require two interrelated moves. First, European and Indo-Pacific middle powers need to co-produce a strategic communications framework that explicitly connects their long-term visions for a rules-based order and clarifies how counter-FIMI activities support—not substitute for—this wider project. Second, on the basis of such a framework, they must identify a limited number of concrete, politically sustainable areas for practical cooperation—which would remain in and through minilateral networks—such as joint monitoring methodologies, shared attribution standards, or coordinated capacity building, tailored to differing institutional and cultural contexts.

In short, the current gaps in Europe–Indo-Pacific cooperation on information manipulation are not simply a transitional problem that time will resolve. They reflect deeper structural and cultural misalignments that will continue to inhibit autonomous middle-power collaboration unless they are addressed directly. Yet these same gaps also illuminate where the most constructive work can be done. By treating strategic communications and counter-manipulation not as technocratic niches but as central components of a shared response to both authoritarian

DOI 10.30966/2018.RIGA.17.3

revisionism and hegemonic volatility, Europe and its Indo-Pacific partners can begin to move beyond symbolic declarations towards more durable, mutually reinforcing forms of cooperation, albeit primarily in minilateral formats. In this context, the IP4 countries already constitute a plausible minilateral constellation in their own right, even if their institutional capacities and strategic priorities remain uneven. Whether such efforts succeed will be a critical test of these states' ability to shape—rather than merely endure—the evolving information order.

Bibliography

Aoi, Chiyuki, 'The Indo-Pacific, Geopolitics and Strategic Communications: The Construction of the Indo-Pacific', *Defence Strategic Communications* 14 (Spring 2024): 26–67.

Aoi, Chiyuki, Martin Innes, Emma Martin, and Tara Flores, 'Japan's "Free and Open Indo-Pacific" and Russian and Chinese Information Influence', *Defence Strategic Communications* 16 (Autumn 2025): 175–222.

Bolt, Neville, et al., *Understanding Strategic Communications,* Terminology Working Group Publication No. 3 (Riga: NATO Strategic Communications Centre of Excellence, 2023).

Cha, Victor D., 'Power Play: Origins of the U.S. Alliance System in Asia', *International Security* 34, No. 3 (Winter 2009/10): 158–96.

Choo, Jaewoo, 불통의 중국몽 [The uncommunicative Chinese dream] (Inmoongonggan, 2024), pp. 99–135.

Conley, Heather A., et al., 'Countering Russian & Chinese Influence Activities', *Center for Strategic and International Studies,* 1 July 2020, https://www.csis.org/analysis/countering-russian-chinese-influence-activities-0.

Edney, Kingsley, *The Globalization of Chinese Propaganda: International Power and Domestic Cohesion* (Palgrave MacMillan, 2014).

Engstrom, Jeffrey, *System Confrontation and System Destruction Warfare: How the People's Liberation Army Seeks to Wage Modern Warfare* (RAND, 2018).

European External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats* (Brussels: EEAS, 7 February 2023).

Huang, Zhao Alexandre, and Rui Wang, 'Building a Network to "Tell China Stories Well": Chinese Diplomatic Communication Strategies on Twitter', *International Journal of Communication* 13 (2019): 2984–3007.

Hung, Chen-Ling, et al., *AI Disinformation and Taiwan's Responses during the 2024 Presidential Elections* (Taiwan Communication Association and Thomson Foundation, 2024).

Japan, *National Defense Strategy*, 16 December 2022, https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf.

Japan, *National Security Strategy of Japan*, December 2022, https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf.

Japan, Ministry of Defense, *Defense Buildup Program*, 16 December 2022, https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf.

DOI 10.30966/2018.RIGA.17.3

Japan, Ministry of Defence, 'Keynote Address [by the Defence Minister Koizumi]: The Pacific—at the Center of Resilient Connectivity', 23 February 2026, https://www.mod.go.jp/en/article/2026/02/943b03d55e3e3b350e72c0a3ac7844810c2b3755.html.

Japan, Ministry of Foreign Affairs, 'Eleventh Japan-Australia 2+2 Foreign and Defence Ministerial Consultations ("2+2")', 5 September 2024, https://www.mofa.go.jp/a_o/ocn/au/pageite_000001_00553.html.

Japan, Ministry of Foreign Affairs, 'The Responses to Information Manipulation, including Spread of Disinformation', 4 December 2025, https://www.mofa.go.jp/policy/pagewe_000001_00052.html.

Japan, Ministry of Foreign Affairs, 'The Signing of the US Japan Memorandum of Cooperation on Countering Foreign Information Manipulation', Press Release, 6 December 2023, https://www.mofa.go.jp/press/release/pressite_000001_00027.html.

Kim, Eunyoung, and Minwoo Yoon, 사이버 인지전의 새로운 양상: 한국 온라인 플랫폼 댓글 활동 분석연구 [Cyber cognitive warfare's new patterns: an analysis of comment activities on Korean online platforms], *Korean Journal of Public Safety and Criminal Justice Administration* 22 Nº 5 (2025): 91–108, https://doi.org/10.25023/kapsa.22.5.202512.91.

Kuwahara, Kyoko, 'Japan Must Reboot Its Disinformation Defences', *East Asia Forum*, 24 May 2025, https://eastasiaforum.org/2025/05/24/japan-must-reboot-its-disinformation-defences.

Lee, Jihae, 'President Lee Announces Crackdown on Hate Speech, Racism', *Korea.net*, 12 November 2025, https://www.korea.net/NewsFocus/policies/view?articleId=282088.

Lim, Sunghack, *Foreign Electoral Interference in South Korea: Public Perceptions and Current Landscape*, EAI Working Paper (Seoul: East Asia Institute, 2024).

Martin, Peter, *China's Civilian Army: The Making of Wolf Warrior Diplomacy* (Oxford University Press, 2021), pp. 211–15.

McNeill, Henrietta, 'New Zealand's Statecraft "in and of the Pacific"', in J. Wallis, H. McNeill, M. Rose, and A. Tidwell (eds), *Power and Influence in the Pacific Islands: Understanding Statecraftiness* (Routledge, 2024).

New Zealand, 'Aotearoa's National Security Strategy: Secure Together Tō Tātou Korowai Manaaki', August 2023, https://www.dpmc.govt.nz/publications/aotearoas-national-security-strategy-secure-together-tatou-korowai-manaaki.

New Zealand, Electoral Commission of New Zealand, 'Election Protocols', 2023, https://elections.nz/guidance-and-rules/election-protocols.

New Zealand, 'New Zealand's Pacific Engagement: From Reset to Resilience', Cabinet Paper, Proactive Release, 11 November 2021, https://www.mfat.govt.nz/assets/Cabinet-papers/Cab-Paper-NZ-Pacific-Engagement-From-Reset-to-Resilience.pdf.

Nihon Keizai Shimbun, 「国家情報局」にインテリジェンス機能集約　政府、法案を閣議決定 [Government approves bill to consolidate intelligence functions in a 'National Intelligence Directorate'], 13 March 2026, https://www.nikkei.com/article/DGXZQOUA1221K0S6A310C2000000.

Nihon Keizai Shimbun, 沖縄独立煽る偽情報拡散 [Spread of disinformation promoting independence of Okinawa], 3 October 2024, www.nikkei.com/telling/DGXZTS00012030S4A900C2000000.

Payne, Marise, 'Australia and the World in the Time of COVID-19', Speech, National Security College, Australian National University, 16 June 2020, https://www.foreignminister.gov.au/minister/marise-payne/speech/australia-and-world-time-covid-19.

People's Republic of China, State Council Information Office, *Diaoyu Dao, an Inherent Territory of China*, September 2012.

Peters, Winston, 'Celebrating the 10th Anniversary of Pasifika TV', *Beehive.govt.nz*, 12 March 2026, https://www.beehive.govt.nz/speech/celebrating-10th-anniversary-pasifika-tv.

Peters, Winston, 'New Zealand Announces $10m Pacific Broadcasting Expansion, Support for Pacific Journalism', *Beehive.govt.nz*, 4 September 2018, https://www.beehive.govt.nz/release/new-zealand-announces-10m-pacific-broadcasting-expansion-support-pacific-journalism.

Republic of Korea, Office of National Security, *National Cybersecurity Strategy*, February 2024

Rose, Gideon, 'Neoclassical Realism and Theories of Foreign Policy', *World Politics* 51 Nº 1 (1998): 144–72.

Schweller, Randall L., 'Unanswered Threats: A Neoclassical Realist Theory of Underbalancing', *International Security* 29 Nº 2 (2004): 159–201.

Tapia, Meg, 'The Pacific Disinformation Playbook', *The Interpreter*, 27 November 2024, https://www.lowyinstitute.org/the-interpreter/pacific-disinformation-playbook.

Uhlmann, Chris, and Caitlyn Gribbi, 'Malcolm Turnbull Orders Inquiry Following Revelations ASIO Warned Parties about Chinese Donations', *ABC*, 3 June 2017, https://www.abc.net.au/news/2017-06-06/turnbull-orders-inquiry-following-revelation-asio-warned-parties/8592308.

U.S. Embassy and Consulates in Japan, *Fact Sheet: The Trilateral Leaders' Summit at Camp David*, 18 August 2023, https://jp.usembassy.gov/fact-sheet-trilateral-summit-at-camp-david.

Wang, Clyde Yicheng, 'The Ideology Is Blowing in the Wind: Managing Orthodoxy and Popularity in China's Propaganda', *Political Communication* 41 Nº 3 (2024): 435–60.

Global Reorientation: A Very Short Description of the State of World Affairs

An Essay by Roland Benedikter

Keywords—*world affairs, global systemic shift, re-globalisation, big-picture analysis, grand narratives, theory versus practice of international relations, strategic communication, strategic communications*

About the Author
Dr Roland Benedikter is an interdisciplinary political scientist and sociologist based at the European Academy/Eurac Research Institute for Applied Social Sciences in Bolzano/Bozen, Autonomous Province of South Tyrol, Italy. He holds the UNESCO Chair in Interdisciplinary Anticipation & Global-Local Transformation and is the Co-Head of the Center for Advanced Studies.

Abstract
The world is undergoing a period of profound reorientation. This process, characterised by the combination of uncertainty, acceleration, and change, is calling into question familiar assumptions, mechanisms, and relational structures. How could a concise summary of the planetary situation look in an applied policy perspective? To anticipate the future of the security field, the primary task is to understand the current tension among a variety of factors, processes, and actors, that is, to develop an actively inter- and transdisciplinary view that includes the maximum number of trans-sectoral key dialectics, systemic shifts, and interrelated trajectories. What are the key pillars in terms of concepts and analytical components needed to read the evolving big picture, and what prospects

DOI 10.30966/2018.RIGA.17.4

are emerging at their intersection? This essay lists the main building blocks for a contemporary reading of events and developments to consider in an inter- and transdisciplinary medium-term perspective. It is a woodcut sketch with the intention to function as a practical and flexible toolkit. The elements discussed should be combined according to the needs of contextual understanding and anticipation, applied to concrete problems, and then placed in the overall surrounding environment in flux. The aim of this condensed map is to obtain a malleable picture of the essentials that incorporates continuities and dynamics and can be used to prepare concrete actions at the intersection of Ideal- and Realpolitik.

Shifting Interconnections

The first—and perhaps most obvious—key observation regarding the current state of world affairs is the shift in processes, habits, and modalities of *interconnectivity*. The 2020s have seen the trend to a decreasing embedment of the great powers in international order patterns, including a weakening commitment to them, which concerns both the whole and its parts. This trend is the result of a slow but steady escalation of decoupling visible already since the mid 2010s. The facts that (1) Russia since then has exited most trans-systemic agreements,[1] (2) China has transformed into a *de jure* member of global cooperation treaties which signs all of them but then regularly ignores them or does the opposite, for example with regard to human rights, neocolonialisation in Africa, or ocean protection,[2] (3) a growing number of countries like North Korea or Venezuela have been moving outside the international order and consensus,[3] and (4) the Trump II administration in January 2026 alone exited sixty-six international organisations, thus disrupting the course of the traditionally cooperation- and agreement-oriented

1 Dmitri Trenin, 'Russia's Changing Identity: In Search of a Role in the 21st Century', *Carnegie Moscow Center,* 2019, https://carnegie.ru/commentary/79521.

2 Roland Benedikter and Verena Nowotny, *China's Road Ahead: Problems, Questions, Perspectives* (Springer International, 2014).

3 Roland Benedikter, 'The New Global Direction: From "One Globalization" to "Two Globalizations"? Russia's War in Ukraine in Global Perspective', *New Global Studies* 17 № 1 (April 2023): 71–104, https://doi.org/10.1515/ngs-2022-0038.

DOI 10.30966/2018.RIGA.17.4

Western-centred global democratic alliance[4], are just some significant examples in contemporary historical symptomatology that point to a latent erosion of globalism[5] and to some extent even of internationalism. This loosening of ties is the more impactful as this development co-occurs at the hands of former founding members and factual supporting pillars of the global liberal order established since the 1990s, among them the US, on whose exceptional power and protection pro-internationalist global bodies depended until recently. Whether this erosion is only temporary or lasting is as yet unknown. Be that as it may, since the second half of the 2010s, influential nations have left global organisations and agreements such as UNESCO or the Paris Climate Agreement, while newly concluded intercontinental agreements such as the EU-Mercosur free trade agreement have proven so far to be rather weak substitutes for what seems to be indeed the inclination of the current historical phase towards a loosening of planetary ties and cooperation patterns. Whether a similar development within global interest groups such as OPEC—which the United Arab Emirates exited in April 2026, providing a 'heavy blow' to the coherence of the group of oil-producing countries[6]—points in the same direction or can lead, on the contrary, to a more permeable arrangement between producers and consumers on the globe remains to be seen.

Nevertheless, the process of transforming and transformed interconnections has led to a subtle but noticeable remodelling of interconnection *logics*.

4 The White House, *Withdrawing the United States from International Organizations, Conventions, and Treaties that Are Contrary to the Interests of the United States: Memorandum for the Heads of Executive Departments and Agencies*, 7 January 2026, https://www.whitehouse.gov/presidential-actions/2026/01/withdrawing-the-united-states-from-international-organizations-conventions-and-treaties-that-are-contrary-to-the-interests-of-the-united-states. Cf. Matthew Lee and Farnoush Amiri, 'US Will Exit 66 International Organizations as It Further Retreats from Global Cooperation', *AP News,* 8 January 2026, https://apnews.com/article/united-nations-trump-international-organizations-withdrawal-d704fb9b444dc9cf569865d391b544a6, and Euronews, *'Trump Withdraws US from UN Climate Treaty and 65 Other Global Bodies'*, 8 January 2026, https://www.euronews.com/2026/01/08/trump-withdraws-us-from-un-climate-treaty-and-65-other-global-bodies.

5 Manfred B. Steger, *Globalization in the 21st Century* (Rowman and Littlefield, 2024), and Manfred B. Steger, Roland Benedikter et al. (eds), *Globalization—Past, Present, Future* (University of California Press, 2023).

6 Maha El Dahan, 'UAE Leaves OPEC in Major Blow to Global Oil Producers' Group', *Reuters*, 28 April 2026, https://www.reuters.com/markets/commodities/uae-says-it-quits-opec-opec-statement-2026-04-28.

DOI 10.30966/2018.RIGA.17.4

One crucial aspect of the respective transition, which has been in place since the 2010s, has been branded the 'second grand transformation'[7] after the Industrial Revolution. It is related to—and co-triggered by—the combination of neo-nationalist market mechanisms teaming up with advanced technologies such as AI or chatbots which are concentrating venture and risk capital, thereby creating semi-independent power pools half-allied or parallel to politics and replacing known civilisational, cultural, and social patterns in grand style.

Yet the most important platform of this fundamental 'relational change' is at the global level, that is, where until recently the guiding logics of 'classical' neoliberal-cosmopolitan globalisation unfolded.[8] Because of the widening split between its realist (neoliberal) and idealist (cosmopolitan) factions and the resulting gradual decline of their (unholy) 25-year-alliance of 1990 to 2015, for about a decade now the question 'Is globalisation coming to an end?' has become increasingly relevant due to the ensuing ruptures in globalism, the reshoring of economies, polarisation by inequality, and the sociopolitical focus on renationalisation. This distinguishes the 25-year-long phase of 'happy' or stable globalisation from 1990 to 2015 from the current phase of 'mature' or volatile globalisation which has characterised international development patterns since the beginning of the 2020s.[9] It is no coincidence that the present is sometimes already referred to as the 'post-globalization era',[10] even if this may be too generalising and not equally applicable to the very different contexts that have surfaced over the past few years manifesting increasingly individualised characteristics and features.

Overall, we are observing—partly self-referential or cyclical—core trends of stagnation, disruption, reconstitution, and rearrangement, such as:

7 Branko Milanovic, *The Great Global Transformation: National Market Liberalism in A Multipolar World* (Allen Lane, 2025).

8 Steger and Benedikter, *Globalization—Past, Present, Future.*

9 Roland Benedikter, Ingrid Kofler, and Katharina Crepaz, *'What Is Advanced Globalization? The State of Globalization in Our Time'*, in Barrie Axford and Richard Huggins (eds), *A Modern Guide to Globalization,* Elgar Modern Guides (Edgar Elgar, 2025), pp. 79–101, https://doi.org/10.4337/9781802205695.00008.

10 Victor Roudometof, 'How Should We Think about Globalization in a Post-Globalization Era?', *Dialogues in Sociology* 1 Nº 1 (2024): 13–26.

DOI 10.30966/2018.RIGA.17.4

- *Slowbalisation*—the slowing down of global integration.

- *Deglobalisation*—the dismantling of common international standards and practices.

- *Splinternet*, including *splinter-connectivity*—the demarcation of different, per se highly differentiated and diversified intelligent technology systems, which, however, continue to be interdependent clearly above the level of a minimum common denominator.

- *Noonomisation*—the fragmentation of the global economy into systemically competing blocs of 'noonomies' (Sergey Bodrunov[11]), i.e. more context-dependent wellbeing models where traditional generalising economic priorities do not stand in the first place any more. These models, however, continue to be based on interlocking information patterns that jointly follow the logics of striving for a 'society where life is worth living' common to most trans-sectorally and inter-disciplinarily organised societies based on individualised patterns of knowledge (Nico Stehr[12]).

- *Competing modernities*—the coexistence of geopolitically competing visions of modernity and a good life, both individually and in society. Over time they have led to diversified concepts of modernisation. In a changing worldviews ecosystem, the Western and European dreams of competitive-capitalist versus social market economy have come to an end. Instead, in a now more multipolar environment there are profoundly diverse conceptions of the good life and the ideal society. They nevertheless cannot do without each other in their resource dependency and financial and technological intertwinement, and thus continue to operate in a field of tension between

11 Sergey Bodrunov, *Noonomy* (Apple Academic Press, 2025).

12 Niko Stehr, *Knowledge Societies* (SAGE, 1994).

DOI 10.30966/2018.RIGA.17.4

alternative visions of state and private capitalism reprojected into the so-called UN Post-2030 Agenda,[13] prolonging a dialectics which, contrary to the hopes of the 1990s for overcoming this dichotomy, continues to dominate international development, for example at the intersection between the competing interests of the US and China.

- *Pervasive competition*—a situation where high disruption and low cooperation dominate and where structural shocks occur amid continued strategic rivalry. Unlike in the first two decades of the twenty-first century, such rivalry is barely hidden from public visibility any more behind traditional goodwill declarations and diplomacy, and thus becomes a broadly perceived 'natural condition' which, in turn, impacts its conditions and produces a self-fulfilling hermeneutical circle of expectations, events, and reactions, which leads to new projections, and so on.

- *Post-hegemonic era*—the twilight of Western supremacy both ideology- and power-wise, and both implicitly (in lifestyles and future projections) and explicitly (in developmental concepts and power behaviour).

- *Open multilateralism*—the weakening of *normative* orders, as conceived as the lead blueprint of long-term stability and development by the second half of the twentieth century, and their replacement by post-normative ad hoc and on-sight 'fluidities'.

- *Post-agreement era*—the return of *factual* orders, combined with power projection policies, as enacted until the middle of the twentieth century.

13 Jeffrey Sachs, 'SDGs and Beyond: Rethinking Multilateralism for the Post-2030 Era', *UN SDGLearncast,* n.d., https://www.unsdglearn.org/podcast/sdgs-and-beyond-rethinking-multilateralism-for-the-post-2030-era.

DOI 10.30966/2018.RIGA.17.4

- *Changed understandings of interaction*—the normalisation of the primacy of day-to-day and event-related dialectics instead of lasting global ethical rules.

- *Changed understanding of conflict*—thinking, acting, and anticipating not primarily according to ideas of peace orientation and the dignity of the human being, but in terms of the general, silent reacceptance of human nature as a permanent conflict on a scale of escalation levels ranging from minimal to extreme. Conflicts are once again taken as naturally given and considered the 'normal' state of affairs by a majority of actors, rather than peace, which has to be created by conscious effort.

- *Divided understandings of timelines*—democracies tend towards 'presentism'; autocracies, towards 'long-termism'. This has created a fundamental paradox in international affairs, since democracies tend to conceive themselves as universal and autocracies as time-limited. This has led to the contradictory situation of democracies as universalist yet presentist and autocracies as time-limited yet long-termist. Both presentism and long-termism have proven to be ambiguous approaches, since they both present advantages and disadvantages: presentism is more flexible, while long-termism follows a plan against all odds; presentism cannot address complex challenges and develop relations appropriately over time as needed, while long-termism is more vulnerable to sudden black swans. In addition, democracies are more stable since their leaders are replaceable at any given moment, while autocracies depend disproportionately on single persons whose life time is limited and therefore must be extended at any price, as the overheard conversation about a desire for a 'transhuman' lifespan between Xi Jinping, Vladimir Putin, and Kim Jong-un showed in Beijing

DOI 10.30966/2018.RIGA.17.4

in September 2025, on the occasion of China's celebrations to mark eighty years since the end of World War II.[14]

- The *narrowing of the historical frame of reference*—the focus of recent years has shifted from the 'wide' prospective of the twenty-five years of 'happy globalisation', which were seen at the time as an incubator and pioneering state for the whole of the twenty-first century, to the 'narrow' or restricted contemporaneity of re-globalisation, which after the all too many teachings of terror and disruptions now conceives itself much more modestly as a temporary state of transition, locked between the desired progression to more cooperative mechanisms of the twenty-first century and the factual regression into those of the second half of the nineteenth century.

- *Progressive nationalism*—a global trend towards differentiating nationalism to make it more acceptable by broader parts of the population, including particularly the middle class and the political centre, by combining regressive and progressive patterns in a national framework with strong nation-consolidating traits but including some leftist-internationalist elements. As has been asserted, in the 2020s many nations across political systems 'have increasingly embraced what could be termed *progressive nationalism*. This political project rhetorically combines progressive ideals, such as inclusion, identity politics, and wellbeing, with the exaltation of a national identity. Perhaps shadowed by the global emergence of national and authoritarian populisms, this phenomenon has gone largely unnoticed … [it can be] identified [by] a rhetorical commitment to

14 Emily Atkinson, 'Hot Mic Catches Xi and Putin Discussing Organ Transplants and Immortality', *BBC World*, 3 September 2025, https://www.bbc.com/news/articles/cr70rvrd41ko.

DOI 10.30966/2018.RIGA.17.4

decolonisation and youth wellbeing, spuriously dissociated from the processes of globalisation and capitalism.'[15]

- *Re-globalisation*—an umbrella term for the transition phase of the 'global systemic shift'[16] since 2015 addressing primarily, but not only, reshoring and renationalisation, reordering forms of power distribution, new hybrid ways of internal and external legitimacy acquisition, and shifting forms of relationality, networking, and attraction, all without commonly grounding rules or specific agreements as to how these respective changes should occur, and where they should ultimately lead.

- *The 'cosmologisation' of globalisation*—with the rise of the space economy and the resumption of lunar and space exploration by all the major powers, the foreseeable advancement of asteroid mining and other extraterrestrial resource-securing measures, and the start of space tourism, the expansion of humanity beyond earth has begun. This also includes a probable massive increase in the number of satellites orbiting the earth, as applications for 1 million satellites had been submitted by 2025. Regardless of whether humanity will be a spacefaring species by the middle of the century or not, this will lead to the extension of globalisation mechanisms, logics, and regulations from earth into space. It also entails a more in-depth 'beyond global' political debate among the world powers, which will in any case lead to the strengthening and evolution of space diplomacy—which is why degree programmes relating geopolitics to space economics and space law are now springing up everywhere, for example at LUISS University in Rome with the master's in space law and geopolitics,[17] which

15 Marta Estellés, 'Global Citizenship Education Overlooked: Curriculum Policies and Progressive Nationalism', *International Review of Education* (24 April 2026), https://doi.org/10.1007/s11159-025-10191-0.

16 Roland Benedikter and Katja Siepmann, 'Global Systemic Shift Redux: The State of the Art', *New Global Studies* 9 Nº 2 (2015): 167–98, https://doi.org/10.1515/ngs-2015-0014.

17 LUISS University Guido Carli, Rome, *'Space Law and Geopolitics'*, 2026, https://lsl.luiss.it/en/offerta-formativa/space-law-and-geopolitics.

started in 2026, or at the Space Institute of the University of Michigan.[18] In the long term, space expansion promises huge gains for traditional power politics which go far beyond anything possible on earth—for example, the conquest of entire planets at least theoretically.[19] As a recent report from Cornell University suggested:

> Life is possible on 45 planets. Over 6,000 planets have been discovered so far in other solar systems; life could have developed on 45 of them. This is the conclusion reached by a study from Cornell University. These planets are situated exactly at the right distance from their star, so that it is likely to be neither too cold nor too warm there. In addition, the planets must possess water, carbon and a solid core for the formation of carbon chains to support the potential development of life. If a planet is too close to a star, it evaporates; if it is too far away, it freezes, astrophysicist Lisa Kaltenegger says.[20]

The report did not suggest the potential of directly reaching any of these planets within a foreseeable timeframe, but pointed towards the logical future of space travel where new forms of interrelation with planet earth might come into sight.[21] In sum, for reasons of resource securitisation, population gains, and power expansion, the 'search for other earths' and the strategic 'narrowing down of targets' is becoming a priority for many powers on earth, as much as their efforts to impact the evolving space law in order to avoid new conflicts potentially related to its development.[22] Besides the fact that international law

18 University of Michigan, Space Institute, *'Space Law & Policy'*, 2026, https://space.umich.edu/education/spacelaw.

19 Anthony P. D'Costa (ed.), *The Oxford Handbook of the New Space Economy* (Oxford University Press, 2026), https://global.oup.com/academic/product/the-oxford-handbook-of-the-new-space-economy-9780198881049.

20 ORF [Austrian National Broadcasting Agency], *'Auf diesen 45 Planeten könnte es Leben geben' [Life could be possible on these 45 planets]*, 25 April 2026, https://science.orf.at/stories/3234783.

21 Abigail Bohl, Lucas Lawrence, Gillis Lowry, and Lisa Kaltenegger, 'Probing the Limits of Habitability: A Catalogue of Rocky Exoplanets in the Habitable Zone', *Monthly Notices of the Royal Astronomical Society* 547 Nº 3 (April 2026), stag028, https://doi.org/10.1093/mnras/stag028.

22 Kathy Hovis, 'Where to Find Other Earths? New List Narrows Down the Targets', *Cornell Chronicle,* 19 March 2026, https://news.cornell.edu/stories/2026/03/where-find-other-earths-new-list-narrows-down-targets.

DOI 10.30966/2018.RIGA.17.4

> is starting to be partially transferred into space law already as we speak, the history and main points of the exact ways a 'cosmologisation' of globalisation will unfold until the middle of the century are still to be determined.

These—at first glance very diverse and inhomogeneous—dynamics describe *one and the same process* from different angles and in sometimes contrasting or even opposed perspectives and interpretations. Yet they essentially boil down to the same conclusion: globalisation in the mid 2020s is not simply reversing itself or regressing, as some have falsely claimed, but it is changing its face. It is not ending, but transforming into new, more complex patterns. Multidimensionality and systemic ambiguity are in the process of replacing mono-dimensional leadership, simple causal explanations, and analytic reducibility. Therefore, with a view to the overall state of affairs, we should rather choose the umbrella term *re-globalisation* instead of *deglobalisation* or *slowbalisation* to characterise what is ongoing.[23] On balance, the approximative umbrella term of re-globalisation, although far from being perfect in itself,[24] may be closer to the character of the times and hold true until the middle of the 2030s, probably leaving its traces beyond this time period.[25]

23 Roland Benedikter, 'What Is Re-Globalization?', *New Global Studies* 15 Nº 1 (March 2021): 73–84.

24 Ephrat Livni, '"Reglobalization" to the Rescue?', *New York Times*, 5 April 2024, https://www.nytimes.com/interactive/2024/04/05/business/shoptalk-reglobalization.html.

25 Roland Benedikter, 'Re-Globalization: Aspects of a Heuristic Umbrella Term Trying to Encompass Contemporary Change. An Introductory Overview', in Roland Benedikter, Ingrid Kofler, Mirjam Gruber (eds), *Re-Globalization: New Frontiers of Political, Economic and Social Globalization*, Rethinking Globalizations 95 (Routledge/Wiley, 2022), pp. 7–32.

DOI 10.30966/2018.RIGA.17.4

Effects on the Security Field: Increasing Complexity Produces the Request for Better and More Precise Inter- and Transdisciplinarity

Caught amid these dynamics, the security field is without doubt dramatically transforming not only militarily, as seen in the recent conflicts in Ukraine and the Middle East, but also structurally. Due to the combination of uncertainty, acceleration, and systemic liminality which characterises the re-globalisation era, security is reducible neither to safety nor to stability any more. For the sake of saving some sort of disrupted continuity, it is rather being increasingly tied to inter- and transdisciplinary anticipation. With anticipation we do not mean prediction—which is impossible, since the future by definition does not exist—nor planning for potential scenarios ahead, since in face of growing complexity there would be too many to prepare for specifically. Rather we mean working with the future in the present by taking into account multiple potentials and a wide range of unpredictables, and preparing for a variety of possible events and developments which are increasingly interconnected in fluid or hybrid ways among each other, in order to be ready when one of the options or clusters materialises. Anticipation is in its core about having trained the preparedness muscles in case something totally different or surprising occurs. With regard to the security field, in the midst of current geopolitical and technological shifts we observe ramifications which elevate anticipation to a must, such as:

- *The systemic hybridisation of the security environment.* This includes, in particular, the hybridisation between state and private actors. For example, non- or semi-official actors, such as space entrepreneur Elon Musk, supply satellite internet to warring Ukraine without clear affiliation to NATO or the US or other state security providers. Private techno-investors such as Peter Thiel are providing security information to public entities in grand style (e.g. Palantir). And techno-oligarchs such as Sam Altman, who seem to be privately obsessed with Napoleon, are allegedly dreaming of a world where security is administered

DOI 10.30966/2018.RIGA.17.4

by a sort of chatbot-integration of information. Yet is the 'Napoleon' imagery compatible with Trump's USA, a new European alliance, or NATO? The more complex the cluster of securitisation gets, the more it induces unpredictability and must be addressed as an emerging aspect of hyper-interactivity.

- *The pluralisation of security-relevant dual-use technologies*. While everybody is talking mainly about AI, more specifically the chatbot sub-transformation will change the everyday use of information towards an 'integration pluralism', and bio- and quantum-computing might converge with advanced robotics—an overall process of intertwinement and fusion leading to manyfold and oscillating options of adaptation and use which may unfold profound consequences for trust in information reliability and security, and thus impact the fundamentals of open societies.[26]

- *The re-scientification of security*. Simultaneously, the AI revolution remains undoubtedly one of the dominant *convergence* processes across literally each and every relevant technological and societal field over many years to come. Fields Medal-winning mathematician Terence Tao has said artificial intelligence 'is not just another technology': '"It really is forcing us to rethink fundamental questions—what is a mathematical proof? What is a paper? What is the purpose of our profession?" With mathematics generally immune to AI's biggest failing—unverifiable mistakes—the field is well-positioned to act as a proving ground for the technology, Tao says.'[27] Yet whether, as a consequence, mathematics will rise to *the* centre point of the security question as a whole is not so certain.

26 Cf. Roland Benedikter, *Die Chatbot-Transformation: Veränderung von Demokratie und Internationalen Beziehungen*, Globale Gesellschaft und Internationale Beziehungen (Wiesbaden: Springer, 2026.

27 Davide Castelvecchi, '"The Job Description Is Changing": Mathematician Terence Tao on the Rise of AI', Nature, 27 April 2026, https://www.nature.com/articles/d41586-026-01246-9?. See also: Flora Graham, 'AI forces us to rethink maths, says Fields medallist.' *Nature*, 28 April 2026, https://www.nature.com/articles/d41586-026-01403-0.

DOI 10.30966/2018.RIGA.17.4

- *Civil-data developments influencing the security field*. This is another field of the contemporary hybridisation of security matters. Most of them come from the creative interface of technology–democracy–civil society and science. For example,

> Scientists have unveiled *GlobalBuildingAtlas*, a map of almost every building in the world. The team combined satellite imagery and machine learning to render 2.75 billion buildings in 3D at a spatial resolution of 3 metres by 3 metres. The map opens new possibilities for disaster risk assessment, climate modelling and urban planning, says study co-author Xiaoxiang Zhu, an Earth observation data scientist. The dataset can also be regularly updated to help researchers track how urban areas develop over time.[28]

What is not said is that this research is, like a rapidly increasing amount elsewhere, obviously dual-use and can serve military or intelligence matters as well, especially since it is situated at the interface between classical security institutions and civil organisations. Another example for a similar development is the AI prediction of extreme weather events:

> A new artificial-intelligence-enhanced weather forecasting approach is helping meteorologists to predict extreme weather events such as very heavy rains. AI tools have previously struggled to forecast extreme events that they have few data on. To make a more effective model, researchers combined an AI model with a physics-based climate model, and added mathematical tools that analyse the statistics of rare events into the mix. In early tests, this hybrid approach simulated the probabilities of extreme heatwaves as accurately as the older, non-AI method, but much more quickly.[29]

Innovative instruments of real-time cartography may also serve as strategic opportunities—and therefore become parts of the securitisation field, contributing to its latent universalisation.

28 Mohana Basu, 'Giant 3D Map Shows Almost Every Building in the World', *Nature,* 11 December 2025, https://www.nature.com/articles/d41586-025-04036-x.

29 Alexandra Witze, 'This AI Model "Studied" Physics—and Learnt to Forecast Extreme Weather', *Nature,* 11 December 2025, https://www.nature.com/articles/d41586-025-04055-8.

DOI 10.30966/2018.RIGA.17.4

- *The rise of neural data to critical core resource within the ongoing decade*. Ever more inter- and transdisciplinary research indicates there is a connection between information and consciousness.[30] As innovation in most cases lies in the spark between fields, this connection will become a crucial focal point of security & innovation research. Especially the rise of neurotechnology will make sure that it is not only AI, but perhaps even more so neural data which will become the new key resource of the twenty-first century, leading to a neuro-world dominated by a transnational neuro-culture by the middle of the century at the latest. As a consequence, biopolitics will gain both in theoretical and practical importance.

- *The rise of the concept of cognitive security*. Cognitive security[31] is a lead term that is rapidly gaining traction across basic research in the natural and social sciences, and specifically at their interface which is destined to become one frontier of the future of security, together with automatisation, AI, and 'light, small, cheap', where intelligent beats heavy, big, costly, and stupid. It was part of the historical symptomatology when NATO chief scientist Steen Søndergaard released two groundbreaking strategic reports on cognitive warfare[32] and resilience[33] in December 2025. The fact that whole new branches of inter- and transdisciplinary sciences have been announced on related alternative routes, such as 'Cognitive Field Dynamic (CFD)

30 Bobby Azarian, 'The Hidden Connection between Information and Consciousness: The Missing Link between Physics and Experience May Be Simpler Than We Thought', *Psychology Today,* 17 December 2025, https://www-psychologytoday-com.cdn.ampproject.org/c/s/www.psychologytoday.com/us/blog/mind-in-the-machine/202512/the-hidden-connection-between-information-and-consciousness/amp.

31 James Crum, Aaron R. Allred, Sarah R. Bostrom, Emily Doherty, Melissa McLain, Erin Richardson, Cara Spencer, Richard E. Niemeyer, Allison P. A. Hayman, Chad Tossell, Marta Čeko, and Leanne Hirshfield, 'Understanding the Neurocognitive Mechanisms of Cognitive Security', *Neuroscience & Biobehavioral Reviews* 179 (2025), 106448, https://doi.org/10.1016/j.neubiorev.2025.106448.

32 Janet M. Blatny and Steen Søndergaard, *Cognitive Warfare* (NATO Science and Technology Organization, 2025).

33 Janet M. Blatny, Lucas Cox, Alvaro Martin-Blanco, and Steen Søndergaard, *Resilience* (NATO Science and Technology Organization, 2025).

DOI 10.30966/2018.RIGA.17.4

Sciences'[34] in December 2025, points to a field of inquiry with high relevance and transversal impact potential which so far finds only a strongly time-delayed place in traditional knowledge institutions. Many of the truly innovative approaches come from outside traditional academia, which underscores a fundamental challenge: the outsourcing of innovative and avant-garde integrated futures research, which by necessity presents a high component of inter- and transdisciplinarity, to private and 'alternative' venues. This is another argument playing into the widespread sense of impending doom surrounding the traditional university which in times of ChatGPT, Grok, Gemini, and Mistral could step by step become an outdated model of knowledge-and-know-how production and diffusion.[35] This points to the necessity of new institutional arrangements for requirements that concern matters of futures which, as the boundaries-crossing development of new technologies suggests, are security-wise becoming matters of life and death.

- *The interrelation between cognitive security, CFD sciences, cognitive warfare, narrative superiority, and defensive stability.* Together with the still rather new categories of cognitive security and cognitive warfare, there is also the new topos of *narrative warfare*. Perhaps the most important aspect of these advanced security categories is not their extension per se, but their rapidly growing and increasingly effective interrelation, which creates new conditions for action. In a thoughtful publication of December 2025 for the Cyfluence Research Center, Athena Tong showed that China, for example, applies its own 'masterclass' of cognitive warfare through its 'Doctrine

34 Don Gaconnet, 'Announcement: Cognitive Field Dynamic Sciences', *LinkedIn,* December 2025, https://www.linkedin.com/posts/dongaconnet_announcement-cognitive-field-dynamics-sciences-activity-7408969953288126464-bPkh/.

35 Michael Sommer, 'Die erschöpfte Universität' [The exhausted university], Hanse Wissenschaftskolleg HWK Dellenhorst/Bremen, *YouTube*, 15 December 2025, https://www.youtube.com/watch?v=2DI0SUKdaA4.

DOI 10.30966/2018.RIGA.17.4

for Strategic Narrative Superiority'.[36] This approach is in principle wise because cognition and narration are always closely interdependent.

- *The competition between humanism and transhumanism in basically all mentioned categories, approaches, and strategies*. This rather new, yet already fundamental, dialectics occurs both within the advanced economies and along the lines of the democracies versus non-democracies divide. Democracies tend to humanism, and non-democracies to transhumanism, particularly in the military field. In both democracies and non-democracies, the merger between human and machine moves from interaction to convergence, and thus may produce new security-relevant 'transhuman' instruments and devices at increasing pace. The question is how this may affect the so far clearly humanistic attempts of regulating security matters and conflict, for example with agreements on non-proliferation and the banning of certain weapons.

- *The progressive integration of the life sciences into security matters*. This trend goes beyond the mere merger of humans and machines. It includes the living in the broadest sense in processes of technological transformation. The merger between the living and technology progresses fast and, for example, transforms animals in controlled weapons, such as pigeons, which has given rise to a 'classic' new life.[37] Although this trajectory has a long history, it seems to have been evolving to new levels lately.[38]

36 Athena Tong, 'Cognitive Warfare Masterclass: China's Doctrine for Strategic Narrative Superiority', *Cyfluence Research Center (CRC),* 29 December 2025, https://www.cyfluence-research.org/post/cognitive-warfare-masterclass-china-s-doctrine-for-strategic-narrative-superiority.

37 Ike Swetlitz, 'Why a Russian Startup Is Putting Brain Chips in Pigeons: "Bio-Drones" Have Advantages over Robots, Company Says', *Bloomberg News,* 18 December 2015, https://www.bloomberg.com/news/newsletters/2025-12-18/remote-controlled-pigeons-what-we-know-about-neiry-and-its-russian-backers.

38 Jonah Fisher and Oksana Kundirenko, 'Runaway "Spy Whale" Fled Russian Military Training, Says Marine Scientist', *BBC,* 13 November 2024, https://www.bbc.com/news/articles/c1ml3n1x4zro.

DOI 10.30966/2018.RIGA.17.4

- *The increasing employment of 'Agentic AI', including large language models (LLMs), in autonomously spotting, identifying, and evaluating sensitive security matters*. Agentic AI can be considered as a meta-level of generative AI, as it employs LLMs but integrates them in ever more autonomous intelligence systems which operate at even more complex and higher levels, and thereby continuously evolve:

> Agentic AI systems are composed of one or more agents that fundamentally rely on an AI model, such as an LLM, to interpret and reason about the state of the world, make decisions and take actions. […] LLM-based agentic AI systems contain the LLM itself, alongside external tools, external data sources, memory and planning workflows. These components enable the system to perceive its environment and, where applicable, take action to achieve its goals. Compared with traditional LLM systems, agentic AI systems distinguish themselves by accomplishing underspecified objectives, acting autonomously, following goal-directed behaviours and creating long-term plans. Agentic AI systems are intended to operate without continuous human intervention. While a human typically designs and configures the system, some agentic AI systems are also capable of autonomously creating, or 'spawning', sub-agents to accomplish specific sub-tasks. System design includes defining goals, providing conditions on which to act (called 'triggers') and making information available to the AI service.[39]

  As such models seem to present both new chances and risks to an equal extent, at least from the viewpoint of potential manipulation and human decision-making, Western security institutions recommend the 'careful adoption of Agentic AI services' into security matters.[40]

- *The growing divide—and competition—between collective human intelligence and interconnected technological 'net intelligence'*.

39 Australian Government and Australian Signals Directorate, 'Careful Adoption of Generic AI Services', 1 May 2026, https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/careful-adoption-of-agentic-ai-services.

40 Ibid.

DOI 10.30966/2018.RIGA.17.4

This trend is connected to the term of 'ethical intelligence', as a term of both legitimation and action: where will the values of 'information integration' be coming from in the 2030s? Value aspects will become a decisive parameter for how to 'future' the security field. This makes groundbreaking efforts such as UNESCO's 'Recommendation on the Ethics of Artificial Intelligence' (2021) and its newer 'Recommendation on the Ethics of Neurotechnology' (2025) crucially relevant for the general direction of the human–transhuman divide regarding intelligence.

- *The integration of normative and explorative approaches under the umbrella of anticipatory preparedness*. Explorative human collective intelligence assessment units (and their specialised subunits) will play an ever greater role vis-à-vis advanced AI and chatbot 'integration' and dissemination of knowledge.

- *The growth of 'predictive policies'*. As the rapid change of warfare in the Russia-Ukraine war from humans to machines and from planned (unflexible) to prepared (flexible) has shown, anticipation will be crucial, and all actors will have their own professional futures literacy units on different levels. It remains to be seen how new tools such as 'predictive securitisation' will make their entry into the theory and practice of the security sphere in the bigger geopolitical dimension. The futurisation of risk, threats, and opportunities in a techno-world will dominate the sector earlier than expected.

- In contrast (and at least in Western democracies partly inbuilt in all former aspects), a '*grand political narrative of ecology*' exists,[41] but is no longer as strongly in vogue as in the 2000s and 2010s. In many contexts it is being partly replaced by a

41 Jean-Louis Missika, 'The Life and Death of Grand Political Narratives', *LSE European Politics*, 12 June 2024, https://blogs.lse.ac.uk/europpblog/2024/06/12/the-life-and-death-of-grand-political-narratives.

DOI 10.30966/2018.RIGA.17.4

more conservatively interpreted general concept of resilience, and the security context is no exception.

- In the light of all these dimensions, overall there is an increasing importance of *cultural diplomacy vis-à-vis traditional security diplomacy*. Given the diffusion of military logics into the broader social sphere of societies, the degree of cultural acceptance of these logics will become an important indicator for the further path of securitisation in open societies.

What is certain is that the transversality of security mechanisms that becomes practical and concrete with these elements will—and must—lead to a more interdisciplinary net of measures. The new forms of threats require better cooperation of military with non-military, particularly social science and educational institutions. This is because the 'new' pluri-disciplinary security front will have a strong foothold in the mental and educational preparedness which will have to be rooted in a world of 'post-formality' and tailored, contextualised, and rationalised respectively.

There will, of course, be even more aspects to consider, among them the 'crisis of authenticity of leaders',[42] and the publicly perceived absence of capable statesmen and stateswomen in times of transition,[43] as well as the typological division between negative (risk-oriented) and positive (opportunities-oriented) professional 'futuring' and social prevision. Also, the rise of the 'meaning of life' question to core place in the self-understanding of security and safety among millennials and subsequent generations used to crisis-ridden, hyper-technological, and hyper-complex worlds from their birth on will gain in importance, which makes it necessary to better integrate security considerations into the broader societal context.

42 Steven Umbrello, 'The Crisis of Authenticity: Lonergan, Peterson, and the Collapse of the Modern Self', *Mediated by Meaning,* 11 December 2025, https://mediatedbymeaning.substack.com/p/the-crisis-of-authenticity.

43 Ibid.

DOI 10.30966/2018.RIGA.17.4

Important in the outlook on all these mosaic stones of innovative security trends are two points. First, not to make a natural law of them, but to treat the situation as what it is: a human-made, ongoing, and open process which presents the need to connect the many dots situationally. Second, a sound balance is needed between defensive and offensive approaches and judgements. These can be provided by futures capacities, that is, futures literacy and foresight units which can develop futures thinking to a practical collective capability to become a useful strategic asset with regard to inclusivity and participation.[44]

Global Orders in Transition

Scholars have proposed various models to describe the resulting transformation of international orders which these mechanisms of reorganisation and reorientation have set in motion. Three of the current typologically constituted models are:

- *Two globalisations* (Benedikter and Steger). This refers to the change in the concept and practice of 'one globalisation for all' which dominated from the start of the 1990s until around 2014–16, with 2015 as a kind of watershed year[45] that marked a turning point in world politics, economics, and society. This three-year phase induced the transition from post-Cold War optimism towards an era defined by populist nationalism, new geostrategic competition, and intensifying social polarisation. The following pre-2020s period, then, marked a stalling of the previous decades' progress in reducing inequality and a 'backlash against globalisation'. Symptomatic historical signal events were the European migration crisis; Brexit; Trump I; China becoming the largest global economy at the end of

44 Roland Benedikter, 'Futures Thinking Becomes a Priority for All Globalized Societies', *Discover Global Society* 3, article no. 7 (9 February 2025), https://doi.org/10.1007/s44282-024-00128-7.

45 Espen Barth Eide, 'Geo-Economics and Politics—2015: The Year Geopolitics Bites Back?', *World Economic Forum*, 7 November 2014, https://www.weforum.org/stories/2014/11/2015-year-geostrategic-competition.

DOI 10.30966/2018.RIGA.17.4

2014; China experiencing a stock-market crash in 2015 and starting to expand in the South China Sea; Russia intervening in Syria; high-profile terror attacks, against *Charlie Hebdo* and the Bataclan in Paris, as well as in San Bernardino, signalling a rise in Islamic terrorism in the West; the signing of the Paris Agreement under the United Nations Framework Convention on Climate Change; the launch of the Sustainable Development Goals; the signing of the Trans-Pacific Partnership; the start of broad social media influence; the Iran Nuclear Deal.[46] Since then, a new macro-competition between different political systems and their underlying value systems has gradually developed, focusing on vertical versus horizontal models of social organisation, that is, autocracies versus democracies. It has led to a split in both the previously accepted concept of globalisation and its contextual ways of realisation. The effect is today a situation of 'two globalisations for two competing blocs', that is, a globalisation of non-democracies versus a globalisation of democracies, which both drive forward their competing global orders and opposed development visions, at the same time remaining interrelated on multiple levels by intertwined financial, economic, and security interests.[47]

- *Three globalisations* (G. John Ikenberry). This concerns the geographical distribution of developmental logics on the planet. According to Ikenberry, these can be classified geo-typologically: as the logics of the West, the East, and the South. They have developed increasingly different patterns, perspectives, and approaches, and are struggling to find a new common order in the 2020s.[48]

46 James M. Lindsay, '10 Events That Changed the World in 2015', *The National Interest*, 16 December 2015, https://nationalinterest.org/blog/buzz/10-events-changed-the-world-2015-14640.

47 Benedikter, 'New Global Direction'. Cf. Manfred Steger, 'De-Globalization or Re-Globalization? Unmasking the Populist Paradox', in Benedikter et al., *Re-Globalization*, pp. 33–42.

48 G. John Ikenberry, 'Three Worlds: The West, East and South and the Competition to Shape Global Order', *International Affairs* 100 Nº 1 (January 2024): 121–38, https://doi.org/10.1093/ia/iiad284.

DOI 10.30966/2018.RIGA.17.4

- *Four globalisations* (Benedikter and Cruz). This concerns the structure of geopolitical power *interdependencies*. This structure is expanding through the rise of non-aligned regional powers, which are gaining in importance due to the splits in the global order.[49] As a consequence, the Global South must be added to the previously dominant logics of the West, the East, and the North. The Global South does not feel connected to nor wants to be easily assigned to any of the other three main geo-directions, but pursues, by the majority of its members, an approach of Active Non-Alignment (ANA). This approach attempts to maintain flexibility and expand reactivity in relation to the other three blocs in order to derive maximum self-interest from ad hoc coalitions.[50] The ANA approach, which particularly extends in parts of Africa and South America, is highly differentiated among its supporters and further increases the overall degree of international complexity.[51]

These three models, which differ in terms of framing and methodology, reflect the diversity of forces currently shaping the international scenery. Together they illustrate the fluidity and structural controversies inherent in today's international system. In their inherent logics they have led to a diplomatic and political mood of general reversibility, provisionality, and open uncertainty of affairs. Indirectly, though, they also indicate potential points of convergence in the great transformation which can and should be cultivated.

49 Council of the European Union ART Team, *EU Forward Look 2026: Playing By New Rules?*, January 2026, https://www.consilium.europa.eu/media/i1ojzcng/2025_2122_art-forward-look_final_jan26_web.pdf.

50 Roland Benedikter and Carlos Cruz-Infante, 'AI in Latin America: Attempts of Regulating Artificial Intelligence within the Geopolitical Paradigm of Active Non-Alignment (ANA): A Critical Review', *Journal of Transatlantic Studies* 24, article no. 11 (February 2026): 1–27, https://doi.org/10.1057/s42738-026-00156-y.

51 Roland Benedikter, 'The Ethics of AI in Latin America: Approaches to the Use and Regulation of Artificial Intelligence in the Contemporary ANA Region', *Studi Politici: Journal of Political Science* Nº 1 (2025): 105–25.

DOI 10.30966/2018.RIGA.17.4

New 'Grand Narratives'

Against the backdrop of these divergent *and* overlapping understandings of order transitions and in the absence of a strong joint perspective, major powers and regional actors alike are developing their own new 'grand narratives', also known as 'lead narratives', to create their own points of (temporary?) convergence. In doing so, they are pursuing a fourfold goal: (1) to bring some sort of stability to the 'fluid' situation of vacillating but still struggling order patterns; (2) to assert an idealised identity *internally* towards their populations, elites, and intellectuals for the sake of unification; (3) to claim their ambitions *externally* in the global reorientation of peers; and (4) to integrate their ambitions by interrelating the internal and external spheres and position them in the concert of powers. The most important 'grand narratives' of the mid 2020s are, in no particular order:

- China: *The New Chinese Dream of Great National Rejuvenation*
- USA: *Make America Great Again (MAGA)*
- Russia: *Eurasia*
- India: *Make India Great Again (MIGA)*
- Latin America: *Active Non-Alignment (ANA)*
- Africa: *Active Non-Alignment (ANA), United African Democracy (UAD), New Pan-Africanism*
- Asia-Pacific: *No China Hegemony*
- United Arab Emirates: *New Arab Dream (NAD)*
- Saudi Arabia/Qatar: *Sovereign Arabic Islam/Religious Hypermodernity*
- United Kingdom: *Global Britain*.

This list could go on, as it constantly expanding and ramifying. What these narratives have in common is that they function as 'strong' assertions in a hermeneutic circle in which reality and aspiration do not always coincide, and thus must be connected with each other by a sort of 'heroic' story to create this connection as a self-fulfilling prophecy. In terms of their intended effect, the narratives put forward a story that

DOI 10.30966/2018.RIGA.17.4

is supposed to fulfil a (partly forcedly) inclusive and, at the same time, regulatory function. The evoked image of an ideal identity does not always correspond to the wishes of the population on the ground, and instead in many cases it has a—directly or indirectly—disciplining or even 'unitarian' character. As representatives of the Dubai government stated at the Dubai Future Forum 2025, some 'grand narratives' are intended to contribute to what they called the 'National Cognition Potential' by seeking to make it measurable, and thus also to some extent make the 'lead narrative' (in this case, of the 'New Arab Dream') manageable and controllable. Dubai is even proposing the introduction of this parameter of 'National Cognition Potential' for the whole world from 2026 onwards, arguing that it could introduce a more realistic comparative measurement of future potentials among nations beyond gross national product or educational diversity.

Differing Ideas of Rightfulness and Justice

Another lowest common denominator of the new grand narratives is the desire for a 'return to one's rightful place', that is, what they postulate as a return to a sense of justice. However, this demand for justice is always directed primarily at their own interests and their own understandings of the term 'justice'. The myth of the 'return to one's rightful place' is often formulated as a restorative demand, which gives the grand narratives backwards-directed legitimacy and clout, that is, as it may appear to the public, a 'clear direction' allegedly able to integrate past and future through narration. In so doing, the grand narratives unfold both an attractive function externally (soft power) and an integrative function internally (mythology of a common future to close ranks and reduce internal diversity). Overall the grand narratives of the mid 2020s are mostly artificially constructed and usually have little to do with the everyday lives of the population—even though they claim to be an expression of those lives. Therefore, they are propagated and disseminated in 'strong' and often populist ways in democracies, and in often suppressive and violent ways in autocracies.

DOI 10.30966/2018.RIGA.17.4

The Return of Culture (in the Broad Sense) as a Core Political Force

Finally what the new grand narratives have in common is that they, in principle, tend to valorise cultural aspects, although in ambiguous ways, especially those of a propagated national or civilisational 'identity culture' or 'legitimately dominant culture'. The narratives thus tend to oppose the idea and reality of a common 'cultural world order' that has been emerging in the 2000s as a kind of common consciousness of humanity and as one progressive result of globalisation. Such a joint human culture spanning the planet was indeed propagated, for example, by the UNESCO-MONDIACULT Conference, the largest cultural conference on earth, held in Barcelona in September–October 2025. The conference, held every three years in a different geopolitical space, called for universal cultural rights and the introduction of an 18th Sustainable Development Goal on culture by 2030. In the coming years, according to the United Nations and UNESCO, world culture should even be elevated to a transversal 'alternative' diplomatic actor. If this were to succeed only partially, it could influence the new grand national narratives, reorientating them perhaps towards a more interactive coexistence.

Looking at the overall picture, the question should not be underestimated in the long term as to what impact these grand narratives will ultimately have on the history of ideas, that is, the intellectual and political history of their countries and the debate about the history of ideas on the international stage. This question can, as of now, only be answered in a preliminary manner according to specific countries. What is certain is that grand narratives will entail a wide spectrum of contextual effects and that these effects will, over time, intertwine and thus influence the course of the whole of international affairs. The juxtaposition of grand national narratives in all parts of the post-Covid-19 world versus a jointly propagated world culture illustrates the diversity of forces that are currently vying for dominance in the immaterial-intellectual and proto- and para-ideological spheres—with claims that often extend

DOI 10.30966/2018.RIGA.17.4

beyond their own spheres of influence, and perhaps with effects that may transcend their known intentions.

The Impact of Re-Globalisation on Existent Global Platforms

The changing global scenery resulting from these developments is having a significant impact on international institutions, relationships, and political and diplomatic mechanisms. *Four* key concepts thought to be outdated by European progressives have been experiencing a meteoric resurgence since the 2020s, and particularly since the end of the global Covid-19 pandemic in May 2023:

1. sovereignty
2. legitimacy
3. autonomy
4. self-sufficiency.

The last of these is a particularly complex term that lies somewhere between self-reliance, independence, and autarky, and which—precisely because of the overlappings between these three meanings—has become characteristic of the re-globalisation era.

These four concepts effectively shape *two* contrasting models of relationship that will influence the macro-development in the coming years in dialectical, yet paradoxically interconnected ways:

- *Independence in community*. This is the grand guiding vision of the North and the West. The focus remains on the whole, but with a stronger self-reference. Networks of interconnections remain decisive, particularly in the resource (rare earths) and chip sectors. Example: the European Union. It is primarily seeking to consolidate itself economically (internal market),

DOI 10.30966/2018.RIGA.17.4

politically (suspending enlargement), and militarily (establishing an EU army), but at the same time wants to continue to advocate globally interconnected 'social contracts' on ecology, liberal democracy, and a culture of agreement-making and rule of law. Nevertheless, with all this the EU is clearly suffering from a 'Gulliver syndrome'[52] (Stefan Kooths), that is, going from being the biggest in a world of dwarves to a world of giants where one is the smallest actor. As a solution strategy, the cooperation agreement of April 2026 between the European Union and the United States on securing critical minerals in a strategic long-term perspective was meant to pave the way for a contract of exchanging these 'internally' in the future.[53] This indicated a renewal of a closer interconnection within the more confined space of transatlantic cooperation, which underscores the direction of restricted cooperation between systemic affiliates (democracies) versus the 'cooperative rivalry' towards systemic antipodes like China (non-democracy). Something similar might be extended from earth into space in the 2030s, when the space economy will fully develop and employ systematic space exploration in order to secure minerals, materials, and territories, thus expanding globalisation into cosmologisation, including some basic laws of globalism that might expand to become 'cosmologisms'.[54]

- *Community in independence*. This is the grand guiding vision of the East and the South. The focus is inward but the approach to the global sphere remains to some extent aware of its dependence on a larger whole. Nevertheless, the decisive factor is the value found in the self. Example: China. When the

52 Josef Bertignoll, 'Europa leidet am Gulliver-Syndrom' [Europe suffers from Gulliver syndrome], *Südtirol online,* 10 December 2025, https://www.stol.it/artikel/wirtschaft/europa-leidet-am-gulliver-syndrom.

53 Andrea Shalal and Simon Lewis, 'US, EU Deepen Cooperation on Critical Minerals with Eye to Broader Agreement', *Reuters*, 24 April 2026, https://www.reuters.com/world/china/us-eu-deepen-cooperation-critical-minerals-with-eye-broader-agreement-2026-04-24.

54 Lowell S. Gustafson, 'Globalization and the Universe: A Short Re-Locating', *Global-e: A Journal of Global Studies* 16 Nº 9 (15 December 2025), https://globalejournal.org/global-e/december-2025/globalization-and-universe-short-re-locating.

DOI 10.30966/2018.RIGA.17.4

> Chinese government, which took the greatest profit from the nation's accession to the global liberal-capitalist system in 2001, nowadays talks about 'globalisation', it is usually talking about its own global interconnectedness, and when it talks about 'the world', it is talking mainly about its own role and position in the world, claiming it to be central geopolitically, ideologically, and economically. At the same time the nation remains aware of its dependence on the international financial and economic system, and therefore advocates the cautious continuation of a somewhat restricted and selective multilateralism.

Both these major models ultimately act in favour of their own interests, including their own value structures, identity artefacts, and traditions. This results in three patterns of interaction between the international powers expected for the upcoming years, as produced by the current global reorientation:

a. post-normative pluri-polarity instead of normative multipolarity
b. complex rather than linear interdependence
c. cooperative rivalry (Joseph Nye).[55]

This constellation does not mean that the global system established at the interface between economics, politics, and culture in the two and a half decades between 1990 and 2015 is coming to an end. Rather, it is, as said, taking on a new face. The timeframe and scope of this re-globalisation process are open. What is certain, though, is that existent global platforms such as the UN and its sub-bodies will have to deal with even more complex patterns and may potentially lose influence on the overall process for a length of time still to be determined. This does not make them superfluous, but rather all the more necessary as stabilisers and central transfer points, which are increasingly scarce in the second half of the 2020s.

55 Joseph Nye, interview, 'Cooperative Rivalry Can Move Relations Forward', *China-US Focus*, 22 March 2024, https://www.chinausfocus.com/foreign-policy/interview-with-joseph-nye-cooperative-rivalry-can-move-relations-forward.

Global Systemic Shift

The contemporary sum of multifaceted reorientation is a state of dynamic liminality—an intermediate phase characterised by the absence of clear centres and the omnipresence of seemingly undirected, poorly aligned, yet strong transformation forces. A second characteristic is a widespread psychology of governments that in face of the uncertainties of their citizens reclaim a leading role without being fully able to deliver. And a third characteristic is that the world is moving less towards multipolarity (a normative concept of distributed order) and more towards pluri-polarity (a factual concept of open transformation related to zones and realms of influence).

The return of the Monroe Doctrine as 'Donroe Doctrine' (or Donald Trump Doctrine)[56] reflects this threefold shift. It marks the return of essentially secluded geopolitical spheres of influence in which the strongest prevails, if necessary by force, thereby redividing the world in geography-based sectors of dominance centred on the great powers and undermining the shared, joint, and equal international sphere that the post-WWII idea of a liberal, rules-based global order intended to implement on a permanent basis. It remains disputed whether this return is specific to the 'Trumpism' since 2016, or if it has de facto characterised the politics of China's Xi Jinping (for example, in the South China Sea) or Russia's Vladimir Putin (for example, in the form of the so-called 'Russian belt' or, as Putin calls it, 'Russia's near abroad',[57] with its underlying strategic concept, the 'Eurasia' ideology,[58] and the proto-religious narratives underlying and accompanying the related wars in Crimea and Ukraine[59]).

56 See Nandika Chatterjee, 'The 200-Year-Old Foreign Policy Vision Underlying Trump's "Donroe Doctrine"', *Time*, 7 January 2026, https://time.com/7343795/trump-venezuela-monroe-doctrine-history.

57 'The Global Story: Putin's Pursuit of Russian Greatness', *BBC,* 14 January 2026, https://www.bbc.com/audio/play/w3ct71gd.

58 Sara Dixon Klump, 'Russian Eurasianism: An Ideology of Empire', *Wilson Center*, 7 July 2011, https://www.wilsoncenter.org/publication/russian-eurasianism-ideology-empire.

59 Roland Benedikter, 'The Role of Religion in Russia's Ukraine War. Part 1: A Map of the Situation', *Zeitschrift für Außen- und Sicherheitspolitik (ZfAS)* 16 Nº 1 (March 2023): 79–100, https://doi.org/10.1007/s12399-022-00931-7 and https://rdcu.be/c1H8l [free version]; Roland Benedikter, 'The Role of Religion in Russia's Ukraine War. Part 2: Developments and Perspectives', *Zeitschrift für Außen- und Sicherheitspolitik (ZfAS),* 16 Nº 2 (June 2023), https://doi.org/10.1007/s12399-023-00947-7 and https://rdcu.be/dbpkN [free version].

DOI 10.30966/2018.RIGA.17.4

Both China's and Russia's approaches of 'the strongest prevails' were launched in rather systematic ways before Donald Trump's rise to power. Be that as it may, the most important supporter of multilateralism based on international law and the rule of law to date remains a rather weak Europe, which is seeking to strengthen itself through remilitarisation and by forging long-overdue global partnerships,[60] for example through free trade agreements with non-Western geopolitical areas such as South America via Mercosur.[61]

In this process the ideologies of the 'happy globalisation' phase of 1990–2015 (cosmopolitanism and globalism) have rapidly evolved into more complex and contradictory self-conceptions. Cosmopolitanism is essentially retreating to the capitalist societies of the West, where it is rejected by a growing number of voters (a *contradictio in adjecto*), and globalism is now torn between liberal and illiberal globalism, for example between European and Chinese governments (*ditto*). Furthermore, in the wake of this development the crucial relationship between sustainability and resilience is changing to become ever more often dialectical, with a shift of the centre of gravity away from sustainability towards resilience. This puts a rather conservative stamp on the immaterial background of the re-globalisation process, since resilience is more about 'bouncing back' in concrete contexts, while sustainability is more about encompassing forward transformation in an encompassing grand vision. Resilience is rather self-referential and non-normative, while sustainability is rather universal and normative. Which of the two will have the upper hand in the post-2030 agenda remains open. In the ideal case, the outcome of their dialectics may be their step-by-step integration towards a *resilient sustainability* and a *sustainable resilience* of interconnected societal models and policy practices around the world.

60 Bundeskanzler Helmut Schmidt Stiftung, *Strengthening Partner Europe!, BKHS Magazine* № 5, 2025, https://www.helmut-schmidt.de/fileadmin/BKHS_Magazine_2025.pdf.

61 Carlos Cruz Infante and Roland Benedikter, 'Can the EU-Mercosur Trade Agreement Be Saved?', *LSE European Politics,* 20 November 2023, https://blogs.lse.ac.uk/europpblog/2023/11/20/can-the-eu-mercosur-trade-agreement-be-saved.

DOI 10.30966/2018.RIGA.17.4

Finally, the most fundamental relationship for every planned policy: the relation between uncertainty and unpredictability is evolving. The two are not the same thing, and this is becoming increasingly clear in international diplomacy. Uncertainty is the common condition of all, but there are deep differences regarding unpredictability. *Uncertainty*, on the one hand, is becoming the civilisational norm in the age of acceleration (Thomas Friedman) and is to be addressed by all global actors together, with the institutionalisation of professional anticipation as a new scientific discipline. On the other hand, *unpredictability* in international relations should be eliminated according to the consensus of a majority of agreement-oriented powers like the EU, while some major players such as the US, China, and Russia are, in contrast, using it even programmatically in what they conceive as the renewed 'great chess game' of global politics. To overcome unpredictability and to deal pro-positively with uncertainty based on new forms of interdisciplinary competence will bring competitive advantages to those who develop them as 'prime movers'.

Will There Be a New Solid Order Soon?

The prospects for the consolidation of a new order potentially following the current global systemic shift are debated heatedly. The questions are many and the subject of intense discussions in global forums: will the transition phase last until 2030, 2040, or 2050? And what should this phase be called, with an appropriate umbrella term able to capture its essence in historical retrospect: global systemic shift? Post-2030 agenda? The post-formal era? The era of new cultural diplomacy?

It does at least seem plausible that the contemporary global systemic shift will transform not only individual indicators but also parameters of (post-)postmodern societies—across most political levels, albeit not necessarily in interaction with one another. According to the model of contemporary change that we have developed from the applied policy

DOI 10.30966/2018.RIGA.17.4

experiences of recent years,[62] this means that all '6+4+1' core parameters of society may be changing:

a. *Their six basic typological sectors*, each with its own independent but interacting system and discourse logics:
   - economy
   - politics
   - culture
   - religion/spirituality
   - demographics
   - technology.

   Each of these sectors must be considered to be evolving dialectically in at least four dimensions, namely in the opposing pairs of left–right (ideology) and top–bottom (classes, and elites versus populists).

b. The *living nexus between the six sectors: the bio-socio-psychology*. It acts as a hermeneutic circle between the sectors, creating a breathing-in and breathing-out rhythm at their intersection. The bio-socio-psychological nexus reflects volatile power relations between the sectors, as well as collective convictions, historical (temporary) paradigms, and prejudices in dispute for epochal supremacy.

c. Lastly, the *four types of driving forces* acting in and among the sectors *and* the nexus, as Manfred B. Steger conceives them in his analysis of (re-)globalisation:
   - people (embodied factors)
   - things (material/objective factors)
   - ideas (disembodied factors)
   - institutions (institutional factors).[63]

62 Roland Benedikter, 'What Is Transformation Design? Applying Transdisciplinarity to Govern Change', *Humanities and Social Sciences Communications* 12, article no. 1869 (2025), https://doi.org/10.1057/s41599-025-05640-y.

63 Steger, *Globalization in the 21st Century*.

DOI 10.30966/2018.RIGA.17.4

Given the complexity of such multiplicity of sectors and factors in play, it is highly unlikely that a new solid global order will be forming soon.

A Warning against Falling Apart

Economically, change will most probably continue to be networked and, to some extent, shared by necessity, trying to bar the emergence of new major ruptures in supply chains, trans-systemic pandemics, or wars. Nevertheless, the creator of the term 'soft power', Harvard scholar Joseph Nye, warned from President Trump's first term until the end of his life in May 2025 against the increase in bilateral agreements instead of joint global development. Without the UN, he warned, the world would lose its only functioning joint platform of peaceful co-evolution, and thus sink again into the chaos of hundreds of ever-changing bi- and multilateral relations according to circumstances and the mood of the day, thus making the complex world of the twenty-first century factually ungovernable.[64]

In retrospect a common networked and interactive human consciousness that could guide humanity through crises by means of shared policies was idealistically pursued after the Second World War with the founding of the UN, its sub-organisations such as UNESCO, dedicated to peace and reconciliation through education, science, and culture, and other world organisations such as the WHO or the World Bank. However one might criticise them, these global bodies are still, eighty years later, the only plausibly shared platforms of humanity. That is why they are potentially useful also in times of 'deep' transition, such as the current world phase. The curtailment of the idea of a global community by systemically different and competing forces, as seen in the 'algorithm-supremacy war' between the US and China, could signal a return to the power politics of past times. A consequence could be the stagnation of the UN sustainability agenda, the UN Agenda 2030, and the UN Post-2030

64 Joseph S. Nye, 'The Soft Power of the United Nations', *Project Syndicate*, 12 November 2007, https://www.project-syndicate.org/commentary/the-soft-power-of-the-united-nations.

DOI 10.30966/2018.RIGA.17.4

Agenda,[65] which is intended to stabilise the planet in its fundamental existence and can only be implemented collectively.

This is why the weakening of the UN, in view of the still wide-open yet in any case hyper-complex post-2030 decade, is a decisively bad idea. Nevertheless, the initiatives that undermine the status of the UN are multiplying. For example, the Gaza 'Board of Peace'[66] installed by Donald Trump to end the Gaza conflict[67] has been regarded in principle as a positive initiative, but also as a direct competitor of, if not a contextual substitute for, the UN in a crucial geopolitical area with potential international fallout and worldwide implications. The inclusion of such an initiative in a larger, diplomatically better-established context would probably have made more sense. The latest popular media topos of 'Trump's new world order'[68] might be an overstatement, given that despite the US president's 'strong' reordering of things he seems to have no clear plan vis-à-vis such a new order, how to erect it to make it last, nor where to go with it in the medium to long term. Therefore, Trump's actions, despite all the 'Make America Great Again', are hardly a lasting substitute for the role and tasks of the UN and other multilateral organisations. Trump's statement during the Israel–US–Iran war in March 2026 that the US would not need NATO any more since its members had left the US alone in a war he had not discussed with them previously—and did not assist the US sufficiently, for example following Trump's call for help in securing the Strait of Hormuz—hardly changes this fact. The more Trump's solipsism grows, the more his 'reorientation' of the US and the globe could become just temporary, since, as former US secretary of labor

65 Cf. Annette Froehlich (ed.), *Post 2030-Agenda and the Role of Space: The UN 2030 Goals and Their Further Evolution Beyond 2030 for Sustainable Development* (Springer Nature, 2018).

66 Aaron Boxerman, Isabel Kershner, and Natan Odenheimer, 'What to Know about Trump's "Board of Peace"', *New York Times,* 19 January 2026, https://www.nytimes.com/2026/01/19/world/middleeast/trump-board-of-peace-gaza.html.

67 The White House, *Statement on President Trump's Comprehensive Plan to End the Gaza Conflict,* 16 January 2026, https://www.whitehouse.gov/briefings-statements/2026/01/statement-on-president-trumps-comprehensive-plan-to-end-the-gaza-conflict.

68 Katya Adler, 'Trump's New World Order Has Become Real and Europe Is Having to Adjust Fast', *BBC World*, 16 February 2026, https://www.bbc.com/news/articles/cddn002g6qzo.

DOI 10.30966/2018.RIGA.17.4

Robert Reich, among many others, pointed out,[69] the US cannot be a 'lonely superpower' any more, as in the era of 1990–2010. Under the now much more complex circumstances of the 2020s and the already initiated path to the 2030s, even the US needs multilateral support. Given that Trump's time in office will not last forever, more moderate and collaborative approaches could secure the positive achievements of his era for longer.

The result to be avoided in the remaining 2020s and then in the 2030s is therefore clear. What the UN described in 2021, on its seventy-fifth anniversary, as the current 'era of conflict and war' would, if continued, harm all communities on the planet if this era is not transformed into a better cooperational one by long-term, forward-looking measures implemented wisely, and step by step, to heal some of the wounds of recent years. The stagnation of the global sustainability agenda, or its replacement by ideologies of neo-nationalist resilience, as well as concepts such as the every-man-for-himself 'rebirth of resilient nations',[70] would be a mistake in view of systemic crises and would have negative consequences for the whole planet. As a result, a further dilution of international agreements, the international rule of law, and global cooperation pacts into bi- or multilateral 'special relations' should not be encouraged in the common interest of all who participate in the future of a globe in the meantime driven by global, not national or local, problems.

These learnings are increasingly debated publicly on the international stage. At the Munich Security Conference 2026, where NATO's Strategic Communications Centre of Excellence (StratCom COE) presented its pathbreaking research on the 'NextGen Information Environment',[71] Chinese foreign minister Wang said the UN was not perfect but still the

69 Robert Reich, 'Dear Allies of America, Please Don't Confuse Our President with Us', *The Guardian,* 19 March 2026, https://www.theguardian.com/commentisfree/2026/mar/19/donald-trump-american-ally.

70 Alon Helled and Carlo Pala, *Adapting Nations: National Resilience between Contemporary Statehood and Identity* (Springer, 2025).

71 Neville Bolt and Elina Lange-Ionatamišvili, *The NextGen Information Environment* (NATO Strategic Communications Centre of Excellence, 2026), https://stratcomcoe.org/publications/the-nextgen-information-environment/339.

DOI 10.30966/2018.RIGA.17.4

best basis for global cooperation of all nations. He thereby acted as the main defender of the UN against the fervent attacks of US secretary of state Marco Rubio, who instead declared that the role, impact, and reach of the UN was in reality—and should be—'very limited'. Meanwhile EU Commission president Ursula von der Leyen spoke in favour of a new, rather retro-solipsistic Europeanism in security affairs. This all sent an ambiguous signal for the coherence of the world's democracies, and of international cooperation at large. Nevertheless, it manifested the real state of the global order system, of traditional diplomacy and, in general, of contemporary balancing efforts in international affairs.

Impulses for Renewal

Despite all this fragmentation, in the present there are also positive prospects provided by forward-driving impulses. True trans-systemic renewal could, as mentioned, come from culture: raising awareness, augmenting insight through sensibility, science and futures education, delivering a sense-making positivity for new generations, and integrating fundamental challenges such as climate change with anticipatory strategic thinking and research can be generally shared goals, irrespective of political or ideological divides. Hope also lies in recent innovative, trust-building initiatives of meta-political bodies such as:

- the UN Summit of the Future (September 2024)[72]
- the UN Pact for the Future (October 2024)[73]
- the MONDIACULT Cultural Agenda until 2050 (October 2025)[74]

72 United Nations, *Summit of the Future,* New York, 20–23 September 2024, https://www.un.org/en/summit-of-the-future.

73 United Nations, *Pact for the Future (A/RES/79/1),* New York, October 2024, https://www.un.org/pact-for-the-future/en.

74 UNESCO, *MONDIACULT Conference 2025,* Barcelona, 29 September–1 October 2025, https://www.unesco.org/en/mondiacult.

DOI 10.30966/2018.RIGA.17.4

- UNESCO's Recommendations on the Ethics for Artificial Intelligence (2021)[75] and the Ethics of Neurotechnology (2025)[76]
- a series of new international cooperation agreements, such as the UN High Seas Treaty, which formally puts a third of the global oceans under protection by 2030 and has been ratified by eighty countries, including China (January 2026).[77]

All these initiatives intend to place a stronger accent on interdisciplinary futures instead of sectorial presents. They aim to transform the global agenda and their carriers in more forward-looking bodies of reference, thus avoiding the paralysis of polarisation by pointing towards possible, desired, or probable common futures. Cross-sectoral and consciously inter- and transdisciplinary initiatives such as UNTRAD, the UN Unit on Non-Traditional Diplomacy founded in Bruges in 2021,[78] could also play an important role in progressing the current situation towards more solid trajectories. Like the UN 'futures offensive' as a whole, UNTRAD places education, science, and culture at the centre of the post-2030 agenda. To some extent, non-traditional diplomacy could complement and, where needed, temporarily even replace institutional functions of the currently widely paralysed UN Security Council or the International Court of Justice.

A final factor for revitalisation could be, as mentioned, the bolder institutionalisation of futures thinking, futures competence, and futures research on all three micro-, meso-, and macro-levels of international interconnectivity. Integrating 'the future', or better the diversity of 'futures' in the plural, more actively into the theory and practice of international relations could identify common areas of development goals across political systems and their ideological rivalries. 'Futures' can

75 UNESCO, *Recommendation on the Ethics of Artificial Intelligence,* Paris 2022, https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

76 UNESCO, *Draft Recommendation on the Ethics of Neurotechnology,* Paris 2025, https://unesdoc.unesco.org/ark:/48223/pf0000394866.

77 UNU/EHS, *What Is the High Seas Treaty and Why Is It Important?,* 16 January 2026, https://unu.edu/ehs/article/what-high-seas-treaty-and-why-it-important.

78 UNU-CRIS, *Unit on Non-Traditional Diplomacy (UNTRAD),* https://cris.unu.edu/UNTRAD.

DOI 10.30966/2018.RIGA.17.4

also act as alternative diplomacy or science diplomacy *sui generis*. As the landmark UN Summit of the Future in New York in September 2024 demonstrated, the topic of futures will become ever more essential for escaping the dead ends of the global reorientation phase for *three* reasons:

1. All global actors have profound future needs due to acceleration and uncertainty.
2. Futures do not exist, and therefore appear less dangerous for the present than immediate day-to-day agendas.
3. A discussion about the prospects of the international community seems easier with regard to unknown futures than one about the all too well-known present.

In all this, the growing importance of 'futures staging'[79] and 'futurecasting'[80]—that is, doing good and showing it—can play the role of an instrumental renewal of 'soft tools' for transnational understanding and bridge-building.

It is thereby indicative that when the task is to venture into the unchartered territory of futures, the strategic commands of close to decision-making military apparats in the world often play an avant-garde role out of necessity, albeit usually preferring forecast to the more transformation-oriented approach of anticipation. Nevertheless, the fact that, exemplarily, NATO is pushing its foresight capabilities on different levels simultaneously because of the faster-changing and more volatile international environment, including 'long-term transformational forecasting and foresight, operational assessment, strategic directions and support to leadership, academic analysis of structural trends and emerging or disruptive technologies',[81] could help pave the way to

79 Will Hartigan and Arthur Horobin, *Policy Fit for the Future: The Australian Government Futures Primer* (Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2024).

80 Michael Shamiyeh (ed.), *Practices of Futurecasting: Ways of Sharing Imagined Tomorrows* (Birkhäuser, 2025).

81 Andrzej Jacuch, *'Strategic Foresight in NATO and Strategic Commands—An Analysis of Methodologies and Institutional Architecture'*, *Przegląd Nauk o Obronności / Defence Science Review* Nº 21 (2025), https://doi.org/10.37055/pno/209867 and www.defencesciencereview.com.pl/pdf-209867-131697?filename=Strategic-Foresight-in-NA.pdf.

DOI 10.30966/2018.RIGA.17.4

a broader integration and adaptation of 'futures' into the cultural and civilisational mainstream.

Outlook: A World in Transition

It was a sign of the times and a summary of the situation of world affairs when, on New Year's Eve 2025, a militarily powerless figure like Pope Leo XIV (US citizen Robert Francis Prevost) criticised the plans of the major powers to divide up the world according to their interests. He stated that 'the plans dominating the world today' were 'strategies aimed at conquering markets, territories and spheres of influence. Armed strategies cloaked in hypocritical speeches, ideological slogans and false religious motives.'[82] Simultaneously, a similarly powerless figure like Austrian president Alexander Van der Bellen, the leader of a formally neutral, small country at the centre of the European continent, analysed the 'emergence of a new world order'[83] in which 'the law of the strongest increasingly prevails'.[84] He added that, in response, 'only a strong and united Europe can affirm itself […] on the basis of a new European patriotism'.[85] Echoing the international resurgence of the 'sovereignty' motif, Van der Bellen's analysis was that

> Europe must determine its own path: 'We can lead the way and show the world that there is another path between the law of the strongest and purely capitalist interests. This path takes the rule of law, human freedom for self-development, and gender equality seriously, balances interests, and does not leave anyone to hunger or homelessness.' To become more independent from the 'arbitrariness of foreign governments,' Europe must become independent in energy supply and in the digital world, argued Van der Bellen.

82 'Papst kritisierte Aufteilung der Welt durch Großmächte' [Pope criticizes the division of the world by the major powers], *Katholisch.de*, 1 January 2026, https://katholisch.de/artikel/66605-papst-kritisiert-aufteilung-der-welt-durch-grossmaechte.

83 'Van der Bellen: "Sind in neuer Weltordnung angekommen"' [Van der Bellen: 'We have arrived at a new world order'], 5 January 2026, https://orf.at/stories/3416267.

84 Ibid.

85 'New Year's Address with Appeal: Van der Bellen Calls for "European Patriotism"', *Vol.at*, 1 January 2026, https://www.vol.at/new-years-address-with-appeal-van-der-bellen-calls-for-european-patriotism/9898241.

DOI 10.30966/2018.RIGA.17.4

> Europe must also become 'sovereign' in its defense capabilities. 'The European Union is one of the largest economies in the world. It is time to recognize our own strength and see that we have bargaining power.' The states of Europe could serve as a 'model for all the states of the earth: An example that it is possible to coexist peacefully. In this sense, the European stars continue to shine and provide guidance when it gets dark elsewhere.'[86]

Overall, despite Van der Bellen's slightly too solemn tone, it is plausible that in the second half of the 2020s and probably continuing throughout the 2030s the global system will pass through a phase of profound reorientation, which will continue to characterise the phase of 'advanced globalisation'.[87] In it the West, Europe, and the loose alliance of global democracies must re-vision, reform, refine, redefine, and reframe their place.[88] All signals point towards the fact that the current systemic change is not going to stop soon. The hallmarks of the coming years will consist in dynamic liminality and the (temporary) primacy of factual over normative forces. Economic and cultural innovations are needed to navigate this transition phase. The coming years will depend, *first*, on whether and how a balance can be struck between sovereignty and community, autonomy and interdependence, resilience and sustainability, impact and influence. *Second*, they will hinge on whether and how exactly a new, shared global sense of purpose can be promoted through a more active and interactive anticipatory and futures orientation.

That said, a last, self-referential point should be noted in conclusion. The political sciences as the—nominally—main contemporary analysts of the ongoing global reorientation are revealing themselves in times of upheaval and deep change as what they are: not sovereign commentators, but often productively irritated and sometimes astonished multiplicators

86 Ibid.

87 Benedikter et al., 'What Is Advanced Globalization?'

88 Roland Benedikter, 'Reglobalization, Whereto? A Summary and Outlook of Six Years of Reglobalization, 2019–2025', *Global-e: A Global Studies Journal* 16 Nº 10 (December 2025): 1–13, https://globalejournal.org/global-e/december-2025/reglobalization-whereto-summary-and-outlook-six-years-reglobalization-2019. Cf. Roland Benedikter and Ingrid Kofler, 'Globalization's Current Transition Phase: The 5 R's', *Global-e: A Global Studies Journal* 12 Nº 36 (August 2019), https://globalejournal.org/global-e/august-2019/globalizations-current-transition-phase-5-rs.

DOI 10.30966/2018.RIGA.17.4

of messages always at risk of becoming—mostly unconsciously—servants of questionable political decisions, dependent on the actions of others and to no extent intellectually superior to politics. These sciences are in the process of realising, as things grow more serious than in the 'happy globalisation' phase of 1990–2015, that they have their own 'holistic' responsibility. With their attempts at description and understanding they have the obligation to contextually reflect which role they are playing in the global transformation described in this short outline.[89] This means, among other things, that they cannot view the present phase of global reorientation just from a Western European viewpoint, but should consider the whole in which diverse and increasingly competing, partly distorting voices are interwoven though global media and publishing outlets.

As a consequence, some of the traditional concepts in political analysis have to be changed to be (1) less Eurocentric, (2) more inter- and transdisciplinary, and (3) more realistic against the background of contemporary all too idealistic scientific knowledge-production. For example, the concept of 'world' as a partial founding term of 'world affairs' seems to be scientifically outdated. This is a concept that strategically rose in the medieval ages as the conceptual basis of extension and expansion (crusades) and later dominated early modernity, including the first decades of European nation states in the second half of the nineteenth century, the short incubation phase of which almost immediately led to global war, that is, World War I. In overcoming such implicitly outdated terms and to meet the requirements of understanding needed in the phase of hyper-complexity, we have to realise that scientific knowledge tells us to differentiate. 'World' implies there is a cognitive-mediated unity shifting stably with the observer including knowns and unknowns, subjective and objective spaces, which in reality is not the case. Nevertheless, the concept of 'world' somehow suggests there is a fundamental unity between personal, national, and universal interests, that is, myself, the planet, and the κόσμος. In today's scenery this is a problematic implication, since in this sense 'the world' would be a known and per se stable and

89 Roland Benedikter, 'Politikwissenschaft und "die Zukunft"' [Political science and 'the future'], *Zukunft: Die Diskussionszeitschrift für Politik, Gesellschaft und Kultur* 77 Nº 9 (2023): 32–35.

DOI 10.30966/2018.RIGA.17.4

reliable horizon. This is an illusion which must be overcome for the sake of a new, more humble realism.

What lies ahead of us? In the coming years, economy and culture are likely to become more promising mediators and forward-drivers than politics, which have tended to turn inward since the end of the 2010s. In the 2020s, previous development logics and international institutions, including classical concepts of globalisation, have lost influence. Nevertheless, a positive new globalism and a new constructive cosmopolitanism are possible and can rise out of the ashes, if they rely more strongly on interconnecting forces such as technological interconnectivity interpreted as a global cultural process, the related economic and social implications, and, possibly via the nascent space economy, the imminent expansion of humanity into space as a new common frontier, which could become a unifying force in principle.

Be that as it may, in view of the—desirable, possible, and probable—characteristics of contemporary change, one thing seems to be sure: in turbulent times, global platforms interconnecting all of humanity will play an even more crucial role in co-shaping peace and overall progress. This is because history has taught and continues to teach that evolution is, in most cases, better than revolution. In principle, evolution causes less harm and bears the hope for more participatory patterns. Therefore, the international system of cooperation, represented by institutions such as the UN, UNESCO, the United Nations University, or the OECD should be preserved, refined, and where needed reformed and further evolved. The reason for this advice is simple. Realistically speaking, the UN and its like form the only functioning platforms that hold together the family of nations, and thus the peoples and, as a consequence, the human beings on the planet. Ultimately the international system of interchange and creative mutual trust and assistance represented by the main global bodies established since 1945 stands for what it means to be human in our historical phase, and most probably even beyond.

The Rupture of the International Rule of Law and the Rise of Tech Sovereignty

An Essay by Malik Āl Dahlan

Keywords—*usable legality, tech sovereignty, Authoritarian Stack, Tenant State, variable geometry, strategic communications, strategic communication*

About the Author
Malik R. Āl Dahlan is Honorary Professor at the University of St Andrews and Adjunct Professor at Peterhouse College, Cambridge. His work spans transnational law, Islamic legal theory, and institutional design. He is the author of *The Hijaz: The First Islamic State* and writes the Arabic column series تاراوح يفي رطلا (Al-Tarif Dialogues).

Abstract
The international rule of law is not failing for want of activity. Courts are busier, treaties multiply, resolutions proliferate. Yet the decisive functions of rule, namely perception, classification, and enforcement, have migrated from parliaments and ministries into code and hardware owned by a new class of technical sovereigns. This essay diagnoses that migration through two concepts: the Authoritarian Stack, in which legal exceptions are automated and exported, visible most sharply in Gaza's algorithmic battlefield, and the Tenant State, in which governments still raise the flag while renting perception, enforcement, and infrastructure from private firms. Against this backdrop the essay develops the idea of usable legality, the capacity of legal order to function as the operating system of behaviour rather than as a screensaver, resting on credible

DOI 10.30966/2018.RIGA.17.5

commitment, clear attribution, and reliable enforceability. In place of a nostalgic return to universalism, it proposes variable geometry with a binding core: algorithmic auditability, data locality with interoperability, and distributed verification ecosystems. It closes by reframing strategic communication as the engineering of trust in a knowledge economy where legitimacy will increasingly be judged by operational effect rather than procedural fidelity.

On paper the international rule of law has never looked stronger. Courts are busier. Treaties multiply. UN bodies churn out resolutions with algorithmic regularity. Yet the more often the law speaks, the less often it compels.

What has changed is not the vocabulary of order but the architecture of power. Sovereignty has slipped its Westphalian frame. It no longer lives primarily in parliaments, ministries, and the maps of schoolchildren. Increasingly it lives in code and hardware—in the systems that see, sort, and act long before any courtroom hears a case. The state still raises its flag. But it is a tenant now, renting reality from those who own the infrastructure.

This diagnosis did not emerge in a faculty common room. It emerged in a classroom full of master's students in strategic communications, many of them working with NATO or national ministries, who came with a simple question: if their field exists to help states make sense of conflict and cooperation, what happens when the state itself no longer owns the means of perception?

The answer begins with rupture.

DOI 10.30966/2018.RIGA.17.5

Rupture without Revolution

At the World Economic Forum in Davos on 20 January 2026, Canada's prime minister, Mark Carney, named what many leaders had been feeling but had not yet articulated: 'a rupture, not a transition.' Not just the familiar friction between markets and geopolitics, but a deeper break between the legal grammar that still describes the world and the operational grammar that now runs it.

You can see that rupture most clearly in Washington. On 7 January 2026 the President of the United States signed a memorandum instructing agencies to withdraw from sixty-six international organisations and instruments, thirty-one UN entities among them, deemed 'wasteful, ineffective, or harmful' to American interests. The gesture was not just policy; it was theatre. The following day, in an interview with the *New York Times*, he remarked that he did not 'need international law', and that his 'own morality' was 'the only thing that can stop me'.

Something important has happened when the leading architect of the post-war legal order feels confident enough not just to violate rules—as many presidents have—but to renounce even the performance of compliance. In earlier eras power still felt obliged to speak the language of law, however hypocritically. Now, in some capitals, even that ritual seems optional.

But the problem runs deeper than one president's bravado. The international legal system is not simply under strain; it is quietly becoming performative. It still produces resolutions, judgements, and communiqués. Yet in the places where power is most intensely exercised—on the battlefield, in data centres, on platform dashboards—those texts increasingly arrive too late to shape reality. Law is becoming a commentary track.

If there is a concept that separates law as theatre from law as infrastructure, it is usable legality: a legal order's ability to function as the operating system

DOI 10.30966/2018.RIGA.17.5

of behaviour, not the screensaver. Usable legality rests on three pillars: credible commitment (promises that actually guide future action); clear attribution (someone real is responsible when things go wrong); and reliable enforceability (rules bite across power hierarchies, not just at the margins).

Those pillars are now eroding. And the erosion is easiest to see in the places that most observers would rather not look.

The Black Box Battlefield

In recent years Gaza has become a laboratory for what might be called the Authoritarian Stack: a tiered system in which exceptions to international law are not merely declared but digitised, automated, and eventually exported.

Classical international humanitarian law assumes a human commander who weighs military advantage against civilian harm, applying the principles of distinction and proportionality in each strike. The system is imperfect, but there is at least an identifiable mind at the centre of the decision.

In Gaza that premise has begun to disintegrate. Investigations by +972 Magazine and Local Call, amplified by other outlets, have described the use of a system called 'Lavender', which compiles vast quantities of data—phone records, social media activity, pattern-of-life indicators—to generate a 'kill list' of suspected militants. A companion system, nicknamed 'Where's Daddy?', is said to track those individuals in real time and flag moments when they return home, prompting strikes on residential buildings. Officers retain nominal authority to override the recommendations, but the volume of targets and the speed of operations mean that, in practice, human review is often perfunctory.

The legal problem is not simply that such systems may be over-inclusive or biased. It is that they create a war without a defendant. When a drone

DOI 10.30966/2018.RIGA.17.5

destroys an apartment block because an opaque model decided that one occupant matched a certain probability profile, whom does the law hold to account? The programmer? The contractor? The commander who clicked 'approve' on hundreds of targets in a night? The company that built the model using proprietary data and trade-secret code?

The law cannot cross-examine an algorithm. It cannot imprison a loss function. It can only reach human beings. But by the time a court assembles enough evidence to reconstruct the chain of decisions, the responsibility has already dissolved into a fog of technicalities and jurisdictional hedges.

Gaza is not a unique aberration. It is an early test case. What is normalised there today—outsourcing lethal attribution to proprietary systems—will be sold as a capability to other states tomorrow. The exception is becoming the template. And it is not the only domain in which sovereignty has begun to migrate.

The Tenant State

If this new world has a philosopher-king, it may be a Silicon Valley investor who once wrote that he no longer believed 'freedom and democracy are compatible'. His company, named after Tolkien's 'seeing stones', is not just another software firm. It is an attempt to turn data into a proprietary reality.

Palantir Technologies began as a niche tool for intelligence agencies. Today it sits at the heart of Western defence planning. Under the US Army's TITAN programme, Palantir is building AI-enabled ground stations that fuse streams from satellites, drones, and ground sensors into a single 'game-changing' picture of the battlefield. A nation's most precious asset in conflict—situational awareness—is no longer produced by its own bureaucracy. It is delivered as a subscription service.

DOI 10.30966/2018.RIGA.17.5

This is the birth of the Tenant State: a state that still performs sovereignty in symbols but rents its capacity to perceive and act from private technical sovereigns. The flag is national. The dashboard is not. The Tenant State is not a metaphor. It can be mapped across at least four layers.

First, the virtual border. When platforms like Meta and Google decide what billions of people can see and say, they are not merely moderating content. They are exercising planetary jurisdiction over speech. A tweak to a ranking algorithm can decapitate an industry, marginalise a language, or erase a protest movement without any court order. The old frontier posts and customs houses still exist, but the real border—the line between visibility and oblivion—runs through proprietary code.

Second, the hosting of the state. As governments move their tax systems, health records, and defence communications to cloud providers such as Amazon Web Services or Microsoft Azure, they are effectively 'hosting their sovereignty'. In normal times this looks like efficiency. In a crisis, access to compute and to storage becomes a geopolitical ration, decided in corporate boardrooms as much as in cabinets.

Third, the quasi-belligerent. In one recent conflict, the decision of a single satellite internet provider to limit or extend coverage allegedly affected the viability of military operations. The infrastructure was neither neutral nor fully under state control. It became an independent actor in war, not clearly captured by the Geneva Conventions.

Fourth, the death of the fact. In Syria, in the Ukrainian city of Bucha, and now in multiple theatres, satellite imagery and open-source investigations have produced what once would have been regarded as definitive evidence of atrocities. And yet every image is now met with the same response: it is fake, it is staged, it is AI-generated. The 'deepfake defence' has become a reflex. If no fact can be common, no law can be shared.

This is not simply a regulatory lag that better drafting can fix. It is structural. International law was built for a world in which the state held

DOI 10.30966/2018.RIGA.17.5

the decisive levers of surveillance, censorship, and violence. It is now confronted with a world in which those levers have migrated to entities it does not recognise as subjects. Sovereignty has become stack-based.

The state sits on top, still visible, but the decisive functions—perception, classification, enforcement—run underneath, in private code. When you can no longer clearly say who decides, you can no longer credibly say who is responsible. And when responsibility evaporates, the third pillar of usable legality—enforceability—collapses with it.

From Law as Ritual to Law as Infrastructure

To understand what is at stake, it helps to go back to three thinkers who once framed the debate about international order.

Kenneth Waltz, the realist, taught that in an anarchic world, outcomes are driven by the distribution of capabilities. Law matters only at the margins. Crimea's annexation in 2014, or the US invasion of Iraq in 2003, seems to confirm his point: legal arguments proliferated, but tanks and planes decided.

Robert Keohane, the institutionalist, argued that even in an anarchic system, states can build regimes—trade rules, environmental agreements, monetary frameworks—that make cooperation rational by increasing transparency and punishing defection. The global trade system, for decades, was an example: imperfect, unequal, yet broadly reliable.

Stanley Hoffmann offered a warning that now feels prophetic. Law, he suggested, can constrain power only so long as the powerful see restraint as in their interest. Once they no longer do, and begin to apply legality selectively—insisting on strict rules for their adversaries and exceptions for themselves—public faith in the system erodes. Law then persists as language but loses its authority.

DOI 10.30966/2018.RIGA.17.5

We now live in Hoffmann's world. Norms are invoked, but increasingly as weapons rather than restraints. Institutions still function in 'safe' domains—air traffic control, postal conventions, maritime safety—because they rarely collide with the interests of technical sovereigns. The bathwater of routine cooperation remains warm. Yet in the existential zones—war, truth, security—the heater has been unplugged.

The test of any international legal order, therefore, is no longer how many treaties it can produce, but whether it still delivers usable legality where it matters most. Does a judgement change behaviour on the ground? Does a treaty genuinely bind the powerful when their interests shift? Can a civilian, somewhere far from the corridors of power, rely on the law to protect their life and dignity when the drones are overhead?

By those measures the system is failing.

Three Kinds of Deterioration

The erosion of usable legality is accelerating along three fronts: norms, institutions, and knowledge.

Norms erode when violations become routine rather than exceptional. The UN Charter's prohibition on the use of force and guarantee of territorial integrity were designed to make war the last resort. Yet recent years have normalised cross-border strikes, cyber operations, and de facto annexations as tools of statecraft. When the most powerful actor openly declares that international law binds only when convenient, the prohibition remains in the dictionary but disappears from strategy.

Institutions overstretch when they keep expanding their mandates while losing the political support that once made those mandates meaningful. The International Criminal Court has issued arrest warrants for leaders of small and mid-sized states and armed groups, but for most of its existence the overwhelming majority of its defendants have been African. When the

DOI 10.30966/2018.RIGA.17.5

court sought arrest warrants against a major power's leader for alleged war crimes, enforcement remained purely symbolic. When it turned its attention to the allies of Western governments, those same governments began to question its legitimacy. A court that cannot credibly touch all sides communicates not universality but hierarchy.

Epistemic corrosion is the decisive deterioration in a knowledge economy. Law presupposes a shared factual substrate: bodies, borders, dates, casualty counts. Today that substrate is crumbling. Disinformation campaigns contest every datum. Deepfakes threaten to flood the public sphere with plausible fabrications. Data localisation laws fracture the information environment: one jurisdiction requires local storage, another demands extraterritorial access, a third bans certain flows outright. Soon large language models trained on different corpora will generate different 'worlds' for different publics. If we cannot agree on what happened, we cannot agree on what is lawful.

Critics sometimes respond that this diagnosis verges on apocalyptic. Planes still land safely. Contracts are still enforced. Trade still flows. If the rule-of-law heater were truly broken, they say, we would feel the cold.

The reply is simple: in many places we already do. The warmth persists only because we are sitting in the shallow end of the tub. At the deep end—where war, surveillance, and security converge—the water has already turned to ice.

Variable Geometry with a Binding Core

If Mark Carney's rupture has a constructive implication, it is this: stop pretending that universality will enforce itself. Start building structures that can hold under asymmetry.

The post-war system was designed around a simple aspiration: one set of rules, applicable to all, enforced by shared institutions. That aspiration

DOI 10.30966/2018.RIGA.17.5

was always imperfect; power carved exceptions for itself. Yet the ideal of universality performed a stabilising function. In a world of technical sovereigns and tenant states, universality as a design principle is no longer sufficient. What we need instead is variable geometry with a binding core.

Variable geometry means accepting that not every state, company, or platform will participate in every regime in the same way or to the same degree. Some will localise data; others will not. Some will submit their targeting algorithms to independent audits; others will refuse. Some will sign on to binding rules about cross-border content moderation; others will treat them as suggestions.

The task is to identify and harden a binding core of usable legality that remains non-negotiable, even amid this differentiation. That core is not a wish list of values. It is a set of operational guarantees: a minimal standard of restraint in the use of force, especially against civilians; a baseline of fidelity to accepted obligations, including transparent exit procedures; and a commitment to custodianship of shared goods: human dignity, environmental integrity, and the integrity of knowledge.

In practice that would require three types of innovation.

First, auditability. We must move from verbal treaties to enforceable algorithmic audits. The right to 'peer into the box' of systems that make life-or-death decisions—whether in targeting, credit, or content—is the twenty-first-century equivalent of the right to inspect weapons programmes. Without it, law is blind.

Second, data locality with interoperability. Data localisation is often framed as protectionism or censorship. It can also be a way to reclaim a modicum of sovereignty—keeping citizens' data within legal reach—while still allowing regulated, audited flows across borders. The choice is not between total openness and total closure. It is between anarchic flows governed by corporate terms of service and structured flows governed by public rules.

DOI 10.30966/2018.RIGA.17.5

Third, verification ecosystems. Fact-checking as we know it will not survive the flood of synthetic media. What is needed is a distributed infrastructure of verification: cryptographic provenance for images and videos; open, tamper-evident ledgers for key public facts; and transnational observatories that track and certify basic indicators of violence and humanitarian access in real time. This is not a technical fantasy. It is a political decision to fund and mandate tools that already exist.

None of this restores the lost innocence of the 'rules-based order'. But it does sketch a path from pure performativity to partial functionality—a way to make fragmentation workable rather than fatal.

The Knowledge Economy Transition

Beneath these institutional questions lies a deeper shift: from extractive sovereignty to knowledge-based sovereignty. For most of modern history, states derived their power from territory, population, and physical assets. Oil, ports, factories, conscripts. The law reflected that reality. It was about borders, tariffs, and guns.

In the knowledge economy, value resides in information architectures: educational systems, research networks, verification institutions, digital public infrastructure. States that invest in these capabilities can still act as landlords of their own reality. Those that do not will become tenants in other people's epistemic empires.

The actors that will thrive in this transition will be those that build three things.

First, institutional credibility: courts, regulators, and oversight bodies that can be trusted to act predictably and transparently, including in matters of data and AI. Without that, no amount of rhetorical commitment to 'the rule of law' will matter.

DOI 10.30966/2018.RIGA.17.5

Second, knowledge infrastructure: universities, laboratories, public-interest tech organisations, and statistical agencies capable of generating and verifying knowledge at scale. In a world of algorithmic propaganda, the ability to say, convincingly, 'this is what happened' is as important as the ability to say 'this is what the law requires'.

Third, impact-based legitimacy. In the nineteenth century, legitimacy was often dynastic. In the twentieth, it was ideological. In the twenty-first, it will be operational. Citizens—and foreign publics—will judge institutions less by their adherence to procedural formalities and more by measurable effects: reductions in violence, increased access to education and healthcare, the preservation of a liveable environment, the protection of truth in public life.

This shift has implications not just for diplomats and lawyers, but for strategic communicators—the Sympodium master's students who first wrestled with these ideas in Riga. Their craft has traditionally focused on narratives: crafting messages that align public perception with policy goals. In the age of technical sovereignty, their role becomes more structural. They are no longer just the storytellers of power. They are potential designers of the verification and accountability systems without which any story collapses into noise.

If lawyers are the architects of credible commitment, strategic communicators are the engineers of trust. They can help design infrastructures that withstand epistemic attack: resilient information channels, transparent decision logs, participatory feedback loops. In a world of deepfakes and dashboard wars, those who can build and maintain such systems will be as central to sovereignty as those who command armies.

DOI 10.30966/2018.RIGA.17.5

Beyond NATO

It is tempting, especially in Western capitals, to treat these questions as technical challenges for NATO committees, G20 task forces, or EU working groups. How should the alliance handle AI on the battlefield? How can democracies regulate social media without undermining free speech? How do we deter adversaries who weaponise data?

These are important questions. But they miss a more fundamental one: who gets to decide what counts as peace, and where those decisions are made?

In the twentieth century, strategic choices about war and peace were largely monopolised by states and alliances. In the twenty-first, some of the most consequential decisions—whether to extend satellite coverage over a conflict zone, whether to deploy an experimental targeting algorithm, whether to amplify or suppress footage of an atrocity—are being made in corporate boardrooms and server farms.

We therefore need a new kind of international settlement, not just a military alliance, that can make strategic decisions about peace in the knowledge age. I have argued elsewhere that international organisation is entering a third constitutional phase: neither the League of Nations of 1919 nor the United Nations of 1945, but an institutional settlement that redefines sovereignty as responsibility exercised within radical interdependence.[1] Read in that frame, even a proposal as blunt as President Trump's 'Board of Peace' registers, from the opposite direction, an intuition the scholarly argument reaches as well: that decisions about war and peace can no longer be left only to generals and diplomats, and that ad hoc bargains between governments and firms will not carry the weight now being placed on them. What is required is a standing, plural, publicly accountable forum in which states, technical sovereigns, and representatives of affected communities negotiate the rules for the systems that shape reality.

1 Malik R. Āl Dahlan, 'The Third International Organization' (forthcoming, 2026).

DOI 10.30966/2018.RIGA.17.5

The point is not to create yet another acronym on the international circuit. It is to recognise that as long as those decisions are left to ad hoc bargains between governments and firms, they will remain opaque, unaccountable, and skewed towards the interests of the strongest.

This matters to the American reader not because it flatters their sense of exceptionalism, but because the same forces that hollow out international law abroad are already eroding constitutional guarantees at home. When platforms decide what political speech is visible, when predictive-policing algorithms disproportionately target certain neighbourhoods, when critical infrastructure depends on private cloud contracts, the question 'who rules?' is not an abstraction. It is a local, daily reality.

The lease on the old model of sovereignty is expiring. The question is not whether power will migrate into technical systems; it already has. The question is who will own those systems, who will audit them, and on whose behalf they will act. We can continue to perform legality while outsourcing control. Or we can treat knowledge, verification, and restraint as the core public goods of the twenty-first century and build institutions worthy of them.

History will not wait for our choice.

When Disruption Is a Goal in Itself: Constructing Hybrid Threat Actors in Wargaming

Maria Golubeva

Keywords—*wargaming, strategic communications, strategic communication, hybrid threats, strategic ambiguity, strategic differentiation*

About the Author
Maria Golubeva is a fellow at the Centre for International Security, Hertie School, and the founder of crisis simulation company Meleys. She has served as a Member of the Latvian Parliament (2018–22) and as Minister of the Interior (2021–22). She holds a PhD in History from the University of Cambridge.

Abstract
This article looks at the ways wargaming can reflect the diversity and ambiguity of rationales of hybrid threat actors in the time of a fracturing liberal international order. Sections cover wargaming as a research method; hybrid, subthreshold, and grey zone threats, including *hostile state actors, ambiguous state actors, and hostile non-state actors*; the role of the information environment in constructing hybrid threat scenarios; and constructing hybrid threat actors. In offering a more accurate representation of disruptive actors, and not assuming they have an overarching geostrategic rationale, wargaming can offer a better analytical tool for understanding and preventing peacetime disruption.

DOI 10.30966/2018.RIGA.17.6

Imagine a major port city at night. The work in container terminals slowing down, most dock workers away until the morning, the lights around a new hydrogen or LPG terminal still on. Now imagine a handful of USVs loaded with explosives and directed by agents from a safe distance—tiny boats, not easy to spot for the port radars, but easy to hide in a nearby marina. And consider that in all maritime attacks on European infrastructure known to the public since 2022, detection occurred after damage, not before.[1]

While this may appear, at first sight, a problem for hard security and defence experts, it is at least in equal measure a problem that can be addressed in a wargame that focuses on the disruption such an event would cause in the information environment—the communicative space shaped by media systems, platforms, cultural norms, and audience cognition.[2] The chances of detection and prevention, and the scale of disruption and its political and economic consequences, depend not only on the capacity of security and intelligence services but also on the resilience of the information environment before, during, and after the attack.

This article looks at the ways that wargames focusing on hybrid threat scenarios can construct the motivation and course of action of threat actors (both state and non-state) to retain analytical and educational relevance in the changing landscape affected by the fracturing international order and the rise of hybrid warfare. It addresses the diversity of rationales of hybrid threat actors and the need for wargame designers to recognise, rather than obfuscate, the strategic ambiguity and strategic diversification behind their actions.[3]

1 Based on all instances of damage by marine vessels in the Sahaidachnyi Security Center sub-threshold warfare tracker, https://sahasec.org/tracker.

2 J. Lipinska, 'Strategic Communication in the Face of Contemporary Threats to the Information Environment', *Humanities and Social Sciences* 28 № 4 (2021).

3 For a review of literature on strategic ambiguity, see P. Bach, C. Schmitt, and S.C. McGregor, 'Let Me Be Perfectly Unclear: Strategic Ambiguity in Political Communication', *Communication Theory* 35 № 2 (May 2025): 96–106. For a multidisciplinary discussion of strategic ambiguity, see N. Bolt (ed.), 'Strategic Ambiguity', Special Issue, *Defence Strategic Communications* 12 (Spring 2023). This article follows Bach et al. in understanding strategic ambiguity as 'polysemy [...] aimed at audiences from varying interpretive communities; and by which polysemy the communicator stands to gain some specific advantage'.

DOI 10.30966/2018.RIGA.17.6

The article refers to hybrid threats primarily in the sense defined through EU and NATO policy documents, as explained below. The existence of a vast body of academic debate regarding the use of the term 'hybrid warfare' is not central to the article's argument; however, the existence of this debate is important to mention.[4]

Some studies on the subject of 'hybrid warfare'[5] see it specifically as a means to achieve superiority by maximising strategic ambiguity. Mumford and Carlucci argue ambiguity is the defining essence of hybrid warfare,[6] and the Hybrid Centre of Excellence, Helsinki, has dedicated a paper to strategic ambiguity in hybrid warfare (2020). Both publications define hybrid warfare in a manner that seems captured by military theory—assuming that hybrid warfare 'includes the strategic application of the use of (ambiguous) force to gain territory or attain another strategic goal'.[7]

As argued in this article, geostrategic understanding of hybrid threat actors' objectives presents an unnecessary narrowing, because hybrid attacks can be guided by aspirations that are not geostrategic—e.g. by ideological contestation of norms underpinning political institutions and regimes.

The article also looks specifically at the ways wargames focusing on hybrid threat scenarios depend on reconstructing the information environment where different types of threat actors engage in interpretation and meaning-making.

4 F.G. Hoffman, in *Conflict in the 21st Century: The Rise of Hybrid Wars* (Potomac Institute for Policy Studies, 2007), argued that a new phenomenon blending conventional capabilities, irregular tactics, terrorist acts, and criminal disorder had emerged in warfare. Freedman argued the label 'hybrid warfare' gives 'coherence to what was often no more than a set of ad hoc and improvised arrangements' (L. Freedman, *Strategy: A History*, New York: Oxford University Press, 2013).

5 See n. 4 on the debate regarding the use of the term.

6 A. Mumford and P. Carlucci, 'Hybrid Warfare: The Continuation of Ambiguity by Other Means', *European Journal of International Security* 8 Nº 2 (May 2023): 192–206.

7 A. Mumford, *Ambiguity in Hybrid Warfare*, Hybrid CoE Strategic Analysis 24 (Hybrid CoE, 2020).

DOI 10.30966/2018.RIGA.17.6

Wargaming as a Research Method

In essence, wargaming is a way to model the behaviour of different actors and to analyse their possible course of action, and it is the more useful analytically, the more factors and conditions of decision-making context it replicates. This includes, but is not limited to, factors of compressed time, stress, incomplete or too abundant information, and systemic complexity of decision-making contexts, including information environments.

Wargames generate insights and hypotheses by drawing conclusions from observing human decision-making and interaction. In his foundational work *The Art of Wargaming*, Peter Perla outlined the cycle of research where scholars and practitioners test operational concepts by analysing a series of wargames.[8] More recent publications remind us that wargaming can be used to study rare events or topics where evidence is difficult to observe.[9] Hybrid actors' attacks on civilian infrastructure are one example of such an event. While increasingly frequent, they often employ combinations of sabotage, infiltration, and/or cyberthreat tactics coupled with information manipulation and influence—'a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes […] conducted in an intentional and coordinated manner'.[10]

The utility of wargaming as a research method derives from its capacity to simulate decision-making conditions that are difficult or impossible to study through traditional experimental or observational approaches. These provide insights into the motivations and perceptions of decision-makers by 'explicitly allowing human decisions that are made under the press of time and on the basis of imperfect or incomplete information to influence

8 P. Perla, *The Art of Wargaming: A Guide for Professionals and Hobbyists* (Naval Institute Press, 1990).

9 E. Lin-Greenberg, R. Pauly, and J.G. Schneider, 'Wargaming for International Relations Research', *European Journal of International Relations* 28 Nº 1 (2022).

10 Bolt, N., 'Foreword: Is this the Age of Disinformation or the Age of Strategic Communications?', *Defence Strategic Communications* 14 (Spring 2024).

DOI 10.30966/2018.RIGA.17.6

the course of events'.[11] This characteristic distinguishes wargaming from purely quantitative simulations based on mathematical models, or static case studies describing specific cases bounded by circumstances that may not be repeated in other contexts.

Methodologically, wargaming exists in a liminal space between experimental research and qualitative observation. Well-designed wargames should lead to results with good ecological validity—the extent to which behaviour under test conditions mirrors real-world behaviour.[12] Research conducted from 2011 to 2016 on the Deterrence and Escalation Game examined cyber operations and crisis escalation across six years of iteration, revealing that despite variations in scenarios and participants, decision-makers consistently exhibited risk-averse behaviour when confronting potential escalation dynamics on behalf of the adversary.[13] While iteratively designed wargaming studies like this are rare, wargaming as a method is increasingly used to study decision-making during critical disruptive events, not only by researchers but also by the media industry that uses tabletop wargames with commentary by experts. One example of this use of wargaming is the series of podcasts titled *The Wargame*, which gathered former top decision-makers and military experts to record the decision-making process by the UK and Russia in a hypothetical scenario of military escalation.[14]

Research using wargaming methodologies has illuminated several critical psychological processes that characterise decision-making during disruptive events. Dynamic interaction between opposing players creates what researchers term 'real-time feedback to their decision making', enabling participants to observe relationships between cause and effect as they unfold.[15] One of the uses of this real-time feedback is to encourage

11 J. Schneider, 'Cyber and Crisis Escalation: Insights from Wargaming', U.S. Naval War College, 2017, https://paxsims.files.wordpress.com/2017/01/paper-cyber-and-crisis-escalation-insights-from-wargaming-schneider.pdf.

12 Lin-Greenberg et al., 'Wargaming'.

13 Schneider, 'Cyber and Crisis Escalation'.

14 See the Sky News *Wargame* podcast, 2025, https://open.spotify.com/show/4lHtW6x1D6R0E1QmGLkBK1.

15 A. Kuehn, 'Assessment Strategies for Educational Wargames', *Journal of Advanced Military Studies* 12 № 2 (2021), www.usmcu.edu/Portals/218/5_JAMS_12_2_Kuehn_1.pdf.

DOI 10.30966/2018.RIGA.17.6

participants to explore different perspectives to understand adversary thinking,[16] which is essential not only in classical military wargames that originated in the nineteenth-century kriegsspiel,[17] but also in contemporary hybrid threat scenarios.

Another concept from historical and contemporary wargaming research that is relevant for hybrid threat scenarios is 'logical tact'. Namely, the subconscious judgement required to succeed when insufficient time exists for theoretical reasoning. It implies that wargame participants under compressed time conditions develop intuitive decision-making capabilities that transcend checklist-based approaches. This phenomenon was observed in crisis simulations employing multiple communication platforms simultaneously, where participants must process both spurious and important information under severe time pressure, mirroring the cognitive overload conditions of actual command centres.[18] In hybrid threat scenarios, the use of multiple communication platforms (emails, group chats, social media, legacy and digital news media) is essential for recreating the information environment, including complex information ecosystems consisting of so-called mushroom websites, automated bot accounts, troll farms, and other AI-assisted amplification tools that threat actors increasingly deploy.

Important insights for hybrid threat scenario wargames come from research into the resilience of critical infrastructures, where wargaming has been employed to model cascading failures and interdependencies between systems. Recent work introducing 'resilience games' specifically designed for the preparedness of critical infrastructure demonstrates how game mechanics can embed sector interdependencies and enforce

16 Ibid.

17 T. Hagenloch, '"Game On!" A Research Project on the Prussian Kriegsspiel', *British Journal of Military History* 7 Nº 2 (2021).

18 S. Downes-Martin et al., *Distributed Wargaming*, Report of the Simulation Interoperability Standards Organization (SISO) Wargaming Study Group (SISO, 2021), https://paxsims.wordpress.com/wp-content/uploads/2021/08/distributed-wargaming-siso-report-final-20210823-v2-1.pdf [accessed 11 May 2026].

cascading failures when critical facilities fail. Players must balance strategies of defence and recovery with limited resources.[19]

'Hybrid', 'Subthreshold', and 'Grey Zone' Threats

While historically wargaming has focused primarily on kinetic warfare scenarios, this article deals exclusively with wargames modelling hybrid threats, otherwise known as subthreshold or 'grey zone' threats. Hybrid operations present a real threat to societies that are not in conflict zones and are not alerted to the possibility of disruption in their immediate environment.

Different organisations and scholars use different terms to describe subthreshold threats and attacks. The European Union uses the term 'hybrid threats', defined as a 'mixture of coercive and subversive activities, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare'.[20] This understanding is predicated on the international law that arose in the historical period when warfare between states had been circumscribed by a set of rules, and war was waged by state armies. It implies that 'hybrid threats' signify a departure from that order.

Other organisations prefer the term 'grey zone threats'. RAND defines 'grey zone' as 'an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and non-military actions and the attribution

19 C. Schwartz, '*Access Denied* and *Sector Down*: Introducing Resilience Games for Critical Infrastructure Preparedness', *Cyber Defense Review* 10 Nº 2 (2025): 163–78, https://cyberdefensereview.army.mil/Portals/6/Documents/2025-vol10-iss2/CDR_V10_N2_Schwartz_ResGames_RA_IP.pdf.

20 European Council, *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats—a European Union Response,* 2016.

DOI 10.30966/2018.RIGA.17.6

for events'.[21] However, this definition remains problematic because it is embedded in the logic of conventional military conflict. The same report states that the aim of grey zone warfare is to challenge, constrain, or deny an adversary's access to geostrategically important areas.[22]

The geostrategic understanding of grey zone threats reduces the phenomenon to a chosen conventional conflict strategy of state actors, as the term 'geostrategic' itself is historically linked to a territorial or geographic direction of a state's foreign policy and strategy.[23] This is not the case with hybrid threat actors in more than one way. There are at least two clauses that need to be added to qualify the claim that hybrid actors pursue geostrategic goals: (a) non-state actors also engage in hybrid warfare, sometimes without the mandate or guidance from state actors (see multiple studies on insurgency[24]); (b) for both state and non-state actors, hybrid warfare may pursue a wide range of goals which are not always geostrategic in the sense of acquiring or denying territorial access.

An example to illustrate both clauses is the activity of ideologically motivated hacktivist collectives, which sometimes act as proxies for state security services, but sometimes undertake similar actions on their own. Rather than seeking to deny or gain access to a territory, hacktivists disrupt governments or corporations that they nominate as ideological enemies, while also undertaking criminal acts for personal financial gain. The group called Anonymous Sudan that carried out multiple major attacks on governments, universities, and media companies, among others, in 2023 and 2024, proclaimed it was fighting for Islam as well as for the Palestinian cause.[25]

21 L.J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression below the Threshold of Major War*, Research Report (RAND Corporation, 2019), p. 8.

22 Ibid.

23 C.S. Gray and G. Sloan (eds), *Geopolitics, Geography and Strategy* (London: Frank Cass, 1999).

24 S.N. Kalyvas, *The Logic of Violence in Civil War* (Cambridge: Cambridge University Press, 2006); J.D. Fearon and D.D. Laitin, 'Ethnicity, Insurgency, and Civil War', *American Political Science Review* 97 Nº 1 (2003).

25 Cyberint, 'Behind the Mask of Anonymous Sudan: An Analysis', 2023, https://cyberint.com/blog/research/anonymous-sudan-an-analysis.

DOI 10.30966/2018.RIGA.17.6

A reductionist approach that narrows hybrid attacks to a form of subthreshold warfare undertaken by states in lieu of or prior to conventional military conflict does not include the full spectrum of multi-domain, multi-vector hybrid threat actors, who apply a range of undeclared, asymmetric actions to disrupt the functioning of infrastructure, institutions, and societies. Nor their efforts to reshape the information environment. Private entrepreneurs behind amplification websites and troll and bot farms are an intrinsic part of the complex ecosystem instrumentalised by state actors to manipulate information domains.[26] And these efforts may be coupled with cyber activities, sabotage, criminal data theft, and intelligence gathering. Sometimes, as in the case of Russia, security and intelligence, and counterintelligence units responsible for information operations and influence campaigns, are the same as those responsible for undertaking actual sabotage.[27] This represents the ultimate coupling of systems in a hybrid threat landscape. As pointed out in the recent NATO StratCom COE report on the NextGen Information Environment, 'the security domain is hybridised—private actors exert growing influence and operate with significant autonomy, sometimes independent of state control'.[28] Hybrid threat wargame scenarios can and should reflect the diversity and ambiguity of objectives pursued by state and non-state threat actors, not just their tactics.

The tactics, techniques, and procedures (TTPs) of hybrid threat actors can be reconstructed in a game in one or several domains, with the information environment as the crucial domain where interpretive activity or sense-making happens.

To be credible and analytically useful, a wargame should replicate the preferred technological methods of disruption and discursive

26 European External Action Service, *4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats* (EEAS, 2026), p. 26, https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en.

27 CheckFirst, 'Unveiling GRU's Information Operations Troops with OSINT and Medals', 9 February 2026, https://checkfirst.network/unveiling-grus-information-operations-troops-with-osint-and-medals.

28 N. Bolt and E. Lange-Ionatamišvili, *The NextGen Information Environment* (NATO Strategic Communications Centre of Excellence, 2026).

DOI 10.30966/2018.RIGA.17.6

contestation used by hostile state actors, ambiguous state actors, and hostile non-state actors.

Hostile state actors (Russia, China, and Iran, and their military and civilian structures) possess a wide range of means for causing disruption that could still be qualified as subthreshold. For instance, historical data from 2022 to 2025 shows that Russia is likely to use sabotage of critical civilian and military infrastructure in Europe and cyberattacks on public institutions and private companies. It favours those means that make directly attributing attacks to Russia difficult to prove evidentially and therefore legally. Nor does Russia place a premium on making detection impossible in principle either to signal strength or because of the gap between detection and formal attribution, which often requires courtroom-level incontrovertible evidence.[29] Historical data also shows that China, for the most part, does not engage in active disruption of civilian and military infrastructure in Europe, but it does position itself in IT systems of companies and public institutions in Europe and the US,[30] adopting a disposition for potentially causing disruption (or projecting strength in a different way). It applies a different repertoire of tactics below the radar in the Indo-Pacific, where the term 'grey zone threats' has been applied.[31]

In information warfare these states engage both through their specialised agencies but also through proxies who treat disruption of targeted states, institutions, and societies as a business model. They can be referred to as disruptors for hire.

Ambiguous state actors do not, as a rule, take risks to employ means of physical disruption that allow easy attribution (acts of sabotage by state agents that can be apprehended or identified), as that would mark them publicly as adversaries and might lead to loss of benefits from existing

29 CEPA, *Hesitation Risks Escalation* (Center for European Policy Analysis, 2026).

30 Insikt Group, *Charting China's Climb as a Leading Global Cyber Power*, *Recorded Future*, 2023, https://www.recordedfuture.com/research/charting-chinas-climb-leading-global-cyber-power.

31 A. Insisa, 'Hybrid After All: The "Grey Zone", the "Hybrid Warfare" Debate, and the PLA's Science of Military Strategy', *Defence Strategic Communications* 12 (2023).

DOI 10.30966/2018.RIGA.17.6

strategic alliances. They do, however, increasingly engage in information manipulation aiming to disrupt policies, institutions, and societies in strategic ally countries. They also use disruptors for hire as proxies in their cognitive warfare operations.

Hostile non-state actors include, but are not limited to, the following groups: hacker groups and hacktivist collectives; criminal groups and networks; disposable sabotage proxies; terrorists and terrorist organisations. Cyber operations represent the primary technological vector through which putative hostile states conduct peacetime sabotage. Advanced persistent threat (APT) groups, often tightly integrated with state intelligence services, conduct sophisticated campaigns against critical infrastructure, government institutions, and private sector targets—banks, grid operators, and utility companies, airports, and other transport hubs. Russia's GRU-affiliated[32] Fancy Bear (APT28) and FSB-associated Cozy Bear (APT29) are the best-known cyber APTs, but there are many others. Their operations extend beyond simple data exfiltration to include infrastructure reconnaissance for potential kinetic follow-on operations (cyberattacks). Some of the same structures that conduct these operations are also responsible for information operations, especially those located in the ex-GRU and FSB ecosystem.

Targeting of critical infrastructure is a significant feature of state cyber operations. The power-grid attack in Ukraine in 2015, attributed to Russian state actors, demonstrated the capacity to conduct sabotage on infrastructure during ostensible peacetime, disabling electrical systems serving 230,000 residents.[33] Election interference through cyber means represents another technological vector. At an earlier stage (Russian operations against the 2016 US presidential election) hostile actors combined infrastructure probing with information manipulation and amplification, establishing a template subsequently deployed against

32 As of 2010, the GRU was officially renamed the Main Directorate of the General Staff of the Armed Forces of the Russian Federation; however, the old name is widely used in the literature.

33 R.M. Lee, M. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Electricity Information Sharing and Analysis Center, E-ISAC, 2016).

DOI 10.30966/2018.RIGA.17.6

European elections.[34] Since 2022, critical infrastructure sabotage by kinetic means has also been attributed to actors directly linked to authoritarian states, particularly Russia.[35] The use of drones to paralyse airports has emerged as a new and increasingly frequent way of disrupting large transport hubs, and is attributed to proxy agents of Russia.[36]

Ambiguous state actors do not, as a rule, engage in attributable technological disruption. Exploiting energy asymmetry represents one mechanism through which ambiguous state actors leverage conditional hostility. Hungary's maintenance of energy dependencies on Russian gas supplies, combined with its previous resistance to EU energy independence initiatives, enabled it to extract political concessions from energy-vulnerable alliance partners while maintaining plausible deniability regarding strategic alignment with external adversaries.

Hostile non-state actors employ technological methods that often mirror or exceed state-level sophistication, while maintaining ambiguous attribution and enabling plausible deniability for state sponsors who may coordinate their activities (but not always).[37]

Hacktivist collectives combine political motivation and technical capability. They conduct cyber operations framed as ideological activism while frequently providing operational capabilities accessible to state actors through coordination or outsourcing. Groups such as Cyber Av3ngers, affiliated with Iran's Revolutionary Guard Corps, conduct destructive operations against infrastructure targets, while maintaining ideological framing as resistance to imperialism.[38] The Handala Hack Team similarly

34 R.S. Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (U.S. Department of Justice, 2019).

35 Sahaidachnyi Security Center, https://sahasec.org/tracker.

36 Tamsin Paternoster and Noa Schumann, 'Fact-Checking Europe's "Drone Problem": Why Are Airports Closing over Drone Sightings?', *Euronews*, 20 November 2025, https://www.euronews.com/my-europe/2025/11/20/fact-checking-europes-drone-problem-why-are-airports-shuttering-over-drone-sightings.

37 TNO (Netherlands Organisation for Applied Scientific Research), 'Non-State Actors in Hybrid Conflicts and Campaigns', TNO Report V1925 / TNO-2021-R12556, 2021.

38 Research Special Operations, 'What to Know about CyberAv3ngers: The IRGC-Linked Group Targeting Critical Infrastructure', *Tenable*, 9 April 2026, https://jp.tenable.com/blog/what-to-know-about-cyberav3ngers-the-irgc-linked-group-targeting-critical-infrastructure.

DOI 10.30966/2018.RIGA.17.6

operates with apparent ideological motivation for the Palestinian cause. Anonymous Sudan is a religiously motivated group whose alignment with Russia has been claimed, but most sources see it as independent.[39]

The technical capabilities deployed by hacktivist groups have evolved substantially, with capabilities that were once the exclusive preserve of state-sponsored APT groups having now become available to well-resourced non-state actors. The distinction between ideological collectives, criminal groups, and state-coordinated operations is increasingly blurred. A more recent approach that can be used by aligned and unaligned non-state actors is the manipulation of AI chatbots and other AI-powered technologies. Prompt injection can cause AI systems—both large language models and smaller corporate AI—to override security guardrails and conduct disruptive actions. They may intrude in organisational data systems, launch cyberattacks, or produce textual outputs that are 'poisoned' by adversaries.[40]

But the cyber domain is not the only one where non-state actors operate. Sabotage of undersea cables by shadow fleet ships, arson, and attempts to plant explosives in cargo planes are all examples of less technologically advanced but more kinetic actions undertaken by non-state proxies aligned with hostile states.

All these tactics form the repertoire of hybrid threats and can be reconstructed in a wargame.

39 BBC, 'Anonymous Sudan Hacks X to Put Pressure on Elon Musk over Starlink', 31 August 2023, https://www.bbc.com/news/technology-66668053. See also Cyberint, 'Behind the Mask'.

40 Bolt and Lange-Ionatamišvili, *NextGen Information Environment*.

DOI 10.30966/2018.RIGA.17.6

Constructing Hybrid Threat Scenarios: The Role of the Information Environment

Constructing wargame scenarios focusing on hybrid threats is both a methodological and epistemological task. Not all strains of wargaming are suited to gaming credible hybrid threat scenarios. But this article will focus on two: competitive security wargaming and information environment wargaming.

The 'competitive security gaming' concept, developed by Deon Canyon, reframes wargaming around strategic, operational, and tactical competition rather than pure military conflict. It borrows from the focus of business wargames on competitor behaviour and strategic options, but orients success measures around national security objectives and political-strategic outcomes.[41] It is particularly suited to constructing scenarios with hybrid threat challenges because of its focus on non-kinetic aspects of security. Hence it frames security competition with the aim of achieving outcomes in the economy, societal stability, and internal and external influence. To create a security wargame, Canyon emphasises five principles: urgent threat, coupling of systems, sense-making requirements, consequence management, and complexity. From a strategic communications perspective, the sense-making requirement is the most important: the game must push participants into active interpretation, not just mechanical move-making.[42] Canyon explains sense-making in competitive security wargames in ways that suggest interpretive activities that attempt to influence epistemic states: participants must frame information in ways that make sense to others, and construct and communicate narratives or interpretations that influence other players' perceptions and choices.[43]

41 D. Canyon, *Competitive Security Gaming: Rethinking Wargaming to Provide Competitive Intelligence That Informs Strategic Competition and National Security* (Daniel K. Inouye Asia-Pacific Center for Security Studies, 2020), https://dkiapcss.edu/wp-content/uploads/2020/11/N2542-Canyon-Rethinking-wargames.pdf.

42 Ibid., p. 8.

43 Ibid.

DOI 10.30966/2018.RIGA.17.6

This principle is similar to wargaming the information environment as practised by NATO.[44] And it is rooted in an understanding of strategic communications that focuses on discursive change with a strategic approach to the information environment:

> Strategic Communications is strategic because it focuses on discourse change in the long term. It is strategic because it navigates a dynamic and contested information environment. It is strategic because tactics should be coherent and consistent within a strategy that evolves once the planners' best intentions encounter the friction of real events.[45]

Most wargames do not deal with contestation as a long-term strategy. There are, however, ways of embedding wargame participants' actions in a common understanding of long-term strategic goals. An example of such a method is a matrix which requires that overall the communications narratives of the sides should be informed by common strategic objectives in the information environment. Which can imply both epistemic and behaviour changes.[46]

These dimensions of wargaming are enabled methodologically by modelling the information environment in its complexity, from games simulating social media and news media with injects by game designers, to complex AI-enabled games modelling the reaction of synthetic audiences or digital twins of real social groups.[47] This level of simulation is heavily dependent on data about the groups, whose behaviour is modelled in the AI-enabled environment. It could be described as a higher order of AI avatars of social media users with a set of parameters like age,

44 Canadian Army, 'Wargaming the Information Environment', *Canadian Army Today, 20 March 2023,* https://canadianarmytoday.com/wargaming-the-information-environment.

45 N. Bolt, *Strategic Communications and Disinformation in the Early 21st Century*, RSC Policy Paper 2021/12 (European University Institute, 2021), p. 4.

46 Based on anonymised interview with strategic communications wargaming expert, formerly of NATO StratCom COE, 2023.

47 A. Bruzzone et al., 'Audience Behavior Modeling for Cognitive Warfare Training in Multidomain Environments'. *Procedia Computer Science* 274 (2025).

DOI 10.30966/2018.RIGA.17.6

gender, social status, education, and political views, creating a synthetic personality. Such synthetic individuals respond to information in the game in a manner that matches the response of their original human prototypes with a high degree of probability.

A bigger challenge, however, is presented by (re)constructing the motivation of threat actors.

Constructing Hybrid Threat Actors

Wargaming both reconstructs and reveals prototypical patterns of behaviour in contested environments. Wargames necessarily establish parameters of expected behaviour through scenario settings, capabilities ascribed to players, and team briefings. At the same time, they still allow space for diverging game outcomes through player agency. The construction of hybrid threat actors in competitive security wargames and/or information environment wargames, however, comes up against an epistemological obstacle. There is insufficient research about the motivations of different kinds of international security actors.

As a recent study reminds us:

> foreign policies are not monolithic, coherent endeavours but the aggregate of the actions of—sometimes more, sometimes less streamlined—agencies and people (politicians and bureaucrats) with differing rationales. In addition, finding reliable data on the motivations behind foreign policy actions is inherently difficult, especially in closed, authoritarian systems, such as China and Russia.[48]

48 N. Balbon and J. Friedrich, *Rationales in the Dark: Empirical Oversights in Assessing Russian and Chinese Influence in the Western Balkans and EU's Eastern Neighbourhood*. REUNIR Occasional Paper 2, 2026, https://reunir-horizon.eu/wp-content/uploads/2026/04/Niklas-Balbon_Julia-Friedrich_REUNIR-OCCASIONAL-PAPER_.docx_compressed.pdf.

DOI 10.30966/2018.RIGA.17.6

The same could be said, with a great deal of confidence, about the motivations of non-state actors.

This leads us to a crucial aspect of behaviour in hybrid threat actors—their employment of strategic ambiguity. While some researchers link strategic ambiguity—deliberate cultivation of vagueness or contradictory signals to complicate adversaries' decision-making—to plausible deniability,[49] other possible reasons for its use also exist. Strategic ambiguity in political communication allows for the capture of a bigger and more diverse audience.[50] And authoritarian regimes have perfected this approach by applying 'strategic differentiation'—crafting distinct government communications across different platforms for different audiences.[51] Democratic actors, too, use strategic ambiguity to achieve their political goals.

A wargame's analytical relevance depends on how closely it models the factors and conditions that shape real-world conflicts and crises. Accurate representation of actors is likely to lead to a more analytically useful result. This presents a challenge in hybrid threat scenarios. A red team's course of action has to reflect the behaviour of hybrid threat actors whose objectives in reality are often obscure.

The range of actors in hybrid warfare has become much broader with the fracturing of the liberal international order, and includes, at the very least, hostile state actors, ambiguous state actors, and hostile non-state actors (hacktivists, criminal groups, and networks). By *ambiguous state actors*, this article implies strategic allies that undertake, under certain circumstances, hostile actions in one of the domains of hybrid warfare, e.g. energy blackmail or foreign information manipulation campaigns, against ally countries. Hungary's foreign information manipulation and influence (FIMI) campaigns against the EU, Ukraine, and NATO

49 C. Campbell, 'Russian Strategic Ambiguity as a Tactic for Desecuritization: A Case Study of the Ukrainian Conflict' (University of Tartu Euro College: master's thesis, 2015).

50 Bach et al., 'Let Me Be Perfectly Unclear'.

51 Duoji Jiang, 'Converging Discourse, Diverging Audiences: Authoritarian Propaganda with Strategic Differentiation' (University of Chicago: master's thesis, 2025).

DOI 10.30966/2018.RIGA.17.6

countries, and US posture on a possible military takeover of Greenland, are examples of situations when strategic allies can be categorised as 'ambiguous state actors' because they no longer behave in conformity with shared norms and strategic goals.

Ambiguous state actors occupy a paradoxical strategic position: they maintain formal alliance relationships and shared security interests, while simultaneously pursuing hostile policies against alliance partners in specific domains. This ambiguity derives from several sources: incomplete preference alignment on specific issues, domestic political constraints limiting strategic flexibility, and the exploitation of asymmetric vulnerabilities in alliance structures.

Each of these broad categories of actors uses hybrid warfare for different objectives and by different means. A wargame scenario and setting has to reflect these objectives and means fairly accurately, in order to have analytical relevance.

Almost all these actors can and do engage in the information environment as much as in other domains—technological, economic, and military. Moreover, their actions in other domains are often intended to have an effect in the information environment—witness successful acts of sabotage projecting the 'weakness' of Western governments and their critical infrastructure.

The real challenge for information environment wargaming lies not in rendering the technological tactics of disruptive actors, rather in the strategic objectives they pursue. The whole strategic communications paradigm requires that actors have strategic objectives. It does not require, however, that those objectives be specifically *geo*strategic.[52]

As multiple examples of threat actors and their activities described above attest, in the new threat landscape not all hostile actors have geostrategic objectives. Strategic objectives are manifest in other ways: in narrative

52 Gray and Sloan, Geopolitics, *Geography and Strategy*.

DOI 10.30966/2018.RIGA.17.6

domination, diffusion or erasure of the liberal democratic order, identity building, and any number of other objectives that political, technological, or military actors may wish to achieve over time. This runs contrary to the geostrategic framework implied in the RAND report on grey zone threats or in the NATO StratCom COE Hybrid Toolkit.[53] But in the few years since their publication, the threat landscape has developed in a number of directions.

Even the most established category of threat actors—authoritarian regimes—do not always act with a clear strategy when they disrupt other countries, societies, and institutions. Authoritarian powers, particularly China and Russia, deploy what scholars term 'sharp power' to penetrate, manipulate, and corrode democratic institutions, norms, and information environments without necessarily pursuing territorial gains or traditional strategic objectives.[54] A growing body of studies suggests that such efforts could be seen instead as part of a wider pattern of hostility towards liberal democracy as a competing model of governance. This is referred to as normative contestation, which involves using mechanisms once found at the core of the international liberal order, such as the UN, to undermine human rights and to legitimise repressive practices.[55]

Normative contestation can be pursued by undermining the security, cohesion, and everyday functioning of society through hybrid attacks, without having the goal of escalating to kinetic warfare. Recent literature marks a shift away from the consensus that authoritarian regimes pursue primarily geostrategic goals in their foreign and security policy. As pointed out by Thomas Risse, a key driver of 'deep contestation' of the liberal international order is 'the survival interests of autocratic regimes in the

53 Morris et al., *Gaining Competitive Advantage*; B. Heap, P. Hansen, and M. Gill, *Strategic Communications Hybrid Threats Toolkit (*NATO Strategic Communications Centre of Excellence, 2021), https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213.

54 C. Walker and J. Ludwig, *Sharp Power: Rising Authoritarian Influence (National Endowment for Democracy,* 2017), https://www.ned.org/wp-content/uploads/2017/12/Introduction-Sharp-Power-Rising-Authoritarian-Influence.pdf.

55 S. Joshi, *Authoritarian Challenges to the Liberal Order* (Tony Blair Institute for Global Change, 2018), https://institute.global/insights/geopolitics-and-security/authoritarian-challenges-liberal-order.

DOI 10.30966/2018.RIGA.17.6

current world order that are directly threatened by political liberalism'.[56] Disruption of daily life and functioning of democratic societies thus becomes a goal in itself, and can be a plausible explanation for multiple and growing hybrid attacks on Europe not only by Russia but also by other authoritarian state actors.[57]

Disruption of 'enemy' societies is also seen as rich material for information campaigns targeting domestic audiences in authoritarian countries. Witness Russia's campaign to portray Europe as freezing after turning away from consuming Russian gas.[58] More direct and conventional propaganda of rejoicing at the devastation caused to enemies has been part of the output of hacktivist collectives like Handala (Palestine) and Killnet (Russia).

In the world of volatile strategic alliances and crumbling international order, a wargame scenario should not always model threat actors with clear geostrategic objectives. Sometimes disruption per se is their primary and ultimate objective. Nevertheless, the decision to mirror real-life scenarios where disruption is caused by a hostile actor without a clear geostrategic objective presents several challenges to wargame designers.

The first challenge is a *credibility gap.* The scenario of a wargame is, in essence, a fiction. It has to comply with the same rules of credibility that apply to fiction. Namely, narrative transportation[59] that allows the participants to focus on the reality of the game and suspend their disbelief. To act in a setting of artifice, participants must disregard the fact that there is no real country named Arcana, that there is no North Atlantic Council meeting happening on the day of the game,

56 T. Risse, 'Conclusions: Deep Contestations and the Resilience of the Liberal International Order', in A. Wiener, D.A. Lake and T. Risse (eds), *Deep Contestations of the Liberal International Order* (Oxford University Press, 2026).

57 See C. Edwards, *The Scale of Russian Sabotage Operations against Europe's Critical Infrastructure* (International Institute of Strategic Studies, 2025), https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf.

58 D. Shcherba, '"The West Is Freezing": Russia Wants Others to Suffer without Its Gas', *UkraineWorld, 20 December* 2022, https://ukraineworld.org/en/articles/analysis/ru-west-freezing.

59 M.C. Green and M. Appel, 'Narrative Transportation: How Stories Shape How We See Ourselves and the World', *Advances in Experimental Social Psychology* 70 (2024): 1–82.

DOI 10.30966/2018.RIGA.17.6

that there is no drone attack reported in actual media. And then act as if all of these circumstances were true. Narrative transportation needs understandable motives ascribed to all actors, because narrative thought is a way of making meaning, including making sense of people and their intentions.[60] If there is no identifiable objective pursued by a hostile actor or a red team in the scenario, this obstructs sense-making and creates a credibility gap in the narrative, lowering participants' engagement.

One of the ways to avoid this pitfall is to elaborate the ideological framework relied upon by the hostile or ambiguous actors, offering an explanation for their disruptive behaviour. Even though their course of action exhibits no geostrategic objectives, it can preserve logical tact and credibility through adherence to a specific set of ideological tenets that have to be made known to the participants. Thus, for instance, if the red team is modelling an AI enterprise led by a visionary bent on ending liberal democracy, and the scenario involves major disruptions caused by this leader and their followers, the players in the blue team should be exposed to the ideology of this leader through texts, videos, or other sources prior to the game or in the early stages of the game, before they engage in preventing or deterring the disruption caused by this actor.

The second challenge is the need to reflect, for analytical purposes, the behaviour of hybrid threat actors that lean towards *strategic ambiguity.*

There is no clarity regarding the nature and scope of strategic objectives of hybrid threat actors among Western political actors and institutions—as illustrated by Janičatová and Mlejnkova, who empirically examine how ambiguity is perceived and narrated in Western institutional responses.[61] More recently Balbon and Friedrich have analysed an extensive body of literature on foreign influencing and concluded that 'it largely neglects the question of rationales as a dedicated research focus. Existing scholarship assigns various motivations for China's and Russia's foreign influencing

60 J. Bruner, *Actual Minds, Possible Worlds* (Harvard University Press, 1986).

61 S. Janičatová and P. Mlejnkova, 'The Ambiguity of Hybrid Warfare: A Qualitative Content Analysis of the United Kingdom's Political–Military Discourse on Russia's Hostile Activities', *Contemporary Security Policy* 42 № 3 (2021): 312–44.

DOI 10.30966/2018.RIGA.17.6

behaviours, but these explanations remain underdeveloped in terms of systematic empirical investigation'.[62] Rationales behind the actions of various parts of authoritarian governments are often ascribed on the basis of overarching historical theories of their actions. They explain the tactics of Russian hybrid attacks as a continuation of Soviet spy practices without taking into account multiple dimensions of technological, political, and social factors that have shaped current practices.

While wargaming cannot substitute for empirical investigation of hybrid threat actors, it should at least construct their course of action based on a defined set of objectives, even if those are intentionally obscured. For wargaming purposes, to reconstruct an approach of strategic differentiation or to create ambiguity in the tactics of threat actors aiming at plausible deniability is equally possible. It requires simulating multiple information channels intended for different target audiences. Wargames that make use of simulation environments of augmented reality—such as Conducttr, Prevency, and Meleys[63]—can easily ensure that participants are exposed to several simulated social media platforms, blogs, and media outlets used by threat actors to create differentiated narratives.

In one hybrid threat scenario wargame designed by the author, the threat actors—played by two red teams—represented a unit of the GRU, responsible for sabotage and information manipulation campaigns, and a media agency from the Western Balkans, a 'disruptor for hire' responsible for amplifying narratives. Rather than focus their information campaigns on a single strategic objective, they created an ecosystem of social media profiles, blogs, and partnerships with (unsuspecting) media, and used this ecosystem to pursue a set of separate objectives which together sought to change the meaning of national security for different audiences inside the country. Different tactics were employed to pursue individual objectives under this strategy. A series of blogs by co-opted influencers created moral panic about illegal migration at the land border. Individual members

62 Balbon and Friedrich, *Rationales*.

63 Conducttr, www.conducttr.com; Prevency, https://prevency.com/en; Meleys, https://meley-s.com.

of government were attacked in a series of hard-to-verify claims of corruption or neglect. And campaigns featuring NATO and the EU as threats to national sovereignty were conducted on social media. While the messages and storylines of multiple campaigns were not mutually coherent, strategic differentiation worked in ways a unified, coherent set of narratives could not achieve. The perceived need to respond to each of the campaigns drained resources available to government players (such as communications staff time), and campaigns exaggerating the risk presented by migration drew the attention of politicians away from other security vulnerabilities. These two factors combined to reduce the government's ability to pursue defined national security priorities in a situation of escalating threat.

To sum up, constructing the behaviour and objectives of hybrid threat actors is a useful but complex task for wargame scenario design. It is not limited to the realistic modelling of their TTPs. Constructing relevant objectives pursued by both state and non-state actors is an important part of creating analytical value. In this regard, representing ambiguous or unclear, non-geostrategic objectives, such as ideologically driven or competition-driven disruption, presents a particular challenge. Wargame scenario design can and should avoid credibility gaps in presenting the objectives of hybrid threat actors, and should make expert use of strategic ambiguity and strategic differentiation.

Bibliography

Bach, P., Schmitt, C., and McGregor, S.C. 'Let Me Be Perfectly Unclear: Strategic Ambiguity in Political Communication', *Communication Theory* 35 Nº 2 (2025): 96–106.

Balbon, N., and Friedrich, J., *Rationales in the Dark: Empirical Oversights in Assessing Russian and Chinese Influence in the Western Balkans and EU's Eastern Neighbourhood*, REUNIR Occasional Paper 2, 2026, https://reunir-horizon.eu/wp-content/uploads/2026/04/Niklas-Balbon_Julia-Friedrich_REUNIR-OCCASIONAL-PAPER_.docx_compressed.pdf.

BBC, 'Anonymous Sudan Hacks X to Put Pressure on Elon Musk over Starlink', 31 August 2023, www.bbc.com/news/technology-66668053.

Bolt, N., 'Foreword: Is This the Age of Disinformation or the Age of Strategic Communications?', *Defence Strategic Communications* 14 (2024).

Bolt, N. (ed.), 'Strategic Ambiguity', Special Issue, *Defence Strategic Communications* 12 (Spring 2023).

Bolt, N., *Strategic Communications and Disinformation in the Early 21st Century*, RSC Policy Paper 2021/12 (European University Institute, 2021), p. 4.

DOI 10.30966/2018.RIGA.17.6

Bolt, N., and Lange-Ionatamišvili, E., *The NextGen Information Environment* (NATO Strategic Communications Centre of Excellence, 2026).

Bruner, J., *Actual Minds, Possible Worlds* (Harvard University Press, 1986).

Bruzzone, A., et al., 'Audience Behavior Modeling for Cognitive Warfare Training in Multidomain Environments', *Procedia Computer Science* 274 (2025).

Campbell, C., 'Russian Strategic Ambiguity as a Tactic for Desecuritization: A Case Study of the Ukrainian Conflict' (University of Tartu Euro College: master's thesis, 2015).

Canadian Army, 'Wargaming the Information Environment', *Canadian Army Today,* 20 March 2023, https://canadianarmytoday.com/wargaming-the-information-environment.

Canyon, D., *Competitive Security Gaming: Rethinking Wargaming to Provide Competitive Intelligence That Informs Strategic Competition and National Security (*Daniel K. Inouye Asia-Pacific Center for Security Studies, 2020), https://dkiapcss.edu/wp-content/uploads/2020/11/N2542-Canyon-Rethinking-wargames.pdf.

CEPA, *Hesitation Risks Escalation* (Center for European Policy Analysis, 2026).

CheckFirst, 'Unveiling GRU's Information Operations Troops with OSINT and Medals', 9 February 2026, https://checkfirst.network/unveiling-grus-information-operations-troops-with-osint-and-medals.

Cyberint, 'Behind the Mask of Anonymous Sudan: An Analysis', 2023, https://cyberint.com/blog/research/anonymous-sudan-an-analysis.

Downes-Martin, S., et al., *Distributed Wargaming*, Report of the Simulation Interoperability Standards Organization (SISO) Wargaming Study Group (SISO, 2021), https://paxsims.wordpress.com/wp-content/uploads/2021/08/distributed-wargaming-siso-report-final-20210823-v2-1.pdf [accessed 11 May 2026].

Duoji Jiang, 'Converging Discourse, Diverging Audiences: Authoritarian Propaganda with Strategic Differentiation' (University of Chicago: master's thesis, 2025).

Edwards, C., *The Scale of Russian Sabotage Operations against Europe's Critical Infrastructure* (International Institute for Strategic Studies, 2025), https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf.

European Council, *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats—a European Union Response*, 2016.

European External Action Service, *4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats* (EEAS, 2026), https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en.

Fearon, J.D., and Laitin, D.D., 'Ethnicity, Insurgency, and Civil War', *American Political Science Review* 97 Nº 1 (2003).

Freedman, L., *Strategy: A History* (Oxford University Press, 2013).

Gray, C.S., and Sloan, G. (eds), *Geopolitics, Geography and Strategy* (Frank Cass, 1999).

Green, M.C., and Appel, M., 'Narrative Transportation: How Stories Shape How We See Ourselves and the World', *Advances in Experimental Social Psychology* 70 (2024): 1–82.

Hagenloch, T., '"Game On!" A Research Project on the Prussian Kriegsspiel', *British Journal of Military History* 7 Nº 2 (2021).

Heap B., Hansen P., and Gill M., *Strategic Communications Hybrid Threats Toolkit (*NATO Strategic Communications Centre of Excellence, 2021), https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213.

Hoffman, F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars* (Potomac Institute for Policy Studies, 2007).

Insikt Group, *Charting China's Climb as a Leading Global Cyber Power*, *Recorded Future*, 2023, https://www.recordedfuture.com/research/charting-chinas-climb-leading-global-cyber-power.

Insisa, A., 'Hybrid After All: The "Grey Zone", the "Hybrid Warfare" Debate, and the PLA's Science of Military Strategy', *Defence Strategic Communications* 12 (2023).

Janičatová, S., and Mlejnkova, P., 'The Ambiguity of Hybrid Warfare: A Qualitative Content Analysis of the United Kingdom's Political-Military Discourse on Russia's Hostile Activities', *Contemporary Security Policy* 42 Nº 3 (2021): 312–44.

Joshi, S., *Authoritarian Challenges to the Liberal Order* (Tony Blair Institute for Global Change, 2018), https://institute.global/insights/geopolitics-and-security/authoritarian-challenges-liberal-order.

Kalyvas, S.N., *The Logic of Violence in Civil War* (Cambridge University Press, 2006).

Kuehn, A., 'Assessment Strategies for Educational Wargames', *Journal of Advanced Military Studies* 12 Nº 2 (2021), https://www.usmcu.edu/Portals/218/5_JAMS_12_2_Kuehn_1.pdf.

Lee, R.M., Assante, M., and Conway, T., *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Electricity Information Sharing and Analysis Center, E-ISAC, 2016).

Lin-Greenberg, E., Pauly, R., and Schneider, J.G., 'Wargaming for International Relations Research', *European Journal of International Relations* 28 Nº 1 (2022).

Lipinska, J., 'Strategic Communication in the Face of Contemporary Threats to the Information Environment', *Humanities and Social Sciences* 28 Nº 4 (2021).

Morris, L.J., et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression below the Threshold of Major War* (RAND Corporation, 2019).

Mueller, R.S., *Report on the Investigation into Russian Interference in the 2016 Presidential Election (*U.S. Department of Justice, 2019).

Mumford, A., *Ambiguity in Hybrid Warfare*, Hybrid CoE Strategic Analysis 24 (Hybrid CoE, 2020).

Mumford, A., and Carlucci, P., 'Hybrid Warfare: the Continuation of Ambiguity by Other Means', *European Journal of International Security* 8 Nº 2 (2023): 192–206.

Perla, P., *The Art of Wargaming: A Guide for Professionals and Hobbyists* (Naval Institute Press, 1990).

Research Special Operations, 'What to Know about CyberAv3ngers: The IRGC-Linked Group Targeting Critical Infrastructure', *Tenable*, 9 April 2026, https://jp.tenable.com/blog/what-to-know-about-cyberav3ngers-the-irgc-linked-group-targeting-critical-infrastructure.

Risse, T., 'Conclusions: Deep Contestations and the Resilience of the Liberal International Order', in A. Wiener, D.A. Lake, and T. Risse (eds), *Deep Contestations of the Liberal International Order* (Oxford University Press, 2026).

Sahaidachnyi Security Center, 'The Everywhere War: Sub-Threshold Warfare Tracker', https://sahasec.org/tracker/.

Schneider, J., '*Cyber and Crisis Escalation: Insights from Wargaming'*, U.S. Naval War College, 2017, https://paxsims.files.wordpress.com/2017/01/paper-cyber-and-crisis-escalation-insights-from-wargaming-schneider.pdf.

Schwartz, C., '*Access Denied* and *Sector Down*: Introducing Resilience Games for Critical Infrastructure Preparedness', *Cyber Defense Review* 10 Nº 2 (2025): 163–78, https://cyberdefensereview.army.mil/Portals/6/Documents/2025-vol10-iss2/CDR_V10_N2_Schwartz_ResGames_RA_IP.pdf.

Shcherba, Dzvenyslava, '"The West Is Freezing": Russia Wants Others to Suffer without Its Gas', *UkraineWorld*, 20 December 2022, https://ukraineworld.org/en/articles/analysis/ru-west-freezing.

Sky News, *The Wargame*, podcast series, 2025, https://open.spotify.com/show/4lHtW6x1D6R0E1QmGLkBK1.

What Does It Take to Release a Political Prisoner?

A Review Essay by Natalya Kovaleva

Entry Point—123
Museum of Free Belarus, Warsaw, 20 January – 1 March 2026.

Keywords—*political prisoners, hostage diplomacy, Belarus, US foreign policy, authoritarian legitimisation, values-based communication, strategic communication, strategic communications*

About the Author
Natalya Kovaleva is a New Generation Europe Foundation Academy Fellow at Chatham House, where her research focuses on political prisoner diplomacy and the dynamics of international negotiations under conditions of sanctions and isolation.[1]

'They kept saying, "Someone like you will never get out of here alive." And I believed them.' We sat in an eerily empty coffee shop in Vilnius; my companion had paused over her coffee.

It was a standard line, apparently. The kind used by prison security officers to erode the hope of many Belarusian political prisoners who were arrested following the mass protests of 2020 and 2021. The largest in the country's post-Soviet history, they erupted after Alyaksandr Lukashenka claimed victory in a presidential election widely deemed fraudulent. What followed was a sweeping crackdown: arrests, repression, and international condemnation. Yet some, like the woman sitting across from me, got out. On 13 December 2025, after months of quiet negotiations between Minsk

1 The views expressed in this essay are exclusively those of the author.

DOI 10.30966/2018.RIGA.17.7

and Washington, she was among 123 political prisoners released and deported from Belarus.

With balaclavas over their heads and hands tied with tape, they were taken across the border into Ukraine. From there, they moved on to cities where Belarusian exile had already taken root: Vilnius, Warsaw, Berlin. The exhibition *Entry Point—123* at the Museum of Free Belarus in Warsaw gathered more than thirty objects that made that same journey.

An aluminium spoon. A rusted coil heater. A small waffle towel labelled with its owner's surname. A jacket much too thin for the Belarusian winter. Once ordinary fixtures of prison life, these items are now among the few records their owners have of the years spent in detention. Many were stripped of their possessions on departure, their diaries and manuscripts confiscated in an attempt to erase the inner life that the state found threatening even at the point of expulsion.

Some, though, managed to smuggle out what mattered. Among the most striking objects in the exhibition was a 'mutka'—a small pouch fashioned from the film lining of a cigarette packet. Often filled with coffee, tea, or sugar, it could circulate as prison currency or be kept as a private reserve. Beside it sat a transparent plastic bag knotted at the centre. One side held two teabags, the other—a matchbox concealing a deck of handmade playing cards. A forbidden item smuggled out in the haste of abrupt departure. The very presence of such items, with little value beyond the prison walls, in a Warsaw exhibition hall implies their owners did not think they were being released; rather, moved to another facility, where a few grams of coffee or a small deck of cards could prove useful.

Phased releases of political prisoners have become a key feature of US–Belarus dialogue in recent years, making it perhaps the most productive American diplomatic effort in the region. Each round of talks has been followed by a release of a group of people—human rights and pro-democracy activists, journalists, opposition figures, foreign

DOI 10.30966/2018.RIGA.17.7

Source: Museum of Free Belarus

DOI 10.30966/2018.RIGA.17.7

nationals, and just ordinary Belarusians who joined the 2020 protests or spoke out about them online. Since July 2024 over 500 people have been freed on the back of these negotiations, with up to 900 political prisoners still behind bars. Many—like the group of 123 released in December 2025—have been deported from Belarus with no way of return. Stripped of their country, the chance to see their families, and even identification documents vital for setting up their new life, they have suddenly found themselves in exile.

The importance of saving lives as part of this diplomatic effort cannot be overstated—tangible humanitarian outcomes speak for themselves. Yet it is worth interrogating what lies behind these stated humanitarian aspirations, what interests are shaping this unlikely diplomatic engagement on both sides, and—most pressingly—whether Western engagement could balance important short-term outcomes with the risks of entrenching this practice in the long run. If the goal is to release all political prisoners, what would give a regime any reason to stop taking them? The answer requires an understanding of how the Belarusian regime arrived at this point, and how long it has been on its way.

Political Imprisonment in Belarus

Political imprisonment is not a new tool in Lukashenka's arsenal. Having stayed in power since 1994, he has systematically used it to remove opponents, intimidate the opposition, and deter dissent. In the run-up to his first re-election in 2001, the OSCE's observation mission documented 100 cases of political intimidation and harassment across the country, including arbitrary detentions and arrests.[2] By the next presidential election in 2006, Lukashenka had begun targeting his key opponents. Among them was Alyaksandr Milinkyevich, the candidate endorsed by the main opposition bloc, who saw eight of his representatives detained

2 OSCE/ODIHR, Republic of Belarus: Presidential Election, 9 September 2001 (Warsaw, OSCE/ODIHR Election Observation Mission Report, 2001), p. 14.

DOI 10.30966/2018.RIGA.17.7

Source: Museum of Free Belarus

DOI 10.30966/2018.RIGA.17.7

or arrested days before the polls opened.[3] The head of the KGB, the Chief Prosecutor, and the Interior Minister would later declare that the arrests had been necessary to avert a violent coup staged by the opposition 'under the guise of elections'. Anyone who protested on election day, they warned, would be 'considered as terrorists under Article 289 of the penal code'.[4]

Still, protests followed. Within days, another presidential candidate, Alyaksandr Kazulin, was detained. Within weeks, he was sentenced to five and a half years in prison for hooliganism and incitement of mass disorder.[5] In 2010, state repression went further. Seven out of nine candidates were arrested and subjected to interrogations by the KGB in the aftermath of that year's election, alongside almost 700 protesters, journalists, and civil society activists.[6] Running against the incumbent had become, in effect, a criminal act.

Citing external interference and incitement of a revolution, in 2020 Lukashenka cleared the ballot of strong candidates months before the election. Detention orders came for prominent critics of the regime and key rivals, including Siarhei Tsikhanouski, a popular blogger and pro-democracy activist who was arrested days after announcing his intention to run for the presidency. His wife, Sviatlana Tsikhanouskaya, ran in his stead, uniting behind her diverse opposition groups that had been stripped of their leadership. When Lukashenka declared himself the winner with over 80 per cent of the vote, few believed the result. Hundreds of thousands took to the streets across the country in protest. Almost 7000 people were detained in the first four days alone—beaten in police vans, held in degrading conditions, tortured in detention centres.[7] Beyond neutralising immediate opposition, these arrests had a longer

3 OSCE/ODIHR, Republic of Belarus: Presidential Election, 19 March 2006 (Warsaw, OSCE/ODIHR Election Observation Mission Report, 2006), p. 16.

4 Ibid.

5 'Belarus Opposition Leader Jailed', *BBC News*, 14 July 2006, http://news.bbc.co.uk/1/hi/world/europe/5178714.stm.

6 OSCE/ODIHR, Republic of Belarus: Presidential Election, 11 October 2015 (Warsaw, OSCE/ODIHR Election Observation Mission Report, 2015), pp. 7, 23.

7 'Belarus: Unprecedented Crackdown', *Human Rights Watch*, 13 January 2021, https://www.hrw.org/news/2021/01/13/belarus-unprecedented-crackdown.

DOI 10.30966/2018.RIGA.17.7

purpose: under Belarusian law each conviction carried a lifetime ban from running for office. The crackdown was also the largest Belarus had ever produced, and the hardest for the outside world to ignore.

This ever-intensifying pattern of repression has long had an external audience. Each high-profile arrest drew international condemnation. Each wave of sanctions amplified the pressure on an increasingly isolated regime. Over three decades Lukashenka has learned to convert that pressure into leverage.

The first test came in August 2008. Minsk released three political prisoners—former presidential candidate Kazulin, youth activist Andrey Kim, and businessman Siarhei Parsiukevich—and called it a gesture of goodwill ahead of the parliamentary elections. The US delegation arrived in the capital for high-level talks within days. Loans worth USD 3.5 billion from the International Monetary Fund followed shortly after. In 2015 six others were pardoned ahead of the presidential election. The EU, which had long insisted on the release, lifted individual sanctions on almost 140 Belarusian officials in response—even as the OSCE found that the election had fallen short of democratic standards. These early opportunistic releases, designed to soften Lukashenka's image domestically while easing external pressure, confirmed the utility of political prisoners as leverage in diplomatic negotiations.

The 2020 crackdown and the growing international isolation of Belarus in its aftermath created fertile ground for the regime to transform political prisoner diplomacy into a fully fledged foreign policy tool. The brutal handling of the election sparked a wave of criticism and new sanctions against the regime, with the EU refusing to recognise Lukashenka's legitimacy. His decision to force a Ryanair passenger flight to land in Minsk to arrest journalist Raman Pratasyevich in May 2021 drew near-universal condemnation, triggering another wave of European sanctions. More restrictions were imposed in connection with Minsk's assistance to Russia in the latter's war against Ukraine, which was launched in part from Belarusian territory. By 2022 Belarus faced a level of Western

sanctions unprecedented in its post-Soviet history. Meanwhile, the prison population swelled, with the number of politically motivated arrests reaching 1500 people by April 2023.[8] Among them were pro-democracy and human rights activists, journalists, and foreign nationals whose cases drew sustained attention in Western capitals.

It was these people that Lukashenka would eventually bring to the negotiating table to find his way out of economic and diplomatic isolation.

A Perfect Storm

When thinking about hostage diplomacy, it is easy to default to a transactional logic. To evoke an image of a Cold War prisoner swap on the Glienicke Bridge in Berlin: people exchanged by warring sides in the dark of night. This familiar template is used to this day. Famously in August 2024 the Kremlin swapped detained Americans, including the *Wall Street Journal* reporter Evan Gershkovich and former US Marine Paul Whelan, along with several Russian opposition figures, for its agents and criminals held in detention across the world. It became the largest international prisoner exchange since the Cold War. Yet the scale and continuity of what the Belarusian regime has achieved in recent years are arguably unprecedented in modern diplomacy.

With few diplomatic options available amid Minsk's profound isolation, Lukashenka turned to hostage diplomacy as a primary instrument of political communication. At first, it was used to signal openness to dialogue and create favourable conditions for negotiations.

Unilateral pardons began in July 2024, loosely coinciding with backchannel talks with representatives of the Biden administration.[9]

8 'Political Prisoner Count in Belarus Hits 1,500 people', *Viasna*, 21 April 2023, https://spring96.org/en/news/111494.

9 By May 2025, 300 political prisoners were pardoned by the regime, presumably in an attempt to soften its image domestically ahead of elections and to signal readiness for dialogue with Western partners. '42 More Political Prisoners Pardoned in Belarus', *Viasna*, 8 May 2025, https://spring96.org/en/news/117925.

DOI 10.30966/2018.RIGA.17.7

Yet no high-profile releases occurred until Donald Trump arrived in office. Anastasia Nuhfer was among the first US citizens to be freed from detention. Her sudden release in January 2025 took place on the day of a disputed presidential election in Belarus and within a week of Trump's inauguration. It quickly grabbed the attention of US officials. The same day, Secretary of State Marco Rubio announced the news on social media: 'Thanks to @POTUS leadership, Belarus just unilaterally released an innocent American, ANASTASSIA Nuhfer, who was taken under JOE BIDEN!'[10] Quickly translated into a political win, the release spoke to Trump's key foreign policy commitment of bringing home Americans wrongfully detained abroad.[11]

Suddenly there was an opening. In February 2025 Deputy Assistant Secretary of State Christopher Smith arrived in Minsk, becoming the most senior US official to visit Belarus in over five years. A US citizen and two Belarusian political prisoners were released as a result. Yuri Zenkovich, the only remaining political prisoner with American citizenship, was freed in April. These early exchanges showed that Washington's talks with Minsk delivered clear and measurable results, however humble the releases. A regular rhythm of negotiations injected enough confidence on both sides to continue, eventually turning ad hoc meetings into a dedicated and sustained diplomatic track. Before the end of the year, three more releases of political prisoners and foreign nationals followed, each greater than the last: 14 in June, 52 in September, and 123 in December. What began as a signal of openness became something much more ambitious. A dedicated diplomatic track promised to boost legitimacy, offered a way out of diplomatic isolation, and delivered US sanctions relief.

The intensity of US engagement has—so far—amplified with each release, satisfying Lukashenka's desire to emerge from isolation. The diplomacy of

10 Secretary Marco Rubio (@SecRubio), post on X, 26 January 2025, https://x.com/SecRubio/status/1883501830182948893.

11 In 2025 efforts to release Americans detained abroad were expanded alongside the power of the Secretary of State, who was authorised to designate foreign states or non-state actors as 'State Sponsors of Wrongful Detention' and impose penalties, including sanctions, travel restrictions, and export controls.

DOI 10.30966/2018.RIGA.17.7

dealmaking embraced by Trump, which gives little consideration to the human rights record of those who sit across the table, has raised questions in the EU of whether to follow suit, inadvertently normalising dealings with Belarus on the international stage. The June 2025 talks made clear that Minsk was ready to make concessions to keep Americans engaged. Then, following a meeting with the US Special Envoy for Ukraine, Keith Kellogg, Lukashenka unexpectedly released Siarhei Tsikhanouski, one of the regime's most defiant critics and a prominent leader of the 2020 protests. The message was clear: no political prisoner is off limits, and more of the opposition's heavyweights can be released if talks continue. Ultimately this diplomatic relationship became a legitimising one for Lukashenka, especially since Trump openly recognised him as a counterpart, despite the contrary position of the EU and its allies, which have avoided referring to the Belarusian leader as 'president' since 2020.[12] On one occasion Trump posted on social media:

> I had a wonderful talk with the highly respected President of Belarus, Aleksandr Lukashenko. The purpose of the call was to thank him for the release of 16 prisoners. We are also discussing the release of 1,300 additional prisoners. Our conversation was a very good one. We discussed many topics, including President Putin's visit to Alaska. I look forward to meeting President Lukashenko in the future. Thank you for your attention to this matter![13]

Having spent years as an outsider, Lukashenka managed to emerge as a counterpart, if only for Trump. The reference to Putin's Alaska visit underscored Minsk's potential utility as an interlocutor in the wider Russia–Ukraine settlement—an unlikely yet desirable role promising to restore Lukashenka's regional legitimacy.

12 EEAS Press Team, 'Belarus: Joint Statement by the EU, Australia, Canada, New Zealand and the UK on the Sham Presidential Elections', 27 January 2025, https://www.eeas.europa.eu/eeas/belarus-joint-statement-eu-australia-canada-new-zealand-and-uk-sham-presidential-elections_en.

13 Donald J. Trump (@realDonaldTrump), post on Truth Social, 15 August 2025, https://truthsocial.com/@realDonaldTrump/posts/115033133751064517.

DOI 10.30966/2018.RIGA.17.7

In November 2025 Trump nominated John Coale, an American lawyer who helped negotiate earlier releases, as the US special envoy to Belarus. The appointment signalled that the bilateral engagement was hardening into a sustained diplomatic relationship. Trump's post announcing the nomination made the appeal of this arrangement clear: 'He has already successfully negotiated the release of 100 Hostages, and is going for an additional 50.'[14] Releases of political prisoners, in other words, were delivering the kind of measurable outcomes that the US administration valued. The ultimate goal, as stated by the US negotiators, is the release of all political prisoners from Belarusian jails, with Lukashenka's official visit to the United States and the reopening of the US embassy in Minsk among the likely conditions of a broader agreement reportedly under discussion. Whether this diplomatic relationship endures amid rapidly shifting priorities, geopolitical turbulence, and the distraction of the upcoming US midterm elections is another question. What is clear, however, is that these releases have helped Lukashenka ensure engagement, recognition, and, potentially, a seat at the table he had never been able to approach.

Beyond the diplomatic theatre of symbolic recognition and mutual praise, the talks have delivered concessions for Minsk in the form of sanctions relief. Like the prisoner releases themselves, the easing of US sanctions has, so far, been phased and carefully calibrated. The September 2025 release was followed by the lifting of measures on Belavia, the national airline, and Lukashenka's presidential aircraft.[15] The next two rounds of talks brought the most economically significant steps, removing restrictions on three Belarusian producers of potash fertilisers, the country's most valuable export, as well as two state-owned banks and the Finance Ministry, all of which are now free to transact in dollars.[16]

14 Donald J. Trump (@realDonaldTrump), post on Truth Social, 9 November 2025, https://truthsocial.com/@realDonaldTrump/posts/115520282513349957.

15 U.S. Department of the Treasury, Office of Foreign Assets Control, 'Counter Terrorism Designations; Issuance of Belarus General License', 11 September 2025, https://ofac.treasury.gov/recent-actions/20250911.

16 U.S. Department of the Treasury, Office of Foreign Assets Control, 'Belarus Designations Removals; Issuance of Belarus General License; Rescission of Belarus Directive 1', 26 March 2026, https://ofac.treasury.gov/recent-actions/20260326.

DOI 10.30966/2018.RIGA.17.7

Following the most recent round of talks in March 2026, which led to the release of 250 people, Coale expressed hope that all Belarusian political prisoners would be freed by the end of the year. In exchange the US would remove 80 per cent of its sanctions on Belarus. That would mean lifting all restrictions imposed over human rights violations after the 2020 crackdown. The 20 per cent that would remain are reportedly linked to Minsk's assistance to Moscow in the war against Ukraine.

Ultimately this unlikely US–Belarus engagement was made possible due to a near-perfect storm. Convergence of complementary interests, a disposition for quick diplomatic dealmaking indifferent to its counterpart's human rights record, and simply fortunate timing have produced a unique diplomatic process in which a state releases its own citizens in exchange for reputational and economic returns. Yet the architecture of this arrangement has a considerable obstacle: the EU's refusal to recognise Lukashenka's legitimacy and its continued sanctions pressure on the regime. Without a corresponding easing of EU sanctions, American concessions alone cannot unblock Minsk's key trade flows. Potash cannot move through European transit routes and access the EU market, which means that Lukashenka's wider economic and diplomatic rehabilitation remains out of reach. While welcoming the releases themselves, Europe's wider response has been to amplify sanctions pressure on the regime responsible for systematic repression and complicit in Russia's war against Ukraine.

The European Question

The human rights issues associated with the releases remain a key concern for Europe. The talks surely save lives, but they have not altered the regime's repressive behaviour at home or its systematic application of pressure on those it has forced into exile. What counts as a win for Trump and Lukashenka can be devastating for Belarusians. Some had just a few months left of their sentences before being forcibly deported, leaving their families behind. Others had the police question their

DOI 10.30966/2018.RIGA.17.7

relatives remaining in Belarus about their whereabouts, allegedly as part of preventative supervision measures.[17] As part of this consistent intimidation campaign, in April 2026 the authorities annulled passports of several exiled former political prisoners, effectively making them stateless. Meanwhile, arrests in Belarus have continued, fuelling the so-called 'revolving door' of repression: some people coming out, others going straight back in. This issue was presumably raised by the Americans in the latest round of talks, as in March 2026, for the first time, 235 of the 250 people released were allowed to remain in the country. Whether the US can sustain such conditionality as the talks progress remains unclear.

Europe's response to the Belarus question has been shaped by an entirely different set of moral, security, and strategic commitments. Since 2020 the Belarusian democratic forces in exile have emerged as an internationally recognised, if not universally accepted, alternative to Lukashenka's government. For many European capitals unwilling to deal with Minsk, the movement has become the primary interlocutor in Belarusian affairs. Led by Sviatlana Tsikhanouskaya, who was forced to flee to Lithuania after claiming victory in the disputed 2020 election, the diverse opposition has been joined by many of its leaders, activists, and supporters as a result of the Washington–Minsk negotiations. Among them are human rights defender and Nobel Peace Prize winner Ales Bialiatski, the 2020 presidential candidate Viktar Babaryka, and his campaign manager, Maria Kalesnikava, who in 2020 tore up her passport to prevent officials from forcibly expelling her from Belarus among hundreds of others.

The EU's refusal to recognise the regime has been channelled into support for its critics, independent Belarusian media now based in Vilnius and Warsaw, and civil society groups that have kept the record of human rights abuses at home and supported former political prisoners in rebuilding their lives in exile. The cost of these efforts has fallen disproportionately on Belarus's neighbours. Lithuania and Poland have absorbed the largest

17 'Human Rights Situation in Belarus: March 2026', *Viasna*, 7 April 2026, https://spring96.org/en/news/119989.

DOI 10.30966/2018.RIGA.17.7

share of the deported, including the 123 released in December 2025, providing emergency housing, legal support, and documents that many lacked on arrival. In practice it is these countries, not Washington, that have been living with the consequences of the US–Belarus talks.

This is not to say that there has been no engagement between the US and Europe. As the talks progressed, so has transatlantic coordination on the issue. Beyond technical discussions on process and logistics, the engagement has centred on freeing European citizens detained in Belarus through the American track. By refusing to engage publicly with Lukashenka, several European governments have struggled to safeguard their own nationals—something Washington has proved more effective in achieving. Early release of Europeans appears to have been conducted through backchannel talks with the US. Yet more recent cases reveal signs of careful multilateral coordination. For instance, the release of the Polish-Belarusian journalist Andrzej Poczobut on 28 April 2026—a *Gazeta Wyborcza* correspondent who had spent 1860 days in detention on charges stemming from his coverage of the 2020 protests—required seven countries and two years of diplomacy to achieve.[18] Polish Prime Minister Donald Tusk described it as 'the finale of a two-year-long intricate diplomatic game, full of dramatic twists', made possible by 'the tremendous help of our American, Romanian, and Moldovan friends'.[19] The fact that Poczobut's release required American brokerage to succeed underlines the tension sitting at the heart of Europe's position—one between principle and pragmatism when dealing with authoritarian regimes.

Yet the Belarusian case presents Europe with security and strategic trade-offs that go well beyond moral considerations, which makes Washington's pragmatic, transactional logic harder to adopt. Since 2020 Minsk has surrendered much of its strategic autonomy to Moscow, a process that deepened dramatically after Russia's full-scale invasion of Ukraine, when

18 'Belarus frees journalist Andrzej Poczobut', *Committee to Protect Journalists*, 28 April 2026, https://cpj.org/2026/04/belarus-frees-journalist-andrzej-poczobut/.

19 Donald Tusk (@donaldtusk), post on X, 28 April 2026, https://x.com/donaldtusk/status/2049093582007554055.

DOI 10.30966/2018.RIGA.17.7

Belarus granted its territory as a launchpad for Russian forces and accepted the stationing of Oreshnik intermediate-range ballistic missiles on its soil in 2023. For the EU members that share a border with Belarus, this is not just a geopolitical abstraction. Meanwhile, Poland and Lithuania have faced sustained hybrid provocations—drone and smuggler balloon incursions into their airspace, instrumentalised migration flows, and sustained economic coercion—that remain prominent as Lukashenka is being courted by Washington as a diplomatic partner.[20]

Brussels has responded by increasing sanctions pressure even as Washington weakens its own, a divergence that reflects not only different threat perceptions but fundamentally contrasting purposes behind sanctions implementation. This disagreement has a practical consequence: as long as key transit routes through Europe remain blocked, especially through the Lithuanian port of Klaipėda, Minsk is unlikely to profit meaningfully from American concessions alone. Having dealt with Lukashenka for over thirty years and having suspended sanctions before only to reimpose them, Europe is unlikely to alter its robust sanctions architecture unless the regime addresses the conduct that triggered them. This means progress on human rights, an end to military support for Russia, and a cessation of hybrid attacks against its members. Releases of political prisoners, however welcome, satisfy only one of these conditions—and imperfectly, given the concerns about the conditions and terms of release. Europe's position is rooted in liberal democratic values and principles of international law, but it is also shaped by the institutional memory of what Lukashenka does with concessions. While morally defensible, it offers few options for the bloc's Belarus policy beyond the complete isolation of the regime and support for its opposition. It leaves the EU in a diplomatic straitjacket that cannot come off until Lukashenka moves. And nothing so far suggests he intends to.

20 'Parliament Denounces Continuous Belarusian Hybrid Attacks against Lithuania', *News: European Parliament*, 18 December 2025, www.europarl.europa.eu/news/en/press-room/20251211IPR32171/parliament-denounces-continuous-belarusian-hybrid-attacks-against-lithuania.

DOI 10.30966/2018.RIGA.17.7

At What Cost?

Since mid 2024, diplomacy surrounding releases and swaps of political prisoners held in Belarus has settled into a steady rhythm, reaching a scale without precedent in post-Cold War European diplomacy. The Washington–Minsk negotiations have been, in one sense, a genuine success: they secured the release of hundreds of people detained on politically motivated charges, and people who were told they would never get out are alive and free. Yet this engagement has also raised uncomfortable questions about the moral cost of transactional diplomacy, its propensity for rehabilitating authoritarian leaders, and the broader challenges of balancing legitimacy, values, and pragmatism in diplomatic practice.

It is reasonable to assume that the US negotiators working towards the releases have been motivated by genuine humanitarian concern. Yet the broader architecture of the talks—underpinned by performative social media diplomacy and an administration that has shown little concern for the reputational costs of engaging with autocrats—sits uneasily alongside Washington's insistence on the humanitarian nature of engagement. What the talks have delivered for the Belarusian regime goes well beyond the release of prisoners. They have brought recognition, sanctions relief, and the prospect of further rehabilitation. For a White House administration that measures success in clear and quantifiable outcomes, this has been a trade of legitimacy and political wins. The question is what it has traded away, and whether Belarus's example would compel other authoritarians to follow suit in a quest to secure concessions. It seems that now that the genie is out of the bottle, it will be very hard to put it back.

Europe, meanwhile, has outlined the opposite position—and paid a different kind of price. Its reluctance to be seen as legitimising Lukashenka has effectively foreclosed any direct channel to those remaining inside Belarus, the majority of whom rejected the result of the 2020 election and remain in a highly repressive system. While the values-based approach has a strong moral grounding, it has clear consequences beyond

DOI 10.30966/2018.RIGA.17.7

the symbolic. Previous thaws in EU–Belarus relations have led to the strengthening of the country's civil society, independent media, and public connection to Europe—outcomes that complete isolation cannot replicate. The conditions Europe has set are legally and morally sound. They are also, in the current climate, effectively unreachable, which raises the question of whether principled paralysis serves Belarusians better than imperfect engagement.

The deeper question underlying all this is whether such diplomacy accelerates releases or incentivises the imprisonment that makes them possible in the first place. Western engagement is simultaneously a rescue and complicity. Not because Western negotiators intend it this way, but because the logic of this transactional approach makes it structurally inevitable. To negotiate is to validate currency. To refuse is to abandon those still inside. There is no clean exit from this dilemma. Talks save lives, but they may also be extending the life of the system that endangers them.

The Belarus case reflects the growing use of political imprisonment as an instrument of coercive statecraft. Wrongful detention, or let's be honest, hostage-taking, is an established feature of authoritarian policy across Russia, Iran, China, Venezuela, and parts of the Gulf. Lukashenka's phased approach might well become a template for others to adopt. One way to avoid bolstering such regimes in the future could be to minimise the personalistic and ceremonial traits of high-level diplomacy that have made the Minsk–Washington negotiations so useful for the regime's rehabilitation.

A dedicated multilateral body—whether a robust EU office or a broader transatlantic task force—could coordinate releases. But could it be done without conferring the recognition that bilateral engagement inevitably bestows? At the very least, it could sustain institutional knowledge across cases, support the families of detainees, and deploy targeted measures, such as individual sanctions and travel bans, to deter future arrests without the fanfare that makes each release a political gift to the jailer. The Office

DOI 10.30966/2018.RIGA.17.7

Source: Museum of Free Belarus

Political scientist and literary scholar Aliaksandr Fiaduta at the *Entry Point – 123* exhibit. He spent over 1,700 days in detention on charges of conspiracy to seize power in an unconstitutional way. Released in December 2025 as part of the group of 123.

DOI 10.30966/2018.RIGA.17.7

of the Special Presidential Envoy for Hostage Affairs, established under President Obama in response to the ISIS hostage crisis and expanded significantly since, offers a potential blueprint. Institutionalised hostage diplomacy is not only conceivable. It is, in one form, already operational.

If Europe believes in values-based diplomacy, perhaps it is time to treat it as a practice rather than a posture. This means developing multilateral mechanisms needed to bring the wrongfully detained home and advocate for releases of political prisoners. Should this be done without outsourcing the effort to Washington and without waiting for a regime change that may take decades to arrive?

Witness

A Review Essay by Paul Bell

All the President's Men
Directed by Alan J. Pakula. Screenplay by William Goldman based on the book by Bob Woodward and Carl Bernstein. 1976.

Keywords—*conscience, journalism, media, objectivity, partisan, witness, strategic communication, strategic communications*

About the Author
Paul Bell has had a career in two halves. Between 1976 and 1999 he reported in South Africa, covering many of the crucial events which led to majority rule and serving in the electoral commission which oversaw Nelson Mandela's election as president. From the 2000s he switched to strategic communications, led a London consultancy, and built the US military's lead information operations unit in Iraq. He spent 2019–24 in Georgia, observing its descent into elective autocracy.

I remember the day Ben Bradlee of the *Washington Post* came to visit.

I don't remember the year, let's call it 1979 or 1980. I was a young journalist working on the *Rand Daily Mail* in Johannesburg and we had a reputation for crusading, investigative journalism—with our sister paper the *Sunday Express* we had just blown open the 'Information Scandal' involving the secret diversion of state funds into influence operations designed to sustain Western support for South Africa's apartheid government.

I'd played no part in that remarkable investigation, but my closest friend on the paper, Brian O'Flaherty, had—and the office had barely seen him

DOI 10.30966/2018.RIGA.17.8

in months. He would come and go like a ghost, not a word passing his lips about what he was up to. The entire team, chief reporter Mervyn Rees, assistant editor Chris Day, and Brian, was bound by *omertà*. The only others who knew anything were the editor, Allister Sparks, and managing editor, Dave Hazelhurst. All dead now—but in their beds, thanks be; the apartheid state may have harassed them and bugged them and followed them, but it didn't kill them like it did so many others. No, they died of wear and tear, cigarettes and junk food, Diet Coke and diabetes, alcohol and adrenalin.

For me the *Mail's* investigation culminated on a night in early March 1979 when Rees and Day, who had tracked a senior official of the South African government to Ecuador, published their findings. I was down in the works, the bowels of the cathedral. The air thick with ink, foundations shaking under the rolling thunder of the presses as they spewed bound bundles of newspapers and 72-point Franklin Gothic, government-busting headlines out to waiting trucks.

Just seven years earlier, in the Washington of Watergate, Bradlee will have known that moment, stood right there with a Bodoni thunderclap hot in hand. He'll have brought that earth-moving moment with him when he came to call on us. The *Post* and the *Mail,* we were kindred spirits. We shared that same swagger.

It's a blur now. At this distance in time I see Bradlee standing among the newsroom desks, a stick figure, tallish, lean. What I remember is the feeling, the sacred excitement of being close to a god. What he said I don't remember and it probably doesn't matter. I seemed to know it instinctively. The mission. Why we were there.

It's fifty years since *All the President's Men* appeared in cinemas. Though having once seen Bradlee in the flesh, what I remember better, not least because I happened to watch the movie again recently, is Jason Robards's portrayal of him—of which Bob Woodward observed in 2015, in an interview with CBS News, 'It's like they're twins.' Robards's Bradlee is

DOI 10.30966/2018.RIGA.17.8

laconic, distrustful, rigorous, demanding, decisive—as were the two masters who taught me, both women, Lin Menge and Wilmar Utting. But as Woodward recalled in that CBS interview, when, at a critical moment in the Watergate investigation, it was evident the rot went all the way to the top, Bradlee was as overwhelmed as any mortal by its staggering implications.

The film depicts that moment. Woodward (played by Robert Redford) and Carl Bernstein (Dustin Hoffman) visit Bradlee at his home at two in the morning and ask him to come out onto the front lawn and talk there because they're afraid of wiretaps. Bradlee tells them to go home and get some rest. But where Hollywood has him concluding (with theatrical irony) that nothing's at stake other than the First Amendment, freedom of the press, and the future of the country, Woodward reports that Bradlee said simply, 'What the hell do we do now?'

It bears repeating. What the hell do we do now? Now that journalism has changed beyond recognition. Now in this brave new world of ours—with its lies, fakes, algorithms, attenuated attention spans, news-as-entertainment; all those software updates to the unchanging, unending struggle between the hardware interests of, on one hand, power and money and, on the other, 'public interest'—what the hell do we do now?

Or to put it another way, what has become of that 'mission', as I thought I knew it in my years as a journalist? By way of assaying an answer to that question, I went back—like a good historiographer—to an original source, my own notes, written a bit like Suetonius did, way after the fact, and gilded by what was comfortable at the time to remember.

On reading those notes, two things struck me about them, and disturbed me.

The first is how little there was in the notes about that mission which, even as I began to write this, I simply imagined has been alive in me as I heard Bradlee address the staff of the *Rand Daily Mail*. But what

DOI 10.30966/2018.RIGA.17.8

I read in those notes was just one racy story after another—anecdotes, incidents, observations, the idiosyncrasies of characters I had worked with and met. There was no pointed recognition of or commentary on the underlying political and moral crisis that was the cracked and shabby frame to this colourful mosaic of adventure.

The second thing that struck me was how insulated I had been back then. On the one hand, by my whiteness—which so separated my experience from the harshness of apartheid that so affected and damaged the lives of my black fellow reporters. Most of them had been beaten or banned or placed in solitary confinement at one time or another. Zwelakhe Sisulu's father was a prisoner on Robben Island. Peter Magubane had photographed the long line of coffins at the mass funeral for victims of the Sharpeville massacre in 1960, when police had killed sixty-nine protestors. Others like Doc Bikitsha and Harry Mashabela had witnessed the razing of Sophiatown, a Johannesburg suburb and heart of the city's hugely sophisticated urban-black jazz culture, from which had sprung genius like Miriam Makeba and the hit musical *King Kong.* Sophiatown was our little Gaza, not bombed to smithereens but simply bulldozed flat, erased. Not a mass murder but a small social genocide all the same. The white city council built a new suburb there for whites and called it Triomf.

On the other hand, I was isolated by my professional objectivity.

> There were [as my notes record] white *Mail* reporters who became activists, or simply broke laws in furtherance of their journalism—Patrick Laurence had been arrested twice, Ben Pogrund [an important mentor to me] had gone on trial in the Fifties for his coverage of prison conditions, Tony Holiday [who had given me my first tour of the *Mail* when I was seventeen and in the army] would go to jail for supplying information to the ANC. As would Damian de Lange and Marion Sparg for terrorism.

DOI 10.30966/2018.RIGA.17.8

> If other white reporters were chagrined, if their relative insulation was disturbing because their 'stuff' was evidently not stern enough to earn them a jail sentence, they—we—did not discuss it. We were 'objective', whatever that meant. We reported the 'facts', whatever those were, wherever they came from. A*udi alterem partem*, hear all sides, we held to that. We took risks, pushed the margins of laws that prohibited publication of police and military matters, key infrastructure, banned people and organisations. *But* [my present-day rueful italics] *were we hiding behind our professional skirts, using our journalism as a reason to observe and report on, but not act against, the injustices around us and the victimisation of our black colleagues?*

It worried me. Had I been too 'unpolitical'?

Is journalism supposed to be a political act? Is that even a real question? Isn't the answer simply 'Du-uh!'?

I sat on a NATO panel in Riga some years ago and a well-meaning US Army stratcom novitiate asked me whether it was possible to be objective. I replied: 'Objectivity is dead.' I said it without relish, the words sprung from twenty and more years of practice beyond the profession of journalism, in the world of stratcom, influence, and persuasion where perspective is queen and narrative is king and truth is owned by the client. The clap it got was wry. Admissive. Cold comfort. Some verities did indeed die.

But is that really true for journalists now? Is objectivity dead for them too?

One problem is the economics of mass media. Journalism has become so personality-driven. Journalists have become stars. Their value is measured in clicks and likes and ratings, all driven by the emotional responses of their audiences—so that the presentation of facts is more often the

DOI 10.30966/2018.RIGA.17.8

shaping of an opinion that will resonate with audiences, drive those emotions, generate those clicks and likes and ratings—because that's all money. It puts journalists increasingly at the centre of their stories, distorting the frame, refracting facts into meaning and meaning into narrative. But we were never supposed to be the stars of the show, just journeymen. And journalism was never supposed to pay; its reward was truth. Truth that comforted the afflicted, and afflicted the comfortable. Kept society's accounts.

So it was a relief to go somewhere and find that those old verities and values still cling on in stubborn encircled pockets.

In late March 2026, three weeks into a cavalier, pointless war, I travelled to Turda in Transylvania as a guest of the Ratiu Family Foundation, along with journalists from Romania, Moldova, and elsewhere in Eastern Europe, to talk about 'journalism in a time of turbulence'. The Ratiu family know this trade. Its *paterfamilias*, Ion Ratiu, was a young diplomat in the Romanian embassy in London when his government declared for the Axis in 1940. He didn't get home for fifty years. Then, after Ceaușescu fell, he returned with three aims. Become an MP, set up a newspaper, teach Romanians about democracy. Journalism and democracy have stuck with the Ratius: a succeeding generation see, unsurprisingly, a connection between these two enterprises, the former a cornerstone of the latter. And they have endowed academic institutions like the LSE and Georgetown to support both.

I was on a panel discussing journalism and politics in authoritarian states. It's been twenty-seven years since I ceased being a journalist, but only eighteen months since I returned from an authoritarian state, Georgia. There, for five years, I had watched at first hand as that post-Soviet country lost its flailing grip on democracy and fell into the pit of elective autocracy. So for Turda, to allay my imposter syndrome and earn my *locus standi* as a panellist, I decided to stick to what I knew (always a good principle for a writer) and rang round among Georgian journalists I had come to know. We convened in a group online and

DOI 10.30966/2018.RIGA.17.8

spent two hours talking about the state of the profession in their country. Which is, in a word, dire.

Afterwards I mapped out the gist of our discussion in four spheres—material impacts, psychological impacts, potential practical responses, and the ethical dilemma.

The material impact of Georgia's relapse has been devastating. Its oligarchs have outlawed all political activity other than that which they license, strangled freedom of the press, and suppressed all forms of protest. All foreign funding is subject to government approval, cutting off all European aid to civil society. (The Trump Administration ceased its support of its own accord by illegally closing USAID.) As a reporter covering a protest you have as few rights—none, actually—as a protestor. The oligarchs have imagined every possible form of protest and outlawed it. You can be jailed for 'insulting' a public official. Transgressions like stepping off the pavement at a street protest incur a fine of GEL 5,000—€1600 on a good day and well beyond the means of most Georgians. (I know people who have racked up four such penalties and may just have to go to jail to pay their debt to the oligarchy.) Earlier in 2026 Pen International[1] reported that since the end of 2024, dozens of Georgian journalists have been subject to protest-related sanctions, including forty to fifty fined and administratively prosecuted, and at least a dozen detained. Some have received longer prison terms on charges connected with public protests. This includes Mzia Amaghlobeli, who, brave woman, was jailed for two years for slapping a police chief. International monitors have yet to update these figures, but they will have deteriorated since.

The industrial and personal economics are stifling. Advertising revenue is split between government-aligned and other media on a ratio of 10:1 and the oligarchs pressure advertisers to stop supporting unapproved channels. Regional television has gone to the wall, cutting off independent news to the villages. Some independent online media are hanging from their

1 Pen International: 'Georgia: UN Submission Highlights Ruthless Crackdown on Fundamental Rights', 26 January 2026, https://www.pen-international.org/news/georgia-un-submission-highlights-ruthless-crackdown-on-fundamental-rights.

DOI 10.30966/2018.RIGA.17.8

platforms by their fingernails. At the public broadcaster, staff are subject to loyalty tests, and should they show any sign of dissent or 'disloyalty' they are sent warning letters by personnel, punished with salary cuts, demoted, shunted into dead-end jobs, or cold-shouldered. Many hang on in their jobs, keeping their mouths shut and trying to avoid stories that might put them in peril of a conscientious rebellion. The alternative is penury, hungry kids, falling back on the meagre kindness of family and friends. One member of my online 'focus group' told how for a while he and his wife and children had lived off mushrooms he foraged in the forest—until friends rallied round.

No one can say for sure how many journalism jobs have gone, but it will be many hundreds. Last year's intake of journalism students at a leading private university in Tbilisi was 150; this year it was 37. Years ago, when Georgians fondly imagined they might graduate to democracy, professions like journalism and the law were oversubscribed at universities. Now students know better: freedom of speech and the rule of law are a thing of the past, and degrees in those subjects aren't worth the paper they're written on.

Emotionally, psychologically, socially, it's crushing. People die a social death. They are cut off from former colleagues and friends, demonised in public and on social media, ruthlessly smeared, accused of treason and of taking money from foreign powers to subvert the state. And how to start over? Losing a job is bad enough, but to be robbed of both career and purpose is devastating. Depression is a natural consequence and in that state of mind it's doubly hard to find work, especially in an economy as depressed as Georgia's—whatever the government's sunshine statistics say. Those journalists who could leave the country have gone.

I asked the group: practically speaking, what might be done to resist this shutdown? I'd had some ideas and a year ago had shared them with the Foreign Office in London. They'd listened sympathetically but said there was no money. 'V' said to me: 'I know you are looking for a silver lining here. I think it's grasping at straws.' 'V' didn't mean to sound defeatist,

DOI 10.30966/2018.RIGA.17.8

but in truth this part of the discussion yielded very little. Nonetheless, if the European Union is still even remotely interested in trying to roll back the frontier of Georgia's advancing oligarchy, it might, with the support of the big endowment funds and *Stiftungen*, consider establishing some kind of offshore facility, or hub, capable of providing a degree of material support for independent journalism in Georgia, connecting it to the powerful investigative journalism engines that exist in Europe, and connecting expatriate Georgian skills to some means of fighting back against the overwhelming slew of government disinformation and propaganda that props up the oligarchy.

After our call I sent a summary to 'N', an independent television journalist for a sense-check. She came back to me with the ethical question. 'We're in an activist trap,' she said. 'We're being pushed into survival-driven advocacy and it's getting harder to maintain the line between professional impartiality and political resistance. How do journalists remain faithful to their professional principles in a hostile environment that has forced them to become a party to the conflict?'

This stopped me dead in my tracks. And once in Turda, in the hour before I said my piece on the panel, I heard it echoed by Dan Perry, AP's former Middle East correspondent, who came in via video link. 'When journalists insist on the truth, it starts to look like a political position. People start to think of journalists as a lobby.'

So, is this 'resistance' now? Impartiality and 'the truth'—these are a *position* now? And there I'd been wondering whether in South Africa it had been the opposite for me, whether I'd been hiding *behind* impartiality to *escape* 'the truth'. Looking back, I don't think I was afraid of the consequences of the truth; more that I was just too young to understand its depths. Now, having lived almost twice that time again, I see that I have dropped rather further into it, and that to report a revolution factually and objectively is no more than adding definition to its reality. Done with rigour, the truth requires no augmentation.

DOI 10.30966/2018.RIGA.17.8

I see too that journalism is, and always was, a political act. If I know anything of its history, it is that journalism has always been a means of holding people, and governments, accountable to what we loosely consider the 'common weal', the public interest. That it grew in power through the rise of, in particular, the Anglo-European liberal democratic tradition. And that as a principal facet of democratic order, it found its apotheosis in the United States, in the First Amendment of that nation's Constitution, and later in Franklin D. Roosevelt's articulation of the Four Freedoms, in which he asserts that 'the first is freedom of speech and expression—everywhere in the world'. That the other freedoms—of worship, from want, and from fear—followed it is perhaps because, in that order, freedom of speech is a primary weapon for defence of the other three.

The issue to resolve here is that freedom of speech and 'the truth' are different things. Freedom of speech is also freedom to frame, to distort, and even to lie. So what establishes the imperative for facts, and for truth, as key ingredients in the integrity of journalism? And why is that so *political*?

The right to speak is not the issue; the question is what you do with it. Socrates sees the problem. In the *Apology* he refuses to flatter his judges; he insists as a matter of conscience on binding himself to a process of examined truth, tested through the discourse, eschewing the easy line or lie though they might save him the hemlock. For him there can be no contrivance, he is subject to his conscience, it obliges him to be truthful. Journalism, at least the version we signed up for at the *Mail*, borrows however imperfectly from that instinct.

Spinoza walks the issue into public life. For him it's all upside: let people think what they like and say what they think, not because the public racket is an unalloyed joy but because open argument is the only way to leach the fear and superstition out of politics. He supports freedom of speech because he believes that, over time, honest inquiry beats dogma—a position now that feels more like an article of faith than an

DOI 10.30966/2018.RIGA.17.8

eternal truth. Today, as public discourse spins in a deliberately designed welter of confusion, Spinoza might be forgiven for considering a rewrite of that position. On the other hand, he knew, like all good psy-oppers, that 'an affect (emotion) cannot be taken away except by an opposed and stronger affect'—wherein lies the power of propaganda and extremism.

Orwell writes with powerful awareness of how language constructs meaning. He considers how governments communicate and decides that language itself has become a weapon capable of making 'lies sound truthful and murder respectable'. His antidote is less theoretical, more disciplinary: write clearly, name things accurately, strip out the sludge. Do that and, like it or not, you end up in a fight because so many people depend on the sludge to stay in business.

Put those three together. For Socrates, a matter of conscience. For Spinoza, facts and reason—'the truth'—win out in the end. (And, one might add, can cause the collapse of empires built on lies.) For Orwell, calling things what they are, calling them out, as it were, and being ready for the fight. If freedom of speech does, on its own, also shelter the liar and the propagandist, then what makes journalism—on its best days—so integral to the better health of society is that it treats speech as answerable to reality: checks it, verifies the facts, resists distortion. Which is why—in a landscape built on framing and the increasing imposition of alternative realities through brute power or advancing technology—journalism feels so political now. The *right* to speak is cheap. The *choice* to tie that right to truth is where the cost lies.

So, back to the Bradlee question: what the hell do we do now?

Turda was refreshing. The journalists I met were not big guns, stars of their own shows, influencers masquerading as truthtellers. They were journeymen and -women on survival wages. The Romanian Loredana Diaco determined to hold her president to account, to not be professionally seduced by the fact that she'd known him and even quite liked him since God was a boy—even though, when she'd asked him a question

DOI 10.30966/2018.RIGA.17.8

in public, he'd doxxed her by calling her name out three times in front of the TV cameras, so that when she got back to her desk, her email and social media were flooded with hate mail, including the usual sexual threats levelled at women. Alina Radu, a founder of Moldova's Ziarul de Gardă, a Moldovan online investigation journalism unit, was fresh from two years of battle with a Russian propaganda machine intent on diverting Moldova away from its course towards EU accession.

It was quite unlike the media diet I too readily consume these days—TV newscasters, heroic correspondents, big-name podcasters and the like, and a lot more like I remembered it. I was back among foot soldiers, journalists who readily admit that theirs is a trade, who like it that way and have no ambition for stardom. Less gloss, more grit.

In the middle of writing this piece, on Good Friday, I accidentally went to church. Now, unless it's the Vatican, I don't do bells and smells, I don't regularly attend Mass, but I'm a blood Catholic and it's hard to shake, and occasionally I 'drop in'. To sit quietly for a while and remember I've been lucky. (I call myself a Christian, but what I've lately come to think of as a 'Talarico Christian'—after the young Texan James Talarico who has just won a Democratic Senate primary and talks about his faith in terms that utterly and explicitly reject the bloody-minded, hypocritical self-gratification of the evangelical Christian nationalism that has so polluted political discourse in the United States. Talarico talks about Christ in the world, not some shock-and-awe Renaissance fantasy.)

Anyway, a service was in progress so I took a seat self-consciously at the side and slipped into the ritual. Towards the end the priest introduced a hymn that was closer to a 'spiritual', with a cadence well redolent of the struggle against Southern slavery. He talked about those origins, the bestiality and the misery. Then we sang it. 'Were you there when they nailed my Lord to the cross?' And suddenly, to my profound embarrassment, my voice was trembling—indeed the lyrics said I should *tremble tremble tremble*—and tears streamed down my face. And I knew why. Except it wasn't a religious epiphany, it was a professional one.

DOI 10.30966/2018.RIGA.17.8

Those first three words, 'Were you there …?', they're about witness. Being a witness. What it might have been like to witness that crucifixion. What it is to witness Gaza, or Black Saturday, or Iraq (and latterly Iran), or Soweto and Sharpeville and Sophiatown like my old colleagues, and all the numberless imbecilities, cruelties, and crimes that our trade is called upon to *witness*. And that led on to thoughts about rage, because seeing such things *should* make you rage; and that if objectivity were mere detachment, bloodless and unjudging, then what a nonsense rage should make of that kind of objectivity for a sentient human being. Objectivity does not have to be cold. It is not removed from the shock of reality.

We journalists—I dignify myself with that *we*—are *by definition* sentient. Looking back on my career, and wondering why I wasn't angrier earlier, I realise I was too young. I didn't know enough. I wasn't looking hard enough. Strange evidence comes to mind. A young man throws himself out of a high-rise window in Johannesburg's inner-city Hillbrow. It is late at night. Normally we're there *post facto, post mortem*. But I see this happen! The body hits a lamppost on the way down. The police let me into his flat. I see it dimly now, lit by a low red glow, sparsely furnished. I never asked why he'd done it. I just wrote down the facts: name, age, address, found dead on the pavement. It made a paragraph in the nibs.[2] I knocked off at 2 a.m. and went to The Dugout. Drank whisky. Played Tetris. I disengaged too soon.

If we are not sociopaths we are not unmoved by what we witness. Facts may speak for themselves, but conscience makes us wish to understand them and create meaning through them. To be properly objective is not to be disengaged, it is the opposite. The imperative for objectivity and our innate human curiosity engage us in searching sufficiently around an issue to build out our understanding of it, and to resolve it into the closest truth. So I was wrong in Riga to pronounce objectivity dead; that was the influencer speaking, not the reporter.

2 NIB, or news in brief. One of a series of single-paragraph news items in an inner or outer newspaper column.

DOI 10.30966/2018.RIGA.17.8

Objectivity is alive. The journalists I met in Turda know what it is and what it means. If their passionate engagement in defence of citizens' right to know and—through knowing—of their greater freedom and safety"—in the face of ruthless legislative restriction, judicial harassment, sinister intimidation, state-sponsored and AI-driven industrial-scale disinformation, targeted assassination, lethal fire—is a 'political act', so be it. As applied by hucksters, thieves, and despots, what is that label other than a cheap sticker they slap on journalists who dare hold their power to account?

So, back again to the Bradlee question: what the hell do we do now? There is no dilemma here; get over it. From a town council in Kent to the stony heart of the Kremlin, journalism has always been about publishing what others would prefer never saw the light of day. If doing a proper job of journalism makes 'activists' of reporters, so be it. The side they are on is society, no matter what shape it's in. To that extent, we are, or should be, all and always partisans.

The analogy of partisanship can arguably be extended into how the structure of journalism has changed. Historically, we have referred to journalism as the 'fourth estate', a power existing alongside (as was) clergy, nobility, and us, the hoi polloi. That fourth estate changed and divided. For over a century the media has been evolving into new baronies and great powers, serving different political interests, changing those in power when those interests are not served, and now—with the aid of algorithms and artificial intelligence—rapidly accelerating the development of entire new economies around the consumption of information, entertainment, and perception which, whether or not deleterious to the common weal, their owners vigorously defend against the efforts of states to regulate them.

Bound up in such economies, independent journalism survives in important enclaves within legacy media. But outside those large economies, or in small markets like Romania and Georgia, it struggles. The Internet has at least made getting to market cheaper, and off the

DOI 10.30966/2018.RIGA.17.8

back of it, independent journalism survives, not like the regular armies of the barons but as a multiplicity of partisan bands, and making common cause with other partisans where they can.

One of my closest friends is one such partisan. He has not been wounded in battle. His brow is not wreathed in laurels. He simply soldiers on day by day, calling small powers and petty tyrants to account in and on behalf of the community he moved to in the English county of Somerset more than fifteen years ago. He had just quit the rat race, and splashed his savings on setting up a free sheet, which he runs from his home in a village. He called it *The Leveller*. For those who know anything of England under Oliver Cromwell, the name tells you what you need to know about Andy Lee's politics. He is the terror of the county council. In an era when local journalism has all but died, Somerset's councillors must wish Andy had fallen in love with a girl from any other county than theirs. Andy is a historian by training who segued to raising venture capital for tech start-ups, and he can read a balance sheet. Both disciplines incline one strongly to facts, numbers, and the truth of either what happened or is about to happen. So he scrutinises the accounts and reports of Somerset's councils, attends their meetings, sends them letters asking awkward questions, and writes with forensic precision articles that regularly embarrass their officials, expose their incompetencies, and from time to time turn over a stone hiding worms. Two years ago, when the price of newsprint finally outstripped ad revenue and Andy's peppercorn salary, he sold *The Leveller* to what might best be described as a happy-sheet which specialises in country fairs and jumble sales, and took his power-bothering brand of local journalism online with *Somerset Confidential.* A typical recent headline: 'Fury at Somerset Council's "capitulation". After winning the legal battle to prevent the development of Packsaddle Fields on the edge of Frome, local people are now to be prevented from using the land by Somerset Council.' The facts, the truth, the rage, the witness—all there in thirty-six words.

You get the picture. Andy's old 'parliamentary' instincts and passionate belief in popular sovereignty are still afflicting the comfortable on the

DOI 10.30966/2018.RIGA.17.8

county council. He's a partisan. He'd have shown up well in Turda alongside gap-toothed, quietly indomitable Loredana, staring down her president, or the fresh-faced Pavel Szelai of Reporters Without Borders, making a stop between different countries as he monitors the increasingly embattled condition of journalism across the region, or Alina from Moldova, on her three-day furlough from one of the world's toughest information frontiers.

Certainly there was no one there who didn't know the answer to Ben Bradlee's question and—as we in the democracies struggle to rediscover and reassert the political faith and human values that are our bulwark against authoritarianism and the new global disorder—what they do now matters more now than at any time in history.

Tyranny's Temptation

A Review Essay by Mitch Ilbury

Plato and the Tyrant: The Fall of Greece's Greatest Dynasty and the Making of a Philosophic Masterpiece
James Romm. Norton, 2025.

Keywords—*strategic communications, strategic communication, tyranny, leadership, politics, Donald Trump, liberal democracy*

About the Author
Mitch Ilbury is the director of Mindofafox. He co-authored with Clem Sunter the bestselling book *Thinking the Future: New Perspectives from the Shoulders of Giants*, published by Penguin Random House.

Donald Trump, meet Plato.

Can you imagine the conversation? There is no doubt as to who would speak first. Equally little doubt on who would listen more intently. However, it would be a coin toss as to who would walk away more bemused afterwards.

These two characters could hardly be more different. One was a philosopher who distrusted the theatre of politics, believing that the health of a state depended on the quiet authority of wisdom, embodied in a select group of elites specifically trained over decades for the full weight of the task of political leadership. The other belongs unmistakably to the age of spectacle and opportunism—an era when politics unfolds through personality, performance, and relentless algorithmic attention-seeking. Yet, look deeper, and the contrast is not as clear as it first appears, for Plato himself was drawn, more than once, into the orbit of a powerful,

DOI 10.30966/2018.RIGA.17.9

impaired ruler whose court offered the tantalising possibility of turning political theory into political reality.

Plato's encounters with Dionysius the Younger, the unstable yet philosophically curious leader of Syracuse, the most powerful state in the Hellenic world on Sicily's coast, reveal a perennial tension: elegant philosophical visions colliding with the unruly, improvisational character of power. James Romm's *Plato and the Tyrant* examines this encounter between ideal and practice, telling the story of a thinker who hoped to shape politics through reason, only to find himself navigating a world governed more by ego than truth. Plato, in the end, had to descend the cave his philosophy sought to draw us out of.

It is a story that feels uncomfortably modern. When the so-called 'leader of the free world' appears to shake the very foundations on which that world is built, it forces a more difficult question than simple criticism of the man himself. How can a rules-based system so firmly grounded in liberal democratic values produce a figure so apparently at odds with them? Plato's experience in Syracuse points us towards an answer. The stability of any political order rests less securely on its structures than we might like to believe, and more heavily on the character of those who rise within it. If that is true, then the tension is not an aberration but a feature. The same conditions that sustain the system can also give rise to those who test its limits, revealing just how thin the line can be between a political order governed by reason and one pulled towards something far less restrained.

Plato: Hallowed Be Thy Name

I am unsure how old I was when I first heard Plato's name, but I do remember being impressed—like my Brazilian football heroes, he was known by just a single word. It was only at university that I began to grapple seriously with his ideas. The association had matured, but the reverence remained. To me, Plato was quite simply one of the greats.

DOI 10.30966/2018.RIGA.17.9

Each reading of Plato's dialogues—those staged philosophical encounters where Socrates serves as interlocutor—only deepened that sense. And I was hardly unique in this quiet veneration. During the Renaissance, standard editions of his works bore the title *Opera Omnia Divini Platonis*, affixing 'divine' to his name. In the early twentieth century, F.J.E. Woodbridge went further still, referencing him in explicitly godlike terms in *Son of Apollo*.[1] Even Thomas Jefferson, with a hint of scepticism, likened the questioning of Plato to the impiety of challenging an 'apostle of Jesus'.[2] Fair enough. Even after two millennia and armed with zettabytes of digital information at our fingertips, we still turn to Plato, as we do to deities, when asking how to live.

I did not pray to Plato, but for years I intellectually revered him. That was until I read the *Republic*. Lauded as his epic—his 'philosophic Iliad and Odyssey combined'—the *Republic* sets out Plato's vision of the ideal state.[3] Given what I thought I knew of him, I approached it with a certain expectation: here, surely, would be an authoritative account of the political questions underlying the issues that dominate our world. What is justice? What is the best kind of political leadership? How should we balance law and order? What is the ideal relationship between individual, community, and state? And that is precisely what I found. An *authoritative* view.

Plato was writing in a radically different time, shaped by customs and assumptions far removed from our own. Slavery was the norm, women had few rights, and the 'democracy' we think of today looked very different then. But still, I found myself taken aback by just how authoritarian Plato's ideal felt. How could he, whom I had long associated with being the finest form of genuine truth-seeker, advocate for a political ideal that banned poetry, structured society according to a fixed class system from birth, and built ongoing commitment to that strict order through

1 Frederick James Eugene Woodbridge, *The Son of Apollo: Themes of Plato* (Massachusetts: Houghton Mifflin, 1929).

2 *The Papers of Thomas Jefferson, Retirement Series, vol. 7: 28 November 1813 to 30 September 1814*, ed. J. Jefferson Looney (Princeton: Princeton University Press, 2010), 453.

3 Giovanni R.F. Ferrari, *The Cambridge Companion to Plato's Republic,* Cambridge Companions to Philosophy (Cambridge: Cambridge University Press, 2007), xvi.

DOI 10.30966/2018.RIGA.17.9

a 'noble' lie? Is that really what it takes to create a just and flourishing state? And why does that ideal look *so* different from the modern ideals espoused in liberal democratic values? Plato's spell wore off as I dived deeper into his political thinking.[4]

I was akin to the Bard College students in Romm's book: disillusioned by Plato and unconvinced of his relevance today, given the authoritarian bent of his *Republic.* Romm, too, as teacher, found it increasingly difficult to defend—it was anathema to the politics of the country they were in, and wholly challenged the fundamental freedoms at the heart of its constitution so many held dear.

Under the exposing light of modern liberal democratic values, built on individual rights and freedoms, fair and accountable institutions, and political power emanating from the consent of the governed, Plato's so-called *Callipolis*—'beautiful city'—is no oil painting. But it has been said that beauty is in the eye of the beholder. Which is to say: context matters—what you see depends on where you're looking from, and perhaps comparing political ideals now to ideals then is unfair. But behold, the liberal democratic project today is under serious pressure. The shadows of strongmen obscure much of the liberal light; so, we must look again to Plato's *Republic* and ask questions of what insights the comparison *can* yield. Will its ugliness endure, or will our eyes adjust to see something more relevant than ever?

Order through Artistic Control

The *Republic* is a blueprint for rational order, and in it Plato sees little place for art. Nowhere is his suspicion of human impulse more evident than in what he allows people to see, hear, and *feel*.

4 In volume 1 of *The Open Society and Its Enemies*, titled *The Spell of Plato*, Karl Popper describes the *Republic* as one of the most dangerous books ever written. See Karl Popper, *The Open Society and Its Enemies*, Routledge Classics (London: Routledge, 2011).

DOI 10.30966/2018.RIGA.17.9

This instinct follows from his view of what art does. Because art imitates reality—mere copies twice removed of ideal forms—and, more dangerously, manipulates those ideals to stir emotion, Plato treats it with deep suspicion. The result is predictable: large parts of artistic expression must either be excluded or tightly regulated. Poetry, in particular, gets a bad rap:

> Because I think we'll conclude that what both poets and prose writers say about human beings is bad; they say that many unjust people are happy and many just ones wretched, that injustice is profitable if it escapes notice, that justice is another's good and one's own loss. I think we'll forbid them to say such things and order them to compose the opposite kind of poetry and tell the opposite kind of tale.[5]

So, a little Kim Jong-un-ish. No more interesting, nuanced portrayals of fundamentally good, but troubled, protagonists bringing about their own demise—goodbye, Shakespeare. No more resistance art challenging state control over cultural value—forget Ai Weiwei's *Dropping a Han Dynasty Urn* photographic series. No more cool gangster movies with stylish violence providing entertainment after a long day—get used to a shared jail cell, Guy Ritchie and Quentin Tarrantino. In Plato's ideal state, art is sterilised—stripped of much of what makes it challenging, interesting, or engaging.

Yet sterilisation has some logic. It protects against the kinds of contamination that can fester in subtle and destructive ways. Consider Australia's recent and controversial law banning under-16s from accessing social media platforms. It was designed to protect young people from 'the risks and harms of engaging online', and, according to the country's prime minister, Anthony Albanese, 'mak[e] sure that Australian children have

5 Plato, *Republic*, trans. C.J. Rowe (London: Penguin Classics, 2012), 392a4–c4.

DOI 10.30966/2018.RIGA.17.9

a childhood'.[6] The ban came after government-commissioned research found that over 90 per cent of 10–15-year-olds use social media, with seven in ten being exposed to harmful content.[7] And the correlations are difficult to ignore, with rising rates of teenage suicide, distorted perceptions around body image, and the erosion of psychological well-being all associated with prolonged social media use.[8]

At its core, the ban is a judgement call: a decision by the state to limit exposure to certain kinds of content in the name of the public good. It draws a line, however imperfectly, around what young people should and should not see. In a typically forthright Australian manner, the Prime Minister highlighted how the ban sought to move what was an individual or family decision into the scope of the state. No longer would parents 'have to worry that by stopping your child using social media, you're somehow making them the odd one out. Now, instead of trying to set a "family rule", you can point to a national ban.'[9] And by making it a state decision, the politics begins to look a little more like Plato's.

Of course, we must be careful here. It would be crude to collapse all online content into 'art' in the Platonic sense when drawing the comparison. The two are not equivalent. But the comparison is still instructive. Plato's anxiety was not just about aesthetics—it was also about influence. Art, like modern media, appeals to emotion. Emotion shapes character. But emotion, unlike reason, is susceptible to manipulation. It can drive us astray, away from rational guidance on what is best for us. Plato's point is that while art may engage us, it can cultivate precisely the kinds of dispositions that run counter to the health of the state.

6 Anthony Albanese, 'Protecting Australian Kids from Social Media Harm', *Prime Minister of Australia*, 7 December 2025, https://www.pm.gov.au/media/protecting-australian-kids-social-media-harm [accessed 15 April 2026].

7 Australia Government eSafety Commissioner, *Digital Use and Risk: Online Platform Engagement among Children Aged 10 to 15* (2025), https://www.esafety.gov.au/sites/default/files/2025-07/Digital-use-and-risk-Online-platform-engagement-10-to-15.pdf?v=1776510885025.

8 Andrew Solomon, 'Has Social Media Fuelled a Teen-Suicide Crisis?', *The New Yorker*, 30 September 2024, https://www.newyorker.com/magazine/2024/10/07/social-media-mental-health-suicide-crisis-teens [accessed 10 April 2026].

9 Albanese, 'Protecting Australian Kids'.

DOI 10.30966/2018.RIGA.17.9

Through the lens of Australia's social media ban, Plato's proposals seem less alien. What once looked like philosophical overreach starts to resemble something closer to responsible politics. And as liberal democracies—perhaps soon including the UK and parts of Europe—edge toward similar restrictions,[10] they reveal a growing discomfort with the consequences of their own foundational commitment to individual freedom. Echoes of Plato's political project could be heard when the Australian Prime Minister couched 'one of the biggest social and cultural changes our nation has faced' as a 'profound reform which will be a source of national pride'.[11] Limits on individual cultural freedom in the name of the public good.

And if the language still sounds too Platonic and contrary to liberal democratic norms, think again. In April 2026 UK Home Secretary Shabana Mahmood deprived—the official word—Kanye West (also known as Ye) the right to enter the UK to perform at the Wireless music festival due to his past antisemitic actions.[12] This included selling T-shirts adorned with swastikas in his online shop, and posting on X 'I am a Nazi…I love Hitler'.[13] The Home Secretary made the call on the grounds that West's performance at Wireless would 'not be conducive to the public good'—the official language of the law granting those powers.[14] The phrasing may feel jarringly paternalistic—almost as if lifted from Plato's own playbook on curating the moral environment of the polis—but it reflects a live and accepted principle within modern democratic governance. The state, even in systems that prize liberty, still reserves the right to draw boundaries around what is deemed harmful to the collective, deciding—however reluctantly—what its citizens should and should not be exposed to.

10 'The Countries That Have Social Media Bans, or Are Planning to Implement One', *Sky News*, 8 April 2026, https://news.sky.com/story/the-countries-that-have-social-media-bans-or-are-planning-to-implement-one-13526116 [accessed 9 April 2026].

11 Albanese, 'Protecting Australian Kids'.

12 Rajeev Syal and Lanre Bakare Jamie Grierson, 'Wireless Festival Cancelled after Kanye West Banned from Entering UK', *The Guardian*, 7 April 2026, https://www.theguardian.com/music/2026/apr/07/home-office-bans-kanye-west-from-entering-uk-wireless-festival.

13 Ben Beaumont-Thomas, 'Kanye West Sued and Dropped by Talent Agency over Antisemitic Slurs', *The Guardian*, 12 February 2025, https://www.theguardian.com/music/2025/feb/12/kanye-west-sued-dropped-by-talent-agency-and-retail-platform-over-antisemitic-remarks.

14 HM Government, Deprivation of British Citizenship, British Nationality Act 1981.

DOI 10.30966/2018.RIGA.17.9

Embedded Class Hierarchies

Logical consistency is vital for Plato, which is why it should come as no surprise that his ideal structure of the state mirrors what he defines as the structure of the soul of the individual. His *Callipolis* consists of three parts. The rulers are a special breed, trained to lead the state in accordance with the forms and to do so with the wisdom of the highest order, matching the rational, calculating part (*logistikon)* of the individual. The auxiliaries (*epikouroi*), akin to the *thumos*, or spirited, part of the individual soul, sit between reason and appetite as the managing force—think of soldiers, the police, the civil service. And finally, the producers, or to use Marx's reference, the proletariat, make up the rest—those who make things. To use an analogy for all three: the shepherd, the dogs, and the flock of sheep.

A strict hierarchy must be maintained, with no movement between its ranks. In the name of the public good, individual freedom is firmly subordinated, along with any real hope of changing one's position in life. But this is not simply a case of pitying the producing class or envying the rulers. The rulers themselves are bound by equally severe constraints. From a young age, they undergo decades of rigorous education, are barred from owning property or accumulating wealth to guard against corruption, and are denied family life so that nothing distracts them from their duties. Their lives are lived in full view, with their doors always open, like an endless MP surgery. For Plato, this is not excessive, but necessary if we are to take seriously the responsibility placed on those tasked with leading the state.

What begins to grate today, then, is the mismatch: a state claiming authority in the name of the public good, yet staffed by individuals who fall well short of the rigorously formed rulers Plato believed such authority demanded.

If Plato were around now, he would cheer the UK's Home Secretary banning Kanye West from entering the country *on account of her being*

DOI 10.30966/2018.RIGA.17.9

among the state's rulers. That is within her purview. The problem he would have is that she is simply unprepared for the job. Not because she isn't bright and capable, but because being the type of ruler he has in mind requires lifelong preparation of the kind modern-day ministers are woefully lacking.

At the time of making that call, Mahmood would have been in the job as home secretary for little over six months. Plato would laugh at this. And perhaps he is right to. Since 2019, Cabinet ministers in the UK have lasted an average of just eight months in their position—a sharp drop from an already low number, with the average between 1974 and 2023 being just 2.1 years.[15] This is only slightly better than three other prominent democracies: Australia (two years) and France and Italy (each under two years).[16] Can leaders really get to grips with, let alone show real wisdom in, a role of consequential high office in such a short period of time?

This is just one of the reasons why Plato would baulk at modern-day democracies. The accountability, which we treasure, may sound good in theory, but in practice manifests in ways that can undermine other, potentially more important, qualities, such as capability. What we gain in being able to hold ministers to account we lose in substantive wisdom through not affording them adequate time, scope, and job security. Which gets to the crux of Plato's ideal conception of the state: leaders—of a certain kind, rightly trained—are the *only* ones that know what is in the best interests of the public good. And it should be up to no one else but that elite group of people to decide the fate of the state.

And if that makes your liberal democratic stomach queasy, brace yourself for things getting a little stranger still. These permanent distinctions of class are to be backed up by a state-sanctioned lie ascribing worth as emanating from the earth. A kind of metallurgical eugenics programme.

15 Peter Walker, 'Post-2019 UK Cabinet Ministers Last Average of Eight Months, Study Finds', *The Guardian*, 17 March 2024, https://www.theguardian.com/politics/2024/mar/17/cabinet-ministers-last-average-of-eight-months.

16 Ibid.

DOI 10.30966/2018.RIGA.17.9

Identity Built on a Noble Lie

To secure absolute loyalty to one's place in the polis, Plato introduces what he calls a 'noble lie'. Citizens are to be told that their very nature is fixed from birth: the rulers are infused with gold, the auxiliaries with silver, and the wider population with iron or bronze. This is not merely metaphorical, but a foundational myth designed to make hierarchy feel natural, even inevitable. Each person's role is thus presented as something innate and unchangeable. It is not the product of chance or circumstance, but of the very composition of their soul. In this telling, they are not truly born of their mothers, but of the earth itself, bound to their station as if it were part of the natural order:

> 'All of you who dwell in the city,' we will tell them, 'are brothers, but the earth who made you mixed gold in the composition of those among you who are fit to rule. Silver entered into the composition of their assistants, and brass and iron went to the making of the farmers and other craftsmen.' (Book 3, 414–15)

It may sound utterly bonkers, but the story of sovereignty depends on a similar kind of institutionalised fabrication. Think of our passports. These little pocketbooks are signalling devices—official proof of where and when we were born, stamped and certified by the state. Much of our fate is tied to what colour they are and the country name embossed in gold on the front cover. If it says 'Switzerland', then you will be able to access most places around the world, vote regularly on important policies affecting your life, and enjoy a typical slice of the state pie worth over $100,000 per year.[17] Whereas if it says 'Islamic Republic of Afghanistan', you face the possibility of stonings, floggings, or even the amputation of limbs if you step out of line, depending on the prevailing regime.[18]

17 Using GDP per capita as a metric. 'GDP Per Capita (Current US$)', *World Bank*, 12 April 2026, https://data.worldbank.org/indicator/NY.GDP.PCAP.CN.

18 Agence France-Presse, 'Afghan Supreme Leader Orders Full Implementation of Sharia Law', *The Guardian*, 14 November 2022, https://www.theguardian.com/world/2022/nov/14/afghanistan-supreme-leader-orders-full-implementation-of-sharia-law-taliban.

DOI 10.30966/2018.RIGA.17.9

And your economic value? Likely around 0.3 per cent of that of your Swiss counterpart.[19] These differences are not earned in any meaningful sense—they are assigned at birth. So the patch of earth you happen to emerge from does, quite brutally, hold an element of your worth.

The philosopher John Rawls was acutely aware of the injustice baked into such arbitrary determinants.[20] His famous 'veil of ignorance' asks us to design society as if we did not know where we would be born within it—our nationality, class, talents, or circumstances all hidden from view. Stripped of this knowledge, we are forced to think less like beneficiaries of the system and more like cautious architects of it. The odds are that we would construct a far more equal society, precisely because we would want to maximise our chances of landing somewhere decent. For Rawls, this becomes a question of probabilities rather than privilege. You would be far more inclined to design a Sweden—where the likelihood of being born into poverty is extremely low—than a South Sudan, where the risks are starkly higher.[21] In other words, fairness emerges not from a sense of idealism, but from a sober reckoning with chance.

But this neat Rawlsian exercise assumes a level of detachment and rational calculation that rarely survives contact with how people *actually think* about the world.

The political world is simply too vast and distant for most people to grasp in any direct, empirical sense. As a result, we do not engage with it as it is, but as we imagine it to be, or, as Walter Lippmann famously alluded to, as 'images in our heads'.[22] Our political understanding, to that extent, rests on imagination.[23] These mental shortcuts allow us to make sense of complex issues, but they are only loosely tethered to reality. When it

19 'GDP Per Capita (Current US$)', *World Bank*.

20 John Rawls, *A Theory of Justice* (Cambridge, MA: Harvard University Press, 1971).

21 UNDP, 'The Sudan War at Three: The Price a Nation Is Paying', 15 April 2026, https://www.undp.org/stories/sudan-war-three-price-nation-paying [accessed 16 April 2026].

22 Walter Lippman, *Public Opinion* (New York: Macmillan, 1922).

23 Michael Bang Petersen and Lene Aarøe, 'Politics in the Mind's Eye: Imagination as a Link between Social and Political Cognition', *American Political Science Review* 107 Nº 2 (2013), https://doi.org/10.1017/S0003055413000026.

DOI 10.30966/2018.RIGA.17.9

comes to something as abstract as 'immigration'—a category most people encounter only indirectly—these imagined pictures take on even greater importance. People do not form opinions based on immigration itself, but on the composite image they carry of the immigrants: who they think immigrants are, what they believe they look like, how they assume they behave.[24] Which of course can be manipulated through rereferring to them as 'rapists', 'criminals', or 'dog-eaters', or even framing their '*military* age'.[25]

And it is here where perceptions of value seep in. These mental images are not neutral; they come loaded with assumptions about worth, capability, and threat, explaining how and why voters may be divided on policies around immigrants while mostly agreeing on the desirable qualities of immigration.[26] Some passports conjure images of industrious professionals, others of instability or dependence. In this sense we are not far removed from Plato's schema of gold, silver, and bronze. Without ever stating it so crudely, we sort individuals into tiers of perceived value based on where they were born and the stories we attach to those places. The immigrant, then, is not judged as an individual, but as a *projection of category* that collapses complex lives into simplified narratives.

The difference is not that we don't rely on such myths, but that they are not designed for stabilisation like Plato's. His noble lie sought to fix identity, whereas modern political narratives often do the opposite—destabilising it, redrawing the boundaries of belonging in real time. Trump's rhetoric on immigration operates precisely in this space, reshaping the 'image in the head' with remarkable speed and effect.

24 Scott Blinder, 'Imagined Immigration: The Impact of Different Meanings of "Immigrants" in Public Opinion and Policy Debates in Britain', *Political Studies* 63 № 1 (2015), https://doi.org/10.1111/1467-9248.12053.

25 Amanda Terkel and Megan Lebowitz, 'From "Rapists" to "Eating the Pets": Trump Has Long Used Degrading Language toward Immigrants', *NBC News*, 19 September 2024, https://www.nbcnews.com/politics/donald-trump/trump-degrading-language-immigrants-rcna171120 [accessed 19 April 2026].

26 See Jens Hainmueller and Daniel J. Hopkins, 'The Hidden American Immigration Consensus: A Conjoint Analysis of Attitudes toward Immigrants', *American Journal of Political Science* 59 № 3 (2015), https://doi.org/10.1111/ajps.12138, and Nicholas A. Valentino et al., 'Economic and Cultural Drivers of Immigrant Support Worldwide', *British Journal of Political Science* 49 № 4 (2019), https://doi.org/10.1017/S000712341700031X.

DOI 10.30966/2018.RIGA.17.9

The Fine Line of Tyranny

A particular set of letters gives us a better look into Plato *the man*, beyond just his ideas. The 'Platonic letters' come from a collection of Plato's works compiled by the scholar Thrasyllus, from the first century AD. These letters—thirteen in total—are hotly contested. Or at least as 'hotly' as anything can be contested in ancient Greek scholarship. For a long time many of the letters were considered as inadmissible evidence into our opaque understanding of who Plato really was. But James Romm argues convincingly in his book that many of the doubts about the authenticity of at least five of the letters are misplaced, and with them, so too is our understanding of Plato.

In these letters we learn more about Plato's trips to Syracuse, where he sought to engage with the state's rulers—first Dionysius the Elder, and then his son. The younger Dionysius showed the hallmarks of an unstable tyrant yet also possessed a seemingly genuine curiosity for philosophy. His uncle Dion, an avid student of Plato, believed this curiosity could be cultivated and developed. These relationships, and Plato's wider involvement in Syracuse, spanned much of the period during which he was writing the *Republic*. But the Plato in these letters makes moral compromises, shows poor judgement, takes money from autocrats, and is concerned with everyday minutiae—a far cry from the purity of the *Republic*, and more akin to the politics we know all too well.

Yet the lessons here are not about hypocrisy. Even at the height of veneration, those under Plato's spell would have known he was not going to be a living embodiment of his own idyllic form. To quote the Japanese children's writer Tarō Gomi, 'everyone poops'.[27] No, the lessons here are more nuanced. As democracies today come under growing pressure from the renewed allure of authoritarianism, we should be asking what Plato could gain by engaging with a tyrant of Dionysius' calibre. The answer sits either side of a very thin line.

27 Tarō Gomi, *Everyone Poops* (San Diego: Kane/Miller Book Publishers, 1993).

DOI 10.30966/2018.RIGA.17.9

Plato, like many observers now, was deeply frustrated, even cynical, about how governance systems functioned—or failed to function. And while he believed each form of government had its merits, each had its own inherent weaknesses. Aristocracy stands as the highest form of rule, grounded in wisdom and the pursuit of the good, though once it slips into heredity there is no guarantee that those born to rule will possess the rational excellence required. Timocracy preserves much of this order through discipline and honour—Sparta being the obvious model—but with spirit rather than reason in command, it carries the risk of drifting from measured judgement towards ambition. Oligarchy introduces a kind of equilibrium among the few who rule, yet as the love of wealth takes hold it corrupts the very basis of governance, while democracy, for all its internal accountability, elevates freedom to such an extent that it erodes structure altogether, creating the conditions from which tyranny emerges, as a single figure steps in to impose order on the resulting disorder.

What's striking is how little separates Plato's best regime from his worst, at least *structurally*. *Callipolis*, his ideal state, is built on absolute rule by the golden-souled, who govern without any democratic accountability to the many beneath them. Tyranny, in form, looks almost identical. It is just on the other side of a thin line. The difference lies not in the system but in the soul of the person at the top. Get the right person, and you have Plato's utopia; get the wrong one, and you have its tacky gilded mirror image.

It's precisely this logic that drew Plato to Syracuse. If the structure of rule was already in place, then perhaps all that remained was to reshape the man at its centre. Could Plato cultivate the tyrant's flickering interest in philosophy and, with enough guidance, turn an ego-driven ruler into something closer to an enlightened one, to provide a firm nudge across the thin line? This is what the eighteenth-century classicist and poet Thomas Gray had in mind—albeit with a touch more poetic drama—when he suggested that saving a single prince from corruption might be enough

DOI 10.30966/2018.RIGA.17.9

to save the world.[28] Had the experiment worked, it would have stood as a living proof of Plato's ideal: that the right man, properly formed with philosophical wisdom, could make a beautiful city out of an otherwise fragile design.

Enabling Tyranny

Alas, Plato's experiment did not succeed. For the problem with tyrants is that they're more easily flattered than converted to ideas that may challenge their own. Dionysius surrounded himself with writers and ethical teachers to project an intellectual image of himself.[29] Yet they did not bring much challenging truth to their role as moons circling his orbit. His coterie—collectively known across Greece as the *Dionysokolakes*, or 'Dionysioflatterers'—did and said what they could to stay in the ruler's good graces.[30] One story has them fumbling deliberately for food at banquets so that the short-sighted Dionysius could guide their hands, the performance designed to make him feel more capable than those around him.[31]

Sound familiar? Dionysius would be quite at home in President Trump's gilded Oval Office with the steady footfall of visitors queuing to praise him. And this extends to those beyond his immediate orbit, whether it be the NATO Secretary General referring to him as 'daddy', Keir Starmer offering up an unprecedented second state visit with a handwritten note from the King, or a peace prize ceremony hastily arranged not by the Norwegian Nobel Committee, but by FIFA at the bizarre spectacle surrounding the World Cup draw.[32]

28 James Adam, *The Republic of Plato* (Cambridge University Press, 2010).

29 James Romm, *Plato and the Tyrant* (New York: W.W. Norton, 2025).

30 Ibid.

31 Athenaeus, *The Learned Banqueters, vol. 7: Books 13.594b–14*, trans. S. Douglas Olson (Cambridge, MA: Harvard University Press, 2011).

32 Louisa Thomas, 'The Weird Spectacle of the World Cup Draw', *The New Yorker*, 7 December 2025, https://www.newyorker.com/sports/sporting-scene/the-weird-spectacle-of-the-world-cup-draw.

DOI 10.30966/2018.RIGA.17.9

Tyrants are not made in isolation. They are sustained by those in proximity. Flattery is exchanged for access and influence, and over time it reshapes the ruler's sense of reality. When affirmation is constant, judgement begins to slip, and confidence hardens into something far removed from truth. The Dionysioflatterers were not just hangers-on seeking favour; they helped create a political space in which challenge all but disappeared. And this pattern is not confined to ancient courts. Wherever power gathers too tightly around one individual, those nearby tend to adjust accordingly and, in doing so, play their part in making the tyrant.

Plato fell into this trap. While he never made Dionysius the tyrant or supported him, he misread the potential to reshape him. Reshaping requires challenge, and challenge doesn't sit well with the ego-driven. Syracuse was not just a failed experiment in applied philosophy; it was a reminder that power does not yield easily to reason, and that those who hold it are rarely inclined to be reshaped by it. The tragedy is not that Plato tried and failed, but that his failure revealed something enduring: the gap between the ideal and the real is not easily bridged. The philosopher may sketch the blueprint, but the tyrant still wields the Sharpie pen that signs the executive orders.

And yet, Plato's more unsettling insight lingers. The difference between his ideal city and its tyrannical counterpart is not one of structure but one of substance. Both rest on concentrated power, on the elevation of one above the many, on the belief that order is best secured from the top down. The distinction lies in whether that power is exercised by reason or by appetite. That is a thin edge to rest so much upon. We like to think that modern democratic systems have moved us safely away from that precipice, that institutions, norms, and checks provide a buffer against the whims of any single individual. But the recurring appeal of figures like Donald Trump suggests otherwise. When those systems begin to feel slow, distant, or ineffective, the promise of decisive, unconstrained leadership starts to look less like a danger and more like a solution.

DOI 10.30966/2018.RIGA.17.9

Perhaps, then, the imagined meeting between Plato and Trump would not end in outright dismissal. Plato would recognise the symptoms, if not endorse the cure: a political order straining under its own contradictions, a public growing impatient with its limitations, and a figure stepping forward to resolve the tension by sheer force of personality. He would not see a philosopher-king in Trump, but he would not see a complete anomaly either. And that is the uncomfortable point on which this story turns. Tyranny is not some alien form that descends upon otherwise healthy systems. It is a possibility that sits latent within them, emerging when faith in the existing order begins to falter. The question is not simply how to guard against the tyrant, but how to sustain a political world in which we do not go looking for one in the first place.

LEGO: How Should States Communicate in the Attention Economy?

A Review Essay by Louis Brooke and Sophia Krauel

LEGO Resistance Front video series
Explosive Media, www.instagram.com/explosivemediaa.

Keywords—*strategic communication, strategic communications, attention economy, AI, Iran, political communications, social media*

About the Author
Louis Brooke is co-founder and Chief Strategy Officer at Zinc Network.

Sophia Krauel is a strategy director at Zinc Network and specialises in government capacity building.

The story of the video clip is simple: a LEGO version of US President Donald Trump wants to distract from his alleged links to child sex offender Jeffrey Epstein. He orders a strike on an Iranian girls' school. A grieving and vengeful Iranian LEGO soldier launches retaliatory attacks that destroy US ships and bases, sending American soldiers home in flag-draped coffins.[1]

In the weeks following the US and Israel's first attacks on Iran in spring 2026, a steady stream of similar AI-generated LEGO-style videos flooded social media. They tell a story of resistance and anti-imperialism:

1 'WATCH | Iran State Media Publishes Lego-Themed Animation of Strikes across Middle East', ATP Channel, *YouTube,* 12 March 2026, https://www.youtube.com/watch?v=mZ5GI5LaVC8 [accessed 1 May 2026].

DOI 10.30966/2018.RIGA.17.10

the United States is corrupt and oppressive, while Iran fights on behalf of US victims worldwide. The videos reference historical grievances—from war crimes in Vietnam to the treatment of Native and African Americans—as well as online conspiracy culture, ranging from the Epstein scandal to Trump allegedly being controlled by Israel.

Some of Iran's earlier animated videos were set to emotive orchestral soundtracks, seemingly aimed at a domestic audience. Newer videos began addressing US and international audiences more directly, and adopted a sharper, more irreverent tone laced with sarcasm and set to catchy rap tracks reminiscent of American artists like Eminem:

> America first? Oops. Oh boy, that was the slogan you sold.
> But Bibi's pulling strings and your vote is getting cold. […]
> If one nation's going to stand against the Epstein regime's fear,
> It's us till the last breath. We've been doing it for years.
> We're standing here for everyone your system ever wronged.
> They've known all along the enemy was always you.[2]

Traditionally, Iran had primarily relied on religious-ideological propaganda,[3] but its LEGO videos, some of which contain sexually explicit tropes, are unlikely to have been signed off by clerics. While the regime imposed a prolonged Internet blackout on most of its population in 2026, it embraced sophisticated content from regime-friendly, digitally native creators. By shedding its institutional and ideological constraints, Iran was able to compete on an equal footing in the narrative war.

Not only were the clips shared by Iranian and Russian state media, but they were also widely amplified by international mainstream media and even by pro-MAGA bloggers, many of whom covered every new LEGO

2 'Iran Releases Another LEGO Animation Mocking Trump as Information War Continues', ATP Channel, *YouTube,* 9 April 2026, https://www.youtube.com/watch?v=5G9DNx7xIIc [accessed 1 May 2026].

3 David Siman-Tov, Danny Citrinowicz and Reut David, 'Iran's Strategic Communications in the Campaign: Intimidation, Deterrence, and Resilience', *The Institute for National Security Studies,* 23 March 2026, https://www.inss.org.il/publication/roaring-lion-media.

DOI 10.30966/2018.RIGA.17.10

video as a breaking story. The Institute for Strategic Dialogue calculated that posts from coordinated pro-Iranian networks gained a billion views on X over the first month of the war.[4] Users shared the videos, not because they supported Iran, but due to the content's eye-catching, entertaining, and subversive nature.

State Communication in the Attention Economy

Governments have always sought to shape public discourse, but the conditions under which they do so have radically changed in recent years. Until the early 2010s, states operated in an information environment mediated by a relatively small number of broadcasters and publishers with whom they had established and structured relationships. Communication was predominantly one-directional, flowing from institutions to the public via a limited number of gatekeepers, offering clear mechanisms to influence public debate. Moreover, they enjoyed a significant degree of authority and trust with audiences.

In this context, skilled politicians and 'spin doctors' could shape the public discourse through careful framing and narrative building, message discipline, and effective media management. While this did not guarantee positive coverage, the institutional authority of government meant they would at least be heard.

Today's information environment is a much more hostile place for government. It is best characterised as the 'attention economy', where human attention is treated as a scarce commodity, and digital platforms and advertisers compete to capture and monetise user engagement. Most audiences now receive their news primarily from social media,[5] and here governments must compete for attention with a functionally unlimited array of actors including influencers, brands, and news and

4 'How Pro-Iran Networks Gained a Billion Views on War Propaganda', *Institute for Strategic Dialogue,* 15 April 2026, https://www.isdglobal.org/digital-dispatch/how-pro-iran-networks-gained-a-billion-views-on-war-propaganda.

5 Ian Youngs, 'Social Media Now Main Source of News In US, Research Suggests', *BBC News,* 17 June 2025, https://www.bbc.co.uk/news/articles/c93lzyxkklpo.

DOI 10.30966/2018.RIGA.17.10

entertainment outlets, all of which are commercially incentivised to maximise 'eyeball hours'. Communication has become ever faster and multidirectional, with messages constantly reshared and contested across overlapping networks, and is therefore harder to influence in real time.

Although it is not a simple causal pathway or perhaps even the primary cause, social media is making audiences more fragmented, polarised, and cynical. Algorithms rank content according to predicted engagement, a process that recent research has suggested favours content that is emotionally charged, partisan, and hostile to out-groups. This encourages users to cluster into porous, overlapping online 'tribes' organised around shared issues, identities, or worldviews, often defined in opposition to other groups.[6]

The proliferation of generative AI has turbocharged these dynamics by dramatically reducing the costs and time required to produce content. As the Iranian propaganda videos have shown, world-class content can be easily produced at near zero cost, resulting in a superabundance of content. This makes human attention relatively speaking an even scarcer and more valuable commodity, and the competition for it even fiercer.

In the attention economy, governments can no longer rely on their authority to be heard, and the old methods of shaping their story no longer work. This raises a fundamental question: how should states communicate in today's attention economy? One strategy is to 'play the game'—to compete for attention using the same strategies and tactics as every other actor online. At the other end of the spectrum is the choice to try and stick to the old rules of government communication, to stay above the fray, and to maintain a formal and evidence-based communication style even at the cost of reduced visibility. Both ends of this spectrum carry significant risks for government. In this essay, we explore whether there is a viable third path for government communications in the

6 S. Milli, M. Carroll, Y. Wang, S. Pandey, S. Zhao, and A.D. Dragan, 'Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media', *PNAS Nexus* 4 Nº 3 (2025), https://doi.org/10.1093/pnasnexus/pgaf062.

DOI 10.30966/2018.RIGA.17.10

attention economy, one that combines cut-through and impact with epistemic integrity.

We analyse the strengths and weaknesses of these competing approaches across three levels: the epistemic, strategic, and tactical.

The epistemic level refers to how states relate to the truth value of their claims. Traditionally, governments in liberal democracies were expected, at least in principle, to communicate what they believed to be true and to provide verifiable evidence for their claims. Political arguments were generally justified through 'public reasons': terms that citizens with different worldviews could recognise as legitimate, even if they disagreed with the claim itself. For example, appeals to fairness, equality, the protection of life, or the promotion of well-being, rather than to individual interest, religious authority, or sectarian doctrines. Of course, this norm was never perfectly upheld, but transgressing it could carry reputational and political costs. Today, this constraint appears to be weakening.

The strategic level is about what communication attempts to achieve. Governments have always pursued multiple objectives, from informing and persuading to distracting and dividing. However, in the attention economy, the emphasis is shifting away from informing, educating, and persuading and towards mobilisation and maintaining attention and visibility at all costs.

The tactical level refers to how communication is expressed in terms of style, tone, and format. While traditional government communication has tended to rely on formal, institutional language, some actors are adopting more informal, culturally fluent, and at times irreverent modes of expression that mirror the conventions of digital and popular culture, blurring the line between government communications and that of other actors.

DOI 10.30966/2018.RIGA.17.10

Approach 1: Playing the Game

One approach adopted by the Iranian regime in the conflict with the US is to embrace the logic of the attention economy and compete directly with other actors, including influencers and entertainers, on the same terms. Rather than relying on institutional authority, it seeks to ride the algorithm and win attention through speed, volume, and emotional resonance.

At the epistemic level, 'playing the game' means no longer being constrained by trying to communicate verifiable claims or providing evidence or public reasons for one's arguments. The LEGO videos depicting the Iranian military bombing the White House, and President Trump worshipping the Canaanite god Baal, are clearly not meant literally. The aim is not to mislead audiences; they know the intent is not to communicate the 'truth' in any way, rather to entertain and engage—blurring the line between political communication and entertainment. Emotionally, this creates a form of identification between messenger and audiences, a synaptic link between the tribes in which they exist. Practically, any form of digital engagement serves only to amplify the message, harnessing the audience's trust and connections with their wider networks.

At the strategic level the primary aim of communication shifts from persuasion to capturing attention at all costs. Success is measured by virality, visibility, and the ability to shape what audiences talk about. Communication becomes a constant campaign, with an uninterrupted stream of messages designed to maintain momentum. Actors continually aim to set and reset the agenda by issuing frequent statements, announcements, distractions, or provocations that often use shock and humour to crowd out competing narratives.

Governments generally need to build a minimum viable consensus for their policies, securing a plurality of potential voters who broadly support the government's position. Previously governments mostly achieved this

DOI 10.30966/2018.RIGA.17.10

by mobilising their base and winning over the middle ground of public opinion. In the attention economy, however, the strategic imperative has flipped: those playing the game now seek to mobilise highly motivated and vocal audiences at the edges of public discourse because they are the ones most likely to engage online—posting, commenting, and resharing—and therefore to drive virality and visibility. Yet this also results in more heterogeneous and unstable political coalitions that make it even harder for government to communicate effectively.

This means that communicators who 'play the game' need to build ecosystems of online voices that can provide reach and credibility with as many online tribes as possible. Movement-building therefore becomes a central approach for those playing the game. By building a movement of loosely affiliated and aligned influencers, outlets, content creators, and brands, governments have a ready-made distribution network that not only shares messages but reinterprets and repackages them as its own content, to have maximum resonance with its own members.

While this secures reach, it invariably means a loss of message control. Long gone are the days of 'spin doctors' having mastery of the 'dark arts' of shaping public opinion. In the 1990s and 2000s, government communicators built processes and structures to help tame the emerging 24-hour news cycle. But now the speed and unpredictability of information dissemination mean attempts to control the narrative excessively tend only to leave the government looking inauthentic, reactive, and behind the curve.

But what governments that 'play the game' lose in control, they gain in virality. They can become a central node in a network of networks, providing messaging signals for others to reinterpret and amplify. What these networks crave is not polished political communications, but the 'authenticity' that acts as a heuristic to prove the communicator is part of their tribe.

DOI 10.30966/2018.RIGA.17.10

On a tactical level, 'playing the game' means opting for highly informal, satirical, culturally fluent forms of communication that feel native to online audiences. Saturated with a flood of information from all sides, audiences gravitate towards content that is simple, eye-catching, and entertaining, meaning they are then further pushed by algorithms which optimise for engagement. This creates an incentive for political communicators to be as entertaining and shocking as possible.

Volume itself becomes a tool. The advent of guard-rail-free, generative AI tools is now allowing communicators to flood the information environment with content. Explosive Media claimed their ten-person team could produce one high-quality video in just twenty-four hours.[7] Another LEGO film-maker claimed that a one-minute clip took him just thirty minutes.[8] AI-animated videos allowed Iran to rapidly respond to unfolding developments by presenting its version of events in a format designed to entertain as much as inform—drawing on rap, memes, and trolling.

This approach can be seen across Iran's network of communicators, not just Explosive Media. In a video message an Islamic Revolutionary Guard Corps spokesperson mocked some of President Trump's most famous catchphrases*:* 'Hey Trump, you're fired! You know this line. Thank you for your attention to this matter.'[9] Iranian embassies around the world posted witty, well-timed jibes in response to new developments in the war. After Italian Prime Minister Giorgia Meloni criticised Trump over his arguments with the Pope, Iran's embassy in Ghana posted a job application to become Italy's new ally: 'Our qualifications: 7,000 years of civilization, a shared love of poetry, architecture, and food that takes

7 Kyle Chayka, 'The Team behind a Pro-Iran, Lego-Themed Viral Video Campaign', *The New Yorker,* 2 April 2026, https://www.newyorker.com/culture/infinite-scroll/the-team-behind-a-pro-iran-lego-themed-viral-video-campaign.

8 Steven Lee Myers and Stuart A. Thompson, 'Iran's Meme War against Trump Ushers in a Future of "Slopaganda"', *The New York Times,* 24 April 2026, https://www.nytimes.com/interactive/2026/04/25/business/iran-trump-israel-war-memes.html?smid=nytcore-ios-share.

9 '"You're Fired": Iran Military Officer Mocks Trump over 48-Hour Hormuz Threat', *NDTV World,* 23 March 2026, https://www.ndtv.com/world-news/iran-war-irgc-military-officer-mocks-donald-trump-over-48-hour-hormuz-strait-threat-youre-fired-11253190.

DOI 10.30966/2018.RIGA.17.10

longer to prepare than Trump's attention span.'[10] Again, the aim is not to inform: it is to entertain, to disarm, to grab attention.

It is not hard to understand why governments 'play the game'. First and foremost, the underlying commercial incentives that drive the attention economy encourage governments to adopt the same strategies and tactics as any other online voice. The imperative is to harness algorithmic amplification to achieve cut-through at any cost.

A second incentive is that such communication is much harder to counter, fact-check, and take down. Any factual rebuttal by a government to a LEGO animation would be mocked and derided. While some social media platforms like YouTube eventually suspended Explosive Media's channel for violent content, many struggled to find reasons for banning LEGO-style content that was so clearly satirical. Platforms were also faced with the challenge of identifying state attribution when most pro-Iranian content was pumped out by arms-length creative agencies and a plethora of copycat accounts.

Third, such satirical and meme-driven content bypasses audiences' habitual mental defences.[11] Any state-associated messaging is usually received by audiences with a high degree of distrust and cynicism. However, in the comment sections under LEGO videos, critical voices were rare. Instead, users on X and YouTube gave the videos rave reviews. 'They will call it propaganda, but literally nothing in this video is false,' was a frequently echoed comment. Another user added: 'It sounds like Iran cares more for the U.S. than our own President.' Many users simply enjoyed the entertainment: 'I'm making a playlist at this point. These are bangers.'[12]

10 'Iran's Diplomatic Pitch to Italy Goes Viral on X', *Wanted In Rome,* 15 April 2026, www.wantedinrome.com/news/irans-viral-diplomatic-pitch-to-italy-blends-humor-with-strategy.html.

11 Mark Alfonso and Michał Klincewicz, 'AI-Generated Lego Videos and Trump's Poo-Bombing: Welcome to the Iran-US Slopaganda Wars', *The Guardian,* 8 April 2026, https://www.theguardian.com/commentisfree/2026/apr/08/lego-videos-iran-trump-ai-video-meme-propaganda-movie-animation.

12 Comments cited were found under the following video: 'Iran Releases Another LEGO Animation Mocking Trump as Information War Continues', APT Channel, *YouTube,* 9 April 2026, www.youtube.com/watch?v=5G9DNx7xIIc [accessed 1 May 2026].

DOI 10.30966/2018.RIGA.17.10

However attractive these incentives, there is a reason many liberal democracies have been wary of this new approach. Non-democratic adversaries and non-state competitors for attention will always be able to outflank liberal democracies using such methods as they are less constrained by law, civil society, and public opinion. Moreover, while such tactics can appear highly effective in the short term, capturing attention and reaching audiences far beyond traditional political spheres, they come with significant long-term costs. By prioritising resonance over accuracy, they contribute to an ever more polarised information environment, and encourage a culture of cynicism and disengagement in which all political actors and media are met with suspicion. When serious transgressions of international law and war crimes are dismissed as a joke or turned into a meme, the result is a hollowing out of the shared reality on which our democratic systems and international institutions ultimately depend.

Approach 2: Sticking to the Rules

At the other end of the spectrum is a decision to stick to the old rules. To try to remain above the fray, and maintain the government's position as a unique and distinct actor in the information environment. Most liberal-democratic governments currently fall somewhere in this category. At the epistemic level, 'sticking to the rules' means that government communications should try to be evidence-based and offer public reasons for its claims; accepting that, when this norm is transgressed, governments should be held to account. While good communications is always emotive and story-based, the underlying messages are grounded in evidence, and generally distinguish between what is known, what is uncertain, and what cannot be confirmed.

At the strategic level the primary purpose of state communication remains to inform, educate, and persuade. While governments wish to mobilise their base, and distract or even divide or scare their population, these objectives are typically pursued in an epistemic framework (outlined

DOI 10.30966/2018.RIGA.17.10

above). This limits the extent to which communication can rely on shock, provocation, saturation, or entertainment. As a result communication cannot be optimised purely for attention, and governments find it harder to adopt the strategies such as 'flooding the zone' or building movements that have proven effective in the attention economy.

Tactically this approach favours formal institutional formats and styles. There is an inherent desire for state communication to reflect the authority of office, and to preserve its dignity. While many governments have developed sophisticated, multichannel strategies, and actively communicate across all major social platforms, language tends to be cautious, precise, and often technical. Media engagement remains the dominant mode of communication, particularly on foreign policy, with at best clunky forays into harnessing influencers or aligned third-party channels.

This tendency is particularly visible in the European Commission. One study analysed almost 45,000 European Commission press releases between 1985 and 2020 and found that—based on its syntactical complexity and specialised jargon—the Commission had adopted 'an extremely technocratic style of communication'.[13] Similar patterns were observed in the Commission's social media output.[14] This is perhaps unsurprising, given the Commission's legalistic nature, but it also highlights the extent to which its communication remains oriented towards policy precision rather than public resonance.

The statement of EU Commission President Ursula von der Leyen in response to the first attacks on Iran on 28 February 2026 is characteristic of the EU's traditional communications style: 'The developments in Iran are greatly concerning,' she wrote on X, diplomatically avoiding condemning the attacks. 'We reaffirm our steadfast commitment to

13 Christian Rauh, 'Clear Messages to the European Public? The Language of European Commission Press Releases, 1985–2020', *Journal of European Integration* 45 № 4 (2023): 683–701, https://doi.org/10.1080/07036337.2022.2134860.

14 Sina Özdemir and Christian Rauh, 'A Bird's Eye View: Supranational EU Actor on Twitter', *Politics and Governance* 10 № 1 (2022): 133–45, https://doi.org/10.17645/pag.v10i1.4686.

safeguarding regional security and stability. […] We call on all parties to exercise maximum restraint, to protect civilians, and to fully respect international law.'[15] The statement was careful, measured, and grounded in legal principles and international norms, but it is unlikely to have reached beyond policy and media circles.

This emphasis on credibility and restraint is also reflected in the EU's cautious approach to new technologies. While Iran and the US have experimented widely with AI content, the European Commission has moved in the opposite direction, banning the use of generative AI in official communications apart from very limited cases, such as when optimising the quality of footage. While the intention was to reinforce trust and authenticity, the decision also raised some eyebrows. One OECD advisor argued that synthetic content itself was not a problem: 'By refusing to engage with it altogether, the European Commission is missing a leadership opportunity to demonstrate what responsible, transparent use of AI in political communication actually looks like.'[16]

Overall, 'sticking to the rules' has clear strengths. It reinforces institutional credibility, signals seriousness, and helps maintain the norms of liberal democracy and what is left of the international order. Words matter. By sacrificing epistemic integrity for virality, governments risk not merely trading one communication style for another but eroding the norms and principles on which our political and social system depends. Particularly in the international realm, law and norms are fragile; they are fictions that constrain us so long as we all accept that they do. Using language which denigrates or ridicules them is an act of destruction. The risk is that it destroys the very edifice on which liberal-democratic government is built.

15 Ursula von der Leyen (@vonderleyen), post on X, 28 February 2026, https://x.com/vonderleyen/status/2027691363811090828?s=46&t=NHywxWC89R_Tg6AJimB5Bw [last accessed 1 May 2026].

16 Walter Pasquarelli, quoted in Pieter Haeck, 'EU Staff Banned from Using AI-generated Content in Official Communications', *Politico,* 31 March 2026, https://www.politico.eu/article/brussels-eu-ban-deepfakes-ai-generation-official-messages.

DOI 10.30966/2018.RIGA.17.10

However, sticking to the rules comes with serious limitations. Carefully calibrated language can appear distant, inauthentic, or opaque to audiences, and struggles to cut through in a fast-paced, attention-driven media environment. Messages that are accurate, justified, and evidenced are inherently less likely to travel furthest or resonate most widely, as they cannot prioritise shock and entertainment value. They are also less likely to appeal to the motivated fringes of political discourse that tend to drive virality in the attention economy.

The EU might reasonably argue that it has no intention of competing with irreverent or sensationalist content and 'AI slop' in a race to the bottom, and that maintaining standards is itself a strategic choice. Yet in an environment where attention is increasingly captured by actors willing to operate outside these norms, there is a risk that governments that stick to the rules can find themselves unable to get their message heard and shape a coherent narrative among the unlimited content, argument, and opinion to which audiences are exposed. Consequently they can quickly lose control of how they are perceived. The question is not whether liberal democracies should abandon their principles, but whether they can afford to rely on them alone in an increasingly competitive and fragmented information space.

Is There a Middle Path?

The two approaches outlined above present two ends of a spectrum. 'Playing the game' of the attention economy can deliver short-term influence and visibility, but may come at the expense of long-term credibility and ever-weakening trust in norms and institutions, and ultimately leaves governments vulnerable to other players who will outcompete them at their game. 'Sticking to the rules' attempts to preserve credibility and the distinctness of government tone as an actor in the information environment, but struggles to cut through and maintain a stable and broad enough coalition of public support.

DOI 10.30966/2018.RIGA.17.10

Government must forge a middle path, one that maintains epistemic integrity while competing effectively in the attention economy. This is hard. No government has done this successfully, yet three building blocks of an approach are emerging.

Building block 1: Maintain epistemic credibility, but offer meaning

Persuasion based on verifiable, evidenced claims, justified with public reasons, must remain the foundation of state communication. The challenge is to make messages land in an information environment where attention is scarce, government has lost its privileged position, and algorithms (and thus commercial incentives) optimise for engagement above all else and thus favour the shocking, enraging, entertaining, or ridiculous over the accurate.

As Aristotle observed over two thousand years ago, effective communication depends not only on credibility and logic, but also on emotion. People interpret information through their own values, identities, and experiences. Political psychology has repeatedly shown that people judge messages partly by their perceived source: claims from one's own political or social group are often treated as more credible, while claims from opposing groups are more readily discounted, often regardless of their substantive content.[17] Unless messages resonate emotionally, and reinforce audiences' existing identities, values, and worldviews, they are unlikely to be accepted. Today the structure of the attention economy means audiences may be unlikely to even hear the messages in the first place. AI agents are already further filtering and curating content on behalf of users, which may make it even harder to permeate information echo chambers.

17 J.N. Druckman, E. Peterson, and R. Slothuus, 'How Elite Partisan Polarization Affects Public Opinion Formation', *American Political Science Review* 107 № 1 (2013): 57–79.

DOI 10.30966/2018.RIGA.17.10

One way to square this circle is to go beyond delivering facts and information and instead seek to offer meaning. The most effective communicators connect information to what people care about by explaining what is at stake, why it matters, and how it relates to their lives. Storytelling can help with this, by making complex issues easier to understand and more relatable. The goal is not just to impart information in the hope that it changes attitudes and beliefs, but to affirm the social identities, values, and worldviews of the audience. By reconceptualising the core purpose of political communications from delivering messages to generating meaning, government has a better chance of generating the engagement needed to feed the algorithm. It can also begin to nurture networks of overlapping tribes, connected by a wide and heterogeneous set of issues, ideas, values, and stories that offer reach and credibility in a fragmented and polarised information environment.

One of the countries that best combines evidence-based messages with meaning is Ukraine. Since Russia's full-scale invasion in February 2022, Ukraine has been able to tell a powerful story of bravery and resistance in the face of unjustified aggression. While Ukrainian state agencies and high-ranking officials broadly seek to persuade global audiences with publicly justifiable and evidenced claims, they also offer meaning that taps into the values and identities of their audiences. They frame each message as part of a wider narrative of ingenuity and innovation prevailing against brute force, individualism fighting against collectivist tyranny, the defence of democracy from authoritarianism, and even triumph of a brighter tomorrow over a dark today. Tactically they pepper their online communications with sarcasm, memes, and witty one-liners, cutting against the gravity of their communications in a way that makes people want to identify with their cause and amplify their content.

There are clear differences between strategic communications in times of peace and times of war, in which the information environment is just another battlefield. Governments are more selective with the information they provide and face fewer domestic constraints, and it's obviously easier to offer meaning through communications when faced with an

DOI 10.30966/2018.RIGA.17.10

existential threat such as invasion. However, Ukraine's approach has lessons for governments in peacetime.

For example, the EU increasingly finds itself on the communications defensive, fending off criticism of over-regulation, democratic deficit, and political fragmentation. However, the EU has ample material for a meaning-based communications strategy at its disposal. It has one of the most powerful foundational stories of any political project: that of a system built from the ruins of World War II to ensure that disagreements between European states never again lead to war, and one that is increasingly relevant in today's turbulent and dangerous world. It offers people rights and agency; the ability to live, work, travel, and speak freely across borders; and a balance of economic prosperity and social protection. Yet its communications remain focused on providing legalistically framed information to audiences, not on harnessing these materials in ways that help the audience relate to and identify with the EU.

Effective communication cannot reshape geopolitical and geo-economic realities. However, it is a necessary condition of building sufficient consensus and social licence for the difficult long-term policies, such as European rearmament, that might.

Building block 2: Compete for attention through an 'always on' mode

Governments can no longer take visibility for granted. If they are not actively shaping the conversation, they risk being overwhelmed by it. Communication should not be limited to announcements or reactive statements. It requires a continuous campaign that actively prosecutes an argument.

This means consistently bringing something new into the public conversation: a clear line, a strong frame, or a timely intervention that generates reactions. Content does not necessarily need to entertain,

DOI 10.30966/2018.RIGA.17.10

but it must engage. It must be something audiences *want* to consume. It should give audiences a reason to pay attention. The challenge is to do so in a way that feels authentic and purposeful, aligned with broader objectives rather than appearing forced or performative.

So far the 'always on' mode has been exemplified mainly by anti-establishment politicians, rather than mainstream figures. In the UK both Green Party leader Zack Polanski and Reform Party leader Nigel Farage have been effective at creating moments that dominate media coverage. By simplifying complex issues into punchy soundbites, they have channelled raw emotion and mastered the use of high-energy digital formats, prioritising virality over evidence-based argument. Both make themselves highly accessible to the media and the ecosystem of voices in their respective movements, engaging with journalists and influencers in unscripted, authentic ways. They do not wait for moments; they create them. They generate headlines and provide audiences with a steady supply of material to interpret, react to, and amplify.

Incumbent governments must find a way to harness this campaign style of communications, despite the complexity, drudgery, and difficulty of daily governance. This does not necessarily entail a constant barrage of glib attacks on opponents, but rather communicating with purpose, constantly focusing on the *why* and not the *what* of governance. Policy announcements should become one moment in a series of overlapping campaigns that communicate what government stands for and is trying to achieve. And in ways that people find not just credible but motivating and engaging.

Ukraine has also mastered the 'always on' mode, always searching for new tactics to cut through. A striking example came in April 2026, when a Ukrainian soldier hacked into a Russian military recruitment call conducted via Zoom, directly addressing prospective recruits and warning them they would die if they signed up. The clip was widely amplified due to its exciting, entertaining, and shocking nature. While the stunt is unlikely to have influenced decision-making in Russia, its

DOI 10.30966/2018.RIGA.17.10

impact lay elsewhere: signalling to international audiences that Ukraine is innovative, agile, and tough.

Building block 3: Embrace less formal communication tactics by decentralising operationally

Governments do not have to resort to TikTok dances or AI-generated memes to cut through. In fact, government channels mimicking online culture and chasing trends can quickly feel inauthentic and awkward. Instead, governments should consider decentralising communications by moving beyond reliance on a single, centralised channel or voice, and embracing a more distributed model of communication.

One way of doing this is to develop differentiated channels with varying tones and formats. A much-cited example is the French government, which in 2025 dedicated a new official channel to engage audiences that no longer follow mainstream news. While much of France's state communications is formal and traditional, the X account @FrenchResponse delivers informal quips, sharp retorts, and clever headline-grabbing jokes to rapidly puncture false narratives on the platform that aim to damage France's image. The foreign ministry's spokesperson explained:

> Our interests, our image are being attacked in the information sphere. We instinctively feel we've got to turn up the volume and raise our voice to defend ourselves, and therefore actually also adopt the codes on the platforms where we're being attacked. We aren't changing the diplomatic message. We're obviously in favour of multilateralism and upholding the UN Charter […]. Our aim is to create impact. […] To have a reactive channel to respond very swiftly to the manipulation of information, which can be very viral

DOI 10.30966/2018.RIGA.17.10

> and sometimes very serious. […] We're going to post wherever there's debate.[18]

Another way of decentralising communication is by mobilising a wider ecosystem of voices beyond government, spanning civil society, creative industries, influencers, the media, and aligned networks. This inevitably involves relinquishing some degree of centralised control, but it significantly expands reach and resonance. Such partners have a better understanding of the tribes who make up their audiences, and are more adept at using platform-native formats and emerging technologies. Iran's partnership with Explosive Media illustrates the potential of this arms-length approach. Government gives cues and signals, but allows the movement and ecosystem to disseminate the message on their own terms. This also enables government to better meet the pace of the attention economy: while official government communications often face delays due to sign-off processes, affiliated networks of actors can contest harmful narratives, fill the void, and simply maintain presence in near real time.

There is no reason democratic governments could not similarly draw on the creative talent and supportive networks in their own societies to communicate more effectively and authentically. However, these networks cannot be purely transactional. They rely on a broad and heterogeneous set of actors sharing certain stories, meanings, and identities, even if only on specific topics. The MAGA movement is the foremost example of a Western government forging online tribes with divergent beliefs and worldviews into an effective political movement. Government communicators should seek to emulate this success by identifying and harnessing the meanings that turn dissemination networks into genuine movements.

Again, Ukraine is a paragon of this approach: alongside government communicators, there has been an unceasing flow of content from

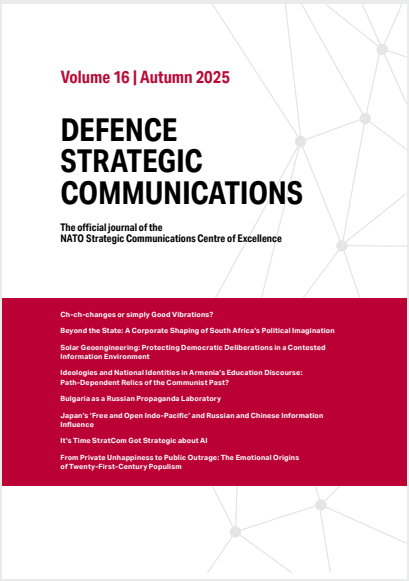
18 Pascal Confavreux, 'The French Response Account, a Tool for France in the Information War', interview by France Inter, *France in the United Kingdom,* 5 February 2026, https://uk.diplomatie.gouv.fr/en/french-response-account-tool-france-information-war.

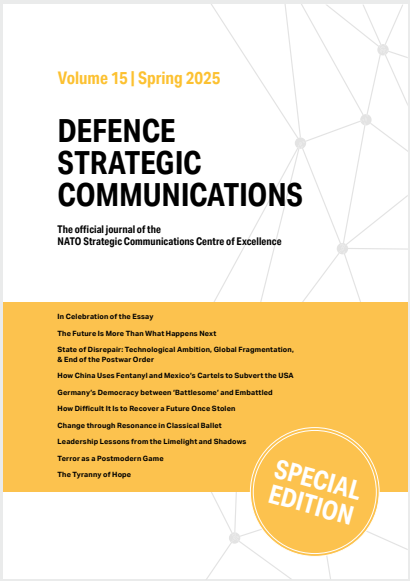
DOI 10.30966/2018.RIGA.17.10

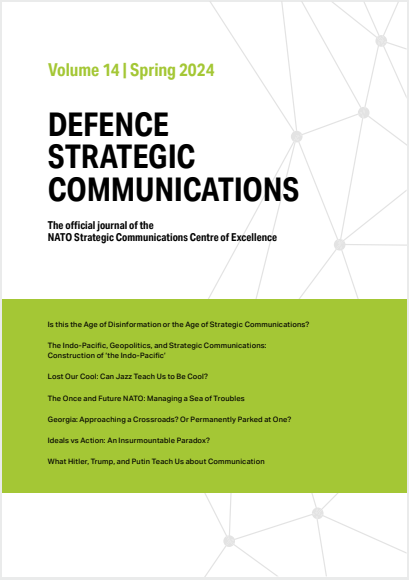
professional media outlets, influencers, bloggers, fact-checkers, and international allies circulating authentic, unpolished content from regular Ukrainian citizens. This has often had the greatest reach and impact. A plethora of different campaigns has been running in parallel, overlapping with and reinforcing each other. Rather than being centrally choreographed, Ukraine's 'beehive mentality' distributes communications across a wide network of actors. This reduces reliance on any single voice and enables rapid, multidirectional amplification of key messages.

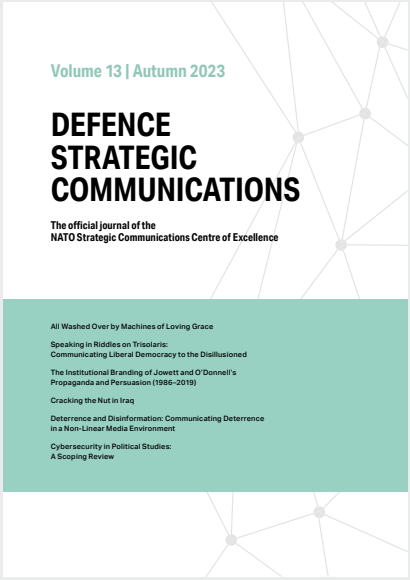
The question is no longer whether democratic states should adapt to the attention economy, but how they can reconcile epistemic integrity with reach and influence. Success will depend on their ability to make messages meaningful, to engage and mobilise audiences through proactive communication, and to scale their reach through a much wider ecosystem of allied voices and channels if they are to achieve impact.

Read all back copies
stratcomcoe.org/publications

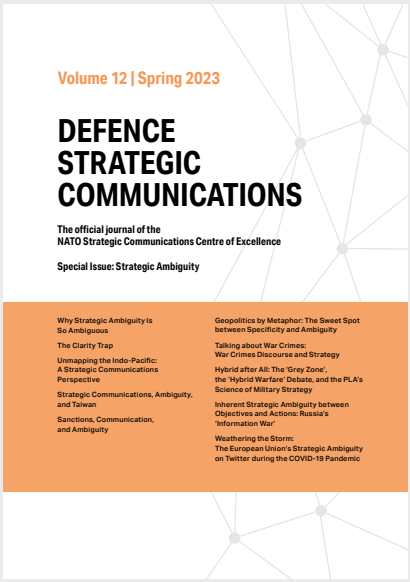


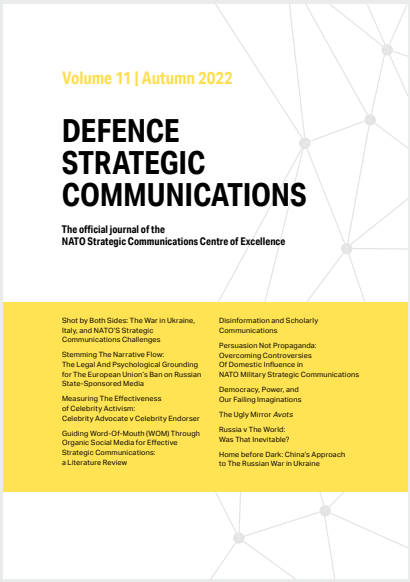


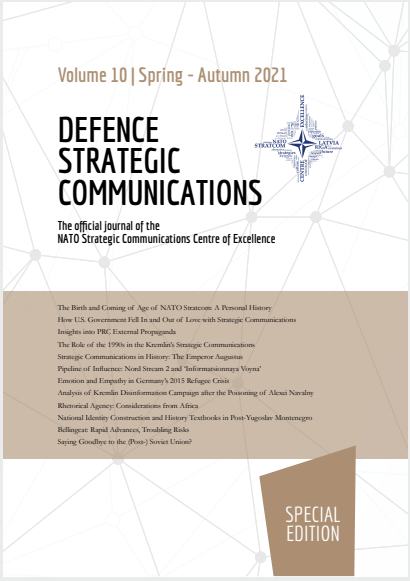


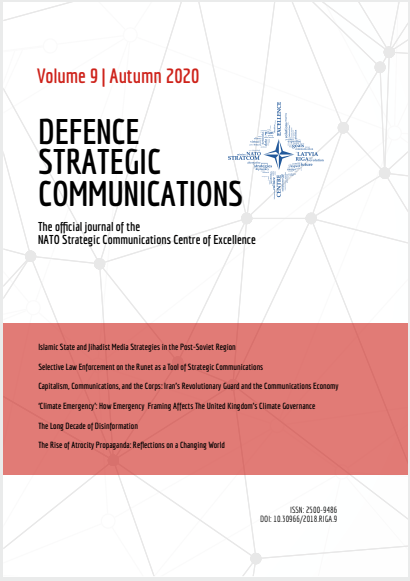


Read all back copies
stratcomcoe.org/publications

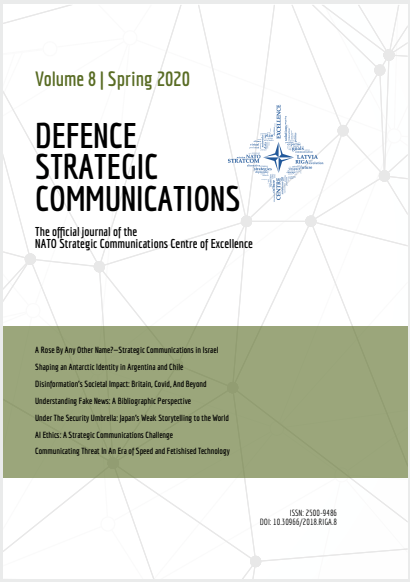


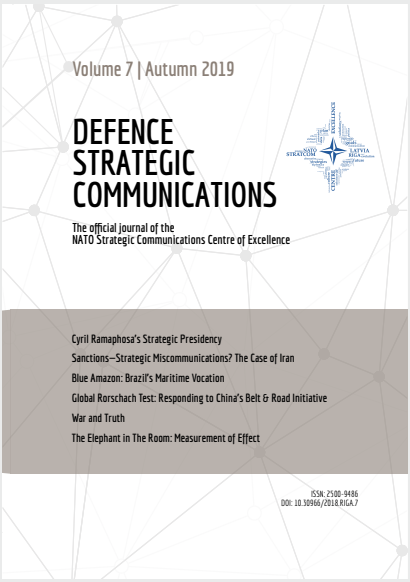


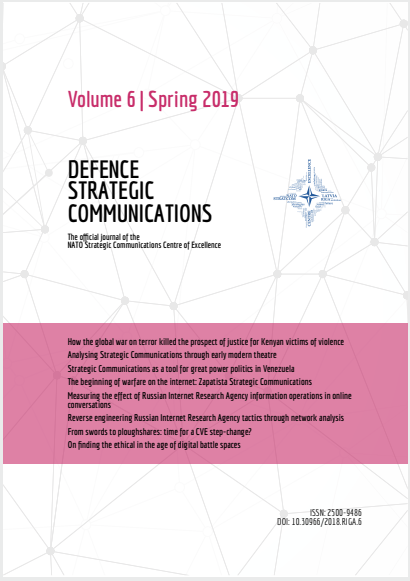


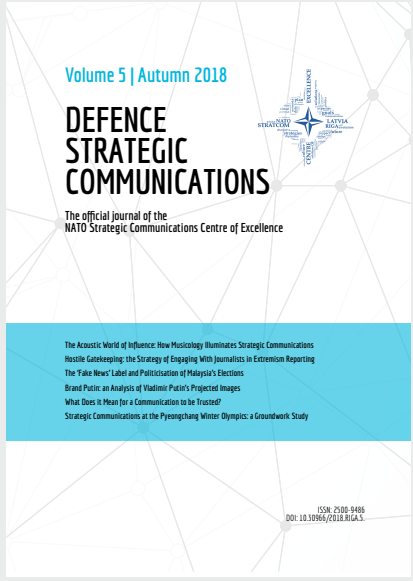


Read all back copies
stratcomcoe.org/publications

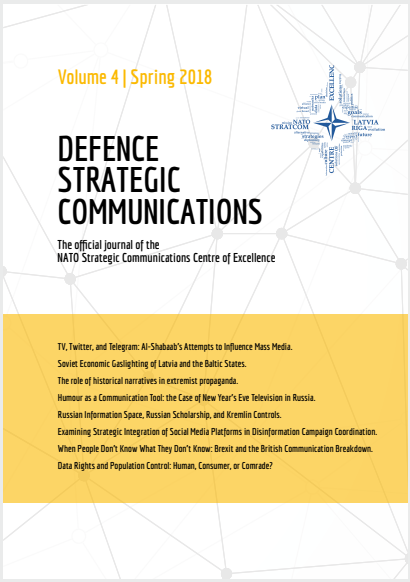


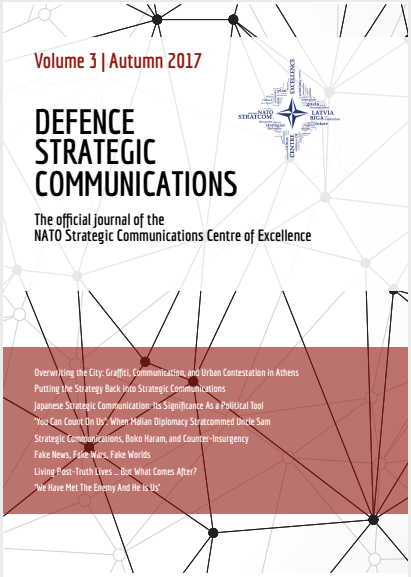


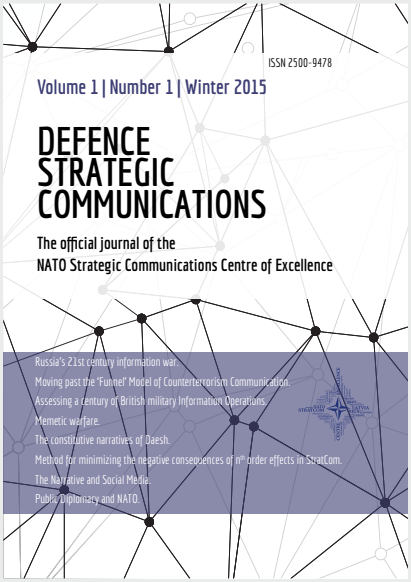




Read all back copies
stratcomcoe.org/publications







EVERYTHING COMMUNICATES

Defence Strategic Communications

ISSN 2500-9486

DOI 10.30966/2018.RIGA.17