Strategic Outlook 11

Wide awake in a world of disorder

Calle Håkansson, Gabriella Körling, Ida Johansson, Carl Marklund, Sofia Olsson, Björn Erik Skovdal, Peter Stenumgaard and Christopher Weidacher Hsiung (eds.)

FOI-R--5951--SE

June 2026

FOI

Strategic Outlook 11

Wide awake in a world of disorder

Calle Håkansson, Gabriella Körling, Ida Johansson, Carl Marklund, Sofia Olsson, Björn Erik Skovdal, Peter Stenumgaard, and Christopher Weidacher Hsiung (eds.)

June 2026

FOI-R--5951--SE

ISSN 1650-1942
Printed in Stockholm 2026 by the Swedish Defence Research Agency, FOI
Cover: Abstract piece Boutique canvas/Shutterstock
FOI-R--5951--SE
Approved by Måns Nilsson

Preface

Geopolitical turbulence: 2026 stands out not as a year of certainty, but one in which volatility itself has become the new normal. Russia's war of aggression against Ukraine has entered its fifth year, underscoring the persistence of instability in Europe's security environment. Developments ranging from the Greenland crisis to the war in Iran have contributed to increasingly strained transatlantic relations. The war in Iran has intensified global concerns over supply-chain security and energy prices, highlighting the deep interconnections between regional crises and the broader international order. At the same time, technological developments in areas such as agentic AI; autonomy, including in robotics; and increased interconnectivity are profoundly affecting our societies, the world economy, and the nature of warfare.

The title of this eleventh edition of FOI's Strategic Outlook, *Wide Awake in a World of Disorder*, alludes to the earlier FOI reports on Russia's attack on Ukraine in 2014 (*A Rude Awakening*) and Russia's full-scale invasion of Ukraine in 2022 (*Another Rude Awakening*). If the world at large hit the snooze button after 2014, or at least kept its eyes wide shut, we are now wide awake in a profoundly dangerous and unpredictable security situation.

This anthology seeks to examine how the rapidly changing strategic and global landscape shapes threats as well as the prerequisites for security, resilience, and defence. The chapters span topics from security policy to military technology, emphasising the breadth of FOI's research and analysis. This year, I am particularly pleased to welcome the external contribution from the NATO Climate Change and Security Centre of Excellence (CCASCOE). This contribution underscores climate change as a threat multiplier.

It is my conviction that anyone who has to navigate the current security landscape will find at least some useful waypoints in this volume for a safer and more secure journey. At the end of the day, research will not prepare you for one future but for multiple futures.

Jens Mattsson
Director-General

May 2026, Stockholm

Table of Contents

Introduction

This eleventh edition of FOI's Strategic Outlook examines the increasingly challenging global political, security, and economic environment facing Sweden and Europe. In 2014, following Russia's annexation of Crimea, FOI published *A Rude Awakening*, which assessed the worsened security situation and its broader implications for global security. Russia's full-scale invasion of Ukraine in 2022 prompted a further set of reflections in the anthology *Another Rude Awakening*, focusing on the war and its implications. Since then, shocks and strains on the international system have multiplied, creating a more disordered and disorientating global landscape. This has inspired the title of this edition, *Wide Awake in a World of Disorder*, which brings together contributions examining ongoing transformations in the world order, with particular attention to security policy, societal security, and military and technological developments. This introductory chapter provides an overview of the current state of affairs and outlines the structure of the report.

The international system entered 2026 visibly strained. Great-power rivalry is continuing to intensify and international norms are increasingly being eroded and challenged. This rivalry is fuelling technological competition and challenging trade relations built around post-Cold War economic globalisation, driving new forms of industrial policy and protectionism. Major powers aim to utilise material resources such rare earth minerals, missile counts, and semiconductor production to enhance and wield power and influence. At the same time, the world has witnessed a sharp increase in the number of armed conflicts. These developments are in turn driving record levels of military expenditure and an ongoing global rearmament. Finally, the prospect of a major great-power military conflict or war cannot be ruled out. Changes to global and regional balances of power and power transitions have historically often resulted in violent outcomes. In our time, the growing strategic rivalry and animosity between the US and China resembles such dynamics, although it is far from certain that the US–China rivalry will lead to a military confrontation.

Today, the rules-based liberal international order, painstakingly constructed after 1945 and extended after 1989, is unravelling under the combined pressure of revisionist powers and domestic disenchantment. Liberal institutionalism is under increasing strain. The International Criminal Court has come under sustained pressure, with sanctions imposed on its officials and threats directed at states that cooperate with it. The World Trade Organization's Appellate Body remains a shell. The United Nations Security Council has been paralysed for years over Ukraine and Gaza. Coercion has also returned as a tool of influence: tariffs, sanctions, and the threat of force are increasingly deployed to extract concessions that, only a few years ago, would have been pursued through negotiation. The cumulative effect is a form of politics that is more transactional, less rule-bound, and more permissive of force.

The United States stands out for the explicitness of its turn under the current administration. National strategy documents and the practice they license have moved decisively from the language of cooperation, partnership, and shared rules to the language of national interest, national security, and reciprocal advantage. Volatility and unpredictability are no longer regarded primarily as costs to be minimised but as instruments to be wielded; the willingness to walk away from agreements is itself a source of bargaining power.

The sharpest expression of this shift is the unsettling of relationships once taken for granted. The United States has pressed Denmark over Greenland and demanded support for its intervention in Iran, which has shaken the NATO alliance and struck at the very core of the transatlantic relationship. As a result, Europeans are being forced to take more responsibility for their own security.

China presents a different and more ambiguous case. Beijing routinely emphasises its commitment to the agreements it has signed on climate, trade, and the law of the sea, contrasting its own constancy with American volatility. In practice, however, the gap between rhetorical adherence and operational compliance has widened: Chinese industrial subsidies persist despite WTO commitments, fishing fleets operate well beyond declared zones, and coercive economic measures are deployed against partners that displease Beijing. In the Indo-Pacific, we are witnessing a more assertive China, with intensifying US–China competition looming in the background.

Russia, in turn, has continued its war of aggression against Ukraine. Yet Russia has also shown how thinly stretched its power projection has become, partly as a result of its full-scale invasion of Ukraine.

Taken together, these developments have produced a striking convergence of analytical judgment: across capitals and ideological camps, the working assumption is that the world order itself is in flux. Foreign ministries, central banks, corporate boards, and editorial pages write of the present moment in terms once reserved for the great transitions of the twentieth century. Talk of a "New World Disorder" has migrated from the margins into think tank reports and ministerial speeches. The implication is that we have passed the point at which restoration is plausible, and that the relevant question is now how to navigate a system without a settled architecture.

Confronted with this combination of pressures, states have responded along a spectrum running from deliberate strategic adaptation at one end to improvisation and muddling through at the other. What we are seeing is a proliferation of hedging behaviours, such as diversification of suppliers, parallel currency arrangements, and multiple alignments held simultaneously.

Whichever characterisation of the present moment proves more apt, the mere conviction that the world order is changing or coming apart has produced two contradictory trends in global affairs. They run in parallel, and recognising both is essential for avoiding the twin errors of premature alarm and complacent reassurance.

The first trend follows from the new assertiveness of the great powers. As the United States, China, and Russia press their interests more openly, force their advantages more often, and weaponise other states' dependencies for security, market access, and critical supplies, middle powers and trade blocs such as the European Union are working, to the best of their varying capacities, to offset the fallout. The EU has accelerated its Critical Raw Materials Act, opened new partnerships from Chile to Kazakhstan, and pursued trade arrangements with the Mercosur bloc that had languished for two decades. Japan and South Korea have deepened cooperation with each other to a degree that would have been politically unthinkable a few years ago. India has cultivated a multi-vector posture that allows it to buy Russian oil, host American summits, and convene the Global South at the same time. The Gulf states have positioned themselves as indispensable interlocutors to all sides at once. Australia, Canada, and the Nordics are seeking to recapitalise their defence industrial bases. Across these cases, the explicit working assumption is that while the hope for its return may linger on, the rules-based order can no longer be relied upon to do the protective work it once did. There seems to be a growing consensus that strategic autonomy in critical sectors such as energy, food, semiconductors, finance, and defence must be built deliberately, even at considerable cost, challenging the market logics of globalisation.

The second trend cuts in the opposite direction. Even as the headlines turn confrontational, the mundane workings of international agendas, institutions, and processes continue, in many places, often silently and surprisingly unperturbed. Standard-setting bodies meet and reach agreement. Health regulators coordinate on pandemic preparedness. Tax authorities exchange information under the OECD framework. Aviation, shipping, and telecommunications regulators issue joint guidance. Central bank governors continue to coordinate, often discreetly, on financial stability.

The combined picture, then, is neither one of orderly transition nor of comprehensive collapse. It is, rather, a system in which the high politics of great-power rivalry coexists with the low politics of continued cooperation, in which middle powers are simultaneously hedging against breakdown and investing in its repair. It is a system in which the most consequential developments in technology, in climate, and in trade will be shaped as much by the cumulative weight of these mundane processes as by the dramatic gestures that dominate the headlines. The strategic task for 2026 and beyond is to hold both pictures in view at once.

Outline of the Report

To take stock of and analyse this current state of affairs, this edition outlines different perspectives on a world order in flux, from the views of the major powers to how science and technology are changing the international order. The contributions in this anthology reflect a broad range of FOI's research and analysis, with contributions from five out of six of the agency's research divisions. The 20 articles in this year's *Strategic Outlook* are organised into three broad thematic areas: Security Policy (Part One), Societal Security (Part Two), and Military and Technology (Part Three). All chapters aim to shed light on different perspectives influencing, or being influenced by, a changing and more challenging world order. Every article provides a short recommendation for further reading. As editors, we are also very pleased to include an external contribution from the NATO Climate Change and Security Centre of Excellence (CCASCOE) in this year's edition.

The editors

Part One
Security Policy

1. The Changing Role of the United States—From Hegemon to Normal Great Power?

Albin Aronsson and Björn Ottosson

When the Cold War ended, the United States emerged as the most powerful state in modern history. Many analysts expected that such dominance would be temporary: other powers would balance against Washington, and the US would eventually behave like a more "normal" great power, restrained, less globally ambitious. Instead, the US presided over decades of unipolar leadership, expanding alliances and sustaining a liberal international order. Today, however, the foundations of that order are less secure. Rising rivals, domestic divisions, and shifting strategic priorities prompt a pressing question: "Is the United States becoming a normal great power?"

When the Cold War ended, many analysts ranging from historians to defensive realists predicted that the United States would finally return to "normalcy." Freed from the existential rivalry that had defined nearly half a century of global politics, they expected the US to scale back its military commitments, reduce defence spending, and assume a more restrained role in world affairs. Realist scholars, in particular, anticipated that the unprecedented concentration of American power would provoke counterbalancing coalitions, arguing that in a system defined by anarchy and the logic of balance-of-power politics, no state would tolerate prolonged unipolar dominance. Yet for nearly three decades, such balancing failed to materialise in any sustained or unified form. Bandwagoning, whereby weaker powers align with a stronger power, ensued, and the United States instead presided over what some called a "unipolar moment," expanding alliances, promoting democracy, and underwriting a rules-based international order.

Today, however, the international environment appears to be shifting. American power remains formidable, but democracy is retreating globally, authoritarian coordination is deepening, and Washington's commitment to the liberal international order has become more selective. President Donald Trump has been described as the first truly post–Cold War president, less invested in global ideological competition and more focused on sovereignty, burden-sharing, and strategic retrenchment. His emphasis on the Western Hemisphere, criticism of allies' defence spending, and scepticism towards multilateral institutions suggest a recalibration of US grand strategy.

Is the United States becoming a "normal" great power, prioritising relative gains, regional influence, and transactional diplomacy over systemic leadership? This essay addresses that question through Kenneth Waltz's well-established three-images analytical framework. It begins with the international system, moves to domestic politics, and concludes with leadership. By proceeding from structure to state to leader, it evaluates whether America's changing role reflects systemic pressures or contingent political choices.

Systemic Change: From Unipolarity to Strategic Rivalry

The global distribution of power has changed profoundly over the last three decades. Following the collapse of the Soviet Union, the United States stood as the unrivalled superpower. The so-called unipolar moment was marked not only by American military predominance but also by the absence of meaningful counterbalancing coalitions. Although the US share of global GDP has remained relatively stable at roughly 25 per cent, the broader distribution of power has shifted dramatically. Most notably, China's rapid economic expansion has elevated it to near-peer status, bringing it closer to the United States in material power than any rival since the late nineteenth century, yet still not equal in military reach, alliances, or global projection. Today, no other state approaches the combined weight of the US and China, and Beijing is in many respects more economically integrated and technologically advanced than the Soviet Union ever was.

These shifts have systemic consequences. The concentration of power that sustained unipolarity has eroded, and structural pressures towards bipolarity have intensified. At the same time, American fiscal constraints have compounded this transition. US federal debt held by the public now stands at almost 100 per cent of GDP and continues to rise. The United States pays more in interest on its debt than on defence, and projections indicate that interest payments will consume an increasing share of federal spending. Historically, great powers that devote more resources to debt service than military capability often experience strategic decline. The growing scarcity of resources, combined with the emergence of a near-peer rival, is acknowledged in the Trump administration's latest National Security and National Defense Strategies, in unusually direct language about limits and trade-offs.

Meanwhile, the long wars in Afghanistan and Iraq, launched after the September 11 attacks, contributed to strategic overstretch. Two decades of counterinsurgency, nation-building, and expanded global commitments strained personnel, readiness, and fiscal resources. A widening gap has emerged between strategic ambitions, such as deterring China, confronting Russia, sustaining alliances, and maintaining global force posture, and the defence budgets and material means allocated to realise them. This imbalance has reinforced doubts among allies and adversaries alike about Washington's ability to uphold expansive commitments over time.

Patterns of alignment are also shifting. During the 1990s and early 2000s, many states effectively bandwagoned with American power, integrating into US-led institutions and security frameworks. That dynamic now appears to have slowed. Instead, hedging has become more common. States seek to preserve economic ties with China while relying on US security guarantees. Defence spending is rising rapidly across Asia and Europe, reflecting concern about China and Russia, and uncertainty about American reliability. Fear has re-entered the system: fear of abandonment, fear of entrapment, and fear that US overstretch may limit its willingness or capacity to respond in a crisis. Such fears can become self-reinforcing, prompting further militarisation and strategic opportunism.

The rapid pace of technological change compounds these trends, increasing uncertainty about the future distribution of power. Technological breakthroughs may reshape both economic productivity and military effectiveness in unpredictable ways. New technologies could amplify the advantages of leading economies, or allow challengers to leapfrog established powers. They may also render expensive legacy military platforms vulnerable or even obsolete, altering the current balance between quality and quantity in force structures.

Yet the ultimate trajectory of the system is undecided. The distribution of power increasingly resembles bipolarity, but it is not clear whether the world is moving towards a stable US–China bipolar order, a more diffuse multipolar configuration, or a hybrid system in which the United States retains a unique, if no longer unchallenged, role as the indispensable power.

Domestic Politics: Fragmentation, Fatigue, and Fiscal Constraints

With the end of the Cold War, the United States no longer faced an adversary comparable to the Soviet Union, and the acute threat perceptions that had dominated political imagination for decades dissipated. As a result, domestic preferences increasingly shape US foreign and security policy, fostering a more inward-looking America. A generational shift has amplified this trend: younger Americans, lacking direct experience of World War II or the Cold War, do not share the intense sense of vulnerability that guided older cohorts. Interest in, and knowledge of, foreign affairs have declined, and politicians struggle to make a persuasive case for broad international engagement.

Early analysts who predicted a return to normalcy argued that the US would move away from the "politics of fear" and ideological conformity of the Cold War, envisioning a rediscovery of domestic democratic traditions. They were partly correct: many Americans have turned inward. Yet this shift has not produced calm civic renewal. Domestic politics are highly polarised, political parties are more ideologically rigid, compromise is rare, and partisan differences increasingly spill over into foreign policy. Large parts of the electorate perceive that both parties' elites pursue foreign policies serving their own interests rather than the broader public, while wars, outsourcing of jobs, and stagnating real wages

have increased scepticism towards both domestic institutions and international commitments. Advances in technology and social media have intensified these dynamics, and have heightened middle-class anxiety about job security, further focusing attention on domestic priorities.

The US faces multiple pressing domestic challenges, including welfare, public health, inequality, political fragmentation, and rising national debt. Polarisation and institutional gridlock make it difficult to address these problems, forcing domestic concerns to take precedence over sustaining a consistent global role.

The result is that the United States is increasingly preoccupied with domestic politics, a focus that is arguably "normal" for a large, multifaceted country confronting internal divisions, economic anxieties, and cultural debates. Technological and social forces reinforce inward pressures, further constraining the country's ability to pursue broad international engagement. Polarisation also creates sharper swings in US foreign policy as power shifts between the two parties.

Presidential Leadership: America First and the Politics of Sovereignty

Since the end of the Cold War, presidents from George H. W. Bush onward have sought to preserve an expansive US role, despite mounting domestic headwinds. Bill Clinton deepened liberal internationalism through globalisation and NATO enlargement, but domestic scepticism grew. George W. Bush entered office with a promise to narrow US interests, yet 9/11 transformed his presidency, producing an interventionist and sometimes unilateral foreign policy. Barack Obama, elected partly on opposition to the Iraq War, recalibrated rather than abandoned international leadership. Though rhetorically committed to the rules-based order, he reduced military deployments, emphasised burden-sharing, and cut defence spending, reflecting domestic fatigue with prolonged wars.

Donald Trump marks a sharper break. Rather than resisting the inward turn, he embraces it. Presenting himself as correcting decades of elite overreach, he unapologetically advances his "America First" agenda, signalling a partial retreat from America's post–Cold War "open door" approach to trade, alliances, and immigration. Stricter border control and reduced immigration become central symbols of restored sovereignty. Trump's rise is best understood not as an independent cause, but as both an expression and a catalyst of popular dissatisfaction with globalisation, elite-driven foreign policy, and stagnant middle-class wages. Through his nostalgic MAGA message, he fuses populism, nationalism, and neo-mercantilism with a hard-nosed assessment of power and geopolitical competition.

Trump's leadership style further distinguishes him. Using social media in unprecedented ways, he bypasses institutions and communicates directly with supporters and foreign leaders, reinforcing personalisation and affective polarisation.

Hyperbolic rhetoric and abrupt tone shifts introduce unpredictability, generating uncertainty among allies and adversaries. Trump's worldview is state-centric and transactional: alliances are judged as bargains requiring reciprocity rather than long-term commitments. He prefers bilateral negotiations, where US leverage is strongest, and shows little regard for multilateralism, arguing that many international institutions are corrupted by states whose interests diverge from those of the US, constrain American sovereignty, and lack intrinsic moral authority. Consequently, he has no qualms about acting unilaterally.

Crucially, Trump questions the long-term benefits of the US-led liberal order. In his view, multilateral institutions enable free-riding, constrain US sovereignty and power, and fail to deliver reciprocal gains. This scepticism reflects a shorter time horizon and a narrower conception of national interest, privileging immediate returns over diffuse, long-term systemic advantages. If broad US global engagement during the Cold War, and especially after it, is seen as an historical anomaly, then aspects of Trump's foreign policy can be interpreted as a "return to normalcy," prioritising domestic strength, tighter borders, selective economic nationalism, aggressive unilateralism, and less responsibility for sustaining global order. Intellectually and rhetorically, Trump situates himself within a tradition of assertive nationalism associated with Presidents Andrew Jackson, James K. Polk, and William McKinley, rather than the bipartisan liberal internationalist establishment that has shaped US grand strategy in recent decades.

However, engaging in war against Iran sits uneasily with this orientation, contradicting the administration's emphasis on prioritisation under constrained resources and risking both a diversion of attention and strategic overstretch. It also conflict with domestic preferences for restraint that have underpinned Donald Trump's political support, with the gap between his choices and the expectations of his political base likely to widen the longer the conflict persists. Taken together, this underscores how leadership choices may diverge from both systemic pressures and domestic political dynamics. The extent to which Trump and his party will face domestic political consequences for this decision remains uncertain, though the November midterm elections will provide an early indication. Any systemic or strategic costs incurred by the US are likely to become clear over a longer time horizon and may not become apparent until after Trump has left office.

Conclusion: Retrenchment, Polarisation, and Strategic Uncertainty

The United States stands at a strategic crossroads shaped by pressures at all three levels of analysis. At the systemic level, the erosion of unipolarity and the dispersion of power generate incentives for retrenchment. If the international system evolves towards multipolarity, with diffuse centres of power and growing regional autonomy, the logic of balance-of-power politics may reinforce a narrower US role. Under such conditions, an inward turn would not represent an aber-

ration but adaptation. Yet the trajectory is not predetermined. If the emerging order consolidates into a bipolar configuration defined by intensifying US–China rivalry, systemic pressures could instead resemble those of a new Cold War. Heightened threat perceptions might reverse domestic fatigue, reinvigorate alliances, and restore a stronger US leadership. In this sense, structure may either entrench retrenchment or compel renewed engagement.

At the domestic level, however, polarisation currently appears self-reinforcing. Political fragmentation, fiscal constraints, and technological disruption demand sustained attention and produce sharp swings in foreign policy. Even if systemic pressures push towards renewed competition, domestic instability may limit strategic consistency. Leadership matters, but it operates within these constraints. President Trump embraces and amplifies the inward turn; another president might resist it. Elections matter. Such oscillation itself contributes to global uncertainty. Recent actions, such as strikes against Iran, further underscore the need to analyse US strategy across all three images simultaneously.

Those who predicted a post–Cold War "return to normalcy" were arguably clearer about what the United States would leave behind than about what would replace it. The future remains unsettled. It is also worth recalling that predictions of retrenchment have surfaced repeatedly throughout history, from interwar retrenchment and post-Vietnam malaise to the economic anxieties of the 1970s, yet the US has consistently demonstrated a capacity for adaptation and renewal. The US retains extraordinary power, resources, and alliance networks, and it could remain the indispensable power if political will aligns with strategy. What is certain, however, is uncertainty: the role America will play in an era of shifting polarity and rapid technological change remains open.

Further reading

Albin Aronsson and Björn Ottosson, 2025, *Drift or Abandonment? Exploring How US Domestic Politics and External Realities May Affect US Security Engagement in Europe 2025–2029*, FOI Reports FOI-R--5777--SE.

The White House, 2025, *National Security Strategy of the United States of America*, Washington, D.C: The White House.

Kenneth N. Waltz, 2001, *Man, the State, and War: A Theoretical Analysis*, New York: Columbia University Press.

2. China's regional policy and its strategic rivalry with the US under the second Trump administration

Johan Englund and Oscar Almén

Fuelled by great power competition and securitisation of economic and technological tools, the global geopolitical landscape is in flux. In the last 15 years, Washington has shifted its focus to the Indo-Pacific region to counter what it identifies as its primary strategic rival, China. However, with its transactional approach to bilateral relations, the Trump administration is sowing doubts about its security commitments towards its allies. China, in contrast, portrays itself to the world as a stable and reliable partner, while prioritising its near region. Amidst these transformational changes, how does China view its immediate vicinity and the strategic rivalry with the US that is unfolding on a regional and global level? This article first discusses Beijing's global and regional views and goals, before examining how it sees its opportunities and challenges under Trump 2.0.

China's ambitions in the world and its view of the international order

From China's vantage point, the global order has long been dominated by a US-led West that sets the rules and terms. Beijing views the world system as being biased by the West's dictums of liberal values and norms, and thereby disadvantageous and unfair to not only China, but also developing countries across the globe. In Beijing's eyes, it is a world order built on power politics and pursued through Western self-interest that is unjust for many of the world's countries.

As it rises in the existing international order, China seeks to expand its international influence as a major regional and global power. It demands that the international community respects and accepts it as a legitimate great power. This both reflects and is rooted in China's overarching goal of achieving the "China Dream" of the "Great Rejuvenation" by 2049, the 100th anniversary of the People's Republic of China (PRC). By this time, China aims to hold comprehensive national power that encompasses national prosperity, a "world-class" military, and the incorporation of Taiwan. Under Xi Jinping, China strives to take centre stage in the world. This stands in contrast to Xi's predecessors, who followed a more cautious foreign policy of "hiding your strength and biding your time." While China's previous leaders sought to downplay China's rise, Xi, on the contrary, promotes it. Driven by the notion that "the East is rising and the West is declining" and that time is on its side, Beijing spreads the narrative that the global power bal-

ance is shifting in China's favour. Whether the top leadership really believes this narrative remains uncertain, but it seems to hold some conviction in China's policymaking circles. Some Chinese senior scholars argue that China has now narrowed the power gap with the US to the point that the US leadership realises that it cannot defeat China, but must engage with it as a peer great power. This, they argue, reduces the risk of military conflict between the two powers.

In light of all this, China seeks to reshape, but not reinvent, the existing international order into one that better supports China's interests and better represents what it considers to be its rightful place as a major power in the world. China wants to "democratise international relations" in a way that focuses on national sovereignty and non-interference in internal affairs, while regarding unilateral interventions in international affairs as detrimental to global order. It introduces a state-centred approach and highlights its own right to development. Beijing's proposed foreign-policy vision encapsulates what it refers to as a "community with a shared future of mankind," which envisions a multilateral and multipolar order that encompasses Beijing's overarching interests.

China's view of its neighbourhood and strategic rivalry with the US

Perhaps nowhere is the collision course with Washington as palpable as in China's near region, where Beijing finds much of its immediate economic and security interests.

Chinese global goals translate directly into how it approaches its neighbourhood. Under Xi Jinping, neighbourhood diplomacy has been prioritised, and the Asia–Pacific is treated as an increasingly important region for advancing China's interests. It closely links developments in the near region with China's larger goal of achieving the Great Rejuvenation. Beijing's long-term vision for the region encompasses an "Asian order" that gradually rejects the US alliance system. This would be replaced by a China-led order where countries "pursue partnerships rather than alliances," and where China brings development to the region and becomes the leader that regional powers depend upon. Just as China advocates a "community with a shared future of mankind" in global affairs, in Asia it focuses on a community among Asian nations. In China's view, there is an exclusive "Asian way" consisting of "Asian values of peace" that should undergird the regional order. By tying its neighbours into its orbit as their rule-setting leader, China positions itself to shape developments in line with its national interests.

Trump 2.0 in China's neighbourhood: Beijing's view

So how has China responded in its near region to the transformative actions that have been undertaken by the second Trump administration? In its bilateral interactions with Washington, the Chinese government undertook sharp countermeasures to Trump's trade war. This forced Washington to a relative and tem-

porary retreat, which validated Beijing's view of its power position vis-à-vis the US. Yet the Chinese leadership is likely acutely aware of its vulnerabilities against Washington, such as dependence on critical technological components and US military and political support for Taiwan, as well as the continuation of the US alliance system in Asia.

However, Beijing treads a somewhat careful line in its near region, knowing the complexities and strong reluctance among many Asian nations to take sides in the competition between the US and China. That said, it has doubled down on sending the message to nations that China is a reliable partner amidst turbulent geopolitical winds and Trump's threats.

On the international stage, China promotes itself as a champion of open and inclusive economic cooperation and of development rather than protectionism. At the World Economic Forum in Davos in January 2026, Vice-Premier He Lifeng warned against the world returning to the "law of the jungle" and said that "a very small number of countries should not enjoy the privilege of pursuing their own selfish interests." He presented China as a champion of the rules-based order, while praising the benefits of "free trade and economic globalisation."

More particularly in its immediate vicinity, China seeks to assert to Asian nations its commitment to globalisation and present itself as a force of stability. Only a week after Trump's so-called Liberation Day, when he announced a broad package of high tariffs on many Asian countries, the CCP held a high-level Work Conference on Neighbouring Relations. The conference sent a message that stable and positive relations with the region are of utmost importance for China and signalled its intent to deepen its regional ties, for example in industrial-chain and supply-chain cooperation. A week later, Xi travelled to Southeast Asia, where he promoted economic support and cooperation and emphasised Asian solidarity against external pressure. By trying to strengthen trade relations in the region amid growing scepticism towards the US, Beijing presents itself as the more reliable partner while at the same time bolstering its position against the US.

Opportunity or challenge?

In many ways, Beijing likely views actions under Trump as an opportunity for China to advance its positions in the region vis-à-vis the US. Some Chinese scholars are very critical of how Trump handles the US relationship with its allies and believe that it creates distrust of the US that will be hard to repair, even if a Democratic administration takes over after him. China, in contrast, has the advantage of continuity, which makes it a more reliable partner than the US. As scepticism of Trump's transactional approach grows, the US could come to alienate Asian nations and diminish trust among regional partners and allies in American security commitments. In the long term, this would play into the hands of China as the responsible and development-oriented actor with which countries seek deeper engagement and greater interdependence.

Under the Trump administration, globalisation and value-based policies are being significantly reduced. For the Chinese government, the American case for de-globalisation provides China with an opportunity to step up as an advocate and bearer of globalisation, even though its own policies very much centre around state-centric and self-reliant approaches. As Washington disengages from a series of multilateral institutions and openly legitimises unilateral actions to secure national interests in international contexts, China may see a chance to enlarge its influence in multilateral settings and international institutions such as the UN. Moreover, sitting in Beijing, the American downplaying of democratic freedoms and rights may look like a good chance for the PRC to advance international acceptance of country-specific governance systems.

Yet, China also perceives risks and challenges with Trump 2.0. While the recent US National Defense Strategy clearly depicts the Western Hemisphere as its primary sphere of interest, reducing China to a secondary focus, there are no illusions in Beijing that the US will withdraw from Asia. Although the strategy posits a more value-free and less critical language to describe Chinese activities in the Indo-Pacific, it nevertheless emphasises the need to establish "a strong denial of defense along the First Island Chain" and seeks to prevent China from dominating the region. From Beijing's perspective, this remains a crucial challenge posed by its main strategic rival to its core interests in the region.

On a global level, in line with its notion of spheres of interests, US dominance in Latin America may create significant obstacles for Beijing in terms of being cut off from critical supply chains and losing access to important export markets. Under the Trump administration, the US openly utilises coercive and hard power in a way that earlier administrations did not. This is a source of uncertainty that Beijing may find difficult to manage. Red lines and subsequent retaliation may come more harshly and unpredictably than China had previously calculated. This was perhaps most obvious in the case of the abduction of Venezuela's president, Nicolás Maduro. The US attack on Venezuela created strong reactions in China. Some nationalist scholars even argued that if the US threatens China's business interests in Latin America, China should do the same to US business interests in Asia.

Indeed, China has persisted in its assertive positions on sovereignty issues in its near region. Military activities around Taiwan have intensified, while its aggressive posture in the South China Sea has only been reinforced, and Beijing has dialled up tensions with Japan. These actions can partly be seen as a test of the Trump administration's response, but they also reflect Beijing's sense that the balance of power in the region is shifting in its favour. To China's neighbours, however, these actions only make US warnings about China as a security threat to the region sound truer, which may undermine the advantages China gains from its increasing economic cooperation there.

It should also be noted that China currently struggles with domestic economic and political challenges, which is likely to reduce its appetite for bold external moves, at least in the short term. The necessary restructuring of China's economy from export-led to consumer-driven is proving very difficult to achieve. Moreover, Xi Jinping's purges of China's military leadership have left the People's Liberation Army crippled, and it will take some time, and some intense power struggle, before a new leadership is in place.

Finally, Trump's hardening line against American partners and allies may also lead them to bolster their defence capabilities and align with American countermeasures against China. If the collective network of American allies and partners is reinforced and their deterrence capabilities are enhanced, rather than causing the network to disintegrate, Beijing's outlook for achieving its long-term goal of a China-led region would look dimmer.

To sum up, while Beijing takes a cautious view of Trump's use of the US's immense military and economic power, in the long run the Chinese leadership expects China's influence in the Asia-Pacific region to grow. Much of that depends on the extent to which the US and its allies and partners can cooperate.

Further reading

Almén, Oscar, Johan Englund, and Björn Ottosson, 2021, *Great Power Perceptions—How China and the U.S View Each Other on Political, Economic and Security Issues*, FOI-R--5040--SE.

Englund, Johan and Oscar Almén, 2024, *Den hundraåriga folkrepubliken—En bedömning av Kinas utveckling och relation till USA mot 2050*, FOI-R--5631--SE.

Weidacher Hsiung, Christopher and Johan Englund, 2024, Facing an Era of Great Power Rivalry: Beijing's Efforts to Build Coalitions and Strategic Relations with the Global South and Russia. In: Christopher Weidacher Hsiung et al., (eds). *Strategic Outlook 10: China as a Global Power*. FOI-R--5620--SE.

3. Russia: Striving Towards Agency in a Multipolar World Order

Maria Engqvist and Emil Wannheden

Russia's security policy since the late 1990s reflects a striving for agency in an international system perceived as Western-dominated. However, the "end of history," as proclaimed by political scientist Francis Fukuyama in 1989, meant very different things for the West and for Russia. Since 2014, official discourse increasingly frames the confrontation with the West as a struggle in civilisational and existential terms. Yet Russia's capacity to exercise agency in a genuinely multipolar order will be constrained by economic and geopolitical limitations.

Russia and the West: Clashing Histories

Having emerged as one of the victorious powers after the Second World War, the Soviet Union exerted unprecedented global influence, usually in opposition to the United States. This stance was perhaps best signified by its permanent membership of the UN Security Council and, of course, by its nuclear arsenal. After the dissolution of the Soviet Union, the Russian Federation became its de jure successor. In this vortex of shifting power, both established and emerging political elites in the newly formed Russian state were under the impression that its superpower status had not disappeared. This view was also reinforced by Western decision-making and behaviour at the time. The fact that the Russian Federation retained both a seat on the Security Council and its nuclear capabilities testifies to the persistence of this notion among Russian decisionmakers.

After a brief period of accommodation with the West pushed by Mikhail Gorbachev during the twilight years of the Soviet Union, Russian security policy decidedly swung in a more confrontational direction under the guidance of Yevgeniy Primakov. After having worked as a researcher, journalist, and diplomat, he became head of the Foreign Intelligence Service (SVR) from 1991 to 1996. He was then Minister for Foreign Affairs from 1996 to 1997 and Prime Minister from 1998 to 1999. Primakov was a prescient political thinker, and his ideas reverberate strongly in the current Russian political leadership. According to Primakov, the liberal rules-based international order, which had the United Nations Charter and the Security Council at its core, had gradually come to be an expression of Western, and in particular American, hegemony. This order had become a tool for dominating the Russian Federation and other non-Western states. For Primakov, the prevailing distorted world order needed to be substituted by a concert of great powers, similar to the diplomatic system of the 19th century in Europe.

This turn in Russian security policy is perhaps best illustrated by the literal mid-air U-turn of Primakov's jet over the Atlantic, which took place when Primakov decided to cancel a visit to the United States over the NATO bombings of Belgrade in 1999. According to Primakov, it was exactly this type of unilateral American measure that undermined global stability. In his words, commenting on the American intervention in Iraq, "the US is pushing forward with a singularly minded agenda of 'unilateralism' where it wants to unilaterally address mankind's vital problems on the basis of Washington's biased views of the global situation. Generally speaking, the world must decide which of the following two models are the most acceptable for preserving the world order: one based on the joint efforts of the global community to counter various threats arising in the world and stabilise the international situation; or the other alternative which calls for unilateral decisions and actions which are in opposition to the UN Charter, as well as the opinion of a majority of states."

Primakov believed that globalisation had increased mutual dependencies. Therefore, it had become more difficult for a single pole to dominate the world; in other words, the process of globalisation undermined American hegemony. As countries became more developed and new centres of power arose, they would challenge the existing hegemon and reshape the world order. However, neither the Russian Federation nor China would ever subordinate themselves to an order dominated by the United States. A multipolar world, he wrote in 2003, "is therefore the main vector of the world's development."

Pushing for an End to the Liberal World Order

Primakov's belief that the current world order would collapse under the weight of its own contradictions is an example of the influence of the dialectical approach, inherited from Marxism-Leninism. According to this interpretation, Russia, as the antithesis of the West, is challenging the status quo and ushering in a new (and better) reality. According to this line of thinking, there can be no stable "end-state," and conflict between Russia and the West is therefore permanent and unavoidable. The current political leaders of the Russian Federation continue to be influenced by dialectics, something of which Western policymakers are often unaware. This inevitably leads to misunderstandings of Russian behaviour and actions.

President Putin's famous 2007 Munich speech was significant not because it introduced new ideas (it did not), but because it signalled that Russia was ready to exercise its existing agency to shape the world order and to create conditions for expanding that agency in pursuit of a greater balance. Agency in this context refers to the ability of a state to shape international norms, institutions, and outcomes rather than merely adapt to them. Russia's agency took the shape of both military interventions (Georgia, Syria, Ukraine) and of increased cooperation with China, India, and non-Western multilateral organisations such as BRICS and the Shanghai Cooperation Organisation. The Western sanctions imposed on

Russia after the annexation of Crimea gave impetus to Russian efforts to begin decoupling from Western-dominated financial systems. Though progress in this area has been mixed, Russia has managed to weaken the system of global financial and economic governance established at the Bretton Woods conference in 1944.

Russian official discourse on world order after the annexation of Crimea in 2014 has assumed a more openly ideological character. For Russian leaders, it is not just a question of power distribution; it is a question of norms and values. Human rights and democracy are considered Western tools for waging indirect warfare against Russia, and they are therefore viewed as a threat to Russia's existence. In addition, and relatedly, in line with Samuel P. Huntington's article "The Clash of Civilizations?" from 1993, the idea of Russia as a "civilisational state" has become even more important. There is a strong intellectual-historical tradition in which Russia is seen as a separate civilisation with unique values and historical experiences; this tradition goes beyond ideology, time, and state formation. Russia, therefore, deserves to be a "pole," not just on the basis of material and economic factors, but because it is a distinct civilisation. Russian civilisation is, of course, seen as founded on Eastern Orthodoxy. The Russian framing of great power competition as a struggle between civilisations with different religious identities also reintroduces metaphysical elements into world politics.

Seeking Agency in a New World Order

Although the Russian Federation has actively taken steps to dismantle the liberal rules-based world order, it is not clear whether it would enjoy stronger agency in a world order based on the art of the deal and the principle that "might makes right." The emergence of a pole in the multipolar world order, as envisioned by Russian political thinkers over the past thirty years, requires the capacity to attract and influence other countries. That capacity cannot be based solely on military power or nuclear weapons. This translates into two major challenges in the Russian search for agency in a new world order.

The first challenge is that Russia lacks the economic resources to compete with other, wealthier countries. RAND estimated that, in 1980, the Soviet Union spent about 7 per cent of its Gross National Income just to maintain its sphere of influence, through subsidies to Eastern and Central Europe, military aid, and covert operations. Today Russia spends perhaps 8 per cent of its GDP on military expenditure, and more still on other expenditures related to the war in Ukraine. It can ill afford to pour resources into a network of alliances, especially if other powers can bid more for their loyalties. Beyond the mere geographical aspect, the recent cases of Venezuela, Iran, and Syria illustrate that Russia is not able to shield its allies from American pressure, even if it would want to. This fact again presents the leaders of the Russian Federation with the issue of credibility. Yet, agency on the cheap still generates some influence, which is better than none.

The second challenge facing Russian agency is its chronic inability to leverage its existing cultural capital in a global context. Both the United States and the Soviet Union managed to master this aspect of agency and attraction during the Cold War with the help of an overarching ideological framework. These respective images of progress and liberty (with fundamentally different points of departure, and thus outcomes) could be used as tools for influence. On the surface, this competition primarily hinged on aesthetic preferences, but its scale shifted from local to regional to global at immense speed during the past decades, with the advent of the internet as a tool for mass communication. Today, when Russian leaders and government pundits moan over the Westernisation of the "Russian way of life," it is not only over the content of competing cultural expression, but also over the lack of means and capabilities to communicate its own ideal reality to the rest of the world.

Conflicting Agency in the Future

The story of Russia's post-Cold War trajectory is not one of mere revisionism. For many in the West, the crisis of the liberal world order appears as an unexpected unravelling. For Russian leaders, this is a long-awaited correction. Yet, dismantling one order is not the same as commanding or even influencing the next one. The ghost of Marxist-Leninist dialectics will continue to haunt Russian security and geopolitical thinking for decades to come, and the metaphysical war between opposites is thus bound to continue in the Russian political realm.

For the past thirty years, Russia has undoubtedly exercised the agency that it does possess, both with tanks and trolls. However, Russia needs more than just defiance to prosper in the multipolar world order that it strives for. It needs attraction, capital, and credibility. On the other hand, Russia's strife for renewal stands in contrast with the country's struggle against modernity itself. Military power may shatter norms and mutual understandings, but it cannot easily build durable coalitions. Nuclear weapons are a means of deterrence, but in themselves they do not generate prosperity. Civilisational rhetoric may mobilise domestic audiences, but is far more difficult to translate into global appeal.

If the threads of the liberal world order are fraying, Russia has indeed helped to pull them. The question is whether the Russian Federation as a state and society has the will and capability to contribute to its imagined multipolar utopia. Agency achieved only through resistance and defiance against a hegemon risks becoming agency confined to obstruction. In a world moving toward transactional power politics, Moscow may find that escaping Western hegemony is easier than escaping its own limitations.

Further reading

Engqvist, Maria, Emil Wannheden, Johan Engvall, Carl Michael Gräns, Tobias Junerfält, Ismail Khan, Jonas Kjellén, Tomas Malmlöf, Kristina Melin, Johan Norberg, and Carolina Vendil Pallin, 2023, *Russia's War Against Ukraine and the West: The First Year*, FOI-R--5479--SE, Stockholm: Swedish Defence Research Agency (FOI).

Gavin, Francis J., "The Future of World Order," *Engelsberg Ideas*, 4 February 2026.

Nicolas, Rambert, "L'Antéchrist de Soloviev: Première Partie," *Le Grand Continent*, 21 March 2026.

4. Preparedness by Europeans – Taking Action in a New Reality

Jenny Ingemarsdotter & Louise Bengtsson

Europe faces a new reality. This message, whether it is coming from Helsinki, Stockholm, Brussels, Paris, or Madrid, raises the question of how this reality should best be met. Looking at new European Union strategies and public support for a common defence and security policy, this chapter explores the future of European preparedness. By considering several perspectives, namely what the EU envisions, what Europeans want according to surveys, and what member states are hesitant about, we outline some of the major challenges and visions for a better prepared Europe.

Amid Russia's full-scale invasion of Ukraine as well as transatlantic turmoil with the second Trump administration, Europe faces a new reality and will be forced to strengthen its capacities. The EU Defence Commissioner Andrius Kubilius has even called for a standing EU military force of 100,000 troops and reforms of EU defence governance. While this may be complicated in practice, the bold proposal reflects the sense of a new and threatening reality for European security.

Moreover, recent events come against an already challenging threat landscape of climate-induced risk, pandemics, economic warfare, disinformation, and potentially dangerous technologies. As concluded by the EU Preparedness Union Strategy, the new reality facing Europe is marked by growing risks and deep uncertainty, thus highlighting the added value of the EU's broad toolbox. To some extent, the repeated lists of threats and corresponding key actions of new strategies tell us something about this new reality.

This chapter explores the core motivations and main proposals that have been put forward regarding a strengthened European preparedness. It begins by considering an important report on European preparedness (informing the EU Preparedness Union Strategy), then turns to what surveys say Europeans want, and concludes with reflections on the way forward for European resilience.

Why, according to Niinistö

When, in early 2024, Ursula von der Leyen, President of the European Commission, asked the former Finnish President Sauli Niinistö to write a report on how to enhance Europe's preparedness and readiness, she cited Niinistö's own words: "Europe has to wake up." Stating moreover that she wholeheartedly agreed with Niinistö, von der Leyen argued that Europe has a lot to learn from

Finland, where defence preparedness is not just the military's concern, but everyone's concern. Exploring this whole-of-society approach to preparedness and how it could be adopted at the European level became an important aim of the resulting Niinistö report (Safer Together, hereafter the Niinistö Report), which was released in October 2024. The report also made an effort to explain why Europe has to wake up.

Beyond its lists of new risks and threats, several more profound reasons can be discerned from the Niinistö Report, and these have since reappeared in several EU strategies on defence, security, and preparedness. Based on our reading and analysis of these documents, we identify and summarise three reasons why Europe needs to strengthen its preparedness:

First, Niinistö underscores that the crises of recent years have not been transitory or isolated. Instead, they "reflect deeper fault lines that severely undermine the fundamentals of the international rules-based order, as well as our planet's biosphere." EU strategies on security and defence similarly refer to paradigm shifts, broader trends, and strategic challenges, sometimes specified in terms of geopolitical, climatic/ecological, and technological shifts. The conclusion is clear: Europeans need to be prepared for a prolonged period of high risk.

Second, considering the strategic challenges facing Europe and the interdependency among EU member states, the Niinistö Report calls for a better use of economies of scale and joint planning. Subsequent EU strategies similarly emphasise the importance of a unified approach, arguing that fragmented and reactive responses are not enough in an increasingly dangerous and fast-moving world.

Third, the goal of a strengthened European civilian and military preparedness is not to wage war, but to maintain peace. Preparedness is described as a key component of deterrence against malicious actors. Admittedly, as Niinistö notes, deterrence is not how the EU has traditionally defined its role in security. However, given the evolving threat landscape, the EU now needs to make it as difficult as possible for aggressors to achieve their objectives, preferably deterring them from acting in the first place.

In addition to these three focal points, strategy, unity, and deterrence, Niinistö also argues that we must be better prepared "not only to survive, but also to thrive in this new reality." Focusing in this context on Europeans rather than the EU per se, Niinistö concludes that preparedness is the opposite of pessimism and hopelessness, and that it concerns everyone.

What do Europeans want?

According to Eurobarometer surveys (the public opinion surveys carried out twice a year on behalf of the EU institutions in all member states), public support for the EU reached record levels in 2025. The surveys also indicate that the

protection of peace and security is the top reason membership is viewed positively. Tellingly, around 80 per cent of respondents support a common defence and security policy at EU level, and around 90 per cent want the EU to act in a more united way to face global challenges.

At the same time, the continent is experiencing a countervailing dynamic of Euroscepticism, represented in particular by populist and far-right parties in the new composition of the European Parliament and government leadership in some member states, as well as right-wing political challengers in France and Germany. These trends have weakened the engine for European integration and capacity for action, reflecting the importance of the domestic political situation in major member states.

Meanwhile, member states also differ in their preferences and focus regarding threats and preparedness. As for civil-military cooperation (inspired by Nordic models of comprehensive or total defence), Sweden is part of a driving coalition together with Belgium, Denmark, the Netherlands, Luxembourg, Finland, Estonia, Latvia, Lithuania, and Poland. However, pushing this agenda forward has faced resistance from countries in Central and Southern Europe, including France, Italy, and Slovenia. For some member states, expanding current mechanisms for civil protection, which in the EU context refers to prevention and assistance during crises, to include an all-hazards perspective and civil-military cooperation is sensitive, due to national preparedness cultures, information sharing, and administrative systems.

In addition, the Eurobarometer polls quoted by Niinistö (conducted in 2024) indicate that EU citizens are calling for the Union to become a stronger actor in defence. For example, two-thirds of respondents agreed that the EU should spend more money on defence. The path towards such increased strength has been the topic of much recent strategic analysis, and constitutes the core subject of the EU Preparedness Union Strategy released in 2025.

Towards a European Preparedness Union

The EU Preparedness Union Strategy that followed the Niinistö Report reflects a further deepening of integration in this field. The strategy sets out 30 key actions for member states to increase preparedness for crises such as natural disasters and hybrid and military threats. One example relates to the ambition to boost the EU's material preparedness for crises, as outlined in a subsequent EU stockpiling strategy (released in 2025).

An array of initiatives has also been pursued in the defence field at the EU level. Plans are underway for an 'internal market for defence' with nine so-called capability coalitions. In addition, the Commission has proposed four flagship projects: the European Drone Defence Initiative (EDDI), Eastern Flank Watch, European Air Shield, and European Space Shield. The Commission's proposal on

military mobility, designed to facilitate the transfer of troops across the continent, was presented in November 2025.

These priorities at the EU level go hand in hand with NATO's increased focus on resilience and civil-military cooperation. For example, the EU has tools that can assist cooperation between member states in achieving their NATO objectives, building on the EU's regulatory powers and economy of scale. However, while coordination between the EU and NATO is of great importance, it can be complicated in practice. One example is the lack of a sufficient mandate for consultations between the organisations' secretariats. When it comes to military planning, some have floated the idea of a European pillar within NATO, while others mention other formats, including partnership with the UK or a Nordic–Baltic format.

Looking back, much has happened in only a few years, and no one can doubt the commitment of the European Commission to the vision of the Preparedness Union. Yet, the challenges ahead are neither few nor small. While defence experts and strategists may be wide awake, Niinistö warns that real, joint action may still be hampered by short-termism and diverging interests.

There is also the question of trust. As Niinistö recognises, moving towards a stronger role for the EU in the context of preparedness and defence will require "a high level of trust—between the Member States and EU institutions, and between public authorities, the private sector, and civil society." Given the stakes, are European leaders ready for this kind of trust?

The seriousness of the situation has been further underscored by former European Central Bank President Mario Draghi, author of the Draghi report on EU competitiveness. In a speech in Leuven in February 2026, he warned that the collapse of the current economic world order may lead to Europe becoming "subordinated, divided, and deindustrialised at once." Notably, Draghi compared the EU's global economic power to its weaker role in security and defence: "Where Europe has federated on trade, on competition, on the single market, on monetary policy, we are respected as a power and negotiate as one. . . Where we have not, on defence, on industrial policy, on foreign affairs, we are treated as a loose assembly of middle-sized states to be divided and dealt with accordingly."

While not everyone would agree with Draghi that Europe needs to move towards a federation, leaders realise what is at stake: our democracy, freedom, and prosperity.

Conclusion and the way forward

No matter what happens on the global stage, Europe and Europeans will be forced to take more responsibility for their own security, a task that the EU is in many ways well-positioned to take on. The EU has extensive means to support member state capabilities through joint legislation, coordination, and financing,

including in areas important for modern-day preparedness such as AI, cyber, hybrid threats, disinformation, economic warfare, critical infrastructure, climate adaptation, research, and innovation, as well as joint industrial policy for the defence sector. The financial muscles of the EU allow for joint procurement and spending. The EU's global role as a trading partner and single market should also not be forgotten in this regard.

To make these technical and economic mechanisms work, cultural and social dimensions also need to be considered. This is why the Niinistö Report discusses at length matters of trust, preparedness culture, and the need for a new mindset. President von der Leyen already appears to have realised the challenges of this endeavour when embarking on her first Commission term in 2019, stating that "if we are to go down the European path, we must first rediscover our unity." Ending on a hopeful note, as European leaders tend to do, von der Leyen also expressed her belief that if we close the gaps between us, we can turn today's challenges into tomorrow's opportunities.

Further reading

Bengtsson, Louise, 2025, Reserapport—Kontaktresa till Bryssel med fokus på civil beredskap och resiliens, FOI Memo 9055, Stockholm: Swedish Defence Research Agency (FOI).

Ingemarsdotter, Jenny and Anna Wetter Ryde, 2024, Draghi-rapporten: Villkoren för Europas självbevarelse? FOI Memo 8658, Stockholm: Swedish Defence Research Agency (FOI).

Ingemarsdotter, Jenny and Anna Wetter Ryde, 2024, Niinistö-rapporten: På väg mot ett europeiskt civilt försvar? FOI Memo 8743, Stockholm: Swedish Defence Research Agency (FOI).

5. India: A Rising Space Power

Samuel Neuman Bergenwall and Anna Maria Wårlind

India, the world's most populous country and fastest-growing major economy, aspires to be recognised as a leading power both on Earth and in space. India's space programme, originally focused on exploration and exploitation for peaceful purposes, is becoming more visibly militarised. Factors driving this shift include not only India's aspiration to emerge as a great power and the increasingly unstable geopolitical environment, but also military confrontations with China and Pakistan, its two traditional adversaries. India's space programme also demonstrates the pursuit of strategic autonomy and a deliberate balancing act between Russia, the European Union, East Asia, and the United States. Thus, India's space activities illustrate both its turn towards militarisation and its strategy of multi-alignment.

This chapter shows how India's space activities underpin its pursuit of great power status, facilitate its shift towards militarisation to meet its security challenges from China and Pakistan, and exemplify its grand strategy of multi-alignment in international politics. Indeed, India is on a positive trajectory to become a major power in the rapidly evolving global order, not just in the Global South. In this context, India has become a closer defence and trading partner of the EU. But it also holds significant challenges, such as deep-seated military and energy ties with Russia. Given India's growing yet complex role in international politics, and its expanding relations with Europe, it is important to deepen understanding in Sweden of India's security and defence policy, particularly in space.

Pursuit of Great Power Status

Thanks to an annual GDP growth rate of about 6–7 per cent, India's role in the international system has grown steadily over the past decades. India is already the world's third-largest economy, after the United States and China, in terms of purchasing-power parity. According to the International Monetary Fund, India's economic outlook is bright, partly thanks to domestic reforms and favourable demographics.

India's nationalistic and optimistic politics have led it to pursue an ambitious space programme, and its rapid economic growth has created the necessary resources for its successes. For over a decade, Prime Minister Narendra Modi and his Hindu nationalist Bharatiya Janata Party (BJP) have been at the helm of Indian politics. The BJP government wants to transform India into a developed country with an economy exceeding USD 30 trillion by 2047, the country's centenary. India already envisions itself as a leading, proactive, and autonomous power in a

multipolar world. This has prompted the government to invest in prestigious civil space projects that align with India's broader ambitions to acquire great-power attributes, such as securing a permanent seat on the UN Security Council, becoming the world's third-largest economy, and emerging as a major military power with a credible nuclear triad. In 2014, an Indian orbiter (Mangalyaan) reached Mars, and in 2023 India became the fourth country to successfully soft-land a spacecraft on the Moon. In 2018, Modi announced plans for an independent programme to send *vyomanauts* (Indian astronauts) into space. By 2035, India also plans to have an operational space station of its own.

Although India's space programme faces challenges, such as resource constraints, and failed rocket launches, it is clearly on its way to become one of the world's leading space powers. However, it does not yet possess all the elements of space power demonstrated by the United States, China, and Russia. Resource constraints, developing heavy launchers and improving its autonomous regional satellite-navigation system are proving challenging. Given the rapid evolution of India's space programme over recent decades, and the priority attached to developing space capabilities, the motivation to address these issues appear high.

Towards Militarisation

India's space activities, which have historically focused on civil applications, have in recent decades shifted towards more openly displaying military motivations and ambitions, in line with India's evolving ambition to become a major power. The Indian space programme originated in the 1960s with the ambition of bringing socioeconomic development and modernisation to the subcontinent. Bolstering science, education and creating high-tech professions within the country continue to be important goals to which the space programme is expected to contribute. Modernising agriculture and improving communication services have been key societal goals driving investments in space technology. Meteorological forecasts and telecommunications services enabled by satellite systems have therefore been prominent activities.

Early developments of the space programme also included the testing and launching of sounding rockets, highlighting the priority India placed on an independent rocket-launch capability as a civil spacefaring nation and reinforcing its strategic autonomy. Following India's war with Pakistan in 1971, and its first nuclear test in 1974, the links between space-launch development by the civil Indian Space Research Organisation (ISRO) and medium-range missile development became more apparent.

This linkage demonstrated an early convergence of military interests in the development of sovereign space-launch capability. Since the mid-1990s, the Polar Launch Satellite Vehicle (PSLV) has also been the workhorse in the Indian space programme, delivering payloads into low Earth orbit. It reduced India's reliance on Russia, its primary launch partner, enabled prestigious all-Indian-flagged

space missions, and became an important component in collaboration with international partners as the global space sector rapidly grew. Hundreds of small satellites belonging to other states have been launched into space using the PSLV, increasing the credibility of India as a business partner and enhancing its status as a spacefaring nation. The commercialisation and provision services to the growing global space market have also benefitted the development of the Indian space programme from a budgetary perspective by bringing in funding from abroad.

Obstacles, Challenges and Rivalries

However, developing heavier launchers capable of supporting more complex missions to higher orbits has been, and continues to be, a challenge. The Indian space programme was held back by US sanctions imposed after its nuclear tests in 1998. This made it difficult to develop launchers capable of reaching higher orbits with heavy loads and steered India towards collaboration with Russia to develop the necessary rocket stages.

The United States' use of military space assets during the Gulf War in the 1990s also incentivized the Indian administration to increase the development of space-based military capabilities. In 2012, only a year after ISRO was removed from the US's sanctions list, the Defence Research and Development Organisation (DRDO) announced that India possessed the necessary means to assemble a direct-ascent anti-satellite, DA-ASAT, capability.

In 2019, DRDO performed a destructive DA-ASAT test, called Mission Shakti (Power), using a Ballistic Missile Defence interceptor, developed under the ballistic missile defence programme, targeting an Indian satellite in low Earth orbit. It was a demonstration of India's ambitions as a military space power, alongside Russia, the United States, and China, all of which had already conducted similar capability-demonstrating tests. The same year, the Defence Space Agency (DSA) was established to streamline the efforts of the armed forces, ISRO, and the Department of Space. The DSA, in turn, superseded the Integrated Space Cell, which was established in 2008 in response to the Chinese demonstration of DA-ASAT capability in 2007. This chain of development illustrates how the rivalry between China and India has been a contributing factor behind the militarisation of India's space programme.

India has taken additional steps towards militarisation in recent years to manage its two external security challenges, China and Pakistan. China's growing presence in space and its military build-up along India's border pose major challenges to India's defence. Since the deadly confrontation between India and China in 2020, space has become more important on the defence agenda. India has worked on the development of a new fleet of intelligence, surveillance, and reconnaissance satellites intended to be launched from mobile platforms.

The significance of space for military operations was reinforced during the brief war between India and Pakistan in May 2025. While India's military lacked the necessary number of military satellites to support its operations, Pakistan reportedly received geospatial intelligence from China, its closest military partner. Current tensions with China and the war with Pakistan have thus further reinforced the militarisation of the space programme. Consequently, the concept of civil-military fusion has gained momentum in India. For example, ISRO, contributed to the military operation against Pakistan in 2025.

Reforming India's Defence: Evolving Military Space Doctrine

As India plans to implement what may be its largest defence reforms since independence, the space domain is likely to be a central focus. These reforms include the establishment of theatre commands and integrated battle groups, and a focus on jointness and multi-domain operations. The Joint Doctrine of the Indian Armed Forces, adopted in 2017, and the Doctrine of the Indian Air Force on Aerospace Power adopted in 2022 articulate India's perspective on military space power and its understanding of the domain. In 2025, an Indian Military Space Doctrine was released. Integrating this doctrine with the 2023 civil space policy, which focuses on the peaceful exploration of outer space, commercial services, and private space activities, will be a delicate task for the Indian administration to manage, as concepts such as space-based deterrence and counterspace measures are brought within the scope of the Indian space programme. This will fundamentally change the global perception of India's role as a spacefaring nation. The gradual militarisation of the Indian space programme will continue, keeping pace with the development of dual-use aspects of space technology.

A Leading Space Power in a Multipolar World

India's role in space is also influenced by its diplomatic strategy, which is characterised by realpolitik, strategic autonomy, and multi-alignment. In other words, India uses transactional power politics and balances between all major powers in order to become a strong and independent pole in the international system. Over the years, India has strengthened its ties with the European Union, the United States, East Asia, the Middle East, and the Global South, while retaining strategic ties with Russia. Even though China is perceived as strategic challenge, India cooperates with it in the economic and multilateral domains. India's multi-aligned approach to global affairs is also evident through its participation in various multilateral organisations. It is a founding member of the BRICS bloc (named after the founding countries of Brazil, Russia, India, China and early member South Africa) and a member of the Shanghai Cooperation Organization (SCO), which is led by China and Russia. India also participates in the Quadrilateral Security Dialogue (QUAD) with the United States, Japan, and Australia.

This multi-pronged strategy is observable in India's international space cooperation. Although India's reliance on Russia may be less than in the past, the two

countries continue to collaborate in space exploration bilaterally and within fora such as BRICS. Notably, since the late 2000s, India has also developed close cooperation with Israel, launching a reconnaissance satellite into space on behalf of its strategic partner. Space is also a key theme in India's relations with France, Japan, the United Arab Emirates, the European Union, and the United States. In 2023, India signed the Artemis Accords, joining the US-led initiative for space exploration.

These international collaborations demonstrate various technical levels of space cooperation and illustrate India's interest-focused strategy and omni-directional diplomacy. However, the collaborations are characterised by ambitions regarding data-sharing, interoperability of services, and pooling of resources rather than by deeply integrated technical collaborations.

India aspires to be an active international space cooperation partner, at the same time as it has become less dependent on foreign collaborations. It has built significant space capabilities of its own, strengthening its strategic autonomy and its role as a leading state in the Global South and beyond.

Looking ahead

In sum, India's development as a space power sheds light on its path towards great power status, its growing focus on military capabilities, and its strategy of expanding autonomy while cultivating relations in several directions simultaneously.

Nationalistic sentiments in India will likely continue to influence the development of its space activities, as the endeavours and successes of the space programme are intertwined with patriotic narratives. Prestigious space projects may be initiated, at least in part, for domestic consumption.

Today India strives to attain the attributes of a great power that come with being a major space power. India emphasises the importance of military space capabilities and recognises the potential to build upon the achievements of its existing civil space programme. Meanwhile, the Indian administration is carefully navigating sensitive discussions with other states during ongoing talks on arms control in outer space. In this context, India appears to be mindful of not limiting its own possibilities to develop the capabilities necessary to balance the influence of other space powers.

As India's space programme becomes more militarised, the distinction between its civil and military space activities is becoming blurred. The focus on civil-military fusion, a term that is frequently employed in Indian strategic discourse, also impacts the space sector.

India's current military space activities reflect its rise, ambitions, and policies in the evolving global order. It now has the power to influence other space powers'

investments and priorities in the domain. This makes India a key actor to analyse in order to understand the future development of both geo- and astropolitics.

Lastly, ongoing turbulence in global geopolitics present opportunities to strengthen defence ties between India and the European Union, including in the space domain. However, it is also important to remember that India actively pursues multi-alignment and strategic autonomy. For example, India continues its military cooperation with Russia, albeit less intensely than in the past. This will pose a challenge for European actors, including Sweden, when seeking to navigate cooperation with India in space. As the world order changes and India–European ties deepen, it becomes more important to study India's foreign, security, and defence policies, both on Earth and in outer space.

Further reading

Wårlind, Anna Maria, Mattsson, Linn and Johlander, Andreas, 2025, *Kina i Rymddomänen - bland skrot och hot - Ett försvars- och säkerhetsperspektiv* [China in the Space Domain – among debris and threats – a defence and security perspective], FOI-R--5673--SE, Stockholm: Swedish Defence Research Agency (FOI).

Bergenwall, Samuel Neuman, 2025, *Hur indiska säkerhetspolitiska tänkare ser på Kina: partner, rival eller fiende?* [How Indian Security Policy Thinkers View China: Partner, Rival, or Enemy?] FOI-R--5780--SE, Stockholm: Swedish Defence Research Agency (FOI).

Bergenwall, Samuel Neuman, 2024, I*ndien som säkerhetspolitisk aktör—konsekvenser för svenska försvarsrelationer* [India as a Security Policy Actor—Implications for Swedish Defence Relations], FOI-R--5588--SE Stockholm: Swedish Defence Research Agency (FOI).

6. Shifting Powers: The Global South in a Changing World Order

Gabriella Körling and Carl Marklund

It long seemed that economic liberalisation, globalisation, and democratisation were making the distinction between the North and the South increasingly irrelevant. However, recent years have witnessed the return of this dichotomy as the Global South has emerged as a geopolitical factor in world politics due to a combination of political, economic, ideological, and institutional factors. While there is a tendency to focus on great power rivalry as a driving force in world politics, dynamics within the Global South are just as likely to shape the future of the world order, calling for a more fine-grained understanding of its political and economic dynamics. The challenge for the Global South is whether growing economic weight and diplomatic coordination will translate into durable rule-shaping power under conditions of geopolitical rivalry, financial volatility, and persistent structural asymmetries.

The Return of the Global South

The Global South, a collective shorthand for developing countries in Africa, Asia, the Middle East, and Latin America, is back. Not that it had ever really gone away. But several dramatic events, such as the COVID-19 pandemic, Russia's full-scale invasion of Ukraine, and the Israel-Hamas war, as well as global negotiations about climate change funding and international tax cooperation (under the UN Framework Convention on International Tax Cooperation), have exposed the persistence of frictions between countries in the North and in the South. For instance, although several countries from the Global South voted to condemn Russia's actions in the United Nations General Assembly, many abstained from voting. Furthermore, few of the countries from the Global South have imposed sanctions on Russia.

The emergence of the Global South as a geopolitical factor on the global stage came as a surprise to many observers. For a long time, it had seemed that the division of the world into a wealthy and industrialised Global North and a poor and developing Global South had lost both its descriptive value and its political salience. Globalisation and economic liberalisation paved the way for economic growth in many countries in the South, leading to increasing economic diversity and a gradual shift in the world economy from the "West" (North) to "the rest" (South). The notion that the division between the South and the North was no longer relevant was reinforced by the ascendancy of the international liberal order, particularly in its post-Cold War form, when the US as the sole superpower sought to extend the reach of liberal norms, markets, and institutions globally,

characterised by optimism and the rallying behind values of multilateralism, co-operation, and democracy.

Moreover, the increasing economic and political diversity within the Global South seemed to indicate that the interests of countries in the Global South would diverge to such a degree that the distinction between North and South would become increasingly meaningless and lose its explanatory value. However, despite these transformations, the Global South, as a unifying category, has persisted and reappeared on the global scene in the last couple of years. There are several political, economic, ideological, and institutional reasons for this persistence.

Economic factors. While the economic divide between North and South is no longer as stark, poor and developing countries are still concentrated in the South. Although the poorer countries of the South might not share economic interests with the (economic) powerhouses of the Global South (such as India and Brazil), some interests are still shared, for instance on questions of human development and climate change.

Political factors. Despite some openings and reforms, the global distribution of power has failed to reflect geoeconomic transformations, such as political representation in key international institutions (for example, the UN Security Council and the International Monetary Fund, IMF) and has not kept pace with the economic rise of Global South states. Furthermore, many countries in the Global South share a historical experience of colonialism and marginalisation that influences their understanding of global political and economic inequalities.

Ideological factors. Current discourses and narratives around the Global South, such as South–South cooperation and an insistence on strategic autonomy in the face of heightened great power rivalry, borrow some of their ideological underpinnings from earlier periods of mobilisation and positioning. These trace back to the Afro-Asian Bandung Conference in 1955 and the Non-Aligned Movement (NAM) established in 1961. This is not to overplay the ideological motivation of countries in the Global South, whose actions are motivated just as much by strategic interests as other countries' are, but to note that historical connections still matter even if the context has changed.

Institutional factors. The institutions and broad coalitions that were created during the wave of "third world" mobilisation of the 1960s and 1970s, such as the NAM and the G77, survived the vagaries of world politics and continued to function even after the attention of the world turned away from the Global South. While the high point of Global South mobilization, exemplified by the push for a New International Economic Order (NIEO), remains in the past, these organisations have survived as important platforms for alliance-building and diplomatic coordination. Economic diversification within the South has not dissolved these ties. Moreover, newer institutions and coalitions have emerged: the African Union (AU), BRICS, and the Asian Infrastructure Investment Bank (AIIB) represent a more recent layer of South-centred institution-building.

BRICS AND SHIFTING GEOECONOMIC POWER

The reemergence of the Global South also needs to be understood against the backdrop of changes in global economic power. Twenty years ago, global power concentrated in the mature economies of North America, Europe, and Japan, whose overwhelming leads in output, trade, technological innovation, and military spending reflected the legacy of the post-World War II order. Two decades later, the balance appears more diffuse. As of 2025, the World Bank states that "low and middle income" economies, roughly encompassing the Global South, account for approximately 35 per cent of the world's nominal GDP, including China's share at circa 17 per cent. These economies account for about 85 per cent of the world's population and are an increasing driver of economic growth. According to Boston Consulting Group, the Global South's combined GDP, excluding China, is projected to grow at an average annual rate of 4.2 per cent through 2029, compared with 1.9 per cent for advanced economies.

The United States remains the single largest economic and military actor, but its relative dominance has narrowed as China is now the world's second largest economy (by nominal GDP), the world's largest exporter of goods, an emerging technological superpower, with an increasingly modern and capable military force. India's rapid growth and rising innovation base, alongside the resource-driven resurgence of countries such as Saudi Arabia and Brazil, point to a broader redistribution of economic weight toward Asia and parts of the Global South. Taken together, these developments trace a transition from a transatlantic-centred system to a more multipolar landscape in which economic scale, technological capability, and geoeconomic ambition spread across a wider constellation of states.

The evolution and expansion of BRICS exemplify this renegotiation. Originally founded in 2009 as a forum for Brazil, Russia, India, China, and South Africa, and significantly expanded in 2023, the grouping has gradually moved beyond symbolic coordination toward institutional consolidation and a more explicit ambition to influence global governance. China is by far the largest economy within BRICS, though India's growing weight may shift internal dynamics over time. Following its 2023 expansion, BRICS' founding members have been joined by Egypt, Ethiopia, Indonesia, Iran, and the UAE. Scholars and analysts characterise BRICS+ not simply as a balancing coalition but as a site of norm production, advancing alternative principles on sovereignty, development finance, and conditionality.

The coordinated call by BRICS finance ministers for reform of the IMF's quota system reflects this structural ambition: to recalibrate representation in Bretton Woods institutions in line with contemporary economic weight and to challenge entrenched leadership conventions. These proposals echo long-standing demands from the Intergovernmental Group of Twenty-Four and other Global South platforms.

At the same time, recent scholarship cautions against overestimating cohesion. Persistent asymmetries within South–South arrangements, including trade concentration, uneven technological capacity, and divergent national interests, continue to constrain collective agency. Contemporary commentary on recent BRICS summits similarly notes the tension between expanded numerical weight and uneven strategic coherence.

Debates over de-dollarization and alternative financial infrastructure have become central to the evolving BRICS agenda. Proposals for cross-border payment systems, local-currency settlement mechanisms, and central-bank digital currency linkages aim to reduce reliance on the US dollar and the SWIFT network. Central banks across emerging markets have simultaneously increased gold reserves and diversified reserve holdings as part of broader strategies to mitigate volatility associated with dollar dominance. In practice, a growing share of trade between major emerging economies is already being settled in national currencies, while new settlement instruments are being developed to reduce conversion risk.

These shifts reflect what recent international political economy literature describes as the geoeconomics of fragmentation and the logic of weaponised interdependence, the recognition that control over financial and technological networks can be used coercively, prompting diversification strategies among vulnerable states. The US response underscores the geopolitical stakes, as demonstrated by US threats of punitive tariffs tied to BRICS alignment.

The Global South and great power competition

While the re-emergence of the Global South is tightly intertwined with the rebalancing of economic power, its geopolitical importance has also grown in light of the increase in great power rivalry and the current transformation of the world order.

Prominent academics and observers, including political scientist John Ikenberry and Finland's President Alexander Stubb, have identified the Global South as one of three competing poles of power, alongside the Global West (the US, Europe, and their close allies) and the Global East (China, Russia). In their reading, the Global West and the Global East are competing for influence in the Global South because both need support from countries in the Global South to impose their respective visions of world order. China and Russia, from different positions and from different histories, have certainly gone to great lengths to increase their influence in the Global South. Both promote ideological visions of a new world order that challenges the dominance of the West, while tightening concrete economic, political, and technological ties with countries in the Global South. So far, the majority of countries in the Global South, true to the tradition of non-alignment and insistence on strategic autonomy, have responded by maintaining relationships with multiple poles of power (the US, EU, Russia, and China), although this at times requires a balancing act.

The recent world turmoil, amplified by the transactional, unpredictable, and often contradictory initiatives from the current US Trump administration, has challenged established norms, upended traditional friendships and weakened the cohesion of the West. In this landscape of uncertainty, states in the Global North find themselves dazed and confused, unaccustomed to the strong-arm approach employed in, for example, the Greenland crisis. But this is not new to most countries in the Global South. Politicians and observers across the Global South are deeply familiar with this style of politics.

In short, the weakening of the liberal international order has not necessarily appeared as unpredictable to observers in the Global South as it has to observers in the Global North. While vulnerable to global economic instability, countries in the Global South are accustomed to political volatility. In this new reality, it will be increasingly important for small- and medium-sized states in the Global South and the Global North to shift perspectives and look for "like-minded" partners beyond the North-South divide to offset the loss of stability and predictability.

Looking ahead, multiple geopolitical flashpoints coincide with profound economic realignments, providing a test for both the strategic autonomy of developing states and the broader contest over the shape of the global order. For nations of the Global South, the challenge is not merely to absorb external shocks, from renewed great-power rivalry to tightening trade regimes, but to consolidate agency in an international system that is fragmenting. Will emerging and developing states be able to convert their large, growing, and increasingly skilled population (demographic scale), market growth, and diplomatic coordination into durable influence over global rules and institutions? If they can manage to do so, key actors in the Global South are set to play a major role in shaping the future world order, rather than merely absorbing the outcomes of geopolitical rivalry between Washington and Beijing.

Further reading

Ikenberry, G. John, 2024, "Three Worlds: The West, East and South and the competition to shape global order," *International Affairs* 100, no. 1: 121–138.

Körling, Gabriella and Carl Marklund, 2026, The Global South in World Politics: Past Legacies, Present Power, FOI memo (forthcoming).

Stubb, Alexander, 2026, *The Triangle of Power: Rebalancing the New World*. New York: Columbia Global Reports.

7. International Military Missions in a Changing World Order

Elin Hellquist and Elin Jakobsson

In times of geopolitical turbulence and amplified uncertainty, it is worthwhile to reflect upon what "makes and shakes" world order. The article contributes to this endeavour by elaborating on how international military missions (IMMs) build upon and shape relationships between states. Since the end of the Second World War, IMMs have been an arena for principled and practical contestation over the limits of sovereignty in international relations. IMMs have gathered a largely foreseeable crowd of contributors and critical bystanders, reflecting the prevalent social dynamics of their time. In turn, experiences in the mission area have fed back into the core relationships that underpin international order, for better and for worse. With essential ties within world order currently unravelling, old truths regarding the social foundations and implications of IMMs need to be revisited. Not only have longstanding enmities flared up along geopolitical conflict lines, but the transatlantic partnership, essential for the post–Second World War order, also faces unparalleled challenges. Meanwhile, the UN is in a tripartite crisis: of legitimacy, political will, and funding. While these combined developments make traditional IMMs sponsored by international institutions less likely, the space for unconventional missions with weaker institutional anchoring is expanding.

Order and Disorder

World order refers to patterns in relationships between units, primarily states, active on the international scene. The history of international relations testifies to alternating relational structures: from pre-modern city-states to empires and onwards to 19th-century multipolarity, post–Second World War bipolarity and post–Cold War unipolarity. The most recent order, the one that many fear is about to collapse, is known by two main names which have different historical roots: the rules-based order (1945) and the liberal international order (1991).

Such descriptions of order are analytical simplifications of relational regularities in the international system. In practice, order is inherently dynamic and incomplete: it is always in the making and never without exceptions. The domain of international military missions exemplifies this point by demonstrating both highly predictable constellations of actors and exceptions to these. When it becomes more common for actors to behave in unexpected ways, the existing order is gradually undermined. If exceptional behaviour becomes sufficiently frequent over time, it may signal that a new, more or less harmonious or conflictual, order is in the making. However, as is clear from the debate on current threats to world

order, it is tricky to define precise tipping points when exceptions are so plentiful that they have become a new normal.

Particularly unruly times, when established relationships are on thin ice but have not yet been replaced by other predictable constellations, can be conceived of as disorder rather than as a materialised new order. A state of disorder is characterised by ambiguity and uncertainty, and thereby poses extraordinary challenges for international actors

International military missions

The deployment of international troops in response to crises on foreign territory has been a recurrent phenomenon in the post–Second World War international order. These deployments come under different labels, from peacekeeping to peace enforcement and stabilisation, to crisis management and humanitarian intervention. All of these variations are examples of IMMs, which are typically carried out by multinational coalitions established within, or with the blessing of, an international institution, such as the United Nations (UN), NATO, the European Union (EU), and the African Union (AU).

IMMs and order

The post–Second World War legacy of IMMs suggests that they both *draw on* existing features of international order and themselves *contribute to* its dynamic evolution.

First, IMMs influence world order through stakeholders' selective decisions on when to act and when not to act. Any decision to deploy international troops entails actively balancing between fundamental principles that, by convention or treaties, structure international relations. Military interventions are prohibited under international law, unless a credible claim can be made that they are justifiable exceptions to the core norms of sovereignty and non-interference. Such justifications include claims that a crisis threatens international peace and security (UN Security Council mandate), that it threatens the local population (Responsibility to Protect, R2P), or that it threatens the interests and security of the interveners (self-defence). A distinct type of justification is that a government requests international military assistance, thus providing active consent that, prima facie, cancels non-interference objections. These justifications are broadly endorsed in theory, but their applicability in concrete situations is often contested. For instance, there is no authoritative objective answer to the question, fundamental to order, of where the domestic ends and the international begins. Moreover, the validity of an invitation to assist hinges, inter alia, on the reasonable legitimacy of the issuing government. Thus, in practice, IMMs do not depend solely, or even chiefly, on the factual circumstances in a potential mission area. Even in highly pressing crises, an IMM will only materialise if there is sufficient political will to become militarily involved.

Second, IMMs demonstrate the institutional underpinnings and limitations of international order. IMMs are agreed upon within different multilateral frameworks, most prominently the UN, the EU, NATO, and the AU and its suborganisations. The weight and profile of each organisation in the IMM domain, as well as the prevalence of ad-hoc coalitions outside of formal institutions, have varied over time. Since IMMs deal with core issues in world order, spanning the full spectrum from war to peace, their trajectories are indicative of the fluctuating status of different institutions in that order. However, over time, the UNSC has retained a unique legitimising role in international order, including for deployments under other institutional headings. ISAF in Afghanistan, Operation Unified Protector in Libya, Operation Barkhane in Mali, as well as AMISOM, ATMIS, and AUSSOM in Somalia are examples of non-UN missions operating under explicit UNSC approval. In other situations, such as the 2003 invasion of Iraq, its initiators insisted on UN-compatibility although the UNSC did not authorise military action. Despite the turning tides in world order, the US asked for the Council's green light for a non-UN International Stabilization Force to Gaza. By contrast, the US and Israel did not seek UN authorisation prior to attacks on Iran in late February 2026. Circumventing the UNSC in this high-stakes case suggests that its longstanding legitimising role may be eroding.

Third, IMMs matter for international order by highlighting the evolution of order-constitutive constellations of states. When an IMM is formed, a powerful state typically takes the initiative and seeks to gather sufficient political support and troop contributions to launch a mission. This process tends to draw on preexisting patterned relationships: the initiator expects allies, or states with special stakes in the situation at hand, to contribute. Meeting such expectations serves as a confirmation of solidarity and loyalty. Candidates for temporary membership in the UNSC highlight their participation in UN peacekeeping as evidence of their commitment to international peace and security. For non-UN missions, participation has often, implicitly or explicitly, been coupled with expectations of reciprocity: that the mission leader would return the favour through military or other forms of assistance if ever needed. The broad composition of, and long-term commitment by, allies and partners in the US-led intervention in Afghanistan is a case in point. France's efforts to Europeanise military operations in the Sahel are another example of IMM participation expected to promote mutually beneficial partnerships.

Fourth, financing and troop contributions are illustrative of the unequal ordering of relations between (groups of) states. Across institutional frameworks, including for African-led operations, "Western" (American, European) money has stood for the lion's share of IMM funding. The exception is China, which in the past decades has become both a major payer (allocated through GDP formula) and troop contributor to UN peacekeeping operations. Meanwhile, both UN peacekeeping and African-led missions rely largely on troops from low-income countries. Arguably, the asymmetry between who funds and who carries out high-risk missions reflects hierarchical inequalities in world order.

IMMs and disorder

The nature of situations that give rise to missions is inherently unpredictable and fraught with strategic risk. Continuous exposure to surprises puts relations within mission coalitions to the test. Especially when things do not go well on the ground, unity of purpose risks being compromised. Moreover, it is hard to design a complex IMM so that all parts march in step. Unclear command structures, obstacles to information-sharing, national caveats, and cultural differences are known vulnerabilities in multinational military missions across types. Frustrations and frictions stemming from such issues can lead to disorder when they undermine order-maintaining alliances. In UN peacekeeping, coordination and cooperation between different national units, between levels of leadership, and between civilian and military mission components are notoriously difficult. Such frictions erode the effectiveness and legitimacy of UN peacekeeping operations and by extension risk undermining the UN's unique status in international order. Even for NATO, the most well-oiled and materially capable IMM organisation, out-of-area operations have unveiled rifts between members, including conflicting strategic visions and gaps in de facto and perceived burden-sharing. Moreover, the validity of the assumption of solidarity-based reciprocity through mission participation has been put into question, most recently and dramatically during the Greenland crisis in early 2026. Denmark's contributions to US-led IMMs have repeatedly been invoked in response to US threats to take over Greenland by force. As summarised by Carsten Rasmussen, chairman of the Danish Veteran Association (31 January 2026): "Denmark has always stood side by side with the USA, and we have showed up in the world's crisis zones when the USA has asked us to. We feel let down and ridiculed. . ."

At the height of the world order now under challenge, IMMs were guided by apparent optimism about the potential to promote liberal norms and values by military means. However, to the extent that liberal interventionism was genuinely value-driven, outcomes did not live up to intentions. Experiences from Afghanistan, Iraq, Mali, Libya, and Somalia highlighted the deep contradictions and unintended consequences of external involvement in countries with contested and fragile statehood. The chaotic exit of international troops from Afghanistan in 2021 became a traumatic synthesis of the liberal West's failure. NATO hardly had the time to process the turbulent withdrawal from Afghanistan before Russia's full-scale invasion of Ukraine made deterrence and defence of allied territory its uncontested priority.

The punctured bubble of liberal interventionism can be understood as a disordering event, which has both shaken order-constitutive coalitions and brought global geopolitical friction into the open. Not only non-UN missions, but also (some instances of) UN peacekeeping have fed antagonistic interpretations between groups of states in international relations. Perceptions of UN peacekeeping in countries such as Mali and the Democratic Republic of the Congo have become overwhelmingly negative, with the now closed MINUSMA and still ongoing MONUSCO failing to meet local expectations or being seen as illegitimate

Western projects. No new UN peacekeeping operation has been authorised since 2017, and the remaining eleven operations suffer from severe budgetary deficits, in large part caused by the US's politically motivated withholding of funds.

Future outlook

The rapidly evolving cracks in world order have spurred much speculation about what an emerging new order will look like, and what it will entail for international peace and security. However, ambivalence and uncertainty, rather than completed shifts, characterise central order-defining relationships and the institutions they operate within. This degree of turmoil in patterned relationships is arguably a state of disorder rather than a materialised new order.

As a direct consequence of a worsened security climate and unpredictable relationships, global defence spending has risen continuously for over a decade, according to SIPRI estimates. The military capabilities that are built can serve different purposes, from deterrence on NATO's Eastern Flank and military support for Ukraine, to special operations, such as those conducted by the US in Venezuela, or large-scale territorial aggression as in Russia's war against Ukraine. For the time being, interest in conventional peacekeeping has declined, especially in missions involving larger numbers of "boots on the ground." Nonetheless, it would be misleading to conclude that IMMs are in general free fall. Rather, the availability of military resources together with shifting relationships may lead to new and/or rebranded forms of international military deployments. Discussions over an international stabilisation force in Gaza, a coalition of the willing in Ukraine, or the US's plea for partner support in the war against Iran, all highlight that the crucial social underpinning of military coalition formation has become more intricate. At the time of writing, it is highly uncertain whether the main traits of IMMs in the post–Second World War order still hold: the centrality of US backing, the reciprocal allied support of the US, and the value of UNSC authorisation.

Further reading

Hellquist, Elin and Elin Jakobsson, 2026, Order and Disorder – International Military Missions 1960-2025, In a forthcoming FOI Anthology.

Hellquist, Elin, 2026, Still Alive? United Nations Peacekeeping in an Age of Geopolitics, In a forthcoming FOI Anthropology.

Johnson, Jamie M., Victoria M. Basham, and Owen D. Thomas, 2022, Ordering disorder: The making of world politics, *Review of International Studies*, Vol. 48, No. 4, 607–625. doi:10.1017/S0260210522000183

8. International law in the new world order—Is international law "dead"?

Sally Longworth

2025 was marked by disruptions in international relations involving major violations of international legal norms, leading many to argue that the rules-based order is coming to an end. This in turn led to the question of what, then, the role of international law is going forward. This chapter addresses this question from an international law perspective. It places the challenges presented in 2025 in the broader context of developments and challenges within the international legal system. It also considers how historical challenges have previously been addressed within that system. This analysis demonstrates that on the whole, States still operate within and develop international law and that, rather than being "dead," international law is likely to be one of the means of addressing the ongoing challenges arising from the changes to the world order.

Introduction

There were many landmarks in international relations during 2025, from the speech by the Vice-President of the United States at the Munich Conference in February, indicating a shift in the structure of international security, to Israel's and the US's attack on Iran in June 2025 and the following "twelve-day war," to the build-up and use of military force in the Caribbean and eastern Pacific, ultimately leading to the US attack on Venezuela in January 2026. In addition to the ongoing armed conflicts that have dominated international headlines, such as those between Ukraine and Russia, Israel and Hamas, and in Yemen, Sudan, and Myanmar, to name a few, there were also brief armed conflicts between India and Pakistan in May and between Cambodia and Thailand in July 2025. As major military powers violate central rules and core functions in the United Nations (UN) remain unable to respond to various crises in the world, some observers question whether States have abandoned the "rule-based order" and what role international law has going forward. Is international law, in fact, "dead"? This chapter assesses the challenges to world order in 2025 from an international law perspective and highlight lessons from history to demonstrate that, far from being "dead," the system of international law is still very much alive. As such, reference to the end of the rules-based order should not be understood as a reference to the "death" of international law. Indeed, international law continues to be critical to States in regulating their relations with one another. That said, the world order is subject to change, which impacts the formation and development of international law. It is important to understand those changes in their proper context so as to pursue the best course of action.

Taking stock of developments in 2025

In between the numerous crises that dominated our newsfeeds in 2025, multilateral treaties continued to be drafted and new areas of agreement for international cooperation were found. For example, States moved forward with historic action to improve preparedness and ensure a more equitable response to pandemics with the adoption by consensus of the World Health Organization Pandemic Agreement in May 2025 and the entry into force of the new International Health Regulations in September 2025. In October 2025, the new UN Cybercrime Convention opened for signature in a ceremony in Hanoi, which concluded with 72 States signing the convention.

Progress also continues to be made in relation to areas relevant to military operations and total defence. In November 2025, the General Assembly's Sixth Committee decided by consensus to launch the process to negotiate an international convention to govern the prevention and punishment of crimes against humanity. At the same time, a major step forward in regulating new military technology has been taken as the current mandate of the Group of Government Experts on Lethal Autonomous Weapons (GGE LAWS) draws to a close in 2026. All major military powers have engaged in this process, notwithstanding their differences in other international fora. All of these examples highlight how States continue to act within the system of international law and use this framework as a means to regulate their common interests and further their positions.

Acknowledging the challenges

At the same time, it cannot be denied that this is a period of change. Nothing demonstrates this more clearly than the multiple breaches of the prohibition of the threat or use of force in relations between States seen in 2025 and early 2026. The flagrant and systemic violations of core norms of international humanitarian law (IHL) and international human rights law (IHRL) seen in ongoing armed conflicts have similarly led to call out the situation as a crisis of humanity. The international community has grappled with how to respond to these challenges due to longstanding structural and procedural difficulties, such as blocking Security Council action and cuts to the UN's budget. Understanding the impact of these changes on the world order and the role of international law is therefore essential to be able to identify opportunities to further Swedish positions most effectively.

These violations are serious breaches of the rules of international law, threatening not only the territorial integrity and political independence of the affected States, but also the interests of all States in international peace and security. They do not, however, necessarily change the content of the rules themselves. The armed attacks against Iran by the US and Israel in June 2025 and later in March 2026, for example, were roundly condemned by the majority of other States as violations of the prohibition of the use of force by States in their relations with each other. The US's military operations off the coast of Venezuela conducted from August 2025 and culminating in military intervention in January 2026 were similarly con-

demned as violations of international legal norms. State practice is important for assessing compliance with international law, as well as developing understanding of what is required by the rules. By condemning these acts, States reassert and reaffirm their understanding of the requirements.

These violations do highlight an ever-present challenge to the system of international law, namely how violations are addressed. Unlike domestic legal systems, where power stems from a constitutional framework and rules are created, implemented, and enforced on a vertical axis, the international legal system operates horizontally. States are the primary actors in the international legal system and are equal on a horizontal axis. They create, apply, and enforce law between themselves. This can make it conceptually challenging to evaluate violations in their proper context.

2025 also marked a historic change in disarmament law. Estonia, Finland, Lithuania, Latvia and Poland withdrew from the Ottawa Convention, arguing that this was necessary in light of the regional security situation. Lithuania also withdrew from the Convention on Cluster Munitions, and Ukraine announced its withdrawal from the Ottawa Convention shortly after. This is the first time any State has withdrawn from either Convention and marks a significant step backwards in the progress that had been made in reducing the disproportionate impact these weapons have on civilians. Challenges are also evident in other disarmament fora, notably in obstructions at the review conferences relevant to conventions on biological, chemical, and nuclear weapons. These obstructions reflect the tensions in global security arising from an increase in international armed conflicts and changes to rearmament policies. At the same time, the Marshall Islands and Tonga ratified the Ottawa Convention, and Vanuatu signed the Cluster Munitions Convention, continuing the general trend of progressively more States being bound by these requirements year on year. Of the 193 Member States of the UN, 112 are party to the Cluster Munitions Convention and 162 to the Ottawa Convention. So, while the vast majority of States continue to support the aims of disarmament law as a foundational part of the architecture of international peace and security, these developments are concerning for the world order.

Learning the lessons from history

This is not the first time that IHL and IHRL have been breached in armed conflict. Historic violations have given rise to the development of new rules so as to address the challenges faced, such as the drafting of the Geneva Conventions in 1949 following World War II, and the drafting of the Additional Protocols of 1977 following decolonisation.

There are now more institutions established to monitor and evaluate these violations than ever before, and more national investigations, prosecutions, and convictions of international crimes in domestic criminal courts than at any other time in history. This has been greatly facilitated by the work of the International

Criminal Court and the principle of complementarity set out in the Rome Statute of 1998, according to which States have the primary responsibility for holding perpetrators of international crimes accountable. The UN's Human Rights Council has established innovative ways to address impunity at the national level by creating mechanisms to enable coordination between States in the investigation and prosecution of international crimes.

In addition to proceedings before national and international criminal courts, individuals have sought reprieve through regional and international human rights mechanisms, such as the judgments and cases pending before the European Court of Human Rights relating to violations of the European Convention on Human Rights in the continuing armed conflict. The ongoing proceedings before the International Court of Justice (ICJ) brought by South Africa against Israel are a further example of States trying to address and settle their differences peacefully through dispute resolution mechanisms. The ICJ has an unprecedented number of cases before it, highlighting the importance of international courts as a means to peacefully settle disputes between States and to reaffirm the rule of law in international law.

This period is also by no means the first time in history that the Security Council has been blocked from taking action due to national interests in the exercise of the veto power by the permanent members. Indeed, the period following the end of the Cold War up to the military intervention in Iraq in 2003 was rather the exception than the rule, during which the Security Council could more fully execute its role as the primary responsible body for international peace and security. In 1950, just five years after the UN Charter came into force, the Security Council was blocked by the Union of Soviet Socialist Republics (USSR) preventing the Council to respond to the military action of North Korea. It was the General Assembly that responded to the crisis by passing the "Uniting for Peace" Resolution in November 1950. The Resolution provides that where the Security Council fails to exercise its primary responsibility for the maintenance of international peace and security because of lack of unanimity of the permanent members, the General Assembly shall seize itself of the matter. Similar to that time, we are seeing major innovations coming from the General Assembly today in response to the blocking of Security Council action. Examples include resolutions condemning the Russian aggression against Ukraine, calling on Russia to be held accountable for its violations of international law in this context, including making reparation for damage and injury, and establishing a register of damage for Ukraine in 2022. Only time will tell if the accumulated combination of the current crisis plus the economic challenges faced by the UN may spur major reform of the UN system or its workings.

Conclusion

Two decades ago, the prominent scholar and sitting judge at the International Court of Justice, Hilary Charlesworth, warned against framing international law's challenges in the language of crisis. Crises are by definition the exception and not the rule, and reviewing an entire system on these narrow terms overshadows the structural dimensions of our analysis and limits our imagination. International law is not the root cause of the crises we are living through today, but it is highly likely to be part of the solution. As such, arguments that international law hinders our responses only exacerbate the problems faced and are themselves a significant threat to the whole system of the rule of law. As noted in Sweden's National Security Strategy 2024, a safe and secure Sweden is based on international law. Sweden therefore needs to be clear in asserting and affirming the norms of international law.

In this period of change, it is clear that the majority of States have rejected anarchy. This is also not the first time that change has been observed within the world order. International legal scholars track these developments from the foundation of the nation-state with the Peace of Westphalia in 1648 as an order based on coexistence. This world order was modified by the introduction of the UN Charter to what has been described as an order based on community and cooperation, with further changes in the post-Cold War period and discussions of "constitutionalism." Whilst there has been much change, there has also been much continuity. References to the end of the rules-based order should therefore be understood not as an end of international law, but rather as a reference to the next change in the world order, in which international law will no doubt play an important role.

Further reading

Charlesworth, Hilary, 2002, "International Law: A Discipline in Crisis," *The Modern Law Review*, Vol. 65, No. 3, May 2002, 377–392.

Croon, Adam, Longworth, Sally, Refors Legge, Maria and Winther, Pontus, 2023, *Vägar till juridisk motståndskraft—Att identifiera och motverka användning av juridiska sårbarheter i rättssystem*, FOI-R--5501--SE, Stockholm: Swedish Defence Research Agency (FOI).

United Nations, 2025, *Shifting Paradigms: United to Deliver*, Report of the Secretary General, September.

9. A new nuclear order

Karl Sörenson and Christopher Weidacher Hsiung

The world is stepping into a new nuclear era. What will replace the old order is highly uncertain. Current arms control agreements and nuclear norms are eroding while great power rivalry is overtaking the global agenda. Understanding the developments and dynamics of this change will be pivotal not only to navigate it but also to make strategic decisions in a more hostile and dangerous world.

Great power rivalry has returned to the forefront of international politics. The rise of China, Russia's resurgence, and the US's efforts to maintain its post–Cold War global dominance are transforming the current world order.

With New START set to expire this year, the last bilateral strategic arms control instrument defining the size of US and Russian nuclear warheads and delivery vehicles will come to an end. However, the end of New START is just the latest in a series of arms control setbacks: the Russian parliament, the Duma, revoked its ratification of the Comprehensive Test Ban Treaty (CTBT) in 2023; only five years earlier, citing repeated Russian violations of the treaty, in particular the development and fielding of the 9M727 (or SSC-8) ground-launched cruise missile, the first Trump administration withdrew from the Intermediate-Range Nuclear Forces Treaty (INF). While China is a signatory to the CTBT, the US accuses China of conducting critical nuclear tests in violation of the treaty. China is a signatory to the Non-Proliferation Treaty (NPT), has pledged not to export nuclear weapons or assist third parties in acquiring them, and has committed itself to the total reduction of nuclear arsenals. That said, China has so far refused to engage in any meaningful arms control agreements and has instead built up its nuclear forces on an unprecedented scale. Add to this the proliferation of India, Pakistan, and North Korea, and the architecture of arms control instruments and nuclear norms that once defined the post–Cold War nuclear era has changed beyond recognition.

A Three-player Game

Perhaps the most defining feature, and indeed the biggest driver, of the new global nuclear order is that it is now a three-player game made up of the US, Russia, and China. This is creating a different strategic situation, in stark contrast to the Cold War period when the nuclear landscape was defined foremost by the bipolar competition between the US and the Soviet Union. Today, these three major players increasingly view nuclear capabilities as a vital part of adapting

their military forces and national security strategies to a new era of geopolitical competition.

For decades, Russia has modernised its nuclear forces, replacing old capabilities with newer, more advanced systems. In one sense, since the end of the Cold War Russia has held a fundamental belief that it must maintain a strong and capable nuclear arsenal, not the least to compensate for its conventional weakness vis-à-vis the US and NATO. Nuclear weapons are perhaps Russia's only remaining source of leverage, especially as its economy, exports, and industrial output falter in comparison with those of the US and China. The pivotal role that nuclear weapons play for Russia has become crystal clear after its full-scale invasion of Ukraine, during which it has repeatedly used nuclear coercion and threats to discourage deeper US and NATO involvement, while also raising the possibility of deploying nuclear weapons to Belarus. Russia's war against Ukraine has also created a new problem for Russia: with most of its conventional forces tied up in Ukraine, any serious challenge to its power may prompt a rapid resort to nuclear escalation, not because of strategy, but because of necessity.

China, which only a decade ago was a minor nuclear power, is in the midst of a substantial transformation of its nuclear arsenal and, some believe, its nuclear strategy. It now possesses a fully operational nuclear triad (land, air, and sea-based nuclear strategic deterrent) similar to that of the US and Russia. Its nuclear forces are more diverse, mobile, and accurate, and the readiness level of the PLA Rocket Force has increased. China's nuclear stockpile has tripled in the last decade, now exceeding 600 warheads and projected to reach 1,000 by 2030. The quantitative and qualitative changes have raised concerns that China is changing its traditional defensive strategy based on assured retaliation to open up options for a more distinct regional nuclear posture, most likely to coerce and deter regional powers and the US from intervening in a potential military conflict over Taiwan.

The US, partly as a response to China and Russia, is also putting renewed focus on its nuclear arsenal. As early as during the Obama administration, the US had initiated a USD 1.7 trillion programme to upgrade its land, air, and sea-based nuclear capabilities, but at the same time sought to reduce the total number in its stockpile and not develop any new weapon types. However, the Biden and Trump administrations have been moving ahead with modernising the nuclear forces, for instance developing more diverse delivery systems, such as the nuclear-tipped Sea-Launched Cruise Missile (SLCM-N) and adding new initiatives such as the Golden Dome missile-defence system as the most extravagant example. The US approach to nuclear deterrence is strategically and economically demanding as it seeks what it calls "damage limitation," which essentially means that the US Armed Forces, including its nuclear forces, seeks to be so robust that even an opponent with equal nuclear force size will stand a low chance of gaining a strategic advantage.

And Then There is the Rest

The global nuclear landscape is made even more complicated as it now also involves many more nuclear-armed states than during the Cold War. This includes not only the traditional nuclear powers of the UK and France but also the nuclear proliferators of India, Pakistan, and North Korea. These states have long held relatively constant nuclear arsenals and postures or developed rather limited nuclear capabilities. But with the crumbling of the legal and institutional framework for arms control and non-proliferation, growing strategic competition between the US, Russia, and China, these states are also taking note and starting to review the capabilities and strategies of their own nuclear forces.

Partly due to Russian nuclear sabre-rattling in the Ukraine war and partly due to concerns over US extended deterrence commitments in Europe, France and the UK are reviewing their nuclear arsenals and doctrines. France is reviewing the number of deployed warheads, has added a nuclear-capable air wing, and is developing a new hypersonic nuclear-tipped cruise missile. This capability development was accompanied by a historic speech by France's President Emanuel Macron in March 2026, in which he opened the door to closer collaboration with key European allies and to their involvement in France's nuclear mission. The UK, whose arsenal is closely tied to that of the US, has just announced plans to rejoin NATO's DCA mission (Dual-Capable Aircraft that can carry the US nuclear gravity bomb B61-12). Moreover, in 2025 France and the UK signed the Northwood Agreement, a landmark step to further coordinate their nuclear deterrence strategies.

Just as Europe is adjusting to a new nuclear reality, India is gradually expanding its arsenal and also developing new delivery systems, much in response to China's nuclear buildup, underpinned by an unresolved border dispute and broader strategic competition over regional dominance in South Asia. India, however, is also concerned about Pakistan, its local arch-rival, which it seeks to deter. Pakistan, which is conventionally inferior to India, must therefore rely on having a credible nuclear deterrent. Moreover, North Korea now has a small but increasingly capable nuclear arsenal, and efforts by the international community to push for North Korean disarmament seem all but dead. The state of Iran's nuclear weapons programme remains uncertain after US missile strikes on nuclear facilities in 2025, but concerns are far from gone in the Middle East where nuclear-armed Israel continues to view Iran as its main regional threat. With the US's latest war in the Middle East aimed at Iran and what is left of its attempt to develop nuclear weapons, the world has taken yet another step into uncharted territory.

The question of acquiring a national nuclear-weapon capability has reawakened in some states that are concerned about the reliability of US security guarantees. For instance, in South Korea there is renewed debate about developing its own nuclear weapons to deter potential North Korean aggression. The same applies to Poland, which has asked to host NATO nuclear weapons and where public debate over a national programme has begun.

The Shape of Things to Come

Historically, the risk of nuclear war has been mitigated by a combination of arms control instruments on the one hand, which temper destructive power and curb arms races, and nuclear deterrence on the other, which aims to ensure that any state using nuclear weapons will lose more than it could ever hope to gain. With arms control instruments gone or under pressure, deterrence, particularly nuclear deterrence, is increasingly becoming the principal strategic tool for mitigating the risk of nuclear exchange. However, deterrence, while often effective, relies on increasing the risk for the opponent, thus also augmenting the overall risk. Far fewer nuclear warheads are deployed today than at the height of the Cold War, but the trend towards more nuclear weapons and fewer constrained rules and norms regulating the global nuclear order heralds more strategically challenging times.

Nuclear weapons are the most powerful weapons humankind has invented, but the underlying technology stems from the 1940s. The impact of technological developments such as artificial intelligence (AI), quantum computing, cyber capabilities, and advanced satellite systems on the role of nuclear weapons in deterrence is not yet clear. On the one hand, innovations can make old systems more precise and add efficiency. However, advances in conventional capabilities, for instance long-range deep strike, can also seriously challenge deployed nuclear arsenals. Improved space and cyber capabilities can make both nuclear coercion and deterrence more difficult, but also possibly enable them. Command and control systems with integrated AI can introduce new risks and challenges as well as improve decision times. Add sophisticated missile defences to the mix and this new variety of technological advances creates a strategic environment that will be challenging to gauge for challengers and defenders alike. This type of uncertainty may at times temper the appetite of a challenger, as the outcomes of an attack against a conventional, but technologically sophisticated, adversary may be difficult to foresee.

For Europe and countries such as Australia, Japan, and South Korea, new technological advances in weaponry potentially provide an alternative, as they may still wish to resist nuclear proliferation without compromising their own security. For all that new technology does, it does not come cheap. Investment in defence capabilities is already increasing in both Europe and Asia, but the pace and variety will pressure countries that currently are struggling financially to keep an acceptable growth rate.

Despite all the new strategic developments, from nuclear deterrence and arms control to nuclear proliferation and advanced technologies, the constant challenge all must face is the cost of defence. The state that can outspend an adversary has always enjoyed a strategic advantage, and states that invest strategically may be best placed to dictate the arms control instruments of the future.

Further reading

Karl Sörenson, 2024, "Prospects of Deterrence: Deterrence Theory, Representation and Evidence," *Defence and Peace Economics*, Vol. 35, No. 2, 145–159.

Christopher Weidacher Hsiung, 2026, China's nuclear strategy and capabilities: An introduction, FOI Memo 9277, Stockholm: Swedish Defence Research Agency (FOI).

Miller, Steven E., Robert Legvold, and Lawrence Freedman, 2019, *Meeting the Challenges of the New Nuclear Age: Nuclear Weapons in a Changing Global Order, American Academy of Arts & Sciences*.

Part Two
Societal Security

10. Preparing Defence for Climate Security Futures

Bruno Charbonneau

Climate change is one of the defining challenges of the 21st century. Human emissions of greenhouse gases have increased and will continue to increase the temperature of the Earth's atmosphere, consequently leading to rising global sea levels, melting ice sheets, altered ecosystems, and an increased frequency of extreme weather events such as droughts, heat waves, and floods, and affecting the health and livelihoods of human communities across the globe. The problem and its solutions encompass and affect large sectors of human activities, from science to economics, to international, national, and local politics, to law, health, and culture, just to name a few.

At the Davos summit in 2026, Canadian Prime Minister Mark Carney gave a historic speech in which he claimed that major upheavals in global systems represented a "rupture" of the international rules-based order. He did not make an explicit reference to climate change, but he is aware that it is and remains one of the defining challenges of the 21st century. As such, climate change is a systemic challenge that brings potentially radical transformations and its share of ruptures, whether those come from the transformations in Earth systems or the ways in which human societies mitigate or adapt to climate change.

In this context, to talk of "climate security" is to analyse and consider the implications of climate change for the security sector and for security policy, relations, and practices. How is climate change transforming the security, strategic, and geopolitical environments? What are the consequences for defence and military organisations? How should these organisations prepare, adapt, and mitigate, and what should they prioritise? The chapter begin by emphasising the importance of how one frames climate security, as one's framework will often define a programme for action. Then, it highlights the specific challenges that climate change poses for defence and military organisations, notably in the context of international tensions and increased defence spending. The chapter conclude with some insights and recommendations on how to move forward, thinking and planning for the radical uncertainties of climate security and defence futures.

Framing climate security

The field of climate-security practice (defined roughly as a mix of academic, policy, and think-tank work and relations) has rapidly evolved and grown in recent years. Early influential logics embraced the threat-multiplier narrative and the

climate–conflict nexus. The former emphasises that climate change multiplies the number of, and exacerbates, security threats. While analytically limited, the political utility of the threat-multiplier concept sustains its influence in policy circles and in defence organisations. The climate–conflict nexus draws attention to the climatic causes of war and violent conflicts, although most of the literature has moved away from trying to establish direct causal links, instead focusing on how climate change can lead to different pathways that might lead to war, conflict, or the possibility of (environmental) peacebuilding.

Slowly but surely, the research and the policy conversations have been moving beyond these limiting logics. Climate change is increasingly recognised as a systemic problem and challenge that transforms the geopolitical and strategic environments and that calls into question common assumptions about security and defence, a "wicked problem" that can hardly be siloed and that involves both short-term and long-term timescales by producing both sudden security crises and emergencies and slow-onset catastrophes.

Climate change is unlike any other topic. From a policy perspective, it cannot be restricted to being another item on the list of an ever-increasing security agenda. It changes the context of security policy and strategy, and thus, arguably, affects the whole security agenda. Moreover, its effects are not limited to the mix of extreme weather events, crises, or emergencies, or the long-term tipping points and collapse scenarios. Human societies are working to mitigate and adapt to climate change, with structural consequences for the evolution of the international state system and the global political economy that, in turn, will impact the trajectories of climate change. In short, it is these interactions and feedback loops between the physical transformations of Earth systems and the transformations of the world of human affairs that highlight the scale and the scope of the complexities and uncertainties that security, defence, and military organisations are facing and must be ready to address.

Despite the high complexity and deep uncertainties that climate change introduces, the evolution of the particular context in which a specific security, defence, and military organisation operates will remain central for analysing and assessing how these organisations should respond and adapt. Climate-security research increasingly shows how climate change interacts with other global challenges and human systems, such as ecosystem collapse, pandemics, economic and political instability, and more. The role of technology and innovation in climate security is an area of burgeoning interest. From advanced climate modelling to AI-driven early warning systems, technological advancements offer new opportunities for anticipating and mitigating climate-security risks. Whether climate change multiplies threats or causes war is not the most productive question for security and defence policy. The priority must be on assessing how the primary, secondary, and (perhaps even) tertiary effects of climate change impact the strategic landscape, the character of war and security, and the purpose and utility of (military) force in a world that is not only rapidly warming but also moving toward adap-

tive and low-carbon technologies (i.e., the energy transition; see the last section). Such a focus demands in-depth knowledge both of global climate change and of how climate change shapes particular strategic contexts, whether such contexts are defined internationally, regionally, nationally, or locally.

Lastly, we must acknowledge the colossal uncertainties that come with climate change and recognise the policy implications, notably in terms of identifying the best course of action. Science does not have and cannot produce all the answers and, even if it did or could, hard political decisions will still need to be made. The possibilities and limits of scientific analysis must be acknowledged so that it can properly inform political judgments, unless it becomes trivialised in the policy space. On the other hand, given the complexities, scientific expertise must also more directly contribute to the policy process. More work and research are needed to build a new or climate-security-adapted science-policy model that empowers expert knowledge so that it can help define the problems and solutions of climate security policy. The challenge is building a sustainable analytical, strategic, and operational capacity for the elaboration of long-term plans while retaining the capacity to react to crises or emergencies.

What about defence?

What does climate security imply for defence and military organisations? How are they affected by climate change? What are they to do about climate change? NATO's 2010 Strategic Concept was the first iteration to formally recognise the impacts of climate change on security. It took, however, the ministerial endorsement of a Climate Change and Security Agenda at the 2021 NATO summit and the 2022 Strategic Concept to acknowledge the implications for the organisation's core tasks and get the ball rolling, including the creation of the Climate Change and Security Centre of Excellence, which received its NATO accreditation in 2024.

First, defence and military organisations will need to adapt their capabilities to the primary impacts of climate change, to increasingly challenging and extreme operating environments, as well as increasing demands to respond and provide assistance when natural and humanitarian disasters occur. A sample list of consequences that are already observable and quantified should suffice: warmer oceans affect sonar effectiveness negatively; a warmer atmosphere decreases strategic airlift capacity; extreme heat increases the number of "black flag" days (when high-risk heat conditions prevail) and affects training and readiness; shifting precipitation patterns and more frequent and intense storms disturb mobility and access to zones of operations; storms, floods, and fires destroy infrastructure; and heat, extreme weather, and natural disaster operations impact soldiers' physical and mental health; and so on.

Second, defence and military organisations must prepare and plan for the disruption of supply systems and logistics chains. The material implications of climate

change for the defence sector and its core business are structural and profound, both in terms of the direct impacts of climate change and in terms of secondary or tertiary effects from the restructuring of the global political economy. Climate risks and vulnerabilities, as well as climate adaptation or mitigation efforts, will disturb, shock, or disrupt supply systems, energy availability, critical minerals, food, water, and health supplies, and more. National climate adaptation and resilience are the necessary conditions for ensuring national security and defence capability. Numerous calculations associated with defence planning processes, procurement, the allocation of resources and the recruitment and training of personnel, and more will depend on how well national governments can adapt and build national resilience. We can expect increasing pressure on defence and military organisations to align with future climate adaptation and resilience priorities and plans.

Third, defence and military organisations must address the first two points while preparing for a rapidly evolving and increasingly uncertain strategic landscape. While the international rupture has seemingly marginalised and eclipsed climate change and climate security agendas, with policy discussions across the North Atlantic community now emphasising national sovereignty, energy security, and increased budget spending, climate change is not going away. In the NATO context, most governments have increased their defence budgets, with, for example, the Carney government promising a doubling in Canadian defence spending by 2030. Such a military buildup presents multiple dilemmas, not least because it locks in future carbon emissions that will exacerbate climate-security risks and vulnerabilities. Global tensions have made it implausible, arguably, to address the problems of military emissions and contribution to climate change through reductions in size, spending, and operations. And yet, as this author have argued elsewhere, there is no scenario in which defence and military organisations can avoid the climate crisis.

Preparing for low-carbon warfare: the future(s) of climate and energy security

It has been said that energy is the "lifeblood" of the military. Critical dependencies—and the vulnerabilities they create—that militaries have on fossil fuels tend to be rediscovered in times of heightened tension and war. Now, the world is moving towards low-carbon technologies and alternative sources of energy. The International Energy Agency estimates that global renewable power capacity will double between 2025 and 2030, increasing by 4600 gigawatts. This growth is dominated by the increase in solar capacity, which should also double in the next five years, with a positive expansion of renewables especially in India, Europe, and most emerging economies.

The deployment of energy alternatives is only one facet of the global energy transition. The other is retirement scenarios for existing fossil fuels infrastructure. As the global energy transition progresses, competition between energy systems

could undermine fossil systems in ways that are nonlinear, potentially leading to sudden supply system collapses, and thus putting constraints on military supply systems. In the short term, there is no technological breakthrough that can sever the tether keeping militaries dependent on fossil fuels. Yet, the reliability of fossil energy systems is no longer guaranteed. Defence and military organisations must plan for the decline and possible collapse of fossil energy services. They must carefully manage decarbonisation, keep a close eye on the decline of fossil systems, and build new energy logistics chains that are not dependent on and vulnerable to the collapse of fossil infrastructure and supply chains. In the coming years and decades, defence planners must push for and invest in energy-related technological breakthroughs that can be deployed at the scale required, rapidly adopted, and diffused across the entire force structure with minimal impact on force design.

The connections between the climate crisis and the energy transition are of crucial importance for defence and military organisations. Analysts, researchers, and strategists must change their mindset and should think in terms of "low-carbon warfare," that is, in systematic ways that account for both climate and energy security futures as the sociotechnological and economic bases of military and defence organisations are being globally transformed. It should be clear that this is not about "greening defence," but about identifying the systemic risks, vulnerabilities, and tipping points where and when the machine might break down given radical global transformations. Through the prism of low-carbon warfare, the distinction between climate mitigation (cutting military emissions) and climate adaptation (for instance, by enhancing "resilience") is secondary because it misses the crucial point that military climate and energy futures are being defined elsewhere. Change is coming irrespective of military preferences. Keeping up with the energy transition may emerge as a far more potent driver of low-carbon warfare and military innovation than the climate security agenda, but it bears repeating that climate and energy futures are intimately tied.

Further reading

NATO Climate Change and Security Centre of Excellence, 2026, *Publications*, accessed 30 March 2026, https://ccascoe.org/publications/.

North Atlantic Treaty Organization, 2026, *The Effects of Climate Change on Security*, final report of the STO Research Task Group SAS-182, STO Technical Report TR-SAS-182, 2026.

Depledge, Duncan, 2023, "Low-carbon warfare: Climate change, net zero and military operations," *International Affairs*, Vol. 99, Issue 2, March 2023, 6

11. Minerals of Power: Rare Earth Dependencies and Strategic Leverage in Europe's Security Order

Benjamin Ståhl and Alexander Gorgijevski

Since Russia's full-scale invasion of Ukraine, Europe's security order has entered a new phase defined by rearmament, sanctions, and the weaponisation of supply chains. This shift has pushed critical raw materials to the centre of economic statecraft. Rare-earth elements such as neodymium, praseodymium, and samarium are indispensable to the magnets, sensors, and guidance systems that underpin precision weapons, advanced radar, and electric propulsion. Mineral access has shifted from economic concern to strategic imperative. China's near-monopoly over both refining and magnet production anchors a structural dependence shaping alliance politics. In response, the US has pursued transactional mineral diplomacy and a "mine-to-magnet" strategy, while the EU relies on regulatory instruments to accelerate domestic capacity. For Sweden, and for Europe more broadly, geological assets become instruments of deterrence credibility and strategic leverage. This article examines how mineral supply reshapes alliance dynamics and economic power in Europe's emerging security order.

From industrial inputs to strategic imperatives

Control of resource value chains has moved to the centre of economic statecraft. When Beijing tightened specific controls on rare-earth elements in 2025, it directly hit Western defence supply chains. This shift mattered less for the economic cost than for the signal it sent: materials essential to fighter aircraft, missiles, and radar systems were now governed by the same administrative leverage as civilian goods, demonstrating how quickly supply dependence can be weaponised.

Rare-earth elements underpin electric actuators and precision guidance and sensor systems in modern military platforms. A fighter aircraft contains hundreds of kilograms of rare-earth components. Substitution is technically possible but operationally costly, increasing weight, reducing efficiency, and requiring re-certification.

As European states accelerate rearmament, these material dependencies have moved from the background of defence planning to its core. Rare earths shape what can be built, how fast it can be produced, and at what scale capability can be sustained under stress.

The strategic salience of rare earths is amplified by the fact that they underpin two of the defining projects of the decade: the energy transition and military rearmament. Wind turbines, electric vehicles, grid infrastructure, and data centres rely on the same high-performance magnets and alloys as submarines, aircraft, and missile systems.

Scarcity affects civilian and military demand in different ways. Civilian industries typically absorb input shortages through price adjustments, product redesign, or delayed delivery. Defence organisations face a different constraint: the requirement for assured access at the moment of operational need. Average availability across a business cycle matters little if a material is unavailable during mobilisation or sustained conflict. Following Russia's invasion of Ukraine, European defence procurement timelines shortened just as climate targets expanded demand for rare-earth-intensive technologies. Stockpiles once considered adequate were drawn down. What might previously have been an inconvenience became a strategic concern.

Military demand is hence modest in volume but decisive in timing. A small shortfall at the wrong moment can have outsized effects on readiness and deterrence credibility. History shows that militaries can adapt to material scarcity through substitution or redesign. Yet such adjustments typically require years of development, industrial coordination, and acceptance of performance trade-offs. The difficulty today is that civilian and military demand increasingly rely on the same value chains and dual-use technologies. The tighter this coupling becomes, the harder it is to treat rare earths as ordinary commodities governed by price signals alone. Instead, they become objects of prioritisation, allocation, and political negotiation.

From resource endowment to value chain leverage

Access to raw materials has always influenced security policy. What has changed is where leverage is exercised and how it is applied. In earlier eras, vulnerability was visible and often bilateral. Coal, oil, and uranium were geographically fixed, nationally regulated, and frequently state-owned. Disruption was blunt and responsibility was clear. Today, dependence is embedded in value chains that stretch across borders, firms, and regulatory systems, often masking where strategic control resides.

Rare earths exemplify this shift. Geological availability is no longer decisive: rare earths are not scarce in absolute terms. Strategic leverage lies in the stages that transform raw material into usable industrial inputs: separation, refining, alloying, and magnet manufacturing. Security-relevant power now accumulates here, rather than at the mine.

The current value chain configuration is the product of deliberate choices. From the 1990s onwards, Chinese central and provincial authorities identified rare

earths as strategic inputs for prioritised industries and pursued vertical integration across the value chain. Local governments offered land, subsidised energy and financing, and tolerated environmental externalities that would have faced opposition elsewhere. Western firms responded to these commercial incentives. European, Japanese, and American companies closed processing and magnet-production facilities at home and relocated manufacturing to China, attracted by lower costs and access to expanding downstream markets. Governments largely acquiesced, confident that global markets would continue to function and that supply security could be treated as a commercial rather than strategic concern.

By the mid-2000s, this division of labour had solidified. Europe retained advanced defence, automotive, and energy industries, but depended almost entirely on imported rare-earth oxides, metals, and magnets. Beijing secured significant extraction capacity abroad, locking in raw material supply. Simultaneously, China consolidated domestic downstream capacity to a level that is now difficult to contest. Today, China accounts for roughly 70 per cent of global rare-earth mining, but more critically, it controls more than 85 per cent of refining capacity and as much as 90 per cent of permanent magnet production. This structure grants Beijing effective administrative authority over the entire value chain, regardless of where the ore is mined.

This dominance provides leverage over the value chain in two modes: restriction and abundance. China has demonstrated the ability to adjust output and access conditions in ways that move prices and reshape competitors' incentives, discouraging investment elsewhere and reinforcing concentration. In this sense, leverage is exercised not only by denial, but by the power to set the terms of normality.

Since 2010, Chinese policy has increasingly shifted from episodic restriction to administrative control. Rather than imposing blanket bans, authorities have relied on licensing regimes that require end-user disclosure and regulatory compliance, allowing access to be delayed, conditioned, or suspended without formal prohibition.

Weaponised interdependence and European asymmetry

The strategic implications of this shift first became visible in 2010, when China restricted rare-earth exports to Japan during a diplomatic dispute. Tokyo treated the episode as a warning. The Japanese government intervened directly, subsidising alternative supply through partnerships with companies such as Lynas Rare Earths in Australia and Malaysia. Costs increased, but exposure fell. The response demonstrated that diversification required policy, not just price signals.

This is the current strategic dilemma confronting Europe and its allies. Rare-earth value chains were built for efficiency and scale during a period when geopolitical risk was discounted. Retrofitting them for security is possible, but it is slow, contested, and deeply political. The question is no longer whether dependence

exists, but how much leverage it confers and how it can be managed without fracturing alliances or markets altogether. The politics of rare earths now unfold within a contested landscape of economic power. Weaponised interdependence has moved from regulatory margins to the centre of trade policy and political rhetoric.

Interdependence also means that policy measures spill over from one sector to another and to other trading partners. In 2022, Washington imposed sweeping export controls on advanced semiconductors, chip design software, and manufacturing equipment destined for China. These measures reframed access to critical inputs as a security issue rather than a commercial one and made political alignment an explicit condition for participation in leading technology supply chains.

China responded by broadening its own menu of economic security instruments. Rather than mirroring US measures sector by sector, Beijing focused on areas where it held structural advantages. Rare earths offered leverage through value chain dominance. In 2025, China expanded the scope of its controls to cover related technologies and products containing Chinese rare-earth inputs, echoing the extraterritorial logic already applied by the US in the semiconductor domain. Licences for military end use would not be approved. Furthermore, licences were required for all cross-border trade, not only from China, which dragged Europe into the dispute.

These developments reverberated through industrial supply chains. In Congressional testimony and regulatory filings during 2025, large US aerospace and defence contractors including Northrop Grumman, Lockheed Martin and Raytheon Technologies explicitly flagged rare-earth supply chain risks tied to China's dominance as a genuine operational concern. They noted that lead times for components containing rare-earth magnets could extend to 18–24 months under normal conditions and that export restrictions would exacerbate programme delays across radar, guidance, and propulsion systems.

In the second half of 2025, following high-level negotiations between Washington and Beijing, China temporarily suspended implementation of its newest rare-earth export controls for one year. The pause coincided with US moves to moderate or defer certain tariff measures after President Trump met President Xi. The sequence reinforced a central point. Rare-earth controls are not an autonomous industrial policy, but an instrument deployed within a broader process of trade bargaining and geopolitical signalling.

In the US, rare earths have moved from an industrial concern to a core national-security priority. The 2025 National Security Strategy places critical minerals at the centre of economic statecraft, framing supply-chain resilience as indispensable to military readiness and strategic autonomy. Federal support has expanded under a "mine-to-magnet" push to rebuild domestic processing and magnet ca-

pacity, including public–private partnerships. Higher costs are explicitly accepted as the price of assured access and insulation from coercion.

Washington has paired industrial policy with coercive trade diplomacy. In late 2025, President Donald Trump signed a series of bilateral critical-minerals agreements with Australia, Japan, Thailand, and Malaysia, tying trade concessions to preferential US access to supply, with negotiations conducted under the shadow of tariff escalation. The earlier minerals accord with Ukraine embedded reconstruction finance in long-term resource access, signalling that critical materials now shape alliance bargains as much as security guarantees. Even the administration's assertive rhetoric toward Greenland and Canada has revolved in part around Arctic and North American mineral assets, underscoring how geology has entered grand strategy.

Beyond bilateral deals, coordination has expanded through the G7 Critical Minerals Action Plan, the enlarged Minerals Security Partnership/Forum on Resource Geostrategic Engagement, and the Critical Minerals Ministerial, inaugurated in February 2026. These formats are formally multilateral, yet in practice largely US-driven. What is emerging is less a neutral rules-based regime than a US-centred economic security bloc, organised around trusted supply chains and the strategic exclusion of China.

Europe confronts this landscape from a position of asymmetry. The EU neither initiated the US–China technology confrontation nor controls its escalation, yet its industries remain heavily dependent on Chinese processing and magnet production without comparable leverage in return. Diversification is urgent but, unlike Washington or Beijing, Brussels' instruments remain regulatory rather than coercive, ill-suited to a contest defined by speed, scale, and executive discretion.

The EU's Critical Raw Materials Act of 2023 and subsequent ResourceEU action plan seek to accelerate domestic extraction, processing, and recycling through regulatory targets and fast-tracked "Strategic Projects," such as the Per Geijer rare-earth deposit in Kiruna, Sweden. Yet these instruments reflect a fundamentally different model from Washington's deal-based mineral diplomacy. The EU relies on market incentives, permitting reform and coordination rather than executive leverage or bilateral resource-for-security bargains.

Weaponised interdependence is therefore no abstraction but the operating environment. Economic power is now exercised openly through supply-chain control and resource diplomacy. For Europe, the question becomes how interdependence can be managed when both rivals and allies treat minerals as strategic leverage rather than neutral commodities. As economic statecraft moves to the centre of geopolitical competition, the EU's task is to navigate a landscape where supply chains are weaponised by rivals and conditioned by allies.

Strategic questions for the next decade

The debate over rare earths is often framed as a supply problem to be solved through diversification, recycling, or substitution. That framing understates what is at stake. The issue confronting Europe and its partners is not whether rare-earth dependence can be reduced at the margin, but how economic power is exercised in an era where interdependence has become a tool of statecraft.

The first question is how much dependence is tolerable. Strategic autonomy does not require eliminating exposure altogether. It requires ensuring that dependence cannot be turned into decisive leverage at critical moments. A shift from near total reliance on a single supplier to a more diversified but still imperfect supply base may be sufficient for deterrence and resilience. The challenge lies in deciding where that threshold lies and who bears the cost of crossing it.

The second question concerns whether Europe is politically willing to endure the time required to rebuild capacity. Reconstructing processing, refining, and magnet manufacturing takes years. Permitting is slow. Environmental opposition is real. Defence qualification cycles are long. During this transition, Europe remains exposed to external decisions taken in Washington and Beijing. Bridging this gap requires interim measures such as stockpiling, long-term contracts, and tighter political coordination. But it also requires accepting higher costs, revisiting environmental standards, and investing in projects that may never be commercially competitive under normal market conditions. These trade-offs are politically contentious. Yet refusing them does not shorten the timeline, it merely prolongs vulnerability.

The third question is leverage. The US can trade market access, financing, and security guarantees for alignment, as the 2025 Ukraine minerals agreement made clear. China wields influence through its dominance of refining and processing. Europe's instruments are weaker. Unless it develops credible leverage of its own, through market size, collective procurement, or strategic investment, it risks becoming a rule-taker in a contest increasingly defined by others.

Finally, there is the question of alignment. Europe's dependence is not only external but asymmetric. Reducing exposure to China often increases reliance on the US. That may be preferable, but it is not neutral. An economic security strategy shaped by "America First" priorities does not automatically align with European industrial interests. In Washington, secure supply chains and access to critical materials are now framed as matters of national security rather than shared economic policy. Navigating this landscape requires clearer choices about where autonomy is essential, where dependence is tolerable, and how alliance politics shape access in practice.

Rare earths are not an isolated vulnerability. They are a case study in how industrial capacity, trade policy, and security strategy have become inseparable. The era in which economic interdependence could be treated as a stabilising force insulated from geopolitics has ended.

Further reading

Ghiretti, F. and C. Ellis, 2026, *Old Priorities, New contexts: The Institutional Roots and New Developments of China's Rare Earth Policy*, RAND Europe.

Rossbach, N., 2023, *Sällsynta metaller och stormaktsrivalitet—En översikt om nya strategiska resurser och risken för råvarukonflikter*, FOI-R--5478--SE, Stockholm: Swedish Defence Research Agency (FOI).

Junerfält, T. and E. Wannheden, 2024, *Manufacturing Vulnerabilities: Chinese Minerals, Semiconductors and Green Technologies in the EU*, FOI-R--5524--SE, Stockholm: Swedish Defence Research Agency (FOI).

12. Security and disorder in the information environment of tomorrow

Sofia Olsson and Lisa Bergsten

You wake up and put your glasses on. Instantly, a woman with a friendly but generic face appears on your lenses and reads out today's headlines: "Interruptions continue after Monday's cyberattack. Biometric data stolen. The heatwave is here." You sit down for breakfast and glance through your messages, whilst the woman continues on to sports. The woman is there, as an ever-present shadow. As you focus on the woman again, she freezes and the picture starts to flicker. You have time to think "Oh no, not again" before a disturbing video of the fires raging in Central Europe appears on the lens. You can sense the smell of burnt skin as the camera sweeps over charred bodies, trees, and communities. You tear the glasses off whilst the words "ACT NOW!" appear. It's the third time this month that this has happened to you.

The war in Ukraine, the latest escalation between Israel and Hamas, and the war in Iran show us the importance of the information environment in today's armed conflicts and the challenges of framing and controlling the narrative in a highly contested and information-heavy arena. The information environment, consisting, among other things, of infrastructure, devices, data, content, networks, perceptions, beliefs, and decision-making, and divided into three layers, the physical, virtual, and cognitive, decreases the distance between the combat zone and the viewer at home.

Today's information environment is also a place for peacetime competition for truth, money, dominance, and influence. Legal restrictions on social media usage for children have been introduced in some countries and are discussed in many more. There is an ongoing European debate on how to handle our great dependence on primarily American-based tech companies and on how ownership of popular social media platforms and AI technology influences our society, geopolitics, and economies.

This article gives a glimpse of possible futures beyond 2030 by describing what the future information environment could look like through a general description of shaping factors and two scenarios. A recurring topic in discussions about the information environment is regulation, which is why it is a decisive factor in the scenarios.

The scenarios are somewhat extreme. This is intentional. The purpose is to expand the reader's perspective and create a basis for discussion about what to expect in the years ahead. Neither the description of the information environment nor the possible futures should be considered truths.

A GLIMPSE OF THE FUTURE

The future will be complex, immersive, and online. Internet access will be essential to everyday life. Devices with advanced wireless communication, as well as technologies such as virtual, augmented, and extended reality (VR, AR, XR), could be deeply integrated into daily life. These tendencies can already be seen today, with everything from sunglasses and clocks to fridges and toothbrushes being online. Handheld devices or wearable tech will still be the norm, as many want to be able to "choose" when they are online.

AI-powered digital assistants can be used on a larger scale in the workplace and assist with everything from administration to overcoming language barriers through simultaneous translation. The use of digital personal assistants in private life will most probably increase, with such assistants functioning rather like butlers and secretaries. They will do everything from scheduling family time and ordering dinner before you even realise you are hungry to scanning social media to curate the perfect feed based on your mood.

Access to energy and electricity will be vital to technological development and implementation, and the geopolitical and economic importance of it will accelerate. Countries with favourable conditions for hosting server halls and other electricity-consuming infrastructure are at an advantage. Debates about how limits to energy and electricity might hinder further R&D will continue, and may increase due to the consequences of global warming.

Overall, the future information environment will be increasingly crowded, fragmented, and contested. While this is true today, the main difference will be the scale. AI-generated content, being cheap, abundant, and convincing, enables both state and non-state actors alike to conduct influence activities at a low cost. A number of tools to assess authenticity, origin, and purpose will have been launched, tested, and rejected.

Manipulation of information with sophisticated techniques such as biometric imitation and microtargeted messaging will be easier and quickly disseminated with the help of autonomous AI and clusters of such agents. In an environment where it is very difficult to tell truth from lie, education in source criticism will be essential for people of all ages. The importance of the sender will increase, and eyewitnesses will be more highly valued, not least in crime investigations.

As individuals curate their own information ecosystems, the risk of personalised radicalisation is unlikely to go away and will lead to new, loosely connected net-

works built around emerging grievances and ideologies. It will be harder to gain and keep people's attention.

Human society will be highly affected. Still, people will adapt and learn to live with and act in this new digital environment. Strategies will differ between people and between states.

Scenarios

The following two scenarios present one future of an unrestricted information environment and one of a highly restricted information environment. Sweden is the illustrative case here however, many of the trends and factors are relevant for Europe as a whole.

A cocktail of anarchy, polarisation, and freedom?

In this scenario, the information environment in Sweden is loosely regulated. The fragmented control of the digital information environment has turned the country into a digital hub for innovation with multiple digital platforms and services, and a haven for both friendly and antagonistic non-state actors' activities in the information environment.

The information environment is still largely reliant on commercial giants owning the crucial underlying infrastructure and critical components. These actors have significant influence on society as they control access to systems, infrastructure, platforms, and people.

On the big platforms, hateful and polarising content is very potent, and tools for microtargeting are heavily used. Still, people use them due to habit and to keep in contact with people internationally. However, because of increased access to open-source code and help of AI, many homemade platforms are in use. Generally, digital innovation is rapid and creative.

Even though there are endless means of communication and sharing experiences with other people, loneliness is common, and having relations with digital assistants and realistic AI-pets ease the sense of alienation. There are ongoing discussions on the impact of this hyper-digital society on the population. A large part of the population only accesses information and news via its "filter bubble," that is, its platforms of choice.

Adversaries keep finding new ways to influence and harm society. The effects of the increasingly sophisticated cyber crimes are tangible. Attribution of these activities, with regard to who is behind them, is still complex and difficult. Due to the fragmented control of the information environment, there have been instances where crimes committed by violent extremist groups in other European countries have been coordinated and executed through the Swedish information envi-

ronment. However, this fragmented control is an advantage for actors who fight for human rights in controlled societies, as they also use Sweden as a base for digital mobilisation and to influence global opinion. Transnational self-organisation based on interest is growing, online and offline.

Control and security—Peace and quiet?

In this scenario, Sweden's information environment has been heavily regulated. This acceptance of infringement of personal integrity and other fundamental rights, such as freedom of expression, in exchange for a feeling of security goes hand in hand with a generally higher acceptance of surveillance, both digital and analogue.

Social media is banned for youngsters throughout the European Union, with screen time limits imposed on youths and recommended for adults. There is a limited range of social media platforms available in the Swedish information environment. Some have left voluntarily, others have been banned on the basis of being harmful to children or covert instruments of hostile foreign influence. Most digital services and social media are accessible only through various means of ID verification; their increased use has led to a growth in crimes of impersonation and increased the value of biometric data.

Some nations have adopted a state-owned super app. Such apps entail payment services and equivalents to social media, and are intended to carry the bulk of communication with government services. A majority of people in nation-states with super apps use them, and accept the infringement of personal integrity in exchange for a feeling of security.

A series of regulations gives the Swedish state access to data in private ownership. Since several large data servers are located on Swedish soil, some states try to put pressure on Sweden to share sensitive data about individuals.

Extremist groups increasingly organise offline and outside of cities in order to avoid surveillance. Their acts are conducted in the physical world and are often spectacular to attract attention. More people engage in civil and local society. Small communities of Analogues are being founded. They reject the digital world and advocate a pre-social-media society in which internet was used sparingly. Other communities find ways around the regulations with new versions of the Dark Web. Some find sanctuary in these unregulated and unsanctioned parts of the information environment, especially in less liberal states.

Balance, effect and total defence

The description of the information environment and the two scenarios highlight the importance of balance regarding regulation. Regulation of technology, behaviour, and content has to be balanced against fundamental rights such as freedom

of expression and personal integrity, as well as innovation and economic development fuelled by technological advances. This is a highly complex issue, where regulations that initially intend to do good may both end up doing harm and have no real effect on the actual problem they are meant to address.

Legislatively, it will be very difficult to keep up with rapid technological development and the possibilities and challenges it brings. This will complicate efforts to govern cyber operations, information manipulation, dual-use technologies, and crimes committed in the information environment using those and other new technologies. All of this poses challenges to trust and social cohesion in democratic societies like Sweden.

The development puts pressure on the whole of society. For the general population, it will be difficult to know how to navigate it: What is true and false, and what can be used without risking harm to myself or others? There is a need to consider what this hyper-digitalised world may mean in the long term for the population's health and society's development. Studies show that youths today struggle to control their usage of social media and that children who spend a significant amount of time on social media gradually develop inattention symptoms and have trouble focussing. What will be the effects on us after several decades in this environment?

At the same time, much of the technology we see today and tomorrow does us good. The information environment, AI content, and social media platforms are at their finest an endless source of knowledge and entertainment and a great way to connect with people, regardless of who we are and where we come from.

For Sweden's total defence, there is much to consider, including who and what to protect. In the "information war," there are new types of digital mercenaries, proxies, or volunteers that may collaborate with the adversary. The line between who is considered a legitimate target becomes muddier. The trends point to a continuation of the transparent battlefield, meaning that the information environment may become an increasingly contested area from a military point of view, including new means of deception through cyber and strategic communications. Protecting citizens against adversaries who attempt to influence us will require an understanding of one's own vulnerabilities, both cognitive and communicative. It will take a whole-of-society effort, nationally and at a European level, to mitigate the consequences of these attempted attacks, and wise regulation to ensure that the balance between safety, protection, and freedom is upheld.

Further reading

Bergsten, Lisa and Olsson, Sofia, 2024, Framtidens informationsmiljö och icke-statliga aktörer, FOI Memo 8569.

Nilsson, Per-Erik and Hellström, Kristina, 2025, *All Eyes on Ukraine: Strategic Communication in the Russo–Ukrainian War, 2023–2024*, FOI-R--5758--SE, Stockholm: Swedish Defence Research Agency (FOI).

Nilsson, Per-Erik, Olsson, Sofia and Ekman, Ivar, 2022, *Den nya informationsmiljöns topografi—Teknik, människa och strategi i osäkerhetens tidevarv*, FOI-R--5342--SE, Stockholm: Swedish Defence Research Agency (FOI).

13. Sweden's defence against hybrid threats

Alicia Fjällhed, Ola Svenonius and Magnus Normark

Hybrid threats are a reflection of the new world order, in which subversive activities are conducted by a foreign power below the threshold of armed conflict in order to promote its strategic objectives. This chapter summarises the main points of a FOI report, published in 2026, which presents a definition and model for understanding hybrid threats in a Swedish context, as well as a toolbox containing four types of tools Swedish society that can use to help deter, detect, and counter hybrid threats. The aim of this initiative is to place the Centre of Excellence for Countering Hybrid Threats' (Hybrid CoE) CORE-model within the context of Sweden's total defence. By doing so, the chapter seeks to explain the Swedish approach and contribute to an international conversation on national perspectives on hybrid threats.

Russia's conduct during its illegal annexation of Crimea in 2014 challenged conventional understandings of warfare. It gave rise to a still ongoing discussion about hybrid threats, as a cluster of activities not necessarily carried out by military organisations or aimed at military targets. Since 2014, the list of activities branded as hybrid threats has grown. Today, it includes everything from tampering with underwater infrastructure to disinformation. These types of activities are presumed to continue to shape the world around us and influence geopolitics and national security for the foreseeable future.

Discussions around these activities are challenged by the various definitions of concepts and by the wide range of concepts applied. The epithet "hybrid" alone has given rise to variations such as hybrid threats, hybrid operations, hybrid activities, hybrid attacks, hybrid war, hybrid means, and hybrid situations. It is also presented alongside concepts such as asymmetrical or irregular warfare. The conceptual confusion arising within discourses in which these concepts are used leads to uncertainties, such as what activities nations seek to deter, how they can be detected, and what actions can be taken to counter them.

Aiming to clarify the meaning of hybrid threats, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki, Finland, has presented the CORE model. This international stance, however, needs to be adapted to national contexts, so that it fits each country's societal system and the threats it currently faces. In 2020, FOI presented its first toolbox for actors in Sweden seeking to address hybrid threats. This chapter outlines the core message of an updated version of that report, which proposes a Swedish definition of

hybrid threats, presents the CORE-SE model as an adaptation of Hybrid CoE's model, and introduces a toolbox for Swedish actors to use in detecting, deterring, and countering hybrid threats.

Towards a common understanding

Although there is no agreed definition of hybrid threats, there are elements that often recur as criteria used to identify the phenomenon. We propose a definition of hybrid threats based on four criteria. In short, hybrid threats are subversive activities conducted by a foreign power below the threshold of armed conflict in order to promote its strategic objectives. This definition also clarifies what does not constitute a hybrid threat. Actions that do not threaten states are not hybrid threats and activities at war are understood as hybrid warfare rather than hybrid threats. In this framework, only actions that meet all four criteria can be categorised as hybrid threats.

First, hybrid threats are in part defined by their consequences, more specifically by being politically subversive. They seek to undermine societal cohesion and to weaken the democratic state. Activities range from overt breaches of national airspace by military forces to covert actions that seek to influence state sovereignty and the people's democratic influence. Individuals may be targets through personal threats, or organisations through actions such as espionage and sabotage, to name but a few examples. Among the most common today are cyber operations whereby actors, for example, unlawfully obtain information covertly, or overtly engage in blackmail.

Secondly, while subversive activities may include actions by military organisations, hybrid threats occur below the threshold of armed conflict. This is, however, a fragile line, as actors design hybrid attacks to ensure that the threshold is not passed whilst also strategically seeking to bend it. In response, NATO stated in 2016 that hybrid threats could invoke Article 5 of the North Atlantic Treaty.

Thirdly, hybrid threats are conducted by foreign powers. Domestic crime, while subversive in nature, thus does not constitute a hybrid threat. Foreign powers can, however, use domestic actors and thereby conduct hybrid threats through these proxy actors.

Finally, foreign powers use hybrid threats to achieve strategic objectives. This is in part linked to their subversive nature, but it also points to the interests driving these activities and to the need to understand how multiple activities can be defined as coordinated and synchronised. Hybrid threats could, for example, aim to harm a country, or influence decision-making in relation to domestic and international politics. Hybrid threats can also serve purposes such as benefiting the attacking country's own population and interests at the expense of the target country's interests.

A Swedish Total Defence perspective

The general character of Hybrid CoE's CORE model is good for fostering a common international understanding of hybrid threats as a whole-of-society concern. There is a need, however, to adapt it to a national context.

Sweden's management of hybrid threats rests within the Swedish total defence concept. The concept is based on military and civil capabilities to deter, detect, and counter foreign attacks, including hybrid threats. The civil and military defence share common objectives for the defence of Sweden, but are also governed by objectives that specify how they should interact, support, and protect each other. The structures, set in place during peacetime, can be quickly activated when needed. These structures can also be used to manage hybrid threats.

The Swedish structures, as described above, fit well within the core model, with some modifications. To capture a Swedish perspective in relation to Hybrid CoE's framework, a national adaptation, the CORE-SE model, is proposed here (Figure 1). Like the original CORE-model, this Swedish version can be used as a diagnostic tool and as a planning device for countermeasures.

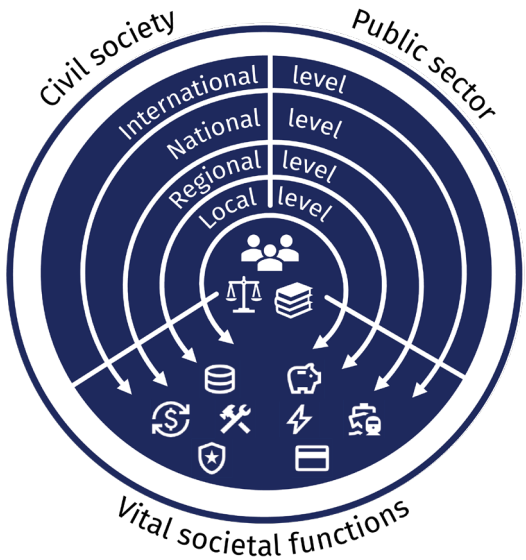

Figure 1. The CORE-SE model

While keeping the CORE model's focus on core values and three fundamental spaces divided into geographical levels, some adjustments have been made to align it with the Swedish context. First, Swedish civil society and the public sector are specified by a set of Sweden's international, national, regional, and local actors. Civil society includes organisations such as religious communities, voluntary organisations, trade unions as well as sports and cultural associations. The public sector includes both military and civil organisations, such as municipali-

ties, agencies, and state-level departments. The services space is presented without geographical layers, rather accentuating the emergency service sectors, which have come to shape Swedish society's "vital societal functions" as defined in the total defence system. This list of vital societal functions is under continuous revision, in which private-sector organisations play an important role across a variety of businesses.

A TWO-DIMENSIONAL TOOLBOX

All actors within the total defence system have an opportunity to support Sweden's defence by deterring, detecting, and countering hybrid threats. To support actors in these endeavours, the final part of the Swedish framework includes a toolbox of countermeasures. As hybrid threats may be diverse and often covert in character, it is vital that the whole of society is engaged in understanding the threat landscape, to help identify cases and alert those authorities that are able to see connections between cases and assess the situation on a national level.

The toolbox encourages actors to look at two dimensions of tools, which together form four strategic approaches. On the one hand, actors may consider reactive tools once a threat has materialised, or proactive ones before an event occurs. On the other hand, actors have the option to act defensively to mitigate harm to themselves, or act offensively to target the attacker (Figure 2).

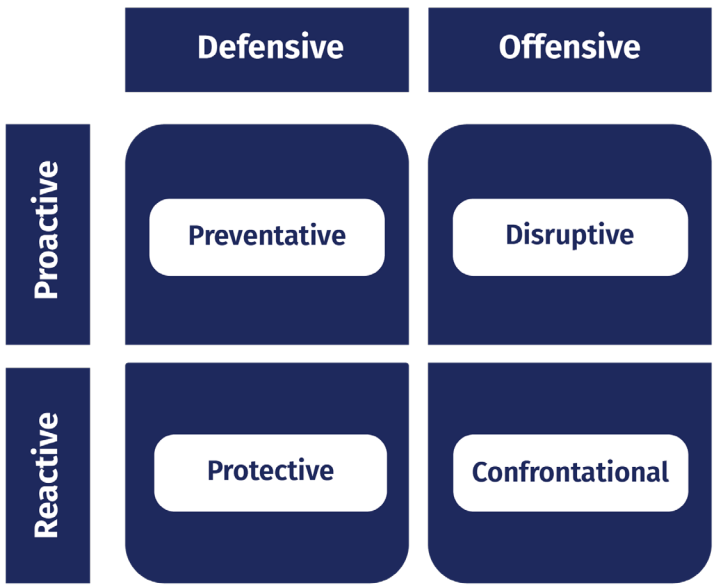

Figure 2. Toolbox

Together, these two dimensions create four strategic approaches to hybrid threats. A proactive defensive approach would, for example, be to include hybrid threats in one's threat and vulnerability assessment as a preventative strategy. In turn, this could motivate proactively offensive tools, such as restricting foreign powers' economic influence through new laws and other disruptive measures.

Another proactive defensive tool is the establishment of alert systems through which weak or early signals of an attack can be detected and shared within a broader community of organisations, contributing to shared situational awareness. This could be combined with reactive tools, such as to defensively counter false information to protect society from hybrid threats or through confrontational strategies offensively attribute the actors behind the very same operation and.

From threats to attacks and warfare

In the past decades, Sweden has started to rebuild its total defence. This is a process occurring in parallel with the increasing risk of hybrid threats, as well as observed hybrid attacks directed at Sweden. The definition, model, and toolbox introduced in this chapter, and expanded upon in the report, are intended to support the nation's collective efforts to deter, detect, and defend Sweden against hybrid threats. We also hope that the description of a national perspective inspire other countries to engage in similar adaptations of international models, as a way to aid international conversations and collaborations.

Given the current state of the world, there is also a need for the Swedish system to take the scenario of armed conflict into account. This includes how hybrid threats fit into the equation, both during a build-up to a war and in the form of hybrid warfare. At the same time, the very concept of hybrid threats challenges us to think outside traditional vocabularies, in order to be able to formulate concepts and practices of strategic importance to help us understand and operate in relation to the new world order.

Further reading

Svenonius, O., M. Normark, A. Fjällhed, and M. Ingeson, forthcoming, *Strategisk verktygslåda för hantering av hybrida hot*.

Appelgren, J., S. Bay, J. Malminen, and E. Zouave, 2020, *Strategisk verktygslåda mot hybridhot: Ett ramverk för gemensam problemförståelse*, FOI-R--4816--SE, Stockholm: Swedish Defence Research Agency (FOI).

Jungwirth R., H. Smith, E. Willkomm, J. Savolainen, M. Alonso Villota, M. Lebrun, A. Aho, G. Giannopoulos, 2023, Hybrid threats: A comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, doi: 10.2760/37899, JRC129019.

14. Open Data—Opportunity or Risk?

Mathias Winterdahl, Åsa Davidsson, Eva Mittermaier and Ulf Söderman

The functionality of today's society is dependent on large amounts of digital data. The prevailing view in the West has therefore been that public data should be open and freely available to promote transparency, innovation, and scientific progress. However, recent geopolitical developments have shifted political priorities, raising concerns about national security and civil preparedness. Particularly in the EU, decision-makers are increasingly determined to augment strategic autonomy and digital governance as a way of achieving digital sovereignty. Simultaneously, they push for more open data in an effort to boost European digital innovation. However, whereas open data can support societal development and economic growth, indiscriminate openness and transparency may endanger national security. By sharing open data, states risk providing adversaries with sensitive information required to reach their goals.

Digital Transformation, Open Data and Geopolitics

During the past decades, society has undergone an unprecedented shift in economic and social relations driven by the digital transformation. Today, digital resources and services play a central role in society. Economic transactions, social interactions, and public services are increasingly taking place in the digital sphere, while digitisation continues to extend into new areas of everyday life. For both private and public organisations, the digital transformation provides benefits such as more efficient management and operation as well as improved competitiveness.

A key driver of the digital transformation is the ability to collect, communicate, and analyse large amounts of data. Since the end of the Cold War, Western countries have aimed to increase the amount of open data. Behind this ambition is the realisation that there are several benefits of open data. Scientific research is often dependent on the availability of large amounts of open data, and the development of new products and services also benefits from open data. Open data is commonly claimed to be a key resource for technological advancements, such as artificial intelligence (AI).

Simultaneously, in the past decade, the world has become increasingly dominated by geopolitical competition among great military and economic powers, a trend also influencing open data. It is now considered a strategic resource used for, among other things, intelligence gathering and technology development. Open data is used by current AI models for training and may also be essential for future technologies, such as the anticipated and potentially revolutionary artifi-

cial general intelligence (AGI). Whoever wins the AI race is expected to occupy a dominant military, political, and economic position globally.

From a national security perspective, perhaps the largest potential short-term risk is that AI can be used to extract sensitive information from open data. For example, it is already possible to use AI to identify retouched areas in aerial images, and thereby, through reverse deduction, identify locations of importance to national defence. Other potential antagonistic uses of AI include the production of fake data presented as true open data.

Another technology with potential geopolitical implications that can benefit from the availability of open data is the development of unmanned systems. Open geospatial data can enhance the performance of autonomous platforms, including self-driving vehicles and unmanned aerial vehicles (UAVs), commonly referred to as drones. In a military context, such data may enable UAVs to navigate in complex environments, such as forests or urban areas, making them more difficult to detect and counter. Given their relatively low cost, similar systems could also be used against civilian targets in grey-zone scenarios or in terrorist attacks. For example, an adversary could use open data to coordinate large numbers of UAVs navigating autonomously through cities to target polling stations during democratic elections.

The development of open data has forced states, particularly in Europe, to reconsider their priorities. From a policy perspective, the European Union (EU) emphasises the importance of data in the digital economy and has taken action to increase its availability and use. With the introduction of the Open Data Directive in 2019, the EU encourages publication of publicly funded data as open data, that is, data in open formats that can be used, re-used, and shared freely by anyone for any purpose, with the explicit aim of promoting digital innovation and a data-driven economy in Europe. In addition, it highlights open data as a means of strengthening democracy, improving transparency, and enabling scientific breakthroughs.

Overall, geopolitical and technological developments present us with a dilemma between openness and protection. Sharing data freely and openly does benefit European businesses and research, but it can also provide adversaries with useful and sensitive information as well as competitive advantages. This dilemma has gained little attention in public debate, particularly at the national level. Emerging research, however, points to linkages between open data and national security concerns, an issue explored further in this chapter.

Public Organisations and Open Data

Public organisations are central actors in this dilemma. They need to balance the political and economic demands for publishing open data against national security. The EU Open Data Directive focuses on public organisations' legal obliga-

tions to share data openly and freely. Simultaneously, these public organisations need to consider national security. The Swedish Open Data Act states that public data should only be released as open data as long as it does not pose risks to national security.

However, it is unknown how to estimate such risks when publishing open data. Both identification and assessment of risks are particularly difficult due to the general lack of documented experiences, examples, and guidelines. Knowledge about adversaries' use of data is usually restricted to national intelligence agencies, which are generally unwilling to share such information.

Risk assessments are essential for managing threats to national security. Public organisations, however, may struggle to translate such threats into concrete considerations when deciding whether to publish data openly. Should actions of an adversary influence government agencies' decisions to release property data? Should municipalities planning to publish school data consider threats of terrorism? While most organisations are accustomed to conducting risk assessments, these typically focus on risks to their own operations rather than on the security of the state as a whole.

The following section presents four perspectives on how open data can pose a risk to national security. These four perspectives can guide public actors when performing risk assessments concerning open data.

Four Perspectives to Consider

There are at least four perspectives on how open data can lead to or increase risks to national security. Firstly, if open data provides adversaries with information that is useful for achieving their goals, it may pose a risk to national security. It can be, for instance, information about the location, function, capability or preparedness of certain facilities, organisations, units or persons of importance to national security. This includes, among other things, critical infrastructure for provision of energy, water, and food; national defence forces and law enforcement agencies; and political leaders, high-ranking officers, and key military personnel. Therefore, the usefulness and relevance of the information for achieving adversaries' antagonistic goals influence the risks.

Secondly, the uniqueness of the data also influences the risk. If there are alternative sources of open data or information, the risks associated with national agencies publishing open data may be less severe if alternatives already exist. For instance, if there are services providing easily accessible satellite images of a certain location, official agencies releasing aerial images as open data may not increase risks to national security if the information is already publicly available. However, this is only true as long as there are no differences in, for example, resolution, accuracy, and informational content. Also, assessing differences between datasets is

far from trivial; even small differences in data can expose new relevant, and potentially sensitive, information.

Thirdly, publication of open data may be detrimental for national security if adversaries save considerable resources, or if the risks they need to take to acquire the information are reduced substantially. In the absence of open data, the adversary may have to spend considerable resources or take substantial risks to be able to acquire the data needed. It can be assumed that a highly determined adversary with resources at their disposal will be able to acquire much of the desired data, even if it is not shared openly and freely. This can be accomplished through, for instance, cyberattacks, human intelligence, or the collection of new data with the help of various technological platforms. However, this usually forces the adversary to spend resources, such as money, time, and personnel, and risk being detected and stopped by the targets' security and intelligence agencies, or being subjected to various forms of punishment or retaliation.

Fourthly, and perhaps most challenging to assess, is the possibility of gaining new information by combining data. Compilation of data and information, that is, the combination of several datasets or pieces of information, either over time or from different sources, is an especially incalculable and complex security issue. A certain dataset may seem harmless in isolation but could lead to the exposure of sensitive information when combined with other data or information. In other words, combining different data and pieces of information may allow the extraction of information that is not evident from the individual datasets or information sources. This risk will likely be exacerbated in the near future due to the proliferation of AI tools that simplify data compilation and combination of various sources of information.

In summary, organisations need considerable knowledge about, for instance, security-sensitive activities at the national level; what information can be assumed to be sensitive and, thus, worth protecting; and the strategic goals of adversaries to be able to fully consider the risks that open data poses to national security.

Final Notes

To conclude, there are both opportunities and risks associated with open data, but whereas the opportunities are well-known, the awareness of the risks associated with open data is still low and needs to increase. Only by recognising the national security risks associated with open data, which may fluctuate and change with geopolitical trends, can society effectively deter and counter its exploitation by adversaries.

Decision-makers also need to ensure that they do not restrict access to data more than necessary to guarantee national security. As one example, in a world increasingly influenced by disinformation and false claims, democratic societies need to ensure transparency and the dissemination of relevant information. In this con-

text, AI and its future development are particularly relevant. AI tools will likely further exacerbate the problem of disinformation, while they may also be used to detect and counteract it. Open data is an essential tool for countering false claims and disinformation. Societies need to balance necessary restrictions on access to data, in order to limit the exposure of sensitive information, with open and free access to data in order to uphold fundamental rights in democracies.

Further reading

Davidsson, Å., Mittermaier, E., Severin, M., Söderman, U., Winterdahl, M., Ciepielewska, M., and Stjernlöf, S., 2025, *Riskbedömning av geodata vid tillgängliggörande som öppna data*, FOI-R--5745--SE, Stockholm: Swedish Defence Research Agency (FOI).

Davidsson, Å. and Stagnell, A., forthcoming, *Att märka ut vår mest värdefulla tillgång: Nationell säkerhet i tre EU-länders arbete med tillgängliggörandet av geodata som öppna data*.

Nikander, J., Jama, T., and Tenkanen, H., 2024, Threats Related to Open Geospatial Data in the Uncertain Geopolitical Environment, *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, XLVIII-4/W12-2024, p. 121–126, doi: 10.5194/isprs-archives-XLVIII-4-W12-2024-121-2024.

15. Prepare for the War of Warehouses!

Ann Lundberg & Maria Hultqvist

Production capacity has become a significant factor in the war in Ukraine. The war is described as a "war of warehouses," highlighting that the ability to defeat an enemy depends not only on military strategy but also on industrial resilience. Several initiatives aimed at expanding and coordinating production capacity have been introduced in multilateral frameworks such as NATO and the EU, as well as in the individual Member States. Among these initiatives, one theme stands out: collaboration. Collaboration between governments, industries, and international institutions is frequently presented as essential for scaling up European production capacity. This raises an important question: What form of collaboration is actually feasible in the kind of market in which defence production operates?

Introduction

Russia's ongoing war against Ukraine has reinforced a well-known lesson; wars are not only won on the battlefield, but in factories and warehouses. In the war between Russia and Ukraine ammunition stocks and supply chains have become decisive for sustaining the fight.

Support for Ukraine, along with the new ambition of the EU's ReArm Europe package, has forced Europe to face the consequences of decades of slashed defence budgets and deprioritised inventories. This has highlighted the importance of the defence industry and its capacity to produce. The war in Ukraine is described as a "war of warehouses" and the question is not only who fights best today, but who can sustain the fight tomorrow.

Several political measures have been launched to increase production capacity and the speed of innovation. In response to the war in Ukraine and increasing transatlantic turmoil, discussions of Europe's own production capacity have emerged. The dependence on American equipment is problematic, both from a burden-sharing perspective and from a European strategic autonomy standpoint. Collaboration among allies to rebuild stock levels and increase European autonomy, has been initiated. Collaboration is often seen as a remedy for most problems associated with defence issues. Collaboration between governments, industries, and international institutions is also frequently presented as essential for scaling up European production capacity. The way the defence market works does not, however, provide an ideal setting for collaboration in general. As Europe seeks to strengthen its industrial base, the question arises of how collaboration among European states can best be shaped without being bound by the obstacles that have previously limited multinational collaboration. What forms of collabora-

tion would be feasible for increasing production capacity in the ongoing rearmament of Europe?

This article takes the defence market as its starting point for a discussion of the conditions for collaboration to strengthen production capacity and the measures NATO and Europe should consider in order to enable a rapid scale-up of production.

The defence market

Security and defence policies influence the market

The defence market has some unique features, as it is subject to security and defence policy considerations because the customer is typically a state. The security and defence policy aspects often manifest themselves through regulations, restrictions, and special agreements between important domestic defence companies and the state. In states with large primary contractors, a strong interdependence often develops between defence companies and the state.

The existence of a domestic defence industry is often the result of deliberate decisions by the state, whether for reasons of autonomy, easier access to equipment, or specific needs. The equipment that is needed also depends on geographical conditions, doctrine, the size of the military forces, and political ambitions. This could, in turn, be connected to historical decisions. As a result, the defence market is home to various similar, but not homogeneous, products. It is often described as fragmented. In economics, the defence market would be characterised by monopolistic competition.

Security and defence policies pose challenges for collaboration

In this setting, where both states and, especially, their domestic companies are invested in each other, international collaboration becomes complicated. Sharing of knowledge and technological know-how could mean surrendering unique competitive advantages for companies and states as well as giving up national employment opportunities. Still, collaboration is seen as a general go-to measure that is encouraged in multilateral contexts like NATO and the EU. Even individual Member States refer to collaboration as a way to gain or maintain competences in the defence industry, and to enable efficient procurement.

The complexity described above poses challenges for most forms of collaboration and, although collaboration is often referred to as a cost-saving remedy, it is not guaranteed to succeed. Instead, success seems case-dependent and therefore not generalisable. Some of the initiatives taken by the EU seek to restructure the defence market and incentivise Member States to procure standardised EU equipment. But common EU equipment only makes sense if all the Member States share political ambitions, doctrine, and geographical conditions. This is not, however, the case.

Production and production capacity

Increasing production and expanding production capacity could be achieved through many different measures. The measures and their effects depend on what the production function looks like and what mechanisms could be activated to increase productivity. In some cases, increased demand could motivate automation or another plant or the introduction of multiple work shifts, but in other cases the increase in demand is not enough to motivate or enable certain measures. Production capacity for wartime is also, to some extent, a future-oriented goal. It takes time for a plant or company to increase production. Some measures, therefore, would have to be pre-emptive, creating the necessary conditions for swift and sufficient production long before it is needed.

Collaboration aimed at enabling greater production capacity will of course also be associated with challenges, given the complexity of international arms collaboration in general. With this in mind, what forms of collaboration would be feasible for increasing production capacity in the ongoing rearmament of Europe? Below, we outline some possible approaches from the perspective of the lowest common denominator and the path of least resistance.

Collaboration in a Multidimensional Demand Setting

If collaboration is challenging because of different needs, the easiest way forward is not to try to change those needs head-on. Instead, it makes more sense to work with and around those needs.

Bottom-up approach

If the end user is not prepared to change requirements, then what about the requirements for components further down the supply chain? Primary contractors, and if needed, countries would need to agree on certain standards when it comes to components. Certain components could perhaps be the same, regardless of whether, for example, the battle tank is assembled in France, the UK, or Germany. Would it be possible to use the same type of tracks or tracks with the same width? The important thing is that companies and countries can meet the specific equipment requirements of each country while components are produced en masse, thereby enabling faster production and longer production runs for subcontractors. This approach could of course affect certain subcontractors if the measure leads to consolidation, and it would probably be easier to implement it the further down the supply chain you go. It would also be easier the more similar the component is to an equivalent civilian component.

A variant of the bottom-up approach would be that subcontractors with similar products are involved in the production of multiple top-tier equipment. In that way, the subcontractor could hopefully use longer production runs combined with small variations to increase production.

Regional needs approach

It seems unlikely that all European countries or NATO allies would agree on common equipment across the board. But it might be possible for a limited set of countries to agree on equipment that is similar enough. Within NATO, for example, some countries share similar geographic conditions. In the Arctic region, countries such as Finland, Norway, Sweden, and Canada have prepared to operate in Arctic conditions. They are therefore likely to have similar requirements for equipment adapted to Arctic conditions. That doesn't mean they want exactly the same things, as there might be differences in political and doctrinal views. However, there is a higher chance of reaching some common ground on how the equipment should be designed while still allowing room for minor adjustments. If a producer could limit the number of variants, and thereby simplify the production process, much would be achieved. It would perhaps allow for standardisation in some parts of the production line, which in turn might enable automation, depending on volume, and productivity increases arising from learning curves. The limited set of variants would then also be available for procurement by other countries, if needed in a NATO context.

Joint ownership approach

As stated above, countries sometimes have difficulties in agreeing on where production should take place. Collaborations often entail demands for *juste retour* and work share. Even procurement agreements could include elements of licensed manufacturing and maintenance. These demands originate from concepts such as security of supply and autonomy. The implication is that production resources are spread across countries, which could be both an advantage for production ramp-up and a disadvantage for efficient manufacturing. A way around this situation is to allow for multilateral ownership of production resources that are needed for the manufacture of equipment necessary for multiple countries. If the equipment could be produced in large jointly owned plants, more efficient production would be possible. If the concern is that a crisis or war would impair the ability to access equipment, then jointly owned production resources would at least improve the accessibility for individual countries.

Future-capability approach

Joint, and perhaps multilateral collaborations might have a greater chance of success if they take place in areas where no country possesses its own capability, and no national industry or production lines currently exist. In such cases, collaboration would not include tearing down existing industry structures, but rather building new ones collectively from scratch. By co-developing new equipment, emerging technologies, or next-generation systems together, states can develop new capability without undermining established national industries.

Concluding Remarks

The approaches outlined above are not easily implemented, nor will they fully resolve the challenges associated with international arms collaborations or the scaling of production within the EU. Rather, the proposed approaches are archetypical strategies for working around locked-in security interests in arms production, under the assumption that country-specific needs cannot be fully harmonised.

But the real issue might be simpler. There is to some extent a choice: scale or differentiation. We cannot have both. A war of warehouses leaves no room for products with different requirements and standards. It demands mass and standardisation to achieve speed. The EU consists of 27 individual Member States with sometimes competing security interests of their own. In collaboration, there is a risk that 1+1=1. In the defence market, that means someone must relinquish autonomy, influence, capacity, or competence, and in doing so also trust another country, or countries, to provide the necessary equipment and competence. Even if this is already the situation for most countries, at least in some areas, giving up more autonomy, or the perception of it, is still politically difficult.

Collaboration to enable the swift production of the defence equipment needed today is necessary. However, it is not enough to tackle the full extent of the challenge facing European countries. To facilitate the development of relevant defence equipment in the future, collaboration must also allow for speedy innovation. Another dilemma for Europe to solve together is the balance between new and old equipment, especially when it comes to what could be stored and still stand the test of time, and what must be produced in the heat of the moment to provide the desired capability.

For Europe, or more specifically, the EU Member States, it is now the moment of truth. Are the Russian threat and the sense of urgency enough to give up earlier national positions, take the leap of faith required to deepen collaboration, agree on common standards, and increase production capacity together, or will the door be closed no matter what?

Further reading

Andersson, J.J., 2023, *Buying Weapons Together (or Not). Joint Defence Acquisition and Parallel Arms Procurement,* Brief 7, April, European Institute for Security Studies.

Lundberg, A., 2025, Where to, EDF?, FOI Memo 9000, Stockholm: Swedish Defence Research Agency (FOI).

Lundberg, A., Hultqvist, M. and Häggbom, G., forthcoming report on production capacity.

Part Three
Military and Technology

16. Russian Electronic Warfare in Ukraine—A Key Area in Preparedness for Future Conflicts

Hampus Thorell

The war in Ukraine has had a huge impact on modern electronic warfare (EW) in ways few nations were prepared for or could foresee. The rapid development of technology related to electronic warfare and the use of drones is now redefining many defence forces around the world. The aggressor, Russia, has for the last 20 years focused on developing and integrating electronic warfare as a key component of its armed forces. From day one of the full-scale invasion, EW has been extensively used in the war in Ukraine. As the war progresses, Russia is continuously adapting its electronic warfare capability as well as its technology to the current situation, and its forces are gaining a great deal of new knowledge from the war, which most likely will be used in future conflicts. For the West to keep up with Russia, it is important to understand the current situation, draw conclusions from it, and conduct realistic exercises under similar conditions. Such work is of vital importance for the future defence against Russia.

A prioritized capability for Russia

In modern times, the Russian armed forces have long been known for possessing a very strong electronic warfare capability, especially within the ground forces. Lessons from conflicts in Chechnya and Georgia led to doctrinal changes in Russian warfare in the early 2000s as well as substantial investments in new and updated electronic warfare complexes.

The results of developments in Russian EW were especially noted in the West during the period after Russia's illegal annexation of Crimea in 2014 and its participation in the war in Syria in 2015. There were many reports of Russia using Ukraine as a proving ground for its most modern electronic warfare systems. In western Ukraine, numerous newly developed and adopted systems from around 2010 were used to locate and disrupt Ukraine's communications. In Syria, the US drew similar conclusions; both navigation systems and radars were affected. Some of the first reports of Russia using the heavy Krasukha-4 complex, capable of jamming many of these systems, originated from this conflict.

In recent years, the number of occasions on which Russia has practiced its EW capabilities in the Baltic Sea region has increased. These incidents involve disrupting GNSS (Global Navigation Satellite Systems), regardless of the impact on security and civilian society.

Attention to Russia's EW capabilities in recent years has led to a greater focus in the West on developing EW capabilities and robustness against their use. As an example, the US launched its major EW programme, Multi-Functional Electronic Warfare (MFEW), largely in response to this. This was primarily the result of US forces training Ukrainian soldiers and then witnessing Russian EW capabilities being used against them, which led to the realisation that these were capabilities the US lacked at the time. Despite a bigger focus on EW, there was not really much progress among the forces of the West in matching Russian EW capabilities, especially in Europe, before 2022, when Russia initiated its full-scale attack on Ukraine.

Extensive use of EW capabilities in the full-scale invasion of Ukraine

Russia's invasion of Ukraine involved many of its most modern electronic warfare complexes, including many of the subsystems comprising the Borisoglebsk-2 complex, a system capable of geolocation and radio-jamming, as well as the heavy GNSS jammer R-330Zh Zhitel. Since the Russian Armed Forces were poorly prepared for the war, however, many of their large EW complexes were either lost or destroyed, especially during the initial stages of the war. This could, for instance, be monitored through the Oryx and Warspotting websites. These websites use open-source intelligence to document both Russian and Ukrainian losses, for which photographic or videographic evidence is available. According to Oryx, almost 100 Russian EW systems were either destroyed or captured before 2026. Similar numbers can also be found on Warspotting. Many of the destroyed or lost systems were large and complex installations on trucks or armoured personal carriers and involved high costs as well as long lead time to replace.

There are no official statistics stating the number of EW systems the Russian forces have lost compared to their total number of EW systems; however, the systems are not likely to be so easily replaced, partly because the origin of the components from which they were designed now makes them harder to procure. There have been numerous reports of captured Russian trophy systems that have been exploited in order to discover and evaluate the systems' capabilities and weaknesses, as well as to map the origins of their components. Summaries of sanctioned components in Russian systems can be found, for example, on websites such as War Sanctions. According to analyses of some of the subsystems of Borisoglebsk-2, many of the key components originated from the US, Europe, South Korea, and Taiwan. This is not unique to Borisoglebsk-2; rather, it is common that most of the critical components in Russian EW systems, as well as other weapons and sensors, are designed with high-performance components developed almost entirely in the US. These components are typically analog/digital converters, FPGAs (Field Programmable Gate Arrays), or GPUs (Graphical Processing Units). These are components that in many ways define the performance of the systems.

Continued sanctions on Russia targeting key components should in theory cripple its ability to produce more advanced EW systems. However, it has become obvious that the sanctions do not work one hundred per cent, and many components still find new ways to slip through to Russia. It is also likely that China will emerge as a new supplier of advanced technology in the near future. China has already made major technological breakthroughs in artificial intelligence that points to a growing capability. There are also many reports of Russia using Chinese systems on the battlefield, such as Chinese battlefield radios as well as Chinese mesh radios and CRPA (Controlled Reception Pattern Antennas) in the Shahed drones. Also, many of the new Russian EW systems are designed with cheap Chinese technology, such as signal generators and power amplifiers. The share of Chinese technology in the Russian military is continuously increasing. It is likely that the Russia–China ties will render future sanctions less effective and reduce dependence on the West.

The crucial impact of electromagnetic spectrum limitations

While electronic warfare against radars and communication systems has played, and still plays, a key role in the war in Ukraine, the major drive for the development of electronic warfare has been the detection and mitigation of unmanned systems, mostly UAS (Unmanned Aerial Systems), also known as drones. The threat from drones has had a major impact on the overall course of the war, and according to many sources, around 80 per cent of all casualties in the war result from drone attacks. Using electronic warfare to detect and jam both control and video links, as well as the navigational systems of the platforms, initially proved highly effective. Both sides of the conflict soon understood the potential of using drones and the need to protect against them. This has led to the development and deployment of a huge number of different EW systems designed primarily to detect and jam drones. These systems have, however, evolved rapidly during the war. In the early stages, the EW systems used to protect against drones were usually designed only for typical drone frequency bands. Soon, both sides started to shift the frequencies of the control links of the drones to more unconventional frequencies in order to mitigate the jammed frequencies. This shift made many EW systems that were designed to only cover a few frequency bands useless, some of them were even at the stage where they had been procured but not yet deployed when the shift occurred. This continuous EW cat-and-mouse game has continued to accelerate throughout the war, and in the current situation there are few frequencies on which drones are not being controlled, and few frequencies that are not affected by jamming.

To cover the vast frontline, huge numbers of EW systems have been deployed. The development of this type of warfare has led to a frontline consisting of millions of soldiers using wireless communication, jammers, and radars that in turn create an immensely congested spectrum.

The war in Ukraine has proven that in a modern conflict the electromagnetic spectrum will be important as well as complex. There will be a combination of military communication, radars, and jammers, as well as civilian telecommunication populating large portions of the spectrum that somehow need to coexist. The West has not been prepared for such a spectrum, nor has it trained under such conditions. Instead, the rules regulating spectrum usage in the West are usually highly rigorous and limit the possibilities for training in a realistic way. Usually only certain frequency bands are used for military communication, while the rest are used for civilian or commercial purposes. The military frequency allocations are usually not sufficient to apply electronic warfare protection techniques, such as frequency hopping, wide signal bandwidths, or other agile or cognitive behaviours. The introduction of systems into armed forces is therefore often carried out using only a few frequencies or small frequency bands in order not to collide with other systems. This makes the systems both easier for an adversary to detect and jam. The use of military frequencies has led to the procurement of many radio systems that work in only a few specific frequency bands rather than across the entire electromagnetic spectrum. The need to consider more agile spectrum usage and training armed forces in situations similar to the one in Ukraine should therefore be prioritised by the West in the planning for future conflicts.

The congested spectrum on the battlefield also creates major technical challenges when developing and implementing EW systems, especially for COMINT (Communications Intelligence) and DF (Direction Finding). The trend among these types of systems is to incorporate more wideband radio receivers in order to cover the entire spectrum instantaneously. The dense spectrum leads to a risk of making these systems more susceptible to high levels of electromagnetic energy. In turn, this may result in saturated receivers and false results. To find signals of interest in a clutter of noise can be a big challenge for EW personnel operating these systems. To handle this situation, the operators of the systems require a lot of training in relevant scenarios.

EW SYSTEMS EVOLUTION

The reason for the destruction or capture of many of the Russian EW systems is a combination of their being considered high-value targets, that they are very stationary during operations and that they tend to have unique visual signatures. As a result, there has been a shift from using mostly large EW complexes to smaller distributed types of systems, which are usually remotely operated. Because of the drone threat and the huge number of EW systems used in the war, many systems have also now been designed to be simple and easy to use, with only a few switches to activate detection and warning of incoming drones, or to activate protection against them by jamming large frequency bands. So instead of just being a capability for certain specialists, EW has now been distributed across the forces on both sides. Many soldiers on the battlefield now have an understanding of EW and spectrum operations. As an example, the risks of being geolocated and target-

ed when activating an emitter, no matter whether it is a jammer, radio, or radar, is knowledge that is now much more widespread than before the war.

Conclusions

Although it is unlikely that other countries will end up in the same situation as Ukraine in the near future, it is nevertheless of great importance to draw conclusions and learn as much as possible from the current situation and its evolution. It is vital to realise that Russia as well as China, North Korea, and Iran are continuously learning from this situation and will gain and share knowledge for use in their future development of EW capability. This may lead to a major impact on future warfare against the West. For Western forces, it should therefore be a priority to match the knowledge gained by the Russians and their allies by training in similar situations and scenarios. Exercises in the West should be heavily influenced by EW, with a focus on jamming of communication, navigation, radars and unmanned systems. In the development of new systems working in the electromagnetic domain (for example unmanned systems, communication systems and radars) it is vital that they are hardened against EW and adapted to a continuously shifting spectrum. The effects of EW, for instance, GNSS jamming, should not be limited to military exercises but should also be included in exercises with civilian actors.

Further reading

Engqvist, Maria, et al., 2026, *The future of Warfare in Russian Military Thinking*, FOI-R--5806--SE, Stockholm: Swedish Defence Research Agency (FOI).

Kjellén, Jonas, 2018, *Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces*, FOI-R--4625--SE, Stockholm: Swedish Defence Research Agency (FOI).

McDermott, Roger N., 2022, *Russia's Path to the High-Tech Battlespace,* The Jamestown Foundation.

17. Thinking about potential Russian nuclear use in Europe

Astrid Nilsen-Moe and August Andersson

The Russian political leadership believes itself to be in a long-term geopolitical conflict with the West and has demonstrated a willingness to attack neighbouring countries, as recently evidenced by the ongoing war against Ukraine. It is therefore not unthinkable that Russia may attack another neighbouring country, possibly one in NATO. The use of nuclear weapons in such a conflict cannot be excluded. Here, we demonstrate a method for thinking about nuclear weapons use by analysing potential Russian nuclear attack against an underground bunker. The method is based on analysis of nuclear scenarios along three key dimensions, in the following order: technical, military and political.

A nuclear threat against Europe

The Russian president Vladimir Putin's time in power has been marked by military conflicts and wars started by Russia: Chechnya (1999–2009), Georgia (2008), the annexation of Crimea (2014), Donbas (2014–), and the ongoing full-scale invasion of Ukraine (2022–). The goals of Russia's political leadership include territorial expansion driven by a perceived need to protect the heartland through the establishment of buffer states, as well as a demand for prestige and international great-power status. This ambition will not fade after a possible end of the war against Ukraine, and may lead to a nuclear confrontation in Europe. To think about nuclear weapons in a systematic way, we suggest analysing nuclear use along three key dimensions, described below.

The aim of this approach is to identify realistic scenarios that go beyond Russian nuclear sabre-rattling or total nuclear annihilation. Once realistic scenarios have been identified, they can be used for military and contingency planning.

The technical, military, and political dimensions

The use of nuclear weapons, like any form of state-owned military force, is ultimately a political decision. As with conventional weapons, the consequences extend across a large array of dimensions (social, health, economic, etc). Nuclear weapons, unlike conventional weapons, are sometimes only considered in the political dimension, because their use may ultimately lead to two states practically annihilating each other, as often envisioned between the US and the Soviet Union during the Cold War. However, there are many other scenarios, including more limited nuclear use, where additional factors may play a large role in deci-

sion-making. To analyse the effects and considerations involved in possible nuclear use, we use three main dimensions:

The technical dimension includes the technical specifications of the nuclear weapon (for example, the warhead and the delivery vehicle, its precision, and yield) and related systems (such as reliability and nuclear command and control) as well as the effects of a nuclear explosion on its target (for example, shockwave, crater, and fireball) and its surroundings (such as radiation and radioactive fallout), and means of evading defence systems.

The military dimension includes the potential gains and losses on the battlefield caused by a nuclear explosion. This is the domain of the military officer and includes the operational objectives, and the opportunities that arise from specifically using nuclear rather than conventional weapons.

The political dimension is influenced by both the technical and military dimensions, but reaches further. It is governed by politicians and includes, for example, effects on the civilian population, joining or leaving international treaties and alliances, sanctions, and, ultimately, uncontrolled nuclear escalation.

Four scenarios of nuclear weapons use

There are a vast number of possible scenarios for nuclear weapons use, most of which can be divided into four broad classes: nuclear weapons signalling, use in space, strategic use, and sub-strategic use.

We emphasise that any use of nuclear weapons depends on the phase of the conflict. For different phases, actions may be an initial strike, an attempt to break a deadlock, or an effort to prevent defeat. The phase of the conflict influences escalation dynamics, and these together influence the type of nuclear use that may be considered. Escalation dynamics are not the focus here, as other methods such as war gaming may be more suitable for such inquiries.

Nuclear weapons signalling involves actions that demonstrate resolve, beyond verbal threats, but without direct nuclear weapons use against the opponent. An example is moving nuclear weapons out of central storage and forward deployment of nuclear forces. A further escalation is a "shot across the bow", where a nuclear weapon is used in proximity to the conflict, but without direct impact.

A nuclear explosion in space can be used to disable satellites and to create an electromagnetic pulse (EMP) that can damage large-scale electronic infrastructure on the ground. Even though none of these effects are expected to directly take human lives, the effects may be very severe. Both effects are associated with low precision and are therefore likely to affect third parties. Therefore, a space explosion can be more escalatory than limited use on Earth.

Strategic nuclear weapons are used for deterrence by threatening essential (nuclear) military installations or civilian targets such as large cities. This type of nuclear weapon use is highly escalatory, and probably would only be considered in extreme situations such as retaliation for such an attack or as a last resort when the war is lost and there is nothing left to lose. Deterrence only works if the threat is credible; therefore, this type of nuclear use can never be disregarded. It would likely result in large-scale nuclear annihilation.

Sub-strategic nuclear weapons (SSNWs) are typically used against military targets to gain a battlefield advantage, and do not threaten the existence of another country. The definitions of SSNWs vary, but generally the term refers to using nuclear weapons in a way that does not escalate to a total nuclear war. It is likely the class of nuclear use most relevant for Russia in Europe, and it is discussed in more detail in the sections below.

Russian sub-strategic nuclear weapons use in Europe

Russian nuclear posture, doctrine, and military thinking indicate that Russian SSNWs should be understood as an extension of its conventional forces, useful for deterrence and coercion as well as for war-fighting. Russia is estimated to have the world's largest SSNW arsenal (up to 2000 warheads), consisting of a multitude of different types, each with a specific military use. These can be delivered by several different platforms, from ground, air, and sea, allowing Russia to strike anywhere in Europe.

Drivers of Russian use of SSNWs during a war in Europe may include conventional forces wavering, Russia losing the war, SSNWs being able to solve a military problem that conventional weapons cannot (for example, rapidly and reliably taking out a critical target), or the political leadership being threatened.

Depending on the operational goal, use of SSNWs may be directed at different types of targets such as *command and control*, including control centres, radar arrays, and air defence; *logistical hubs* such as harbours, railways, and airstrips; *military troops*; *civilian infrastructure* such as power plants; or even the *civilian population* with the aim of trying to break the will to fight. Some, perhaps even most, of these can be defeated using conventional warheads, but nuclear weapons are more reliable for the task and may do so faster and with a higher degree of certainty. Furthermore, nuclear weapons use may affect the will to fight, and shock and intimidate domestic and international communities, while fallout contaminates the battlefield.

Example: a command-and-control bunker

A target for which nuclear weapons may be specifically advantageous compared with conventional warheads is an underground bunker, possibly containing a command centre. We therefore use Russian SSNW employment against an underground bunker in a NATO country as an example in the following analysis.

The technical dimension includes the delivery system used in the attack, and the weapon effects. The most likely use of a nuclear weapon in defeating an underground bunker is a surface explosion. Such an explosion creates a deep crater and shockwaves that can cause crucial damage to the bunker. A surface explosion also ejects large amounts of material with induced radioactivity into the atmosphere. This creates intense radioactive fallout downwind of the explosion. Meanwhile, the site of the explosion will be a source of intense radiation. The war against Ukraine has shown that the Russian leadership has little regard for the lives of its soldiers, or civilians, suggesting that it would be much more willing to accept the risks associated with the secondary effects of a nuclear explosion. However, if Russia wants to use the land that is taken, the radioactive fallout can be an issue.

To assure target penetration, the yield of the explosion needs to match the precision of the delivery vehicle, or more than one warhead will be required. Figure 1 shows the probability that one to three missiles with a given precision will defeat a hardened target as a function of the warhead yield. The figure illustrates two points. First, it is more effective to increase the number of warheads than to increase the explosion yield. Second, choosing a delivery vehicle with higher precision is more effective than increasing the yield of the warhead.

The technical requirements needed to defeat a target (for example, yield, precision, number of warheads, and distance to target) determine what nuclear weapon system and platform may be used. This, in turn, controls what military unit is required, and thus the military planning. Taken together, the technical dimension directly affects the military dimension by limiting the options available.

The military dimension includes the potential success of the SSNW use, the battlefield gain, and the overall effect on the war. SSNWs can either be used in a time-dependent way, where a specific time window must be matched for a successful attack on the battlefield, or in a time-independent way. To reduce uncertainties regarding the success of such an operation, it may be advantageous to use several SSNWs in the attack to ascertain that the target is defeated; see Figure 1.

Crucial for military decision-making is whether the operational objective could be achieved by conventional means, or if a nuclear weapon is required. The consequences of defeating a decisive point such as a bunker containing military leadership or crucial command-and-control systems could have important ramifications for the war, especially if the attack is timed with Russian manoeuvre warfare, such as conventional operations using the opportunity for breakthrough.

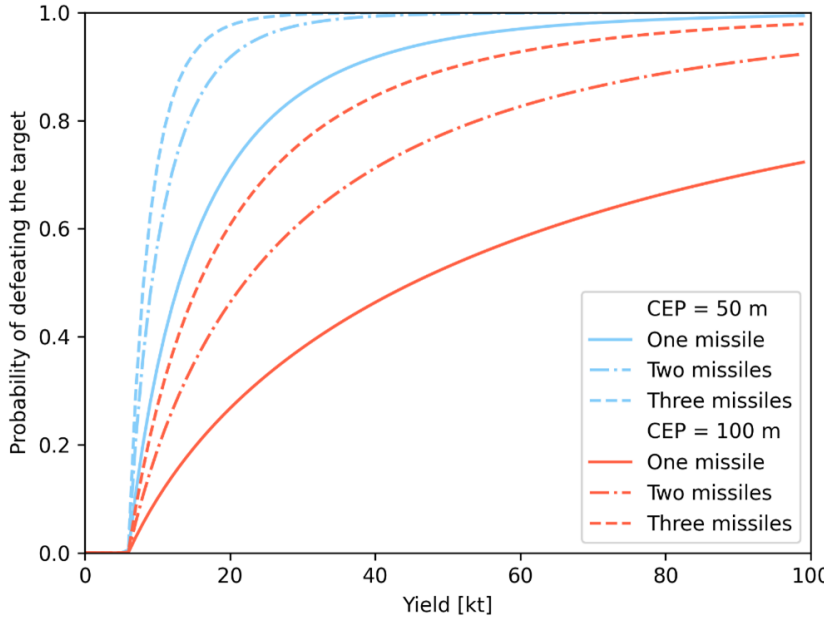

Figure 1. An estimate of the probability (where 0 is impossible and 1 shows that the event will happen) of defeating an underground bunker is plotted against the warhead yield (measured in kt, the equivalent energy in kilotons of TNT). Blue lines show 50-m precision (circular error probable, CEP), while red lines show a CEP of 100 m. Solid lines represent using one missile to defeat the target, dash-dotted lines two missiles, and dashed lines three missiles. The curves cross the x-axis at the minimum energy required for target penetration at the bunker depth.

Due to a general fear of nuclear weapons, a SSNW could also affect the enemy's will to fight.

The political dimension depends on the stage the war is in, which nations are involved, as well as casualties and target type. The potential military and political benefits of nuclear use need to be weighed against possible political costs and escalation risks. Striking a military bunker may be seen as less escalatory compared to striking, for example, civilian targets. For certain operations, it may prove useful to strike several targets. However, herein lies a political risk: striking too many targets or accidentally striking civilian targets may cause a larger reaction than anticipated, potentially triggering uncontrolled nuclear escalation. Where that line goes is likely unknown to the involved parties.

The political consequences of SSNW use include a military response from NATO allies, perhaps using nuclear weapons. It is possible that SSNW use both encourages some nations and dissuades others from getting more involved in the conflict. Responses also include sanctions on Russia and support for the attacked country, as well as potential nuclear weapons proliferation. Overall, these responses may threaten the long-term Russian goals of increased prestige and great-power status, as well as Russia's war aims.

Conclusions

Current debate on nuclear weapons tends to focus on the political consequences: strategic deterrence, civilian casualties, and, ultimately, nuclear annihilation. Given the destructiveness of a nuclear war, a nuclear "taboo" is often invoked. While Russia has adhered to the nuclear taboo in the past, its military thinking suggests that it has always been prepared to ignore it if the gain outweighs the consequences. The risk of Russian nuclear use during a future conflict in Europe is therefore real. However, this does not necessarily mean the end of the world as we know it; rather, we need to identify likely scenarios and prepare for them. There is no denying that even limited use of nuclear weapons will have far-reaching consequences for the global nuclear order. The approach presented herein is an attempt to develop a method for identifying such scenarios so that we can be better prepared if such an event were to occur.

Further reading

Andersson, A., A. Nilsen-Moe, M. Goliath, 2025, Konsekvenstabell för kärnvapenanvändning. Exempel: Rysslands anfallskrig mot Ukraina, FOI memo 8915, Stockholm: Swedish Research Agency (FOI).

Eken, M., K. Suman-Chauhan, B. Aubert, and P. van Hooft, P., 2025, *Understanding Russian strategic culture and the low-yield nuclear threat*. RAND Corporation.

Persson, G., 2025, *Russian Military Thought*. Washington DC. Georgetown University Press.

18. Autonomous Drones, Swarm Technology and Civil Defence: Future Implications of the Russo-Ukrainian War

Johan Markdahl, Jonas Lidman, Anna Andersson, and Peter Bennesved

Drones have taken centre stage in the Russo-Ukrainian war and will likely play an important role in future conflicts. In recent years, many nations have significantly increased their research and development in drone technology as well as drone countermeasures. The future will likely see the development of different types of drone swarms with various degrees of autonomy and human operator involvement. To protect civilian populations against the threat of autonomous drone swarms, legal restrictions are being discussed in forums on international law.

In March 2025, Russia attacked Odessa with numerous drones, wreaking havoc on the civilian population. This attack saw a swarm of Russian Geran-2 drones gathering above the shores of the Black Sea at an altitude and location where they were beyond the reach of Ukrainian air defence. They then struck the city simultaneously, causing fires to break out at three separate locations. Although much larger attacks have since then been conducted, the bombing of Odessa differed from earlier attacks in that it displayed a willingness to increase the complexity of these massive operations by developing new tactics. By gathering at altitude and hitting multiple targets simultaneously, the drones achieved a swarming effect on Odessa that the military, rescue services, and citizens found difficult to handle.

Since the beginning of the Russo-Ukrainian war, simultaneous attacks using several hundred drones and long-range missiles have been launched at Ukraine's civilian and military infrastructure on a daily basis. This war from above is part of Russia's effort to wage a war of attrition. Russia is using long-range attack drones because they are cheaper and easier to manufacture than other comparable weapon systems such as missiles. Considerable economic and military resources are being invested in drone manufacturing. The drone factory in Alabuga, Russia, manufactures about five thousand Geran-2 drones per month. Geran-2 is the Russian variant of the Iranian-developed Shahed-136, carrying a warhead of 50 or 90 kg, and the primary fixed-wing one-way attack drone used by Russia.

Looking beyond the Russo-Ukrainian war, further developments of swarm capabilities are to be expected, and military and civil defence must adapt accordingly.

More drones are being manufactured worldwide. Furthermore, development of autonomous weapon systems could lead to more coordinated swarm behaviour. The attack on Odessa showcases the advantages of swarm tactics. Both military and civilian countermeasures will need to be ramped up to account for a greater number of weapons as well as more advanced manoeuvring and tactics.

Three types of drone swarms

To evaluate defence methods against attacks such as the bombing of Odessa, it is first necessary to understand drone swarms. The word swarm is sometimes used in a military context to designate groups of units that coordinate their efforts to achieve a common goal. We distinguish between three different types of swarms: weapons that attack en masse, socio-technical swarms, and autonomous swarms, which differ in their level of autonomy and operator involvement.

A swarm of missiles and drones that fly together to a pre-programmed target position is an example of weapons that attack en masse. The bombing of Odessa is an example of such an attack. Two advantages of en masse attacks are the favourable cost-benefit equation for the attacker and the saturation of enemy air defence through sheer numbers. For Russia, the cost of a Geran-2 is about USD 35,000. By comparison, a modern mid-range surface-to-air interceptor such as the IRIS-T can cost up to half a million dollars. Furthermore, once the air defence has been saturated, each additional weapon gets through, increasing the total damage.

Socio-technical swarms consist of drones that are remotely controlled by operators. The drones typically stream a video to the operators. The advantage of socio-technical swarms compared to weapons that attack en masse is that the drones can be redirected using information from the video. If, for example, a target has already been destroyed, another target can be attacked instead. One example of socio-technical swarms is the Ukrainian operation "Spider's Web". In this June 2025 attack against Russian airbases, 117 small manually controlled first-person-view camera drones were brought into Russian territory and released at five different locations, successfully destroying several military aircraft.

In the future, advances in technology will likely enable drones to communicate and collaborate in order to complete assigned tasks without human intervention. Such systems would constitute autonomous swarms, in which drones operate independently and coordinately. Autonomous swarms will not require communication with an operator and can therefore adapt faster to dynamic situations, which also increases their operational range. However, the drones still require communication within the swarm.

In swarms, there is a trade-off between quantity and quality, where drones are either plentiful and cheap or few and costly. The key advantages of drone swarms are numerical superiority and coordinated attacks. However, the hardware and software

of each drone must be of sufficient quality to guarantee a high chance of success. Since a drone consists of many subsystems, for example sensors such as cameras and GPS receivers, any significant increase in performance comes at a higher cost. For this reason, in the past, many militaries tended to favour quality over quantity. However, unlike them, Russia prioritises quantity by means of mass production.

As the defender develops its countermeasures, the attacker will try to circumvent them, either by improving the quality of drones, increasing their number in the swarm, or developing new tactics, such as increasing the level of autonomy in the swarm. Since the latter increases performance without the need to increase quantity or quality, it is likely that a shift towards more autonomous swarms will occur. In other words, the development of defence methods could actually lead to more autonomy in the long term, since it may allow the swarm to overcome capable countermeasures

Defence against drone swarms

There are two main types of countermeasures that protect the civilian population and infrastructure against attacks. Active countermeasures, such as air defence, eliminate the threat either by using conventional weapons or through electronic warfare, including the jamming of communications or satellite-based navigation systems. Passive countermeasures, such as fortifications, provide physical protection for the target. To circumvent active and passive countermeasures, the attacker will develop its tactics, for instance by employing more autonomy. This back-and-forth may be realized as an interplay of developments and counter-developments on both sides.

Because the civilian population and infrastructure are larger and distributed over a greater area than military personnel and infrastructure, they are more difficult to defend across an entire country. Long-range air defence, for example surface-to-air missiles and electronic warfare, is more effective than short-range countermeasures such as mobile anti-aircraft guns and interceptor drones. The latter types of defence units must be positioned near potential targets in advance. Moreover, hundreds of drones can swarm to the same position, requiring a large number of short-range defence units at each site. Guarding the entire civilian population and infrastructure against drone swarms using short range defence units is hence infeasible. An exception to this is defence against fibre-optic drones, which have a limited operational range and are therefore restricted to the front, posing less of a threat to the civilian population and infrastructure.

Autonomous drone swarms require communication and positioning to coordinate their efforts. Socio-technical swarms require communication with an operator. Successfully disrupting communication and positioning with electronic warfare means that these swarms degenerate into drone attacks en masse. Electronic warfare is a cost-effective means of defence. However, there are methods to avoid jamming. These include flying at high altitudes, directional antennas, and other

forms of interference protection, as well as alternative means of communication such as satellite and mobile cellular networks. A form of communication that cannot be jammed is fibre-optic cable. All drones in the swarm are then connected to a single control station. For the defender, it therefore suffices to neutralise the control station.

Air defence using conventional weapons relies on radar to follow drones that attack en masse. Surface-to-air interceptor missiles such as IRIS-T or NASAMS can neutralise drones such as the Geran-2, but are expensive. Decoy drones make this even more costly since distinguishing them from attack drones is challenging. Therefore, other more cost-effective alternatives must be considered. One such alternative is interceptor drones, which, like interceptor missiles, are exchanged one-to-one. Another cost-effective means of defence is mobile anti-aircraft guns. However, it can be circumvented by more advanced manoeuvring or by using faster drones at higher flight altitudes such as the more expensive jet-engine-driven Geran-3.

Passive countermeasures protect civilians from drones that hit their targets. These include fortifications such as bomb shelters, other protected spaces, and nets for smaller drones. An important complement to these are warning systems that inform civilians of the type of threat and its estimated arrival time, as the form of protection they need to seek out depends on the threat. Furthermore, since civilian infrastructure such as the electricity grid is targeted, backup systems, like generators, are needed. In the long run, the active countermeasures are likely to fail on occasion. For this reason, passive countermeasures are needed to ensure a successful and endurable defence.

International regulation of drone swarms

International humanitarian law applies to all weapons in armed conflict, including all types of armed drone swarms. The lawfulness of new armed drone swarms must be reviewed before use and they must be used in line with international humanitarian law, that is, the fundamental principles of distinction, proportionality, and precautions.

There is no treaty that specifically regulates drone swarms as such. However, there are discussions to create a new instrument for so-called lethal autonomous weapon systems (LAWS) within the Convention on Certain Conventional Weapons. This forum is based on consensus, so all High Contracting Parties must agree if a future instrument is to be adopted. Strikingly, and in contrast to many other disarmament forums, all major military powers are actively engaged in the discussions on LAWS, which have advanced significantly during the past couple of years.

There is no legal definition yet, but LAWS can be described as weapons and functionally integrated technical components that, after activation, can identify, select, and engage targets without further human involvement. A central aspect is thus

autonomy in critical combat functions. The concept of LAWS hence excludes unarmed drone swarms. Moreover, non-autonomous drone swarms, which require an operator to select the target, would not constitute LAWS. Of the three types of drone swarms described above, only autonomous drone swarms would qualify as LAWS.

A complete ban on LAWS is no longer under discussion, but it was discussed in the past. The current discussion instead confirms that unless a particular LAWS can be used in line with international humanitarian law, it must not be used. It also emphasises existing international law's applicability to LAWS, including that protected civilians must not be attacked and that human responsibility cannot be transferred to machines. Additionally, consensus appears to be forming around regulation of, for example, measures to ensure human involvement, testing, and bias mitigation throughout the lifecycle of LAWS. This aims to ensure that LAWS are developed and used in line with international humanitarian law.

Conclusions and future implications

The bombing of Odessa is an illustration of the current state of the art in swarm attacks en masse. Similarly, Ukraine's operation Spider's Web displays the potential of socio-technical swarms. These examples showcase the latest development of both swarm tactics and technical capabilities. While the discussions on LAWS are advancing towards further regulation that may affect the development of autonomous drone swarms towards better compliance with international humanitarian law, a global ban is unlikely to materialise.

As swarms are both an existing and future threat, military and civil defence must be developed and designed with both active and passive countermeasures in response to the increasing numbers and more advanced manoeuvring made possible by swarm technology. Such measures are necessary to protect both armed forces, military materiel, the civilian population, and civilian infrastructure against drone swarm attacks.

Further reading

Bennesved, Peter, Johan Markdahl, and Anna Andersson, 2025, *Swarming Drones and Civilians - Future Risks and Prospects of Drones and Swarm Technology in Civil Defence*, FOI-R--5668--SE, Stockholm: Swedish Defence Research Agency (FOI).

Kallenborn, Zachary, 2020, *Are Drone Swarms Weapons of Mass Destruction?* U.S. Air Force Center for Strategic Deterrence Studies.

Mandle, J. Layton, 2026, *Consider the Longbow: RMAs, Evolutionary Technology, and Uncrewed Systems*, Defense & Security Analysis.

19. Space - a strategic investment in national security and sovereignty

Erik Fagerström, Max Nyström, and Alexander Hagelberg

Space-Based Intelligence, Surveillance, and Reconnaissance (SBISR) plays a crucial role on the modern battlefield. Conflicts such as the war in Ukraine have shown the enormous advantages that this capability can provide, not only in monitoring military formations and activities, but also in enabling the employment of long-range precision weapons. After the United States temporarily stopped sharing satellite intelligence with Ukraine in 2025, sovereign access to these capabilities has become of even greater importance. This development is reflected in the Swedish Armed Forces' decision to accelerate the procurement of Earth observation satellites. Advances in artificial intelligence enable the analysis of ever-increasing data volumes generated by a growing number of intelligence, surveillance, and reconnaissance satellites. At the same time, the increasing commercialisation of space has added another layer of complexity, as satellites operated by private companies often have clear dual-use. In this context, Russia has stated that commercial satellites may be regarded as legitimate targets if used within an armed conflict.

A TRANSPARENT BATTLEFIELD

An elevated position has always been desirable for intelligence gathering as it allows observers to see further. What began with hills later evolved into balloons and aircraft. In modern warfare, however, the ultimate observation post is located in space.

Orbiting the Earth, satellites offer unique advantages compared to manned aircraft and Uncrewed Aerial Vehicles (UAVs). Unlike airspace, which is subject to national sovereignty, outer space has no defined territorial limits, and as such, satellites cannot be prevented from passing over foreign territory. Space-Based Intelligence, Surveillance, and Reconnaissance (SBISR) can therefore be conducted globally and persistently. In combination with the ability to detect even single land combat vehicles, ships, and aircraft, SBISR must therefore be regarded as a major contributor to battlefield transparency.

In 2025, the United States paused intelligence sharing with Ukraine by temporarily suspending Ukraine's access to the global enhanced GEOINT delivery system, illustrating that SBISR can also serve as political leverage. At the same time, increasing hybrid threats, including attacks on critical undersea infrastructure, have prompted European states to complement or acquire their own SBISR capabilities. This may involve the purchase of commercially available Intelligence,

Surveillance, and Reconnaissance (ISR) data, satellites, or a combination of both. In parallel with national initiatives, the European Union is working to enhance its earth-observation capabilities. The increased prevalence of misinformation, including Artificial Intelligence (AI)-generated satellite imagery, further emphasises the importance of sovereign data capabilities. In early 2026, the Swedish Armed Forces signed agreements to procure Electro-Optical (EO) and Synthetic Aperture Radar (SAR) satellites, accelerating the previous procurement plan by four years. Ukraine's acquisition of a SAR satellite through public crowdfunding similarly illustrates recognition of the importance of dedicated access.

Methods and technology

SBISR relies on three main sensor types: EO imaging, radar-based imaging such as SAR, and Electromagnetic Support Measures (ESM). Commercial EO and SAR sensors currently provide imagery with a very high resolution of around 30 centimetres per pixel. An advantage of EO sensors is the spectral information provided, while SAR sensors produce imagery independent of daylight and cloud cover. ESM systems detect, characterise, and localise electromagnetic emissions, including maritime identification systems, communications signals, and radar transmissions.

Recurring satellite passages over the same area enables near-persistent monitoring, which in turn enables the detection of changes that may indicate anomalies in behaviour. Improvements in this capability are largely driven by the growing number of satellites in orbit. Larger satellite constellations and improved technical capabilities generate an increasing volume of data to be processed and analysed. AI has therefore become a critical tool in the ISR chain. Automatic target recognition algorithms help identify objects of interest within large datasets, which can reduce the workload placed on human analysts. Emerging forms of AI, such as agentic AI, may further improve the efficiency of analysts' workflows. Edge processing, in which data is processed and analysed directly in orbit, enables the prioritised downlink of the most relevant data, while delaying or discarding data that lacks targets or is obscured by clouds. Developments in multimodal AI can further facilitate the interpretation of satellite imagery, particularly in complex scenes, by integrating different types of data such as images and language. In addition, pre-trained AI foundation models can be adapted to specific operational contexts with relatively limited additional training data, increasing flexibility and scalability.

The increasing reliance on AI-driven analysis has in turn triggered the development of countermeasures designed to deceive detection algorithms. Examples include placing tyres on aircraft to alter their visual signatures or painting decoy aircraft on the tarmac, painting the bow and stern of ships to blend in with the ocean, concealing the true length of the ship, and arranging metal scraps in the shape of aircraft to trigger false positive SAR readings. These measures illustrate the dynamic interaction between detection technologies and deception techniques.

Beyond target identification, SBISR supports operational planning through terrain accessibility analysis, for example through assessments of soil moisture and the identification of damaged infrastructure such as roads or bridges. Optical SBISR operating across multiple wavelengths enables multispectral analysis, which can be used, for example, to detect burnt areas. Thermal infrared sensors are commonly used in early warning systems to detect missile launches, including intercontinental ballistic missiles (ICBMs).

ISR ON THE BATTLEFIELD

A key reason why SBISR has gained such a crucial role in the Russo-Ukrainian war is that the airspace is contested. This has significantly limited the use of manned reconnaissance aircraft and more sophisticated unmanned ISR platforms.

UAV systems dominate ISR operations close to the line of contact, typically within 15 to 40 kilometres, enabling rapid target detection and the prompt application of fires. SBISR is less commonly used at the line of contact, as it often operates on longer timeframes. However, UAVs struggle to conduct reconnaissance in rear areas protected by air defences. Systems capable of operating effectively in these areas are manufactured in much smaller numbers and at a higher cost. In this context, SBISR provides valuable coverage at a greater depth, collecting imagery far into rear areas and helping direct more capable drones toward high-priority targets in areas with lower air defence coverage.

SBISR can identify and locate high-priority targets such as air defence systems, self-propelled artillery, and headquarters. These targets can then be engaged, and the resulting damage can then be assessed to determine whether follow-up strikes are required or whether exploitation is possible. Mapping of air defence systems also facilitates the planning of long-range strike missions against strategic and economic targets such as oil and gas infrastructure. In Ukraine, such strikes have been conducted using advanced missile systems as well as One-Way Attack Drones (OWADs). Given the low numbers of advanced missiles and the limited capability of OWADs, exploiting areas with lower air defence coverage is essential.

Minimising the time between tasking, image collection, analysis, and the application of fires is a central operational priority. This has led to the development of concepts such as tactical SBISR. In practice, a tasking request is sent from a ground station to a satellite scheduled to pass over the target area. The satellite acquires the image, after which the data is downlinked at the next available ground contact, analysed, and disseminated to decision-makers.

SBISR AS A COMMERCIAL PRODUCT

Until the last decade, space, and particularly SBISR, was dominated by state actors operating satellites for civilian or military intelligence purposes. In recent years, however, space has become increasingly accessible to commercial actors,

which in turn has made SBISR services more widely available. This has enabled smaller states to acquire SBISR without having to produce, launch, and operate their own satellites. At the same time, states with extensive military SBISR constellations, such as the United States, supplement their capabilities with commercially acquired imagery. One reason for this is that sharing commercially acquired data with partners may involve fewer classification constraints.

Commercial imagery also offers certain advantages compared to imagery from sovereign systems, as commercial providers often have larger constellations and offer greater collection capacity. In addition, commercial satellites operating in low Earth orbit often have shorter lifespans, requiring regular replacement and enabling frequent technological upgrades and continuous improvements.

However, reliance on commercial providers also entails risks. Satellite operators must prioritise among customers, and in areas of high demand timely image delivery cannot always be guaranteed, particularly for lower-priority users. Other risks concern data integrity, such as disclosure of a state's areas of interest to commercial providers and limited control over collected information. When purchasing commercial satellites, states may face further vulnerabilities. The country in which the provider is registered may retain so-called shutter control, potentially restricting imagery provision at a later stage. Furthermore, buyers may lack full transparency regarding the origin and security of components integrated into satellites and payloads.

The increasing accessibility of high-resolution satellite imagery also extends beyond state actors. For example, the Wagner Group, a Russian private military company, procured two Earth observation satellites from Chinese commercial providers, demonstrating that capabilities once limited to sovereign states are becoming more widely available. Media organisations routinely acquire satellite imagery for reporting purposes, and humanitarian organisations use it to document war crimes and crimes against humanity, such as those committed in Bucha, Ukraine, and in Darfur, Sudan. While this enhances transparency and accountability, it also creates opportunities for misinformation through manipulated imagery or misleading contextualisation. These developments emphasise the importance of sovereign capabilities that reduce dependence on intermediaries.

The commercialisation of space coincides with increasing military utilisation and the development of counterspace capabilities. Counterspace operations aim to degrade or deny access to space-based capabilities and range from reversible measures such as laser dazzling and jamming to destructive kinetic or nuclear anti-satellite weapons. Reversible methods may be employed during grey-zone or hybrid warfare scenarios, contributing to strategic uncertainty.

The dual-use nature of commercial satellites and their explicit involvement in armed conflicts raise complex legal and strategic questions regarding their status as potential targets. To date, kinetic or nuclear anti-satellite weapons have not

been used in armed conflict. Russia has, however, stated that it considers commercial satellites legitimate targets for retaliation if involved in support of military operations.

Concluding remarks

The modern battlefield can be described as increasingly transparent due to the improved capabilities of UAVs and satellites, which have substantially reduced the ability of military forces to generate operational surprise. The importance of space was underscored when it was declared an operational domain for warfighting. SBISR is essential for effective long-range fires, operational and strategic planning, arms control verification, border surveillance, troop-movement monitoring, and battle damage assessment. In the period preceding the Russian invasion of Ukraine, satellite imagery clearly showed Russian forces assembling along the Ukrainian borders, indicating the coming invasion. These images also showed, for example, field hospitals, contradicting the Russian narrative that this build-up was merely intended for field training. This illustrates the military and political implications of satellite-derived transparency.

The availability of commercial satellite imagery has increased public awareness of armed conflicts. At the same time, the commercial sector has integrated into national defence ecosystems. Advances in AI continue to accelerate the speed and scale at which satellite imagery can be analysed, supporting applications ranging from conventional arms control to anomaly detection. Although already in use, AI is still in its early stages, and new applications are under development.

The war in Ukraine has shown that controlling access to satellite imagery is a necessity for military planning and can be a means of political leverage. In light of this, sovereign capabilities have emerged as a matter of the utmost importance. Sweden's decision to acquire EO and SAR satellites should therefore be understood as a strategic investment in national security and sovereignty.

Further reading

Hagelberg, Alexander (ed.), 2026, Spaning och övervakning från rymden 2023–2025 [Space-based Intelligence Surveillance and Reconnaissance 2023–2025], FOI report, forthcoming.

Jungnell, Victor, 2016, *Överflygningsanalys* [Overflight analysis], FOI-R--4320--SE, Swedish Defence Research Agency (FOI).

Westman, Jonatan, Frank Guldstrand, Andreas Johlander, Sandra Lindström, Linn Mattsson, Norea Normelli, Ola Rasmusson, Niklas Wingborg, and Anna

Maria Wårlind, 2023, *Omvärldsanalys Rymd 2023—Fokus på försvar och säkerhet* [Global Space Trends 2023], FOI-R--5516--SE, Stockholm: Swedish Defence Research Agency (FOI).

20. From platforms to code: The future defence industry

Martin Hagström

The military–industrial complex of the future might look different from that of the past. Technological developments, from information technology in general to recent achievements in AI, are bringing new expectations and new players into the military-industrial field. The traditional defence industry has long integrated software into military systems; now there are software companies integrating military components into software-based products. However, the requirements for defence equipment are different from those for software products. Will the promises of the new actors hold, and will the old actors stand aside? How will states, which constitute the market and maintain strong ties to the traditional industry, act? The shaping of the future defence industry will affect many, not only companies, but also nations and future defence capabilities.

The defence industry does not operate in a conventional open market economy. Rather, it functions within a highly regulated environment shaped by export control regimes, national security legislation, state procurement policies, and multilateral non-proliferation frameworks. Market access, technology transfer, ownership structures, and even supply chains are subject to political oversight to a degree unmatched in most other sectors. The customer base is narrow and concentrated, with only 25 states accounting for more than 90 per cent of global defence expenditure. Governments are not merely clients but also regulators, sponsors of research and development, and, in many cases, strategic partners.

The United States, responsible for roughly 40 per cent of global defence spending and home to the world's largest defence industrial base, illustrates these dynamics clearly. Over the past three decades, the US defence sector has undergone significant consolidation. The number of prime contractors has fallen from 51 in the early 1990s to five major companies today, which together account for approximately one-third of the US Department of Defense contract obligations. This consolidation has reshaped competitive dynamics, supply chain structures, and the state–industry relationship, raising ongoing debates about resilience, innovation, and national autonomy within the defence industrial base.

Government defence contracting operates under structural constraints. The use of taxpayer funds requires parliamentary oversight and executive branch scrutiny, generating administrative burdens. While these mechanisms ensure accountability, they also increase transaction costs and can slow capability development.

Although the US defence industrial base includes up to 100,000 firms, prime contracting is concentrated among five dominant companies—Lockheed Martin, RTX Corporation, Northrop Grumman, Boeing, and General Dynamics. At this level, the market resembles an oligopoly rather than a competitive buyer's market.

This structure has reinforced a traditional model centred on large organisations, long-term contracts, state-funded R&D, and hardware-intensive platforms such as missiles, aircraft, and armoured systems. While such platforms will remain relevant, future military advantage will increasingly depend on software, autonomy, and system integration.

Software powers future defence technology

Future weapons systems will be increasingly software-defined, with operational effectiveness driven as much by code as by hardware. The trajectory is clear: greater autonomy, rising system complexity, and a growing share of functionality implemented in software rather than in physical components. As complexity increases, systems integration becomes a strategic capability in its own right. Ensuring interoperability and coherent performance across multiple subsystems will require sustained investment in architecture design, integration expertise, verification, and life-cycle software management.

The development of complex, software-intensive systems requires a fundamentally different industrial model than that used for traditional military hardware. Historically, defence primes have specialised in integrating hardware subsystems, with software adapted to platform-specific requirements. Future military capabilities, however, will depend increasingly on artificial intelligence, autonomy, and data-centric architectures, domains driven by cutting-edge research in computer science rather than by platform engineering alone.

During the Cold War, the defence sector was a primary engine of technological innovation. In the post–Cold War consolidation, driven by business logic, reduced defence spending, and pressure for cost reductions, the number of major US prime contractors declined from 51 to five. Following this, innovation leadership shifted toward the commercial sector, particularly in areas such as the internet, personal computing, and consumer electronics. As a result, many critical enabling technologies now originate outside the traditional defence industrial base.

In response, the Defense Innovation Unit (DIU), established by the US Department of Defense in 2015, was designed to accelerate access to commercial innovation, particularly in AI and autonomous systems. By lowering entry barriers for non-traditional vendors and emphasising rapid prototyping and iterative procurement, DIU represents an institutional adaptation to a software-driven innovation environment.

The creation of the Defense Innovation Unit (DIU) signalled an attempt by the US Department of Defense to tap commercial innovation while mitigating the constraints of its traditional acquisition system. At the same time, a new generation of non-traditional defence firms has emerged from major technology ecosystems, including Google, Facebook, and Amazon.

The newcomers

Firms such as Anduril Industries and Helsing illustrate this transformation. Initially focused on AI-enabled surveillance, data fusion, and decision-support software, they have leveraged private capital to expand into hardware and weapons systems. Anduril has pursued acquisitions in autonomous vehicles and propulsion, while Helsing has partnered with established manufacturers such as Rheinmetall and Saab to enter the combat drone market.

The surge of interest in artificial intelligence across defence establishments, accelerated by Russia's full-scale invasion of Ukraine, has reshaped capability planning across the North Atlantic Treaty Organization. All NATO members have increased defence spending and signalled strong demand for AI-enabled systems, driven by the perception that operational advantage will hinge on data exploitation, autonomy, and algorithmic decision-support. This has created both a technology push and a strategic pull: a widespread concern that failure to adopt AI at scale could translate into battlefield disadvantage.

The result is a significant influx of capital into defence technology ventures. Firms such as Anduril Industries and Helsing exemplify a new class of companies attracting substantial public and private investment by promising rapid delivery of AI-enabled capabilities. However, the accelerated pace of innovation and deployment is generating pressure on existing procurement processes, certification regimes, and regulatory frameworks, which are often criticised as slow and risk-averse. How to enable rapid experimentation and fielding of AI-driven systems while preserving accountability, interoperability, safety standards, and compliance with domestic and international law remains an open question.

Procurement: Complex and capability-critical

Defence procurement procedures are not solely designed to ensure market competition, financial accountability, and traceable decision-making. Their complexity also reflects the intrinsic demands placed on military capability development. Equipment must be safe, reliable, and demonstrably fit for purpose. While assessing suitability may be straightforward for simple tools, it becomes considerably more complex for advanced, networked systems operating in contested and uncertain environments.

Military platforms, weapons, and command-and-control systems do not function in isolation. They must integrate into highly complex organisational struc-

tures characterised by dense intra- and inter-system dependencies. Materiel must perform under diverse operational conditions, align with existing logistics architectures, remain maintainable over long service lives, and ensure interoperability with both legacy and future systems. Training burdens must also remain manageable.

These cumulative requirements generate extensive and often rigid specification frameworks. Despite sustained reform efforts aimed at simplification and streamlining, defining and validating requirements for complex military systems remains a structurally demanding task. This underscores a central tension: accelerating innovation must not come at the expense of operational coherence, safety, and long-term sustainability within the broader defence ecosystem.

Predictability and safety are intrinsic requirements in the development and deployment of weapons and other hazardous military systems. Unexpected system failures, such as an aircraft crash caused by software malfunction, pose risks not only to personnel but also to mission success. Systems whose failure may result in catastrophic consequences are classified as safety-critical, and their design and certification impose stringent technical and regulatory demands.

Integrating software into safety-critical functions significantly raises the bar for reliability, verification, and validation. Unlike general-purpose software applications, where a system restart may be inconvenient but tolerable, software in flight-control systems or weapons platforms must meet exceptionally high assurance standards. Such development practices are well established in aerospace and traditional defence industries but differ markedly from mainstream commercial software engineering.

Cultural fusion or collision

The difference between the old and the new reflects a broader cultural gap. Emerging defence technology firms often originate from software environments that prioritise agility, rapid iteration, and continuous feature deployment. In contrast, safety-critical military systems require stability, formal verification, and tightly controlled update cycles. Bridging this cultural and methodological divide will take time and deliberate institutional effort.

Adding to this challenge, segments of the Western aerospace and traditional defence industrial base face demographic pressures, including an ageing workforce and shortages of specialised engineers after decades of industrial restructuring and offshoring. Higher education in the West is in many respects driven by competitive publishing in new research frontiers. Funding pressures and the need for rapid publication make it risky to embark on research paths in classical fields still needed by the traditional defence and aerospace industry. Although the title "rocket scientist" still holds its value, fewer graduate students study areas such as

control theory, aerodynamics, flight mechanics, and other subjects that are still needed in industry.

Software is already a central part of the defence industry, but software and AI algorithms alone do not create kinetic effects. Missiles can be designed to fly higher, faster, and with more adaptive explosive effects, advancements that require expertise from many fields. Bridging the cultures and knowledge of the modern, software-focused industry and the traditional, more hardware-focused defence industry could have transformative effects, but a bridge requires two supports.

A STRATEGIC VISION

The Western defence industry is built on a heritage shaped in a period of high defence spending and educational systems with a long-term perspective, when "rocket scientist" was a coveted title. New technologies do not always replace older ones; they are sometimes complementary to existing systems, which still need to be maintained and further developed. Software-driven companies now entering the defence sector must engage with legacy technologies, not only through acquisitions, but also through intellectual integration to enable continued development. Educational systems need to maintain relevant programmes and attract students to them. Achieving this requires a strategic vision at the policy level. In a market-driven society, this can be a challenge.

There are other countries, mainly in Asia, where the state pursues a clear strategic vision. Over the past three decades, China has built a comprehensive industrial base spanning consumer manufacturing, advanced aerospace, space systems, and large-scale production of autonomous platforms. Its defence spending has grown continuously since the early 2000s and now ranks second globally, behind the United States. Following parallel investments in higher education and the post–Cultural Revolution reconstruction of China's university system, its universities now produce large numbers of engineers and doctoral graduates, strengthening the country's technological capacity. The 15th five-year plan, released in March 2026, underscores the importance of self-reliance not only in production capabilities but also in AI and software development. The aim is for China to eventually become independent of US big-tech companies' software. The shift can already be seen in a number of Chinese-developed large language models, of which DeepSeek is the most well-known.

The strategic question is whether innovation leadership in defence will remain anchored in US-based commercial software technology ecosystems or shift toward competitors able to combine engineering scale, sustained state support, and comparatively fewer regulatory constraints. The answer, in the form of action by policymakers, will shape not only military capability development, but also the future balance between open-market innovation models and state-directed industrial strategies in strategic technologies.

Further reading

Christopher Weidacher Hsiung, Cecilia During, Oscar Almén, Ivar Ekman, Peter Stenumgaard and Annica Waleij (eds.), 2024, *Strategic Outlook 10: China as a Global Power*, FOI-R--5620--SE, Stockholm: Swedish Defence Research Agency (FOI).

Shah, Raj M. and Christopher Kirchhoff, 2024, *Unit X, How the Pentagon and Silicon Valley are Transforming the Future of War*, Simon & Schuster.

US Department of Defense, 2022, *State of Competition within the Defense Industrial Base*, report, Office of the Under Secretary of Defense for Acquisition and Sustainment February.

Author biographies

Oscar Alménn is Deputy Research Director and head of the Asia Programme at FOI's Department of Global Security Policy. He has a background as an associate professor of political science at Uppsala University. Oscar's research focuses on security policy in China and East Asia and China's relations with Sweden. Recent research includes Chinese investments in Sweden, Chinese Communist Party (CCP) relations with the Chinese diaspora, CCP influence over businesses in China, and China's military power.

Anna Andersson is a Senior Researcher in the Department for Legal Studies in Defence. Her research focuses on international humanitarian law, human rights law, and accountability for international crimes. She holds a master's degree in law from Örebro University and an LLM from the Geneva Academy of International Humanitarian Law. She has previously worked at the Swedish Defence University and Oslo University, among others.

August Andersson is a Researcher at the Department for Nuclear Weapon Threats. His research focuses on nuclear weapons. He previously worked as a researcher at Stockholm University, where he obtained a PhD in Biophysics.

Albin Aronsson is a Researcher in FOI's Department for Euro-Atlantic Security Policy, where he focuses on politico-military issues in the United States and NATO. He has recently written about the Trump administration, the US's military focus on the Indo-Pacific, and NATO's strategy for deterrence and defence, including nuclear policy. Albin holds a bachelor's degree in political science from Uppsala University and a master's degree in War Studies from King's College London.

Louise Bengtsson is a Researcher at FOI's Department for Governance and Civil–military Coordination. She has a background in European Studies with a BA from University College London, an MA from the College of Europe in Bruges as well as a PhD in International Relations from Stockholm University. Her research interests include security studies and health policy, with a particular focus on the bureaucratic and diplomatic practices of the EU institutions. She has previously served at the European Commission in Brussels and at the Swedish Ministry for Foreign Affairs, where she completed the diplomatic training programme.

Peter Bennesved is a historian of ideas, project manager, and Senior Scientist at the Department for Civil Protection. His research mainly concerns societal resilience from various perspectives, with an emphasis on civil protection issues. Since Russia's full-scale invasion of Ukraine, Bennesved's focus has primarily been on how developments in warfare technology and security policy affect the conditions for civil protection in Sweden.

Lisa Bergsten is an Analyst in FOI's Department for Strategy and Policy. Her main research areas include strategic foresight and security policy, and she is particularly interested in methods related to future studies. Recent studies focus on the information environment and non-state actors, and strategic foresight processes in the defence sector, as well as on Russia as a threat in 2050. Her current focus is on the US as a military actor in 2050. She has a bachelor's degree in peace and conflict studies from Uppsala University and a master's degree in political science with a focus on security studies from the Swedish Defence University.

Bruno Charbonneau is Professor of International Relations at the Royal Military College Saint-Jean, Senior Scientific Advisor at the NATO Climate Change and Security Centre of Excellence, founding President of the Climate Security Association of Canada, and a member of the NATO Systems Analysis & Studies Panel for 2025–2028. He was Team Leader of the NATO Research Task Group SAS-182 on the consequences of climate change for security, whose final report was released in January 2026. He was awarded one of nine inaugural 2025 NATO Chief Scientist Grants for the project "'Foresight: Planning for low-carbon warfare." His past and current research on climate security and defence, and on international conflict management in West Africa, has been supported by the Social Sciences and Humanities Research Council of Canada, Global Affairs Canada, Canada's Department of National Defence, Organisation internationale de la Francophonie, and other organisations.

Åsa Davidsson holds a PhD in Risk and Environmental Studies from Karlstad University and has experience in the public sector. Her research has focused on societal change, sustainable development, natural hazards, and early warning systems for tsunamis. Since joining FOI in 2024, she has conducted research on risk management and national security and has developed methods for risk assessment and analysis of GNSS dependencies.

Johan Englund is a Senior Researcher at the Asia Programme in the Swedish Defence Research Agency (FOI) in Stockholm, Sweden. Prior to joining FOI, he obtained his PhD in International Relations from the City University of Hong Kong. In 2024, he was a visiting researcher at the Institute of International Relations in Taipei. He also has a background as a desk officer at the Swedish Government Offices. His research interests are Chinese foreign policies and cross-Strait relations.

Maria Engqvist (MA), is an Analyst and Director for the Russia and Eurasia Studies Programme at the Swedish Defence Research Agency (FOI). Her work focuses on Russian security policy, strategic thinking, the development of Russia's Armed Forces, and Russian railway and infrastructure systems. She holds a BA in History, and an MA in Slavic Studies, both from Stockholm University. Before joining FOI, she was a lector at the University of Tartu in Estonia.

Erik Fagerström is a scientist in FOI's Department for Space Systems. His research focuses on space-based Earth observation, with an emphasis on image analysis. Before joining FOI, he did research on internal flow in freezing water droplets. He holds a PhD in Fluid Mechanics and an MSc in Space Engineering, both from Luleå University of Technology.

Alicia Fjällhed is a Researcher at FOI's Unit for Information Environment and Influence. She holds a PhD in Media and Communication Studies, specialising in strategic communication. Her research explores how communication is used as a weapon against Sweden and how it is used as part of the nation's defence. Her work specifically aims to understand how public communication changes as democratic societies move from peacetime to the presence of hybrid threats and ultimately war.

Alexander Gorgijevski is a Researcher at FOI's Section for Economic Security. He holds a PhD in International Management from Uppsala University and has served as assistant professor at Vrije Universiteit Amsterdam (International Strategy) and Linköping University (Industrial Management). His previous research focused on subsidiary initiatives, micro-politics, and headquarters–subsidiary relations. At FOI, his research spans economic security, defence policy, and how disruptive innovation shapes future defence capabilities and strategic competition, with particular relevance for Swedish and European security.

Alexander Hagelberg is a Scientist in FOI's Department for Space Systems. He holds a PhD in Multistatic Synthetic Aperture Radar (SAR) from Cranfield University. At FOI his work is focussed on space-based Intelligence, Surveillance, and Reconnaissance (ISR) and SAR image processing.

Martin Hagström is a Deputy Research Director at the Swedish Defence Research Agency (FOI). His area of expertise is autonomous systems, aeronautics, and unmanned vehicles. His latest research includes work on regulation and legal aspects of unmanned vehicles and autonomous weapon systems. Martin is the programme manager of the Autonomy and Unmanned Systems Area and responsible for supporting the Swedish Armed Forces' research planning. He has served in several different positions, currently as acting head of an autonomy department at FOI, and has participated in many international research projects.

Elin Hellquist is a Senior Analyst in FOI's Department for Security Policy and Strategic Studies. During her PhD studies at the European University Institute, and subsequently as a postdoctoral researcher at Freie Universität Berlin and Stockholm University, she examined the role of sanctions in regional and global politics. At FOI, Elin specialises in international military missions and operations. She also has a longstanding interest in regionalism, with a focus on African and European security architectures.

Maria Hultqvist is an Analyst at FOI's Department of Defence Economics, where she focuses on the defence industry, defence innovation, and materiel supply. She currently leads a research project on defence economics and materiel supply, with the Ministry of Defence as the recipient. Maria has several years of experience working in government agencies, with a focus on monitoring, statistics, and analytical work. She holds a Master of Science (MSc) in Applied Social Research from Stockholm University.

Calle Håkansson is the main editor of Strategic Outlook 11. He is a Researcher in FOI's Department for Euro-Atlantic Security Policy and is one of the editors of Strategic Outlook 11. He holds a PhD in Political Science and is also an associate research fellow at the Europe Programme of the Swedish Institute of International Affairs (UI). His research primarily focuses on European security and defence policy, with a particular emphasis on the EU's development in this field, defence industrial issues, and EU–NATO relations.

Jenny Ingemarsdotter is a Senior Researcher in FOI's Department for Supply Preparedness. She has a degree in civil engineering and a doctorate in history of science and ideas, both from Uppsala University. Her research interests involve total defence and civil defence, focusing particularly on security of supply and European preparedness.

Elin Jakobsson is a Senior Researcher in FOI's Department for Security Policy and Strategic Studies. She holds a PhD in International Relations from Stockholm University and pursued her postdoc at the Swedish Institute of International Affairs. Her previous research has focused on international norm diffusion and climate-induced migration. At FOI, she focuses on international military missions, military doctrine, and special operations forces.

Ida Johansson is one of the editors of Strategic Outlook 11. She is a Senior Scientist at FOI's Division for Defence Analysis. She holds a Master of Science in Engineering Physics and works on issues related to operational capability development, defence analysis, decision support, and civil defence. Her work includes interdisciplinary projects with a focus on methodological development and the assessment of technical and operational capabilities.

Gabriella Körling is the deputy editor of Strategic Outlook 11. She is a Researcher in FOI's Department for Global Security Policy. She holds a PhD in Cultural Anthropology from Uppsala University and has worked at Stockholm University. Her previous research focused on the relation between state, politics, and society in the Sahel, with particular expertise on Niger. At FOI, she focuses on security issues in West Africa and on the politics of external actors' engagement in Africa.

Jonas Lidman is a Research Engineer at FOI's Department for Autonomous Functions and Field Robotics. He holds an MSc in Systems, Control, and Robotics from KTH Royal Institute of Technology. His research at FOI focuses on multi-agent systems, unmanned aerial vehicles, and artificial intelligence.

Sally Longworth is a Researcher in international law at FOI's Department for Defence Analysis. She completed her LLD in October 2022 and also has an LLM from Lund University. She previously held positions at Stockholm University and the Swedish Defence University. She is currently undertaking a post-doctoral research position at Stockholm University's Center for Global Governance analysing the legal governance structure of weapons of mass destruction in international law. Her other research has focused on understanding the relationship between international human rights law, international humanitarian law, and international criminal law.

Ann Lundberg is a Senior Analyst at FOI's Department of Economic Security and currently conducts research on the defence industry and the defence market. She has several years of experience working at the Swedish Agency for Public Management and the Swedish Ministry of Defence. Previous analytical work focused on agency governance, defence investment planning, and business development. Ann has also participated in three major commissions of inquiry concerning defence during her almost 30 years of government service.

Johan Markdahl is a Senior Scientist at FOI's Department for Autonomous Functions and Field Robotics. He received a PhD degree in applied mathematics from KTH Royal Institute of Technology. After graduating, he was a postdoc researcher at the Luxembourg Centre for Systems Biology. His academic fields are control theory and mathematical physics, particularly the areas of multi-agent systems and synchronisation. At FOI, he focuses on multi-robot systems and autonomous drones, for example, the use of drone swarms in the Russo–Ukrainian war.

Carl Marklund is one of the editors of Strategic Outlook 11. He is a Researcher in FOI's Department for Supply Systems Preparedness. He holds a PhD in History from the European University Institute and has worked at the University of Helsinki, Harvard University, and Södertörn University. His previous research focused on Nordic cooperation, geopolitics, and security in the Baltic Sea region, with particular expertise on soft power. At FOI, he focuses on civil–military relations and geoeconomic security issues.

Eva Mittermaier is Deputy Research Director in FOI's Department for Civil Protection. Eva has a long career at FOI, working on various research matters concerning crisis management, societal security, and civil defence.

Samuel Neuman Bergenwall is Deputy Research Director in FOI's Department for International Security Policy. He specialises in India's security policy, but also has extensive experience studying the Middle East. Over the years, he has led FOI projects on Asia and the Middle East, security policy analysis, and future studies. He has degrees in Middle East and North Africa Studies, History, and Development Studies, and has been Research Fellow at Manohar Parrikar Institute for Defence Studies and Analyses in New Delhi.

Astrid Nilsen–Moe is a Researcher at the Department for Nuclear Weapon Threats. Her research focus is on the intersection between policy and technology when it comes to nuclear threats, arms control, and disarmament. Astrid has a PhD in Physical Chemistry from Uppsala University.

Magnus Normark is a Senior Analyst at FOI's Defence Analysis Division, Unit for Information Environment and Influence. His work is primarily focused on state threat actors (hybrid threats, weapons of mass destruction) and support to Ukraine (CBRN defence). He also has experience of research on terrorism and violent extremism as well as intelligence studies. Magnus has worked at FOI since 2002 and was previously employed by the Swedish National Defence Radio Establishment.

Max Nyström is a Research Engineer in FOI's Department for Space Domain and Threat Analysis. His research focuses on space-based observation, with an emphasis on spectral methods and large-scale satellite data management and processing. He holds an MSc in Space Engineering from Luleå University of Technology and has previously worked at the European Space Agency.

Sofia Olsson is one of the editors of Strategic Outlook 11. She is an Analyst at FOI's Department for Information Environment and Influence. She holds a master's degree in War Studies from the Swedish Defence University. At FOI, her research focus is on the information environment as a phenomenon and arena, strategic communications, arts and heritage in relation to war and conflict, and contemporary digital culture.

Björn Ottosson is a Senior Researcher at FOI's Department for Euro-Atlantic Security Policy and manages the Northern European and Transatlantic Security Programme. His work focuses primarily on US foreign, security, and defence policy, as well as transatlantic relations. His expertise also includes international relations theory, foreign policy analysis, and research methodology. In recent years, he has published studies on US–China relations, US grand strategy, and Western military capability. He holds a PhD in Political Science from Stockholm University and has previously held positions at Stockholm University, Södertörn University, and the Swedish Defence University.

Björn Erik Skovdal is one of the editors of Strategic Outlook 11. He is a Researcher at FOI's Department for Collaborative Systems and is one of the editors of Strategic Outlook 11. He holds a PhD in Physics and is currently working within the field of complex systems with a particular focus on modelling and capability analysis of ground combat.

Peter Stenumgaard is one of the editors of Strategic Outlook 11. He is a Research Portfolio Coordinator at FOI's Executive Management Office, Office for R&D, and is one of the editors of Strategic Outlook 11. He holds a PhD in Radio Communication Systems and is currently FOI's coordinator of the European Defence Fund (EDF). He has long experience of research and management and has also been an adjunct professor at both Linköping University and the University of Gävle.

Benjamin Ståhl is a Senior Analyst in FOI's Department for Foresight. He has particular expertise in analysing strategic dependencies in industrial and mineral supply chains, including localisation dynamics and their implications for the development of emerging technologies. At FOI, his research focuses on strategic foresight, technology assessment, and economic security. He holds an MA in International Relations from the University of Kent and a PhD in Economics from Uppsala University.

Ola Svenonius is Deputy Research Director and Research Coordinator at the Unit for Information Environment and Influence at FOI. His research focuses on psychological defence, hybrid threats, and societal resilience, with a special interest in the public's willingness to defend. He manages projects in these areas for the Ministry of Defence and the Swedish Civil Defence and Resilience Agency, among others. Svenonius received his PhD in Political Science from Stockholm University in 2012 and has worked at FOI since 2018.

Ulf Söderman is a Deputy Research Director at FOI's Division of Cyber Defence and C2 Technology, Department of Sensor Networks and Information Systems. His main interest is geoinformatics with a focus on new types of geographic information in 3D and their application to Swedish defence. He has previously worked on 3D terrain mapping and the production of digital 3D terrain models. He has also worked as CEO of a start-up company in forest analysis and inventory using laser scanning. He has an MSc in Computer Science and Engineering and a PhD in Computer Science from the Institute of Technology at Linköping University.

Karl Sörenson (PhD) is the Deputy Research Director at the Strategy and Policy Department at the Swedish Defence Research Agency (FOI), where he heads the Nuclear Weapons Analysis Programme. Sörenson is also a researcher at the Swedish Defence University (FHS) Department for Naval Operations. Sörenson's PhD dissertation, defended at the Royal Institute of Technology (KTH), treated game-theoretic analysis of deterrence with bounded rationality and appli-

cations to military operations. Sörenson's research has focused on nuclear strategy, deterrence, and game theory as well as sea power and naval operations.

Hampus Thorell is Deputy Research Director at the Department for Electronic Warfare Radio Communications Attack Systems. His work focuses on research in electronic warfare and development of electronic warfare capabilities. He holds an MSc in Applied Physics and Electrical Engineering from Linköping University.

Emil Wannheden is an Analyst in FOI's Department for Security Policy and Strategic Studies and deputy head of the Russia and Eurasia Studies Programme. He holds an MSc in Development Economics from the University of Florence and has previously worked as a diplomat for the Ministry for Foreign Affairs of Sweden. Emil's research focuses on Russia's economy and security policy, especially the evolution of Russia's wartime economy, its military expenditure, and the effects of sanctions.

Christopher Weidacher Hsiung is one of the editors of Strategic Outlook 11. He is a Senior Researcher in the Department for Global Security Policy at the Swedish Defense Research Agency (FOI). His research interests include international relations theory, East Asian affairs, Chinese foreign and security policy, Sino–Russian relations, and nuclear strategy with a focus on China. His previous work experience includes positions at the Norwegian Institute for Defence Studies (IFS) and the Embassy of Sweden in Beijing. He holds a PhD in Political Science from the University of Oslo, has been a visiting scholar at Peking University's School of International Studies (SIS), and has studied Chinese language in Beijing, Taipei, and Wuhan.

Mathias Winterdahl is an Analyst at the Department for Branch Capability Development at FOI. His current research interests include, among other things, risks associated with open geodata, the influence of climate change on security of supply, and uncertainty analysis. Mathias holds a PhD in Environmental Assessment from the Swedish University of Agricultural Sciences and has previously studied the production, transport, and degradation of natural organic matter in soils and running waters.

Anna Maria Wårlind is Head of the Space Domain and Threat Analysis Department in the Division of Defence Technology at FOI. She is a specialist in space law, policy, and strategy and has a long background in intergovernmental affairs. Before joining FOI, she was Head of Legal and International Affairs at the Swedish National Space Agency, a Swedish delegate to the ESA International Relations Committee, and served as Chair of the Esrange consultation forum. Anna Maria holds a Master of Laws (LLM) degree from Lund University.

About FOI's Strategic Outlook

FOI's Strategic Outlook is a cross-divisional, forward-looking series of compilation reports first published in 2009. Each volume is structured around essay-style articles written without formal references to ensure an accessible read while addressing complex security and defence issues. The overall aim of the Strategic Outlook series is to showcase FOI's broad expertise while contributing to knowledge dissemination in the defence and security policy debate. This year's volume is the eleventh in the series.

Previous reports:

Strategisk utblick 2009: Säkerhetspolitisk forsränning?
Strategisk utblick 2010: Säkerhetspolitisk nattorientering?
Strategisk utblick 2011
Strategisk utblick 2012
Strategisk utblick 2013
Strategisk utblick 6 (2015)
Strategisk utblick 7: Perspectives on national security in a new security environment (2017)
Strategisk Utblick 8: Totalförsvarets tillväxt – utmaningar och möjligheter (2019)
Strategisk utblick 9: Framtida hot (2021)
Strategic Outlook 10: China as a Global Power (2024)

Acknowledgments

The editors express their gratitude for the support received from FOI's management, particularly the Defence Analysis Division. They are also very grateful to Richard Langlais for his excellent work in language editing across all articles. The layout was superbly designed by Karin Blext, and FOI's Research Support and Administration Division did outstanding work in finalising the publication. Finally, the editors are deeply grateful to all contributors for providing such well-written and important articles, as well as to internal and external reviewers for their valuable input.

This eleventh editon of FOI's Strategic Outlook expores a world marked by intensifying great-power rivalry, eroding international norms, technological competition, economic fragmentation, and rising geopolitical uncertainty. As the international order faces mounting pressure from war, coercion, and strategic competition, states are being forced to adapt to a more volatile and less predictable global environment. The anthology examines developments in security policy, societal security, defence, and technology. Drawing on FOI's unique competence and broad research expertise, it brings together a wide range of perspectives and analyses that help us understand how a changing world order is reshaping international security and strategic affairs.

The Swedish Defence Research Agency (FOI) is a government agency that conducts world-renowned research in the fields of defence and security. Our mission is to generate knowledge and provide specialist support, based on the latest research, to strengthen Sweden's military and civil defence and contribute to their continued development and innovation.

FOI

ISSN 1650-1942

www.foi.se