BALTIC RIM ECONOMIES

Intelligence & Foresight

January 2026
ISSUE no. 1

VALENTYN NALYVAICHENKO
Ukraine's NATO & EU path unchanged

JUHA VAUHKONEN
The strategic importance of Finland's neighboring regions and the growing security challenges

SIR DAVID OMAND
The enduring value of secret intelligence

MARKKU PAJUNIEMI
The Baltic Sea – A sea of war and peace

CENTRUM BALTICUM

To receive a free copy, register at
www.centrumbalticum.org/en

BALTIC RIM ECONOMIES

The Centrum Balticum Foundation publishes the Baltic Rim Economies (BRE) review which deals with the development of the Baltic Sea region.

In the BRE review, public and corporate decision makers, representatives of Academia, as well as several other experts contribute to the discussion.

Centrum Balticum

ISSN 1459-9759

Editor-in-Chief | Kari Liuhto
(responsible for writer invitations)

Technical Editor |
Salla Mattila

Centrum Balticum
Vanha Suurtori 7
FI-20500 TURKU, Finland

www.centrumbalticum.org/en

centrumbalticum@centrumbalticum.org

Data protection description

EXPERT ARTICLES

EXPERT ARTICLES

EXPERT ARTICLES

Centrum Balticum

BALTIC RIM ECONOMIES

To receive a free copy,
register at
www.centrumbalticum.org/en

The 18th Baltic Sea Region Forum is organised on **Monday**, **May 4**, **2026**, at the University of Turku with the theme **Security in Northern Europe and the Arctic**.

We welcome you to join the audience in Turku or to follow the event online.

See the programme and register now:

The event page for the Baltic Sea Region Forum 2026

MATS LÖFSTRÖM

Intelligence as a pillar of security in the Baltic Sea Region

Expert article • 3906

The importance of high-quality intelligence has never been as widely acknowledged in the public domain as it is today. Intelligence services traditionally operate discreetly, with much of their work being necessarily concealed.

While this fundamental characteristic remains, intelligence agencies have in recent years adopted a more open posture. In Finland, both the Security and Intelligence Service, SUPO, and the Defence Intelligence Agency now publish a public National Security Overview and a Military Intelligence Review.

Two years ago, despite the discussion being held under Chatham House rules, Norway and Estonia participated with the head of SUPO in an open discussion at the Helsinki Security Forum. In London, the heads of MI6 and the CIA took part—for the first time ever—in a publicly broadcast conversation arranged by the Financial Times.

Perhaps the most consequential instance of transparency was the decision by the United States and the United Kingdom to issue public warnings and disclose intelligence information regarding Russia's preparations for a full-scale invasion of Ukraine in 2022.

Greater openness by official state actors contributes to strengthening situational awareness within society at large. This is particularly important in an era of rapidly expanding open-source intelligence, exemplified by Bellingcat's exposure of Russia's responsibility for the downing of Malaysia Airlines flight MH17 over Ukraine. At the same time, open-source channels are also exploited to disseminate disinformation and create confusion. In this context, a measured degree of transparency from our intelligence community is both justified and beneficial.

Beyond their traditional mandates, collecting information for political and military decision-makers, countering foreign intelligence activities, anti-terrorism activities and now defending against hybrid threats, intelligence services also play a vital role in building societal resilience in today's complex world. Crucially, they should be able to provide early warning of military threats, enabling states to take preparatory measures, as Ukraine did follow the warnings it received prior to Russia's invasion.

The war in Ukraine has brought into sharp public focus the indispensable role of intelligence in both defensive and offensive operations. Ukraine's partnership with Western intelligence communities has been of decisive importance.

International cooperation is likewise fundamental to Finland's intelligence activities. With Finland and Sweden now full members of NATO, intelligence cooperation among Allies has intensified. Finland seeks to be a net contributor to security within the Alliance, including in the intelligence domain. Finland's intelligence community is a highly respected actor by international partners and is perceived to have strong capabilities. Our closest partnerships remain with the Nordic countries, which collectively enhance stability and security throughout the Baltic Sea region.

The United States is also a key partner for Finland, possessing the world's strongest intelligence capabilities. In October, the Finnish Parliament's Intelligence Oversight Committee therefore visited Washington to engage with representatives of the US intelligence community, to have a historic meeting with the US Senate Select Committee on Intelligence and meeting ten US senators.

International cooperation has also broadened in the sphere of oversight. All democratic societies require effective oversight mechanisms. While intelligence is indispensable, particularly in the current security environment, oversight plays an important role in ensuring that activities are conducted lawfully and appropriately.

Its purpose is not to constrain intelligence agencies, but to safeguard legality, accountability, and public trust. Should legal adjustments be required, responsibility rests with Parliament. As strong advocates of the rules-based international order, we recognize that oversight is essential to its integrity.

Since the reform of Finland's intelligence legislation, the national oversight system has functioned effectively. The oversight committee and ombudsman maintain structured dialogue with the agencies, its members hold the necessary security clearances, and meetings are conducted in secure facilities. Finland's model for oversight has also served as a reference in other countries, in for example Lithuania.

This year in September, Parliament of Finland will host—for the first time—the Nordic Conference on Intelligence Oversight, which convenes biennially. Together with our Nordic partners, we have decided to invite the Baltic states as participants for the first time. This reflects our shared commitment to strengthening cooperation across the Baltic Sea region, where intelligence plays a pivotal role in ensuring safety and stability.

Mats Löfström
Chairman
Intelligence Oversight Committee
Parliament of Finland

VALENTYN NALYVAICHENKO

Ukraine's NATO & EU path unchanged

Expert article • 3907

After the Revolution of Dignity, Ukraine made a choice that cannot be reversed — the path toward the European Union and NATO. This is not a slogan, but a strategic decision born of pain, experience, and the understanding that independence cannot exist without a system of security. The price of this choice has been extraordinarily high. And the responsibility to preserve this course — despite war, corruption, and external pressure — rests on our intelligence and security institutions.

A devastated Security Service of Ukraine

When I first entered the headquarters of the Security Service of Ukraine (SBU) in 2014, after the Revolution of Dignity, I found an empty building — no light, no staff, no leadership. The courtyard was still smoldering with burned documents; inside were the traces of a chaotic escape. Russian intelligence operated openly in Kyiv, with access to Ukrainian databases, defense documents, and personal information.

We had to start almost from nothing — recruiting new officers, rebuilding counterintelligence and cyber defense, and restoring public trust.

Building a new security architecture

From the first days of Russian aggression, we relied on the support of our Western partners. The United States — the CIA, the FBI — and NATO member states extended their helping hand. Together, we built a new architecture of security: joint training programs, analytical exchange, cyber operations, and counterterrorism initiatives.

This cooperation became the foundation of Ukraine's modern security system — the framework that sustains our country amid full-scale war. It has greatly enhanced and strengthened our national resilience.

I am convinced that we must continue this partnership, deepen it, and move forward — especially now, as Ukraine confronts Russia's full-scale aggression, with missiles, drones, and ground forces used as instruments of terror against our independence.

Meeting modern security demands

We must fully abandon the Soviet model — in which security services were tools of political pressure — and transform them into institutions that perform counterintelligence and analytical functions strictly within the rule of law.

This means building analytical capacity, strengthening cyber defense, and ensuring international interoperability — conditions that make Ukrainian security institutions reliable partners for NATO and a true guarantor of safety for Ukrainian society.

Intelligence reform and the renewal of the SBU are key elements of our movement toward NATO. The Alliance is not only about military power; it is about high standards, strategy, coordination, and operational coherence. To stand as an equal partner, we must internalize and apply those very standards.

The strength of our intelligence

Meanwhile, Russia continues to rely on the same old methods I observed long before 2014 — espionage, cyberattacks, and information warfare. Its goal is not only the destruction of infrastructure, but also the corrosion of truth, trust, and unity.

That is why the true strength of our intelligence today lies not merely in countering enemy agents, but in anticipating where and how the adversary will attempt to shape public perception.

During this war, Ukrainian intelligence has become an integral part of the global security system. We share intelligence with our partners, expose Russian spy networks across Europe, and document war crimes. Ukrainian analysts are already contributing to the strategic decisions of our allies.

Our course remains steadfast because it rests not only on political will, but on the professionalism of those who defend the state every day. The Armed Forces of Ukraine, the Security Service of Ukraine, and our intelligence community together form the backbone of Ukraine's Euro-Atlantic integration — not as an abstract aspiration, but as a living, evolving process.

Ukraine as the outpost of European security

For me personally, this mission began more than a decade ago — to make Ukraine part of a world where freedom, security, and the rule of law are held in the highest regard.

Today, Ukraine stands as the outpost of democracy — holding the line against terrorism, cyberattacks, and aggression, defending the free world.

We will not turn back. Our goal is not only to win the war, but to build a state where the law serves its citizens and guarantees their rights, protection, and safety.

That is the true strength of Ukraine. And it is this that proves: our course toward NATO and the European Union will remain unchanged.

Valentyn Nalyvaichenko
Ex-Head of the SSU, MP
Secretary of the Committee on Ukraine's Integration into the EU
Co-Chair of the Group of the Verkhovna Rada of Ukraine on inter-parliamentary relations with the Republic of Finland
Ukraine

ILKKA SALMI

The European Commission security landscape: From technocratic executive to geopolitical actor

Expert article • 3908

The turn towards security, defence and preparedness

For most of its history, the European Commission was seen as a technocratic machine, driving European integration. Students graduating from degrees in European law mastered competition law, the integration of the Single Market and the Economic and Monetary Union. Yet the last years, the world around the European Commission has changed dramatically, forcing the primary economic executive to become a geopolitical actor that is navigating an increasingly complex and hostile world.

The Russian war of aggression against Ukraine marked a defining shift and rupture in the EU's strategic environment. The EU's response, spearheaded by the European Commission, reflected the unity between EU's Member States and strengthened the role of the Union on questions related to hard security. Prospects of enlargement were reenergised while the Russian sanctions regime has grown into a tool of EU policy making.

Two fundamental changes occurred that have underpinned this transformation of the European Commission into a vocal geopolitical player. Firstly, instruments long regarded as purely tools of integration find itself now at the centre of broader conversations about war, deterrence and geopolitical competition. While this framing might be new, many of the underlying work strands have been at the centre of the Commission's power for years. Sanctions, tariffs and export controls have always been geopolitical instruments but now existing policies have acquired new meaning.

Secondly, this geopolitical shift has been reflected in the new political priorities of the second term of Von Der Leyen as the President of the European Commission. Under the umbrella of 'a new era for European defence and security', terms like preparedness, resilience and defence industry have become central to the Commissions rhetoric and policy priorities. The publication of the so-called Niinistö report provided the European Commission with a comprehensive blueprint articulating a new vision for societal preparedness and resilience. With a wide and ambitious scope, it argues for a paradigm shift in the way EU approaches security, away from the more common method of integration through incremental fixes.

The Niinistö report laid the foundation for three major Commission initiatives that signal this institutional shift around security:

1. **ProtectEU/Internal Security Strategy**, which aims to consolidate the Union's ability to detect, deter and mitigate threats from hybrid actors, organised crime or terrorism.
2. **The White Paper on Defence**, exploring how the EU can mobilise industrial, financial and regulatory instruments to support Europe's defence industry.
3. **The Preparedness Union Strategy**, a forward-looking strategy for long-term societal resilience against health emergencies, climate change and hybrid interference.

Together, these initiatives provide a clear framework wherein the Commission is actively defining and claiming its role as the protector of the European project and the EU at large.

The key challenge: information for decision-making

This shift in the political orientation of the Commission raises a fundamental question: does the Commission have access to the right information to take informed decisions on security, defence and preparedness?

Although today's geopolitical environment is almost unrecognizable compared with five years ago, the structures of EU's intelligence-sharing architecture, defined by the limits set out in the treaties on member states' responsibilities on national security, remain fundamentally unchanged. Nevertheless, the most senior levels of the Commission, those taking decisions on sanctions packages, crisis response or defence industries, require more than ever timely and actionable strategic intelligence.

A sharpening of the current mechanisms for information-sharing and situational awareness is therefore a necessity. The Commission's evolving role cannot be sustained based on structures designed for a different era. In this regard, the announcement of the 'Security College' by President Von Der Leyen in March 2025, provides us with a possible blueprint for the way forward. From external and internal security to energy, defence and research to cyber, trade and foreign interference, the Security College meetings carve out a dedicated moment for the College to obtain a joint situational awareness about the security environment that increasingly negatively impacts the daily work of the institution.

Towards a truly geopolitical European Commission

The European Commission faces unprecedented challenges. Its policies and ambitions have adapted accordingly. The task ahead is to consolidate this transformation and to ensure that the Commission has the tools and the information to act decisively.

Europe's security landscape has shifted. It is time that the Commission is also equipped for the role it is increasingly expected to play.

Ilkka Salmi
Deputy Director-General in charge of Security, Workplace and Wellbeing Directorate-General Human Resources and Security of the European Commission

Former Counter-Terrorism Coordinator of the EU, Director of EU INTCEN and Director of the Finnish Security and Intelligence Service SUPO

JUHA MARTELIUS & KARI LAITINEN

Information, intelligence and national security

Expert article • 3909

National security is in a constant state of flux. While national interests rarely change, threats to those interests do. National security and intelligence are increasingly intertwined. Threats and change will dominate our national security landscape for a long time to come, as the operating environment remains highly unstable. The task of the Finnish Security and Intelligence Service is to serve the highest levels of national government. This means a constant need to develop expertise in these areas, with national security and intelligence-led management at the heart of activities.

We are living exceptionally uncertain times, and it is particularly difficult to predict what the future will look like. The world may never have been so complex and hazy as it is now. With the competition between great powers and tensions between states, the importance of intelligence has long been emphasized in the support for the Finnish Government's decision-making in issues relating to national security. It is no coincidence that several European countries have strengthened their national security management and intelligence capabilities.

As the security environment becomes increasingly alarming and national security management more complex, administrative structures, processes and, for example, performance management are also facing a world in which increasingly complex threat scenarios are more difficult to define. From the perspective of foresight and intelligence, this is a significant challenge, and highlights the importance of responsible, proactive, and intelligence-led national security management. Scattered and fragmented action is not responsible policy, let alone conducive to national security.

The importance of intelligence and foresight, as well as intelligence-led management, are emphasized in the national security sector. This applies in particular to the Finnish Security and Intelligence Service, whose core processes and activities are built around data. In anticipating the future, increasingly better information management and intelligence-led management are needed, and not only within our Service. This places considerable demands on the top-level national government and public administration, and thus on security authorities, in terms of expertise and development as well as resources and recruitment.

Due to the challenges of the security environment, we need a broader and deeper intelligence base to support decision-making related to national security and foreign and security policy. Technological development poses its own challenges for national security management. Disruptive technologies create both opportunities and challenges. In the national security and intelligence context, artificial intelligence, quantum computing, 6G technology, and the location of cloud services are factors for which national solutions must be found.

An increasingly challenging issue is related to economic security. Global markets, financial flows, corporate acquisitions, economic partners, and research and innovation activities require foresight and intelligence. Thus, from the perspective of national interests and protecting national security, a multifaceted challenge is posed by strategic dependencies or, on the other hand, the goal of strategic autonomy. It is clear that Finnish national resources are not sufficient for complete self-sufficiency, nor should this naturally be the goal. On the other hand, it is clear that we must be able to understand the vulnerabilities of national interests and thus create long-term guidelines and promote strategic autonomy.

We need better-managed processes that take national security issues into account as comprehensively as possible. It is also important that we develop national intelligence activity and intelligence legislation so that we are better able to respond to the increased demands and changes in the operating environment. Actors identified as critical must take into account the national security strategy, national risk assessment, their own risk assessments, and threat information shared by the competent authorities when implementing measures to increase crisis resilience in their own activities.

The task of security and intelligence services is to provide information that enables countries to navigate the future. The current security landscape also challenges the way we define counter-intelligence and counter-terrorism, and how we scale and measure these threats. The lines between terrorism, influence operations by states, intelligence, and organized crime are increasingly blurred. This demands not only change in the culture within our Service but also in the way we work with our domestic and international partners. Our changing security environment will not wait.

Juha Martelius
Ph.D, Director
Finnish Security and Intelligence Service
Finland

Kari Laitinen
Dr.Soc.Sc., Senior Adviser
Finnish Security and Intelligence Service
Finland

ARNOLD SINISALU

Strategic shifts in Estonia's national security architecture following the 2007 Bronze Soldier riots

Expert article • 3910

The April 2007 unrest in Estonia—commonly referred to as the Bronze Soldier riots—marked a pivotal moment in the country's national security discourse. While the events themselves are widely known and require little elaboration, their implications for Estonia's strategic analysis and institutional security frameworks were profound.

Transformation in strategic analysis

Prior to 2007, Estonia's security planning predominantly emphasized conventional military threats and geopolitical risks. The Bronze Soldier crisis, however, revealed the multidimensional nature of modern conflict. The unrest was not limited to physical demonstrations but included coordinated cyber-attacks and disinformation campaigns, underscoring the emergence of hybrid threats. These threats combine kinetic and non-kinetic tactics—cyber operations, propaganda, and economic coercion—to destabilize target states.

In response, Estonia broadened its strategic analysis to incorporate hybrid threat modeling, early warning systems, and resilience planning. The emphasis shifted toward cross-domain risk assessment, including vulnerabilities in societal trust, political cohesion, and digital infrastructure. This evolution positioned Estonia as a pioneer in conceptualizing and countering hybrid warfare.

Reform of the Government Security Committee

Parallel to the shift in strategic thinking, the Estonian Government Security Committee underwent significant reform. Formerly focused on coordinating executive agencies in national defense planning, the committee redefined its mandate to address the complexities of hybrid conflict. According to the official description, the committee now:

- Coordinates intelligence and defense activities across agencies.
- Develops strategic documents on national defense and security policy.
- Oversees the collection and analysis of security-relevant information.
- Manages classified data protection and inter-agency cooperation.[1]

These reforms enhanced inter-agency coordination, particularly among intelligence, defense, and cyber experts, enabling faster and more integrated responses to emerging threats. The committee's structure now reflects a holistic approach to national security, balancing traditional defense with digital and societal resilience.

Broader implications and case study

The post-2007 security posture also fostered public–private partnerships in cyber defense and established robust early warning mechanisms. Estonia's experience has informed international discourse on hybrid warfare, especially among Baltic and Nordic states.

A notable example illustrating Estonia's counter-hybrid strategy is the 2023 conviction of Sergei Seredenko. He was sentenced to five years and six months for collaborating with Russian intelligence services. The Supreme Court found that **his activities aligned with Russia's influence tactics and could serve as preparatory steps for military aggression or territorial occupation**. Although his writings did not pose a direct threat, the court ruled that his actions fell outside the bounds of protected speech due to their intent and nature. This case reinforces Estonia's legal and institutional commitment to countering foreign malign influence.

Conclusion

The Bronze Soldier riots catalyzed a paradigm shift in Estonia's national security strategy. By integrating hybrid threat analysis and reforming its security governance structures, Estonia has enhanced its resilience and set a benchmark for democratic states navigating the complexities of 21st-century conflict.

[1] https://www.riigikantselei.ee/en/supporting-government-and-prime-minister/councils-and-comittees/government-security-committee (15.08.2025).

Arnold Sinisalu
Ph.D. (Law), Visiting Professor of Security Politics
Johan Skytte Institute of Political Studies
University of Tartu
Estonia

Director General of Internal Security Service of the Republic of Estonia (2013-2023)

ANJA DALGAARD-NIELSEN

Diversity in intelligence agencies: Three reasons why we need more, not less

Expert article • 3911

The Trump administration has endeavored to push back equity, diversity and inclusion (DEI) programs in the federal US government and The White House has made it clear, that the US intelligence community (IC) is in scope. Though the evidence is patchy, news reporting and court files indicate that at least some programs, offices and initiatives are being rolled back.[1]

While DEI programs are under pressure on the other side of the Atlantic, European intelligence services would be well advised to redouble their efforts to promote staff diversity, specifically gender diversity.[2] This article argues why, drawing on extant research on diversity and organizational performance and a small internal survey carried out in the Danish Defence Intelligence Service (DDIS).

Busting the James Bond myth

In 2022, the DDIS ran a number of adds on social media. One of them featured a picture of an unglamorous family car and the text: "If you can remain calm as the kids fight on the backseat, maybe you have what it takes to become one of our new case officers".

The messaging and the untraditional communication channel were intended to debunk the myth, that case officers had to be James Bond-type action heroes and attract a broader and more diverse group of applicants.

Human and military intelligence have traditionally been male dominated disciplines.[3] This is also true when it comes to the DDIS, which grew out of the Danish Armed Forces in the wake of World War II, and remains organizationally anchored to the Danish Defence.[4]

Previous recruitment drives tended to generate a field of highly motivated and skilled, yet predominantly male, candidates with a background in the armed forces. The idea behind the 2022 campaign was simple: The more internal diversity in the cadre of case officers, the greater the chance to match operational opportunities to exactly the right internal profiles and skill sets.

Arguably, however, the potential organizational benefits are broader and not just in the HUMINT discipline.

How gender diversity improves organizational performance

In 2022, the author of this article carried out a small survey to collect perspectives of female and other minority DDIS staff on the role of diversity in organizational performance. The survey was intended to inform management thinking on recruitment and retainment and to feed ideas into the broader HR-strategies.[5] The questions focused on the respondents' personal experiences with representing a (gender) minority in their workplace and on their perception of whether greater diversity had an impact on the way their unit or team approached its daily tasks.

Almost every respondent provided rich accounts, shared anecdotes from daily life, and were vocal about their ideas and wishes for the future. It was evident from the accounts, that several respondents had had long careers in the DDIS and were able to describe the changes they had experienced over time, as the number of female staff grew.

Across from the accounts, three cross-cutting themes were evident: The respondents registered a better work climate, stronger bias check, and better problem solving as the gender diversity of their workplace increased.

First, several respondents took care to underline, that they had never personally experienced harassment due to their gender. Yet, they also related how the presence of more female colleagues had contributed to a, in their estimation, more inclusive culture and a decline in "locker-room jargon".

While an inclusive work environment is likely to be beneficial to staff retention and possibly to staff performance, the second cross-cutting theme spoke directly to a core imperative for intelligence services: Strive to check your bias! The respondents related how, in their experience, more diverse teams were less inclined to think alike and thus less in danger of falling into the trap of groupthink.

Finally, and related to the two previous themes, respondents also indicated that more diversity made for better problem-solving in cases where complexity or novelty challenged existing approaches.

The internal survey was small and obviously not representative. Since responses were written to ensure anonymity, the interviewer had no chance to probe and question the causality of connections suggested by the respondents, ask for additional examples etc.

Yet, extant research in the field of decision making theory, organizational innovation, and organizational performance indicate the same connections as the ones pointed out by the respondents.

Diversity can increase the level of conflict within a group, but it is also a broadly recognized means to improve the quality of analysis and decision-making. Small, heterogeneous groups, where group members feel safe to speak up ensure that more experiences and perspectives are brought to the table and help reduce the risk of group think – a phenomenon by which a group places internal harmony above analytical stringency and avoids asking hard questions – as well as the risk of other analytical fallacies.[6]

Though extant research is ambiguous about the relationship between small group diversity and creativity, it has shown a positive connection between demographic diversity, including gender diversity, and innovation at the organizational level.[7] There is also evidence, that more diverse private sector companies tend to perform more strongly on indicators such as earnings, market value, rentability, and ability to expand into new markets.[8]

In sum, though the internal DDIS survey is small, extant research rhymes with the respondents' accounts: Diversity, better bias-check and stronger problem solving abilities go together.

Attracting a diversity of talent

How do traditionally male-dominated organizations attract a more diverse range of talent? Popular myths and limits to how open an intelligence service can be about its assets and staff may compromise their ability to convince women that they would fit in.

The "Berlingo-adds" of the 2022 DDIS recruitment drive is one example of how to work around such constraints. While the backdrop of Russia's full scale invasion of Ukraine might have played a mobilizing role as well, never before in the recent history of the Service did a posting attract such a large and broad group of applicants, counting 3.400 individuals.[9] At the end of the monthlong internal process of testing, training, and selecting, a new group of case officers could join the ranks, significantly increasing the corps' degree of diversity in terms of gender, age, personal and educational backgrounds.

Three reasons to strive for more diversity

Organizational diversity and inclusion programs have faced political head winds from across the Atlantic.

Yet, arguably, any intelligence service that cares about operational and organizational excellency should strive for more, not less gender diversity. A small internal DDIS survey indicates that diversity rhymes with a better work place culture and extant research underlines that it goes with stronger bias check and more innovation. The DDIS's 2022 recruitment drive simultaneously illustrates, that alternative messaging and social media channels can enable intelligence agencies to cut through popular myths about what an intelligence officer looks like and attract a broader variety of talent to compete for open positions.

[1]Reuters, "US Judge blocks firing of intelligence officers assigned to DEIA programs," 01.04.2025.

[2]Organizational diversity have multiple dimensions such as demographic, cultural, social, cognitive, religious, educational etc. The focus in this article is on gender diversity. From a practical point of view this is a dimension that most organizations can track and arguably a good place to start in the quest for a work environment, which is more inclusive also towards other minority groups.

[3] For carefully researched historical accounts of the role of women in human intelligence and military intelligence, see Liza Mundy, 2023, "The Sisterhood. The Secret History of Women at the CIA", Gloustershire: History Press; Trine E. Michelsen, 2021, "Storfyrstinden", Copenhagen: People's Press.

[4]"Intelligence Outlook 2024", Copenhagen: DDIS, pp. 6-7, available on https://www.fe-ddis.dk/en/produkter/Risk_assessment/riskassessment/Intelligenceoutlook2024/

[5]The sample was generated via a simple snowballing technique and consisted of short, open-ended questions to which the respondents provided written responses. Fourteen staff members contributed, all were anonymous. All respondents were asked for permission to use the results in this article. None objected.

[6] I. L. Janis, 1973, "Groupthink and Group Dynamics," Policy Studies Journal, 2: 1, pp. 19-25; R. J. Heuer, 2008, Small Group Processes for Intelligence Analysis, Report prepared for the Sherman Kent School, available at https://pherson.org/wp-content/uploads/2013/06/02.-Small-Group-Processes.pdf

[7] A. Hundschell et. al, 2022, "The Effects of Diversity on Creativity: A Literature Review and Synthesis," Applied Psychology, 71, 4: pp. 1598-1634.

[8] For a summary of this research, see P. Luthra and S.L. Muhr, 2023, Leading through Bias, Palgrave Macmillan, p. 49.

[9] DDIS, Indblik, Beretning 2021-2022, DDIS: Copenhagen, p. 59, available at https://www.fe-ddis.dk/da/produkter/beretning/beretningsarkiv/beretning-2021-2022/

The author is grateful to DDIS staff, who participated in the internal survey and to Annemarie Peen Rodt for helpful comments on this article.

Anja Dalgaard-Nielsen
Director of Intelligence (May 2021-May 2025)
Danish Defence Intelligence Service
Denmark

NORBERT LOBA

This is not the time to create illusions of security

Expert article • 3912

In November 2025, information appeared in the public domain about the idea of creating a new intelligence structure (institution) within the European Commission. The concept proposed by Commission President Ursula von der Leyen would involve the establishment of a unit within the Commission's Secretariat-General to collect and coordinate intelligence gathered by the national services of Member States and existing EU structures.

This proposal should be seen as yet another manifestation of the EU bureaucracy's efforts to create a transnational structure (in the very important but extremely sensitive area of national security), which is conceptually and organizationally dysfunctional and therefore extremely limited in its capabilities and, as a result, ineffective and even dangerous due to the risks that will arise around it.

What arguments and facts support this assessment?

1. Lack of sufficient trust between EU member states – the activities of (special services) in the field of intelligence and security are based on limited trust and secrecy, as well as the need-to-know rule. Any country that takes its internal and external security seriously is reluctant to share data from its special services, even with its allies, and does so only to a very limited extent (cooperation in the fight against terrorism is an exception to some extent). It is therefore difficult to imagine EU countries passing on truly important and sensitive information to EU "intelligence" structures over which they do not have full control and which they cannot fully trust.

2. Risk of information leaks – the more countries (and their institutions) involved in the circulation of intelligence data, the greater the risk of secret information being disclosed to enemies (or even to "partner" services for their individual needs and benefits). Such leaks could have disastrous consequences for the security of each of the participants (countries) involved in the project. It should also be added that the state structures of some European countries are, unfortunately, much less resistant to infiltration by hostile intelligence services – e.g., the Russian Federation or China.

3. Conflict of competence within existing international structures – the EU already has an entity with similar competences (but limited effectiveness) - the Intelligence and Situation Centre (IntCen) within the European External Action Service (EEAS), which performs a similar role – it analyzes the analytical data obtained and supports the decisions of EU institutions. In fact, IntCen officials openly oppose the concept of a new intelligence unit, as it would duplicate activities and disperse limited resources, exacerbating chaos in this area. Similarly, President Ursula von der Leyen's concept could have a negative impact on intelligence cooperation within NATO (to which most EU countries belong). The North Atlantic Treaty Organization has much more efficient and realistic mechanisms and structures capable of exchanging intelligence, especially in the military sphere. Duplication of such entities could, among other things, weaken transatlantic cooperation and generate unnecessary tensions, especially with the US.

4. Risk of politicization – an EU intelligence unit could become a political tool, and its supervisory dependence on the European Commission (or the influence of the European Parliament) could limit its analytical independence. There is a very real and high risk that those managing of such an entity at a given time will create and impose the directions and substantive (practical) results of the final analytical products produced.

5. Last but not least, legal issues and data protection – the proposed concept could violate national sovereignty, as according to EU treaties, national security (including in the institutional context and the functioning of special services) remains the exclusive competence of Member States. Furthermore, any joint intelligence activities (also based on classified data) would require the harmonization of regulations on classified information and other legal solutions related to the use of such specific and sensitive knowledge.

In conclusion, the idea of establishing a new intelligence unit within the EU structures is unrealistic and potentially harmful. In the short term, it can only serve as a symbolic and apparent declaration of the will to integrate, which is politically advantageous for the current leadership of the European Commission and its political base, among other things in the face of criticism of the weakness of the EU as an institution (but also of specific member states) towards Russia in the past and at present. Pushing for such a solution would result in the creation of yet another ineffective entity (institution), wasting EU funds, creating inconsistency and misunderstandings, and posing serious counterintelligence threats.

Norbert Loba
President of the Board
FRONTLINE FOUNDATION
Poland

loba@frontlinefoundation.eu

JOSEPH WIPPL

Intelligence and National Security

Expert article • 3913

Intelligence is a component employed on behalf of National Security. These two words, intelligence and National Security have different meanings. The meaning of intelligence is straightforward and is objective. Intelligence means information and the analysis of information for the purpose of either understanding a problem or issue and/or taking an action based on that information. All intelligence is information but not all information is intelligence. Intelligence as a component of National Security is generally limited to the sovereign political state. The sources of Intelligence for governments are 1) Open Source, information gathered from the always proliferating public domain, 2) Human Source, information gathered secretly or semi-secretly from recruited, controlled agents and cooperating contacts, 3) Signal Source, information gathered through the monitoring of communications, 4) Imagery Source, information gathered through photography 5) Measurement Source, information gathered through the signatures of materials. These sources of intelligence are funneled together to produce a product of facts and analysis for those political leaders making decisions.

National Security is a subjective concept which can have multiple meanings, depending on how and when this concept is used. On its most basic level, National Security is about keeping the citizenry of a country safe from foreign threats of violence, invasion or subversion. Beyond that, the definition becomes murkier. Anyone can make almost anything a threat to National Security. After the Al Qaeda terrorist attacks against the World Trade Center and the Pentagon on 9/11, the political reaction included viewpoints describing Al Qaeda terrorism as a threat to the existence of the United States. The attacks definitely were a threat to American lives and property, and the government of the United States is constituted for the purpose of protecting American lives and property, however, the attacks did not threaten the existence of the government. Threats can be exploited by politicians, sometimes rightly, sometimes wrongly, to galvanize the population in favor of a political agenda.

What the policymaker would most like to have from intelligence is a warning about events which are about to happen. In other words, the policymaker does not want to be surprised because she/he does not want to be embarrassed by media questions. The policymaker always should have known. The policymaker exists in the present while the intelligence officer also needs to live in the future. That is a fundamental difference. The policymaker is uninterested in applying resources on issues decades ahead because his/her legacy is over when his or her term is over. Before the invasion of Iraq in 2003, the Central Intelligence Agency (CIA) had no human reporting sources in Iraq. In order to have had sources in Iraq in 2003, the CIA needed to begin recruiting sources half a century earlier when Iraq was not viewed as necessarily important to American policy. While not a threat in the 1950s, it was an important country, based on its natural resources and geography. The policymaker should listen to intelligence leaders with an eye beyond the present in the service of National Security.

Prior to the invasion by the United States of Iraq in 2003, the United States did not have dependable, validated sources in Iraq. Instead, the government of the United States government depended on unverified Italian, German, British and Egyptian sources to justify the toppling of the Saddam Hussein regime. There were no other sources to verify or to disparage evidence provided by these individual sources. Another open question remains, did the CIA analysts have sufficient background on Iraq and its leader to voice strongly enough their skepticism about these unverified sources?

Intelligence analysis is an essential component for the policymaker's formulation of national security policy. Any analysis, pre-AI, is impossible without the analyst. The intelligence analyst must have the requisite education and must be able to communicate with the policymaker on a high level both orally and the written word. The analyst should have an area of expertise. The division is between analysis from analysts within their area of expertise or analysis from analysts serving multiple requirements not in their area of expertise. Many analysts have been moved about depending on the requirements of the present, independent of their area of expertise. An example would be moving analytical expertise from the Russia account over to China, the Middle East or Counterterrorism. The problem is when analysts are thought of separate from expertise. True, a good analyst has gained skills required to analyze events not in her or his area of expertise whenever such a need arises. Yet, expertise, even if imperfect, is absolutely essential for intelligence as a service to the policymaker's responsibility to the National Security.

Perhaps the most routine contribution intelligence makes to National Security is keeping the policymaker informed about current events. While media does the same, it does not do so in the same way. Current intelligence for the policymaker is facts and analysis of the facts in a condensed form. The policymaker can ask for detailed answers based on the facts or order a detailed briefing, a 'deep dive' on an issue of important to the National Security. Intelligence for the policymaker is focused on the policymaker's agenda, not the media's attention to events.

Strategic Intelligence is produced in the service of National Security but rarely penetrates the attention of the policymaker. The value of strategic intelligence to the National Security is the effort by intelligence to see into the future. For instance, what might happen in Russia, Turkey, Brazil, Egypt etc. in 10, 20 or 30 years. When a surprise event occurs, as it always has and always will, these strategic analytical studies become a baseline not only for intelligence analysis but also for intelligence collection. Much depends on Intelligence, much more depends on the policymaker.

It is not just about intelligent professionals writing or briefing intelligence but also intelligent policymaker readers and listeners. It helps if the policymaker has had background in international affairs but a good education and willingness to learn with good advisors is sufficient. Without intelligence, making decisions has no building blocks. Any decision then is arbitrary based on instinct rather than facts. Great intelligence from all sources of Intelligence on behalf of National Security does not make policymaker decisions easier rather it makes decisions harder. Great intelligence forces the policymaker to deal with and focus on the consequences of decisions. Great intelligence takes away the option of not knowing or not understanding an issue having to do with National Security.

From Alexander the Great to Genghis Khan to Washington to Bismarck to Churchill and a number of others, many of the great political and military leaders in history demanded to have intelligence and knew how to use intelligence to their advantage. They also had a realistic view of the meaning of National Security and how to advance the National Security.

Joseph Wippl
Professor of the Practice
Pardee School of Global Studies
Boston University
USA

jwippl@bu.edu

RICHARD J. KILROY JR.

Can the Transatlantic alliance survive the Trump presidency?

Expert article • 3914

In March 2025, less than two months into his second presidency, Donald Trump doubled down on his title of "Disrupter-in-Chief,"[1] enacting sweeping changes both in domestic and foreign policy. Along with Elon Musk and his unofficial Department of Government Efficiency (DOGE), Trump ordered mass firings of federal workers, began large-scale deportation operations targeting undocumented immigrants, dismantled the US Agency for International Development (USAID), threatened to withhold federal funding to states that did not support his agenda, all being championed by his highly controversial cabinet agency heads that the US Senate confirmed with little opposition. Americans were reeling from the shotgun approach Trump took to governing though Executive Orders, upsetting the constitutional checks and balances enshrined in the US Constitution.

Internationally, Trump further upset US neighbors, Mexico and Canada, threating tariffs, as well as suggesting Canada could be the 51st state and threatening Mexico with military intervention, labeling Mexican drug cartels as foreign terrorist organizations. He also threatened to retake control of the Panama Canal, as well as annex Greenland from Denmark in a show of force to reassert US dominion over the Western Hemisphere, echoing the expansionist policies of the Roosevelt Corollary[2] to the Monroe Doctrine. In September, Trump sent US Navy warships to the Caribbean Sea to bolster his aggressive counterdrug policies in the region, destroying suspected drug running boats Trump claimed were being used by "narco-terrorists" from Venezuela.[3]

Yet, it is Trump, and Vice President J.D. Vance's actions toward Europe and specifically the future of NATO and Ukraine's sovereignty, that have worried America's allies the most, upsetting the traditional transatlantic alliance. Blaming Ukraine for starting the war, claiming the real threat to Europe is the "enemy within,"[4] leaving Ukraine and Europe out of meetings with Russia (to include a meeting with Russian president Vladimir Putin in Alaska), and publicly berating Ukraine president Volodymir Zelenskyy all signal a major shift in US foreign policy away from its historical commitment to the transatlantic alliance and consensus that Russia is the real threat to Europe.

As a former "Cold Warrior"[5] who spent part of my military career stationed in Germany in the 1980s as an armored battalion and brigade intelligence officer, trained in Soviet military doctrine and tactics, the US commitment to NATO and Europe's defense was never questioned. For US military personnel still serving in Europe today, and those intelligence professionals documenting Russia's threat to America and its allies, their world has turned upside down, leaving many to question the value of their personal commitment to defending democracy against authoritarianism and upholding the principles of the North Atlantic Treaty.

So, what does all this mean for the future of the transatlantic alliance? Will NATO survive a retreat from the United States? Yes, it can.

It should begin by reexamining Canada's proposals in the Washington Paper discussions of 1948, allowing for a means to remove member states which no longer support Article V (collective defense) and openly support authoritarianism over democracy.[6] NATO should also move in the direction of shoring up the alliance with new members, to include Ukraine, which has the most experience in confronting the Russian military. The Ukrainians have defied the odds these last three years in defending their country, confounding Putin who expected a quick victory after Russia's successful annexation of Crimea in 2014. The difference in 2022 was the United States and Europe provided the military support necessary to forestall Russia's advance. NATO countries should call Putin's bluff of threatening the use of nuclear weapons, by supporting a Ukrainian offensive to retake the Donbas and parts of Eastern Ukraine under Russian control.

Even with the United States not backstopping such actions, or suspending all military aid, such resolve on the part of Europe and NATO could create a strong domestic response in the United States by Americans to force political change demanding US support for the alliance. NATO's response to a Russian drone incursion in Poland and Romania in September 2025 demonstrated such resolve, garnering praise from many members on both sides of the aisle in the US Congress.[7] This could help to swing midterm elections to change leadership in the US Congress, with new members willing to stand up to the Trump administration. There are still a number of conservative Republicans who stand with the country's traditional alliances and foreign policies toward Europe who value those relationships over building alliances with Putin and other authoritarian regimes. Coupled with the backlash from many of Trump's disruptive domestic policies, American democracy can recover from the Trump administration's ongoing assault.

Europe and the transatlantic alliance survived Trump's first term. It can survive his second. Although many of the guardrails no longer exist and Trump has surrounded himself with willing acolytes to carry out his worst impulses, there is a tipping point coming with the American people. It is already showing up on street corners with a mobilized public standing up to extremism. Europe may need to stand on its own for a time, but its leaders should rest assured that Trump's America is not the real America and like many tyrants who have come before, their gold statues will eventually fall.

[1] Henniger, Daniel, "Disrupter in Chief Trump," *Wall Street Journal*, January 15, 2025, https://www.wsj.com/opinion/disrupter-in-chief-trump-policy-administration-7cd77662.

[2] The Roosevelt Corollary (1904) to the Monroe Doctrine (1823) stated that the United States would intervene to ensure that other nations in the Western Hemisphere fulfilled their obligations to international creditors, and did not violate the rights of the United States or invite "foreign aggression to the detriment of the entire body of the American nations." https://history.state.gov/milestones/1899-1913/roosevelt-and-monroe-doctrine#:~:text=The%20Roosevelt%20Corollary%20of%20December,to%20the%20detriment%20of%20the

[3] Bekiempas, Victoria, "Republican condemns Vance for 'despicable' comments on Venezuelan boat strike," *The Guardian*, September 7, 2025, https://www.theguardian.com/us-news/2025/sep/07/jd-vance-venezuelan-boat-strike-rand-paul?CMP=oth_b-aplnews_d-1

[4] Nick Paton Walsh, "Vance uses half-truths to lecture a European audience well aware of the threat of authoritarian rule," *CNN*, February 14, 2025, https://www.cnn.com/2025/02/14/world/vances-speech-upsets-european-leaders-intl-latam/index.html

[5] Cold Warrior refers to those members of the US military who served on active duty between 1945-1991. Their service was never recognized by the Department of Defense as an actual military conflict deserving of the awarding of a campaign medal.

[6] The Washington Paper documented early discussions in 1948, leading to the North Atlantic Treaty and formation of NATO in 1949. The concern voiced by the Canadian delegation to the talks at that time was a member state that came under control of a communist regime. Today, it is the threat posed by authoritarian leaders whose policies cause NATO members to question that state's commitment to collective defense and the rules-based international order. See discussions regarding expelling Turkey for its military actions in Syria in 2019. Sari, Aurel, "Can Turkey be Expelled from NATO? It's Legally Possible, Whether or Not Politically Pruden," *Just Security*, October 19, 2019, https://www.justsecurity.org/66574/can-turkey-be-expelled-from-nato/.

[7] Alex Roufoglu, "White House Silence, Lawmakers' Outcry as Russia Tests Poland's Resolve," *Kyiv Post*, September 10, 2025, https://www.kyivpost.com/post/59777#:~:text=more%20confrontational%20stance.-,Test%20of%20resolve:%20bipartisan%20concerns%20emerge,our%20resolve%20in%20NATO%20territory.%E2%80%9D.

Richard J. Kilroy Jr.
Dr., Retired Professor
Coastal Carolina University
USA

Non-resident Scholar
Baker Institute for Public Policy
Rice University
USA

HANNU HIMANEN

Westlessness to helplessness? The liberal order is Europe's to save

Expert article • 3915

We don't speak much of the West anymore. This is because of the fundamental transformation of the transatlantic relationship. Western unity falters when it is most needed. With American leadership in ruins, the "West" is no more. It remains for Europe to pick up the pieces, but the divided continent is not punching its weight. Ukraine's survival adds urgency to the task.

In 2020, the Munich Security Conference published a much talked-about report entitled Westlessness. The term itself was described as "a widespread feeling of uneasiness and restlessness in the face of increasing uncertainty about the enduring purpose of the West".

Little did the authors of the report know where the West would be in five years' time. For more than a decade, they had been looking at a major transformation of the international order in the making. The prime mover of this change was, and continues to be, Russia. By attacking Ukraine in 2014 and then launching a full-scale war against it in February 2022, Russia is openly challenging the rules-based liberal order.

We may well overestimate the extent and significance of the turbulence around us. Yet a new order seems to be emerging, even if its contours still defy us. Timothy Garton Ash, for one, recently identified 24 February 2022, the day of the Russian invasion, as the starting point of a new, yet unnamed era. Carl Bildt wrote in November that "we have entered a period of global disorder".

Russia alone is too weak both economically and militarily to pose a fatal challenge to the existing order. In 2014, it pivoted to the east and has since been seeking support from China. The two countries speak of replacing the American-led "unipolar" order with a "multipolar" one. It is a euphemism for a great power dominated world in which small and medium states would be left out in the cold.

Even by combining their forces, Russia and China would not be able to seriously challenge the rules-based world. It is crumbling not because Russia and China want it to fail but because the main protagonist of the liberal order is allowing it to happen. Since Donald Trump returned to the White House, nothing has been sacred. The rules, values and principles once cherished by the West are in decline. Moscow and Beijing are thrilled.

Europe, slow to move and submerged in internal squabbles, is faced with a quadruple challenge. European nations must, first of all, not only step up their efforts to support Ukraine but also prop up their own defences. It is expensive, as this cannot be a zero-sum game. Political leaders face a Herculean task, as many countries have fallen into a deep hibernation, with their pacifistic electorates rejecting the possibility of a European war.

Secondly, while the United States is not about to abandon NATO, European allies must get used to the idea of finally taking their collective defence seriously. A more European defence alliance is in the horizon, but the EU is not equipped to take that role. The change is gradual, unless Russia decides to seriously test the alliance. Beyond the frontline states such as Finland, this unpleasant perspective is not widely recognised.

Thirdly, European capitals are learning to deal with a fickle, self-centred and thin-skinned president in the White House. As fissures are starting to appear in the MAGA movement, the task will be ever more precarious. Tensions between the White House and the State Department will be exploited by the Kremlin's masterminds. The situation will only become more difficult to manage as 2028 approaches.

Finally, while Russia must not be rewarded with normalising bilateral relations, Europeans have to maintain a carefully gauged dialogue with it. The diplomatic channel with Moscow has been monopolised by American amateurs with little experience in diplomacy. European governments should, however, avoid the fallacy of grandiose summitry with Russia. It takes two to tango, and Russia knows how to play hard.

The centrepiece in all of this is Ukraine – its independence, its territorial integrity, its sovereignty. European support to Ukraine, be it military, political or economic, will only gain in importance and urgency. As important as it is to ensure Ukraine's survival, the stakes are much higher. The future of the liberal order is at stake.

Recognising the cold facts of the situation is a necessary but not sufficient condition. An enormous responsibility for defending Western values falls squarely on Europe's shoulders. However, with its divisions, sluggish decision-making and legalism, Europeans are dismally ill-equipped to carry that responsibility. Europe finally needs to walk its talk. it needs a strategic vision extending well beyond the Ukraine war, and perseverance and resilience to carry that vision through.

Hannu Himanen
Ambassador (ret.), Ambassador of Finland in Moscow 2012 to 2016
Finland

Author of three books, most recently *Where Angels Fear to Tread: Aggressive Russia and Finnish Security* (2024, in Finnish).

This text was finalised on 30 November 2025.

EDVILAS RAUDONIKIS

Nordic and Baltic Eight (NB8): A model of success and responsibility

Expert article • 3916

In an era marked by geopolitical tensions and challenges to long-standing international norms, Northern Europe stands out as a region deeply committed to democratic values, rule of law, freedom, human rights, and a rules-based international order.

The Nordic and Baltic countries - Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway, and Sweden—collectively known as NB8, have become an outstanding example of an open, modern, and results-oriented regional cooperation. Together, they aim to build a safer, more innovative, stronger and more competitive region. With a combined population of approximately 34 million and a total GDP of around €1.7 trillion, the NB8 ranks as the fifth-largest economy in Europe, just behind Germany, the United Kingdom, France, and Italy, and globally comparable to Canada and South Korea. The NB8 countries consistently rank among the global leaders in media freedom, innovation, sustainability, digitalization, happiness, and quality of life.

Success comes with responsibility. These achievements represent a powerful form of soft power, which should be leveraged through strategic storytelling and the sharing of experience on how to create an area of success, based on historical ties, transformation and strategic vision.

The deep historical connections among the Nordic countries date back to the Viking era and were later reinforced through political unions in the 14 - 16th centuries. In the late 19th century, soft cooperation initiatives such as the Nordic Postal Union (1869) laid the foundation for more formal collaboration. These efforts culminated in the establishment of the Nordic Council (1952) and the Nordic Council of Ministers (1971), supported by strong civil society engagement.

On the eastern shore of the Baltic Sea, the historical trajectory was far more turbulent. Countries like Lithuania disappeared from the map following the partitions of the Polish-Lithuanian Commonwealth in the late 18th century, only to re-emerge alongside Latvia and Estonia during the "Year of Independence" in 1918. However, frozen conflict between Poland and Lithuania over Vilnius hindered early Baltic cooperation. Modern Baltic cooperation began even before the restoration of independence in the early 1990s, with coordination among national movements. Inspired by successful Nordic models, the Baltic Council (1989), Baltic Assembly (1991), and the Baltic Council of Ministers (1994) were established to formalize regional collaboration.

The 1990s marked a period of rapid transformation for the Baltic states and the broader region. Nordic countries played a crucial role both collectively and individually. As a group, they shared best practices and regional cooperation models. Individually, they were among the first foreign investors, trainers of civil servants, and advisors to emerging political parties. The results are striking: the standard of living in the Baltic states increased six - to sevenfold, with only Poland experiencing greater income growth within the EU. For small-population countries such as Lithuania (2.8 million), Latvia (1.86 million), and Estonia (1.34 million), openness, media freedom, and value-based political imperatives became binding elements of evolving Nordic–Baltic cooperation. The Nordic model served both as a stimulus and as a compensatory mechanism for the constraints of their small domestic markets.

Strategic thinking has always been a cornerstone of NB8 cooperation. Even when Nordic collaboration excluded foreign and security policy, its robustness served as a strategic counterbalance. After the Baltic states regained independence in the early 1990s, the Nordic-Baltic partnership adopted a clear strategic goal: to facilitate the integration of Baltic countries into European and Transatlantic structures as swiftly and smoothly as possible.

While regional cooperation in the Baltic Sea area has brought many successes, not all initiatives have evolved seamlessly. A telling example is the Council of the Baltic Sea States (CBSS), originally established to support the eastern and southern Baltic Sea countries in their transition toward becoming "European." Following the EU's enlargement, the CBSS shifted its focus toward fostering cooperation with Russia. However, its relevance has since declined due to fundamental value-based divergences, particularly as Russia has come to pose a direct threat to other member states. Today, CBSS faces a critical challenge: redefining its role and structure considering the new geopolitical reality.

In the context of Russia's war against Ukraine, the NB8 regional unity as well as coordinated actions and a unified voice in the international fora has become more important than ever.

The most important recent strategic turning point in the region was the decision by Finland and Sweden to make a final shift in their long-standing security policy from neutrality, through non-military alignment, to full membership in NATO.

A clear example of a strategic approach by the entire Nordic-Baltic Eight (NB8) region is their staunch commitment to supporting Ukraine: seven of the top ten donors, when measured as a share of assistance relative to GDP, are Nordic-Baltic countries.

In conclusion, the NB8 is more than a geographic grouping - it is a model of successful regional cooperation, built on historic roots, wisely adapted to current realities: on shared values, and on a strong sense of collective responsibility.

All this positive experience can and should be globally shared in today's world, which increasingly tends to turn inward and seek solutions nationally. For us as Europeans, it is essential to employ this vast intellectual, administrative, and political capital of this regional cooperation to support Ukraine and Moldova on their path toward full-fledged membership in Euro-Atlantic structures as the Nordics made for the Baltics three decades ago As members of the European family in values, identity, and commitment, they now need our help to be formally integrated into European institutions.

Edvilas Raudonikis
Ambassador of Lithuania to Finland

HEDVIG ÖRDÉN

Rethinking European intelligence cooperation

Expert article • 3917

Intelligence organisations in small European states today face a question: how to navigate an era of increasing international disorder. During the Cold War, the strategic position of Scandinavian states made them valuable collaborators for US intelligence, resulting in long-term partnerships. Intelligence cooperation is based on shared strategic interests but also depends upon mutual trust. With the new US administration, both these foundations are increasingly challenged.

The professionalisation and institutionalisation of intelligence work developed in parallel with the post-war international order. Transatlantic cooperation produced a shared understanding of threats and security challenges among allies while contributing to the generation of common professional norms and practices.

The recognition of shared professional norms and expertise is an essential component of trustful cooperation. Intelligence professionals often define their role as truth-tellers, knowledge producers committed to speaking truth to power. While this ideal is not always realised in practice, it has played a role in distinguishing intelligence work in democratic systems from that in authoritarian regimes. As producers of evidence-based knowledge, intelligence actors require professional autonomy, and the politicisation of intelligence constitutes a professional and institutional failure.

The return of President Trump marked a significant change in transatlantic intelligence relations, both in terms of strategic priorities and in the autonomy of intelligence professionals vis-à-vis the political leadership.

Before his inauguration in January 2025, the President threatened a US takeover of Greenland. The announcement presaged an aggressive move away from Scandinavian allies and marked a significant departure from the ideal of a rules-based international order. In March, US intelligence sharing with Ukraine ceased. While this unprecedented decision was subsequently reversed, the event demonstrated a widening gap in strategic priorities between US and European allies.

The new US administration also challenges the shared professional norms underpinning cooperation. Embracing a populist discourse, the President has previously described US intelligence organisations as part of the 'deep state'. The administration has also shown a lack of recognition for professional autonomy by dismissing intelligence personnel on ideological grounds, by promoting inexperienced but loyal individuals, and by publicly criticising intelligence assessments which contradict political narratives.

These two shifts have provoked a set of unusual public comments on transatlantic collaboration. In October 2025, representatives for the Dutch intelligence services publicly recognised the growing challenges of intelligence sharing. They voiced concerns about politicisation, highlighting the importance of professional norms and expertise for trustful partnerships. In addition, the Netherlands reduced transatlantic intelligence sharing on topics related to Russia and intelligence with human rights implications.

While the transatlantic landscape raises challenges for small European states, the uncertainties also create new opportunities for regional collaboration. Dutch representatives for instance point to strengthened cooperation between Scandinavian states, UK, France, Germany, Poland and the Netherlands, driven by a shared commitment to Ukraine.

If properly managed, transformed collaborative patterns can decrease dependency on the US. They could also provide an opportunity to enhance the democratic legitimacy of intelligence in Europe.

A key professional norm underpinning intelligence collaboration is the ability to keep secrets. This is especially important for small states in unequal partnerships. As a result, cooperation often lacks appropriate structures for democratic oversight, with a potentially greater effect on smaller partners, such as the Scandinavian states. The resulting lack of transparency can decrease public trust in intelligence services and their public communication, creating domestic vulnerabilities.

Navigating the situation, European states should seize the opportunity to address the accountability gap by embedding oversight mechanisms within regional cooperation frameworks. Such structures can be complemented by collaboration among informal oversight actors, such as investigative journalists, academics, and civil society organisations. Multidimensional oversight could enhance public dialogue on intelligence, build public understanding of intelligence work, and thereby strengthen trust.

In this way, the current transatlantic uncertainty may offer an opportunity to adapt to a changing international order and strengthen both security and the legitimacy of European intelligence services.

Hedvig Ördén
Researcher
Psychological Defence Research Institute
Lund University
Sweden

Affiliated Researcher
The Swedish Institute of International Affairs
Sweden

ARTUR GRUSZCZAK

Prospects for stronger and more effective European intelligence cooperation

Expert article • 3918

Jean Monnet once foretold: "Europe will be built through crises, and it will be the sum of their solutions." European intelligence cooperation provides a telling example of the tortuous process of shaping structures and institutions which nevertheless remain below the threshold of efficiency required to overcome the constraining dissensus among EU Member States. Fragmentation along national lines, shaped by distinct security cultures, legal traditions and threat perceptions, hinders genuine progress in intelligence cooperation and calls into question the viability of establishing a reliable intelligence entity at the EU institutional level. The strategic surprise of Russia's full-scale invasion of Ukraine in 2022 revealed deep deficits in the EU's intelligence capabilities and generated seemingly strong incentives for closer cooperation.

However, the existing forms of institutional and functional intelligence cooperation and sharing remain insufficient for preventing and combating persistent hybrid threats, cyberattacks, sabotage and disinformation operations. This is partly due to the essentially intergovernmental nature of collaboration, which restricts access to intelligence – both raw and processed – to authorised national services. It is also attributable to the lack of political will among EU Member States with regard to the development and enhancement of capacities for data collection and intelligence production by EU agencies and bodies.

As an international actor marking its global presence through diplomatic engagement, as well as crisis management and peacekeeping missions and operations under the Common Foreign and Security Policy (CFSP), the EU began in the early 2000s to develop strategic awareness and situational assessment capacities intended to provide its institutions and bodies with reliable, up-to-date, all-source intelligence. This process started with a small analytical unit, SITCEN (Situation Centre), which – following the Lisbon reform of the EU treaties – evolved into the EU Intelligence and Situation Centre (EU INTCEN). Concurrently, the EU developed intelligence capacities through its agencies (the Satellite Centre for geospatial intelligence; Europol for criminal intelligence; Frontex for situational intelligence at the EU's external borders; and the EU Military Staff's Intelligence Directorate (EUMS INT) for defence intelligence). Importantly, the EU sought to foster synergy among these diversified formats of intelligence cooperation. The Single Intelligence Analysis Capacity (SIAC) framework, linking INTCEN and EUMS INT, has been progressively strengthened as a civilian–military analytical format.

These intensive activities, particularly throughout the 2010s, marked what may be termed the "intelligence turn" in European security governance – a gradual shift from ad hoc information exchange towards more structured analytical cooperation. However, this trajectory soon became stalled for several reasons: (1) the denial of formal EU intelligence prerogatives by the European Commission; (2) the strategic sensitivity of intelligence cooperation; (3) low levels of trust in EU intelligence capabilities among Member States; (4) divergent legal and oversight frameworks; (5) limited sharing of highly classified information with EU institutions; and (6) recurring espionage scandals in several EU countries. The unsuccessful attempts to create a coherent European intelligence cooperation structure revealed significant obstruction on the part of Member States. They effectively adopted a dual approach: endorsing the development of intelligence capabilities at the EU level, whilst simultaneously failing to provide substantial input into EU intelligence production.

Russia's full-scale military invasion of Ukraine in 2022 triggered an intensified debate on the EU's response to the war in its neighbourhood, including the strengthening of its intelligence capacities. Yet the prospects for more effective European intelligence cooperation remain bleak. None of the previously identified impediments to deeper cooperation has been significantly mitigated or overcome. Moreover, the European Commission has demonstrated a proclivity for the multiplication of intelligence-related entities. The recent proposal, reported by the Financial Times in mid-November 2025, to establish an intelligence cell within the European Commission's Secretariat-General has raised eyebrows among observers and intelligence professionals alike. While this initiative may be interpreted as consistent with von der Leyen's decision to establish the "Security College", comprising the 26 Commissioners and the President of the Commission, it simultaneously risks downgrading EU INTCEN as a situational centre and reducing its role primarily to supporting CFSP activities. Such an internal manifestation of institutional distrust bodes ill for the coherence and credibility of the Union's intelligence architecture.

Artur Gruszczak
Chair of National Security
Jagiellonian University
Kraków
Poland

artur.gruszczak@uj.edu.pl

ANDREW DEFTY

The case for a joined-up approach to intelligence oversight

Expert article • 3919

In the period since the terrorist attacks of September 11, 2001, the intelligence and security activities of many states have been underpinned by a fusion doctrine designed to break down the silos in which intelligence and security agencies operate. Increased cooperation and coordination of intelligence activities has become a feature of intelligence and security policy both within and often between states. Recent years have also seen the emergence of new agencies and structures to deal with the emerging threat from cyber technologies.

In many states the establishment of intelligence oversight bodies followed after, in some cases many years after, the creation of the intelligence agencies they were tasked with overseeing. There has been a similar lag in the evolution of those oversight structures to deal with the emergence of new agencies and practices. Oversight bodies have tended to remain siloed, locked into structures established in the 1990s or earlier, while cooperation between them has often been limited or actively discouraged. It is time for a more joined-up approach to intelligence oversight aimed at the establishment of more coordinated regulatory frameworks for the scrutiny of intelligence and security agencies.

Why does intelligence oversight matter?

Intelligence oversight is generally defined as a process of supervision designed to ensure that intelligence agencies do not break the law or abuse the rights of individuals at home or abroad. It also ensures that agencies are managed efficiently, and that money is spent properly and wisely. There is no one model of intelligence oversight. It does, of necessity, vary from country to country, and may be defined by a state's history, constitutional and legal systems, and political culture. Existing studies of intelligence oversight have established the view that oversight takes place at different levels, carried out by a range of institutions and actors drawn from the executive, legislative and judicial branches of the state as well as civil society. At each level, oversight bodies are often seen as performing distinct and separate roles, as systems are designed to prevent overlap or duplication, and also to provide the compartmentalisation necessary to ensure security.

Patchwork or jigsaw: the risks of a fragmented approach to intelligence oversight

While the establishment of a range of bodies to scrutinise the work of intelligence agencies is generally seen to have enhanced intelligence agency accountability, the emergence of separate oversight bodies with discrete functions can lead to a fragmented approach which creates gaps in accountability. Just as new intelligence structures and practices have emerged to deal with new threats, the development of intelligence accountability in many states has been a dynamic process with new institutions or powers added to existing oversight structures over time. However, unless consideration has been given to dovetailing new oversight bodies into existing arrangements there is potential for accountability gaps to emerge with the resulting system of oversight more akin to a patchwork than a jigsaw.

Towards joined-up oversight

In the place of regulatory frameworks comprised of discrete oversight bodies with discrete and separate roles, a joined-up approach to intelligence agency accountability should provide for enhanced cooperation between oversight bodies with elements of both horizontal and vertical accountability. Horizontal accountability refers to cooperation between state institutions, such as parliamentary committees and judicial review bodies. This may involve dialogue and sharing of information on issues of mutual concern but might also include a legal duty to refer matters for investigation by different oversight bodies.

Vertical accountability refers to the hierarchical relationships between different accountability mechanisms and also takes account of scrutiny by non-state actors such as the media and civil society organisations. It is relatively commonplace for the executive to be able ask intelligence oversight bodies to conduct inquiries. So-called 'referral reviews' are the principal mechanism for initiating inquiries by the Australian parliamentary oversight committee and are a statutory function of the Canadian National Security and Intelligence Committee of Parliamentarians. It is less common for inquiries to be conducted in response to requests from lower levels of accountability but there is surely a role for parliamentary committees to operate in response the demands of concerned citizens, and in certain circumstance for parliament require the executive to take action.

Some of the most ambitious examples of joined-up oversight relate to the merging of functions between oversight bodies and also attempts at vertical accountability involving civil society actors. The UK for example recently combined the functions of three judicial commissioners responsible for overseeing the work of intelligence agencies and the police, into a single Investigatory Powers Commissioner's Office, with enhanced powers and resources. This body is supported by an independent Technical Advisory Panel (TAP) which advises the commissioners and also government ministers on the impact of changes in technology on the exercise of investigatory powers. Membership of the TAP is drawn from civil society including university professors, and cyber security experts with experience in the private and NGO sectors.

Andrew Defty
Dr., Associate Professor of Politics
School of Social and Political Sciences
University of Lincoln
UK

ARTIS PABRIKS

The role of intelligence for successful governance

Expert article • 3920

There is no state or government in the world that does not recognise the importance of intelligence — the trustworthy gathering and analysis of information necessary for successful governance.

Intelligence gathering, espionage, and information dissemination have always been crucial elements of any government. Their relevance has been equally high in times of peace and during wars. Throughout history, accurate and timely information has helped rulers make sound political and military decisions, avoid or win wars, ensure social stability, and prevent coups, invasions, or assassinations.

Intelligence was one of the main tools of the art of war even according to Sun Tzu, who stated that the essence of war is deception — often executed through intelligence.

In Europe, the 16th-century Renaissance thinker Machiavelli wrote: "As for intelligence, which is the foundation of all enterprises, no prince should ever neglect it. For he who is not well informed cannot possibly govern well." Machiavelli also stressed that saving money on spies is an unwise policy, underscoring the importance of information gathering. Later, intelligence institutions emerged across many countries. In the 19th century, the Napoleonic Wars created the need for structured military intelligence as well. Today, most countries maintain several intelligence institutions responsible for intelligence, counterintelligence, military intelligence, and internal security.

Latvia provides a good example of how civil and military intelligence institutions were established and developed alongside the creation of the Latvian nation-state. From the very beginning, their primary goal has been to assist the government in maintaining and securing two fundamental objectives: external and internal security.

Since the proclamation of the Republic of Latvia in 1918, both internal and military branches of intelligence have served the new democratic government. In 1940, when Latvia's independence was crushed by the Soviet occupation, Latvian intelligence services and their members were among the first to face harsh repression by the invading forces. The Soviets were eager to seize information hidden in the files and minds of the Latvian intelligence community.

On 21 August 1991, Latvia once again restored its national independence after nearly fifty years of Soviet occupation. Following independence, three separate intelligence institutions were created to safeguard national sovereignty and democratic governance.

In November 1991, the State Security Department under the Ministry of the Interior was established, later becoming the State Security Service (VDD). This civilian counterintelligence and internal security service gathers and analyses information, informs state officials, and neutralises threats.

With the reconstruction of the Latvian armed forces, the Information Service of the Ministry of Defence was created on 12 June 1992. In 1994, it evolved into the Defence Intelligence and Security Service (MIDD), responsible for military counterintelligence, intelligence, and a variety of defence-related tasks, including matters of the defence industry.

The third Latvian intelligence institution, the Constitution Protection Bureau (SAB), was established in 1995 and is supervised by the Cabinet of Ministers. It is responsible for intelligence, counterintelligence, and the protection of state secrets. The very name of this office underscores the importance of democracy in modern Latvia, as democratic governance is seen as a prerequisite for national independence.

In the 21st century, intelligence communities worldwide — including those in Latvia — face immense challenges in adapting to a rapidly changing world while maintaining the ability to provide trustworthy information and timely guidance to governments and societies. For Latvia, additional challenges stem from the country's small size, its proximity to a large, aggressive, revanchist power — Russia — and the presence of a sizeable Russian-speaking diaspora.

Among the main global challenges are the rapidly changing nature of societies influenced by the technological revolution and information networks. The world is becoming increasingly polarised and fragmented, while traditional international institutions are under significant strain. These natural challenges, born of human progress, are further intensified by state actors seeking greater influence over global affairs and expressing dissatisfaction with the existing international order. Russia and China — along with at least one major non-state actor, the Islamic world — are leading this acceleration.

To fulfil their mission, intelligence communities around the globe must operate in an increasingly complex environment characterised by massive flows of fragmented information, the growing impact of artificial intelligence, persistent cyberattacks, and an intensifying hybrid warfare that is forcing a redefinition of classical theories of war and peace. Added to this are the rising risks of nuclear proliferation and the potential use of nuclear weapons. One might say we already live in a state of undeclared war, as the boundary between war and peace looks very different today than it did twenty years ago.

Existing international institutions and rules were not designed for such circumstances, which contributes to growing instability. Reforming them requires time and broad international consensus — yet time is running out. This reality only increases the importance of intelligence institutions: if they fail to obtain the right information and provide timely, accurate analysis, state bureaucracies and politicians may fail to make the right decisions.

Another growing danger stems from political institutions themselves. The accelerating chaos of the world, fragmented and polarised societies, the blending of truth and misinformation, and hybrid, cyber, and informational attacks promoted by states seeking to reshape global power dynamics all place mounting pressure on democratic governments. These governments, in turn, increasingly struggle to balance the preservation of democracy — including privacy rights — with the need to provide effective governance and appropriate responses to threats posed by adversaries such as Russia, China, and various non-state actors.

Today, intelligence communities everywhere face mounting challenges — not only to obtain, analyse, and present actionable insights to governing authorities, but also to ensure that their recommendations reach the right decision-makers, and that those leaders are both willing and able to act upon the intelligence they receive.

Artis Pabriks
Dr., Director
Northern Europe Policy Centre
Latvia

Former Deputy Prime Minister, Minister of Foreign Affairs, and Minister of Defence of Latvia

NIGEL WEST

Intelligence influence

Expert article • 3921

The impact of secret intelligence on western governments policy-makers can be hard to assess because, by its very nature, these events are not likely to be recognised for what they were, at the time. Understandably, if an intelligence operation has been undertaken successfully, those responsible may want to repeat the exercise on another occasion. For example, in July 1961 British Royal Marine 42 Commando was landed off HMS Bulwark in Kuwait as part of Operation VANTAGE to deter a threatened invasion of the country by Iraqi troops. As a consequence of this deployment, the regime in Baghdad withdrew its forces from the border. When in January 1972 Guatemalan troops prepared to occupy Belize, Buccaneer fighter-bomber off HMS Ark Royal, flew along the frontier as part of a mission to protect the territory.

Similarly, in 1977, it was feared in London that Argentina intended t launch a surprise invasion of the Falkland Islands, but the aggression was prevented by the deployment of a nuclear-powered submarine, HMS Dreadnought, as part of a naval task force codenamed JOURNEYMAN to strengthen the British colony's defences.

Britain's failure in 1982 to detect the Argentine junta's plan to occupy the Islands led to the conflict which would have a profound and lasting influence over British politics and served to transform Margaret Thatcher's reputation and popularity. Indeed it can be argued that Mrs Thatcher's eleven years as prime minister was dominated by security and intelligence issue dating back to the Suez crisis of 1956 which split the Conservative Party and led to the recall of the U.S. ambassador in London, an unprecedented act of protest offered by the Eisenhower administration.

Tony Blair's government was equally preoccupied with security and intelligence concerns, ranging from the domestic preoccupation of defeating the Provisional IRA's 32-year campaign of terrorism in Northern Ireland, to the controversial decision to join the U.S.-led Coalition to remove Saddam Hussein from power and destroy his alleged stocks of weapons of mass destruction (WMD). Determined to win over sceptics within his own Labour Party, Blair authorized the release of a crucial 2002 Joint Intelligence Committee report that had been largely rewritten by Downing Street staffers. Crucially, Blair insisted that "the assessed intelligence has established beyond doubt… that Saddam has continued to produce chemical and biological weapons, that he continues in his efforts to develop nuclear weapons".

In the House of Commons Blair described the WMD reporting as "extensive, detailed and authoritative" when in reality it had been "sporadic and patchy". Perhaps even more egregiously, in February 2003 the government published a briefing paper entitled Iraq – Its Infrastructure of Concealment, Deception and Intimidation, which purported to draw "upon a number of sources, including intelligence material". Actually, detailed analysis of the content showed that substantial parts of the text had been plagiarised from off the internet.

Many of embarrassments that have afflicted governments of all stripes can be seen to have had their origins in security and intelligence lapses, as demonstrated by hostile penetration of all the major agencies; the Profumo scandal, the SpyCatcher affair, and a dozen other incidents that have undermined successive administrations.

Nigel West
www.nigelwest.com

ARTURO G. MUÑOZ

Intelligence and diplomacy

Expert article • 3922

Intelligence has been an integral facet of diplomacy since ancient times. Policymakers rely on intelligence collection to know the intentions and plans of rival or adversary states, as well as their capabilities. For example, during the 1922 Washington Naval Conference to determine fleet naval ratios, US codebreakers intercepted the Japanese delegation's communications, discovering their secret instructions. This allowed the American negotiators to secure their desired terms. On the other hand, faulty intelligence can seriously undermine diplomacy, as experienced by the Russians in their 1939 Winter War with Finland, the American failure to anticipate the 1978-1979 fall of the Shah of Iran, and numerous other cases.

Analysts play a key role in the intelligence process by making sense of contradictory or incomplete field reporting and helping to weed out inaccurate or irrelevant information. Ideally, governments should base their foreign policies on sound finished intelligence, as opposed to ideological strictures, nationalistic jingoism, or domestic political considerations — as is too often the case. It is not uncommon for leaders who are inflexible to reject accurate intelligence reporting that does not fit their preconceived notions.

Diplomats who implement foreign policy should be aware of the intelligence analysis underlying its formulation. This intelligence process also applies to dealing with allies. They may be seeking quietly to gain an advantage in a friendly relationship and may not want to share their ultimate goals or may want to hide vulnerabilities. In that regard, accurate intelligence is vital for diplomacy because denial and deception can be practiced by friend or foe.

India offers an example of a successful campaign to convince the world that it had no intention or even capability to develop a nuclear weapons program. To avoid Western sanctions, India's official pronouncements insisted that its nuclear research capabilities were strictly for peaceful purposes, while simultaneously hiding their secret weapons program. When Indian scientists detonated three nuclear bombs in May 1998 the deception was revealed. Conversely, in the Cuban missile crisis of 1962, US Ambassador Adlai Stevenson made a classic display of intelligence used effectively for diplomacy. To gain support for the US blockade of the island, he presented to the United Nations declassified imagery of secret Soviet missile bases in Cuba.

In the early days of diplomacy, envoys sent to a foreign country were not only expected to establish lines of communication and trade but also engage in espionage. As intelligence and diplomatic establishments became more bureaucratic over the centuries, a distinction developed between diplomats and spies, even though spies continued to operate under diplomatic cover. This raises the separate practice of "secret diplomacy," usually coordinated closely with intelligence, as in the famous case of US President Richard Nixon's secret overtures to the Chinese government ultimately leading to the "opening" of communist China to the West.

Some scholars and intelligence officials argue that intelligence must be collected clandestinely to be considered intelligence, otherwise it is simply information. The contrary view holds that overtly gathered information can be just as valuable for diplomatic purposes and should be considered as intelligence. By this criterion, diplomats can be considered not only as consumers of intelligence, but also as collectors, due to their valuable contacts and sources of information. To wit, Open Source Intelligence (OSINT) is listed as one of the five main forms of intelligence collection. The Chinese intelligence manual, Sources and Methods of Obtaining National Defense Science and Technology Intelligence gives eloquent testimony to the value of OSINT. Although it does not diminish the importance of human and technical espionage, the manual argues that much of the needed intelligence can be gathered overtly at international scientific conferences and by exploiting studies published in technical journals and other publicly available materials in US corporate, academic, civilian government, and military sources.

Intelligence officials routinely stress that their craft must be apolitical and not be dictated by political agendas. However, the reality is that intelligence has often been politicized in the past, and the trend seems to be towards increased shaping of intelligence collection and analysis to fit political objectives. This not only entails revealing/ declassifying genuine intelligence to make a point but can also include presenting misinformation and disinformation as intelligence. US politicians during the Cold War exaggerated the "missile gap" with the Soviet Union to win elections and justify increased military spending; strong cognitive biases and "group think" among intelligence analysts impeded a dispassionate assessment of the communist threat.

The role of politicized intelligence in shaping foreign policy and diplomacy was evident in the 2003 US invasion of Iraq. In that case, "neo-con" administration officials became convinced that it was necessary to overthrow the Saddam Hussein dictatorship and they manipulated the intelligence process to arrive at two wrong conclusions: (1) Iraq had weapons of mass destruction and (2) the Iraqi regime was allied with al-Qa'ida terrorists. Disregarding basic intelligence procedures for vetting walk-ins, these policymakers embraced the fabricated intelligence reports of an Iraqi refugee in Germany encrypted "Curveball." Some of his falsehoods were presented as facts by Secretary of State Colin Powell at the United Nations on 19 December 2002 to gain international support for an attack on Iraq. That speech became a compelling case of how not to use intelligence for diplomacy. Today (October 2025), politically driven intelligence estimates are being used by opposing diplomats either to convince the public that Ukraine cannot win the war against Russia, or, alternatively, that Russia cannot win.

[1] See Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (CQ Press, 2009).
[2] See Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: Origins, Obstacles and Innovations* (Georgetown University Press, 2008); and Timothy Walton, *Challenges in Intelligence Analysis: Lessons from 1300 BC to the Present* (Cambridge University Press, 2010).
[3] See James B. Bruce and Michael Bennet, "Foreign Denial and Deception: Analytical Perspectives," in George and Bruce, eds., *Analyzing Intelligence*, 423-445; and Donald C. Daniel, "Denial and Deception," in Jennifer Sims and Burton Gerber, eds., *Transforming Intelligence* (Georgetown University Press, 2005), 134-146.
[4] See Lakshya Govani, "Pokhran Bespeaks the Secret Saga Behind India's 1998 Nuclear Tests," 23 May 2025, https://ebnw.net/history/pokhran-bespeaks-the-secret-saga-behind-indias-1998-nuclear-tests/
[5] See Cuban missile crisis: Adlai Stevenson shows photos at the UN proving Soviet missiles are installed in Cuba - Today's Flashback
[6] See Robert V. Keeley, "CIA-Foreign Service Relations," in Craig Eisendrath, ed., *National Insecurity: U.S. Intelligence after the Cold War* (Temple University Press, 2000), 61-75.
[7] See Len Scott, "Secret Intelligence, Covert Action and Clandestine Diplomacy, "in L.V. Scott and P.D. Jackson, eds., *Understanding Intelligence in the twenty-First Century: Journey in Shadows* (Routledge, 2004), 162-179.
[8] The other forms of intelligence collection are Human Intelligence (HUMINT) (espionage), Geographic Intelligence (GEOINT) (formerly referred to as Imagery), Signals Intelligence (SIGINT) (communications intercepts), Measures and Signatures (MASINT) (includes radar intelligence, acoustic intelligence, nuclear intelligence, and chemical and biological intelligence).
[9] Written by Hou Zhongwen and Wang Zongxia, it was published in Beijing in 1991. A US government English-language translation was completed in 2000 and is posted at www.fas.org/irp/world/china/docs/sources.html
[10] Arturo G. Muñoz, book review of William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (Routledge, 2013), in Studies in Intelligence Vol.59, No.4 (Extracts, December 2015), 33-35 @ Chinese Industrial Espionage.
[11] See Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Cornell University Press, 2011).
[12] See Richard Kerr, "The Track Record: CIA analysis from 1950 to 2000," in George and Bruce, *Analyzing Intelligence*, 35-54.
[13] See the detailed description of how the intelligence estimate process on Iraq was manipulated to fit a political agenda in Paul R. Pilar, *Intelligence and U.S. Foreign Policy: Iraq, 9/11 and Misguided Reform* (Columbia University Press, 2001).
[14] See Aram Roston, *The Man Who Pushed America to War: The Extraordinary Life, Adventures, and Obsessions of Ahmad Chalabi* (Nation Books, 2008), 173-228.
[15] See Bob Drogin, *CURVEBALL: Spies, Lies and the Con Man Who Caused a War* (Random House, 2007); Joby Warrick, "Warnings on WMD 'Fabricator' Were Ignored, Ex-CIA Aide says," 25 June 2006, *Washington Post*.
[16] Full Text of Powell's Iraq Speech - CBS News

Arturo G. Muñoz
Ph.D., Senior Political Scientist - Adjunct
RAND Corporation
United States of America

PETER ERICSON

Intelligence and diplomacy

Expert article • 3923

What is the relationship between Intelligence and Diplomacy? That is, I think, an important and quite interesting question, but it begs two other ones: What is in fact intelligence? And what does diplomacy even mean?

Since this article presents my personal opinions, I will also take as the point of departure my own sense of the meaning of those two words.

To me, intelligence is, quite simply, what the intelligence agencies produce. How they obtain their information – be it signals intercepts, human sources, or anything else – is less important to me as a consumer of their products.

One key feature of intelligence is that it is secret. It is narrowly distributed within the government structures, and only on a strict need-to-know basis. Consequently, only a select few individuals within, for instance, the Ministry for Foreign Affairs, have access to intelligence – and the more sensitive it is, the fewer. Due to the high level of discretion and the difficulty guaranteeing information security at embassies and other missions abroad, intelligence tends to be shared primarily between units and officers in the capitals.

In a similar vein, diplomacy is – to me –what diplomats do to manage international relations and interests. What does that mean in practice? When we are on a foreign post we try to get to know people who can tell us about this or that aspect of the host country – foreign policy priorities, domestic politics, the functioning of the economy, business opportunities, fruitful areas of cultural cooperation, a million different things. We try to understand the host country, so we can inform our capital what is going on and, preferably, explain why it happens and how that affects our own country. And maybe how we can influence developments in a beneficial way according to our national – and in the best case mutual – interests.

As the reader may have noticed, both the preceding paragraphs contain a sentence on the role of the capital. While the Ministry for Foreign Affairs may be the main recipient of embassy reporting, it is by no means the only one. Many other ministries – in particular Defence, Justice/Interior, and Finance – are keen readers of reporting from the missions abroad, as is the Prime Minister's Office. Those with a need-to-know are also avid readers of intelligence reports.

Simply put, intelligence services and diplomatic reporting normally cross paths in the capitals, enabling informed policymaking. This is where it gets interesting.

Whereas intelligence often provides pieces of the puzzle – diplomatic reporting can often contribute with the bigger picture.

Intelligence focusses on facts, compiled into larger sets of facts, refined into analysis. As an example, intelligence may recount actions of specific warships or aircraft and makes analytical deductions from the observed actions. But intelligence does not propose policies or reactions to what is observed.

Diplomacy is rooted in analysis, often with a holistic and contextual approach to the issue at hand. Diplomats normally spend several years in the country, often even several tours over a longer period of time. They develop a wide network of contacts in diverse fields of activities and different groupings in society, even building friendships. They immerse themselves in the culture and history of the country concerned. In short, they develop an understanding based on huge amounts of information combined with personal experience, which they can translate into a form that is understood by the recipients in the capital. And they often make policy recommendations or propose courses of action.

If you only use intelligence as the basis of decisions, i.e. only the pieces of the puzzle, you run the risk of applying the sending nation's interpretations, values or interests – or quite simply world view – on the receiving country's motivations, intentions and actions. The diplomats' deep knowledge of the country in question and the resulting ability to provide a more insightful and comprehensive analysis reduces the risk of that fallacy. They provide the bigger picture into which the pieces of the puzzle fit.

Conversely: thanks to the understanding of their country's national interests and priorities vis-à-vis the host country (and sometimes augmented by explicit instructions), diplomats can promote the views and interests of the sending country. They seek to develop common ground with the host country and try to influence the host country's decision-making process. All this is made possible thanks to their local networks and their thorough knowledge of the country.

So, to answer the question at the start of this text: the relationship between intelligence and diplomacy is mutually supportive and complementary. Both are important for a country to conduct an effective foreign policy.

Peter Ericson
Ambassador of Sweden to Finland

TEEMU TURUNEN

Intelligence diplomacy

Expert article • 3924

The main difference between intelligence and diplomacy – as I used to answer when asked - is the whole starting point of intelligence. Taking the world as it is, not as we would like it to be. While both are crucial for any country, we in Europe need to learn to use them more strategically together.

The world of today is in transition. While the old rules-based order is suffering, the new set of transactional rules are not yet fully formed. What is already clear though, is that the new rules are pointing towards a world of strongmen, who again intend to divide the globe in spheres of influence. Strength and interests weigh more than values. A world where might makes right.

This is a dangerous time for European democracies. Europe has been rather slow to interpret the signs of the changing world, or act accordingly. Adversaries have started to think that Europe is risk-averse and weak. We have forgotten what war is like. People die and people suffer. Countries and governments need to make unpopular decisions and sacrifices, trying to survive. While Ukraine has been fighting for its existence, it has also bought us time to prepare for a more dangerous world. We should use this time wisely.

Only recently have we started seriously talking about building up our defence, improving our resilience or making Europe feared again. While we are now increasing our defence spending rapidly, we need to make sure we prepare for the right threats at the right times and build resilience in the right places. And to do it together. Big spending without a joint threat picture or without a common plan would be a massive missed opportunity.

At the same time, dangers of today are much more than military threats. And strength is much more than military capabilities. Finland has been an example of comprehensive security model, including a whole-of society approach to preparedness.

As part of adapting to the new realities and as part of growing stronger together, Europe could benefit from learning to use our intelligence more wisely. We need more foreign policy focus in intelligence, and we need more intelligence in foreign policy.

More intelligence in diplomacy

Intelligence diplomacy does not have a clear definition. For the most part, it is understood as merely declassifying intelligence for diplomatic objectives. Declassifying intelligence before the Russian attack on Ukraine was a very successful example, giving an early warning to Ukraine, helping to unite the global west as well as paving the way for a smoother NATO-accession for Finland and Sweden.

Secondly, intelligence diplomacy is also the term when intelligence directors are used as back-channel messengers. Talking to those parties that one cannot be seen talking to. The most famous recent example was the role of the former CIA Director Bill Burns in Russia or in the Middle East, later declassified.

However, intelligence diplomacy could also be interpreted as a much wider concept. As the use of intelligence, together with allies, or against adversaries, in order to drive common objectives or create leverage. There are lots of tools in the leverage toolbox currently, as authoritarian states have very little moral limitations for weaponizing everything from energy to immigrants.

There are real, pressing threats to European security. Some are serious and deadly, including assassinations, sabotage or extremely harmful cyber attacks. But there are also clumsy proxy projects, cheap information campaigns or practically harmless denial-of service attacks, intended merely to confuse us.

The intelligence services have the capabilities to sort out which is which. They can predict and prevent the serious ones and dismiss the lesser ones. They need to bring the uncompromised, unbiased analysis to the table. Understanding the capabilities, objectives and modus operandi of the adversary, as well as their motives, fears, concerns and red lines. While the picture is never perfect, professional Intelligence is the best tool we have for understanding and countering the adversary.

Foreign policy actors need to use that intelligence – together with other sources of information - wisely and strategically, together with allies. Identifying and exploiting the vulnerabilities of an adversary would also allow us to turn the tables and start ourselves defining the agenda and rules. Otherwise we might get stuck in an endless game of whack-a-mole.

Without the combined understanding of intelligence and diplomacy, we risk either wasting our energy on bluff operations, crying wolf too many times or even worse – failing to show strength when tested or attacked.

More foreign policy in intelligence

While the intelligence services cooperate and share intelligence effectively with partners, their links to foreign policy decision-making might not always be very strong. Their understanding of the decision-maker or his/her realities could be suboptimal. And vice versa. The foreign policy professionals might not be able to interpret the message correctly unless they understand the intelligence cycle, different methods of collection or basic rules of the intelligence analysis. There is also a necessity for a common understanding of the foreign policy needs, in order to direct intelligence collection to the topics, organizations and people that really matter.

Therefore, both sides need to join forces and make sure that the message is well constructed, delivered, received and understood. The last part is fundamental, as intelligence failures typically derive from a lack of communication or understanding between the intelligence service and the decision-maker.

Even when the process is well coordinated on a national basis, and shared with allies, there is no easy way to use it effectively together, especially in multilateral settings.

Furthermore, during the more peaceful post-Cold War period, we have intentionally, and for a good reason, created legal and other hurdles for sharing or using the intelligence more widely than is absolutely necessary. Perhaps this is the right time to reconsider the necessity and scope of those hurdles and make them suitable for the current era.

While never surrendering to a world of disorder or giving up our core values, we could still acknowledge the facts, recognize the severity and urgency of the threats and start preparing ourselves for a more dangerous world. For the world as it is.

Teemu Turunen
Ambassador of Finland to the UK

JUSSI TANNER

Intelligence and foreign policy in military conflict

Expert article • 3925

According to the insipidly overused quote by Clausewitz, war is the continuation of policy by other means. If the main instrument of foreign policy is diplomacy, one is left with the truism that the same policy may be conducted sometimes by diplomacy, other times by warfare.

A popular speaking point goes that, for a given conflict, "there is no military solution, only a diplomatic one". This may be a useful soundbite for strategic communication, but from a Clausewitzian point of view, it is based on a misconception. Diplomacy and warfare are not mutually exclusive alternatives, but rather two different means to the same ultimate end, typically defined as existential interests of the state, such as the survival of its people and constitutional order.

In the context of military conflict, diplomacy can therefore be seen as a service branch that precedes, ties in with, and follows an active, kinetic phase in hostilities. In Northern Europe, the current mood music plays to the oversimplified tune of armed service branches and risks neglecting diplomacy as an essential tool in the box, a critically important tradecraft for all skilled and successful states.

Practically every armed conflict is preceded by diplomatic efforts. Equally, intense diplomacy takes place during every conflict: coalition-building with allies, sympathizers, and fence-sitters, and back-channel negotiations with adversaries, sometimes even with the enemy itself. And finally, every war comes to an end with some version of a diplomatic solution, be it a ceasefire, an armistice, or a proper peace treaty.

In the context of armed conflict, intelligence involves the collection and analysis of information to support tactical and strategic decisions. The underlying assumption is that key decisions should always be based on the best information available. In military intelligence, the end users – or policymakers – are typically field commanders, but they may just as well be politicians, diplomats, or intelligence professionals themselves.

In a way, a diplomat's point of view to intelligence is that of both a practitioner and an end user. In the first role, diplomatic tradecraft tries to reveal information about allies' and adversaries' motives that are otherwise hidden, sometimes by deliberate secrecy, other times, in plain view, by the sheer cacophony of the public space. A diplomat's objective is therefore much like that of an intelligence professional: to separate the relevant facts from lies and irrelevant noise and prepare those facts to leaders in a digestible and actionable format.

In the latter role, as end users, diplomats use intelligence as information for implementing foreign policy. In knowledge-based decision-making, intelligence typically supplements other types of information.
Importantly, as information, intelligence carries no specific value apart from its validity. The operational usefulness on any information lies in its accuracy, not in the method of its collection.

In the professional and public discussion, it is often implied that intelligence constitutes a special kind of information, one that carries inherent value for policymakers. This idea is exacerbated by the fact that most experts who speak about intelligence with authority are, like me, themselves members of a professional class that is heavily invested in the tradecraft. In other words, part of the tribe.

For the end user, this can be treacherous. Intelligence is a notoriously difficult tradecraft. It may provide critically important, timely information, or just as well lead to useless or even dangerous directions. For a real-life policymaker, it is often impossible to recognize the difference until the benefit of hindsight.

When intelligence is flawed, the risks for strategic policymakers become enormous. The case of weapons of mass destruction in Iraq in 2003 is a prime example.

In my own professional career as a diplomat, I have both profited from accurate, masterful intelligence, and suffered from analysis that has been fundamentally flawed. In August 2021, pertinent HUMINT about a coming suicide attack at Kabul airport's Abbey Gate saved not only our mission, but quite possibly lives of my team members, potentially including my own. A few years earlier, outdated and inadequate security risk assessments of Finnish children in ISIS detention camps in Northeastern Syria delayed their repatriations, prolonged their exposure to a radicalized environment, and increased the long-term security risks for the Finnish society.

Both were products of highly capable teams of analysts, with vastly different outcomes for the end user.

A professional, analytically ambitious discussion about intelligence is all the more important when it recognizes that the value of information isn't in the method of its collection, but whether it's good or bad.

Both abound.

Jussi Tanner
Director General for Consular Services
Ministry for Foreign Affairs of Finland

LOCH K. JOHNSON

National security intelligence in a democratic framework

Expert article • 3926

Introduction

Democracies have evolved as a form of government designed to safeguard citizens against the abuse of power concentrated into the hands of single leader. When the United States was founded in 1787, the idea was to establish a constitutional government based on a division of power among an executive branch led by a president, a legislative branch run by lawmakers, and a judicial branch comprised of judges. The backbone of this system was the rule of law. America's spy agencies at the time were expected to follow the law, but they were exempt from the day-to-day procedures of accountability ("checks-and-balances" or "oversight") designed to monitor the fidelity of government officials to the law. Intelligence was considered too sensitive and fragile for "normal" and ongoing government reviews. This was a big mistake.

Many years later, in 1974, it became clear that America's secret agencies had often violated the nation's laws. A major Senate investigation, known as the Church Committee (named after its chairman, Senator Frank Church, Idaho), uncovered domestic spying by the Central Intelligence Agency (CIA) against anti-Vietnam war protestors. The Committee found, as well, the existence of harassment operations carried out by the Federal Bureau of Investigation (FBI) against these same antiwar protestors as well as civil rights activists. Further, the Committee uncovered illegal espionage activities carried out by the National Security Agency (NSA) and the Defense Intelligence Agency (DIA) aimed at anti-war activities. The fact that America's Intelligence Community had violated the nation's laws on a number of occasions and had spied on peaceful demonstrations inside the United States created a firestorm of controversy in the country. Before these discoveries, formal laws specifically tailored to control America's spy agencies had been non-existent; now, after 187 years of "intelligence exceptionalism," things were about to change.

The domestic misuse of intelligence powers made it clear that America's spy agencies required closer supervision, similar to the rest of the U.S. government. Lawmakers realized, too, that more rigorous accountability would have to be directed not only toward preventing spy activities against American citizens, but to ensure that U.S. secret operations overseas were also closely monitored. The CIA and its companion agencies would be expected henceforth to remain within the boundaries of U.S. law at home and abroad.

The Hughes-Ryan Act watershed

The first step toward improved intelligence accountability occurred with respect to CIA covert action---an overseas dimension of intelligence activity. The use of covert action (CA) involves secret operations designed to harass or disrupt other nations, as opposed to intelligence collection activities (classic espionage). Congress enacted the Hughes-Ryan Act on December 30, 1974---just a few weeks prior to the establishment of the Church Committee.

Under these new rules, the president was required to formally approve all CAs. Gone were the days of presidential "plausible deniability." Now the paper trail for CA approvals led directly to the Oval Office and the president. More sweeping still, the president had to report all presidential approvals ("findings") to the appropriate intelligence oversight committees on Capitol Hill. Suddenly lawmakers were also explicitly in the intelligence loop.

The Hughes-Ryan law was majestic in its departure from previous practices. Here is the language of that law: "... No funds appropriated under the authority of this or any other Act may be expended by or on behalf of the [CIA] for operations in foreign countries, other than activities intended solely for obtaining necessary intelligence, unless and until the President finds that each such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of such operations to the appropriate committees of Congress."

That last phrase was revolutionary. Lawmakers at last had the opportunity to examine America's use of CAs before they were implemented. This reporting stipulation did not include all 435 members of Congress, of course, with the problematic security implications that would carry, but rather a small number of their colleagues on the Senate Select Committee on Intelligence (SSCI, pronounced "sissy") and the House Permanent Select Committee on Intelligence (HPSCI, pronounced "hip-see"). The creation of these two panels was the core recommendation of the Church Committee; their members would act as surrogates monitoring intelligence on behalf of the entire Congress.

How wise was it to bring some degree of democracy into the dark corners of CA---an experiment unprecedented at home, in other nations, or throughout history? From the vantage point of decreasing ill-considered---and at times even illegal---covert actions, it made sense. What about intelligence collection (espionage) and counterintelligence, however? Should they be closely monitored by a president and lawmakers as well?

The Intelligence Oversight Act of 1980

In 1980, the United States enacted a sweeping Intelligence Oversight law to supplement and refine Hughes-Ryan. This new law underscored that "prior" reporting to lawmakers on SSCI and HPSCI would be mandatory for "all" intelligence activities, not only covert action. Intelligence collection operations and counterintelligence would also have to be reviewed by lawmakers in advance of their implementation. With this chance for genuine debate within the confines of SSCI and HPSCI, lawmakers could now rebuke untoward proposals across the intelligence board---even threaten budgetary retaliation should the executive branch ignore guidance from SSCI and HPSCI. Prudently, the statute permitted a two-day reporting delay in times of dire emergency. Even then, though, the law required reports in advance to a small group of eight congressional leaders who became known as the "Gang of Eight."

The Oversight Act of 1980 established clearer boundaries for intelligence activities. This unprecedented attempt to bring America's secret agencies into the full workings of a democratic society was remarkable---and supported not only by intelligence reformers, but by leaders of the secret agencies themselves, who welcomed lawmakers to the burden of sharing in this difficult decision-making process. This approach to intelligence accountability carries high merit---indeed, is a lynchpin of democracy---since a truly free society must perpetually guard against the misuse of powerful secret agencies within their midst.

Loch K. Johnson
Regents Professor Emeritus of International Affairs
School of Public and International Affairs (SPIA)
University of Georgia
USA

See, also: Loch K. Johnson, *Spy Watching* (New York: Oxford University Press, 2018); *The Third Option: Covert Action and American Foreign Policy* (New York: Oxford University Press, 2022); and *National Security Intelligence*, 3d ed. (Cambridge, UK: Polity, 2025).

MARK PHYTHIAN

Intelligence and the politics of threat

Expert article • 3927

In the autumn of 2025, the UK's Secret Intelligence Service (SIS, aka MI6), saw the arrival of a new Chief ('C'), Blaise Metreweli, the first woman to head the organisation. Typically for a career intelligence officer in the UK, little is known about Metreweli. We do know that after studying Anthropology at Pembroke College, Cambridge, she joined SIS in 1999 where, prior to this appointment, she was Director General Technology and Innovation. Previously, she held operational roles in the Middle East and Europe and, at some point in her career, held a Director-level role in MI5.

Since 1945, each generation has seen itself as facing a more dangerous and uncertain world than previously: just look at the language of past defence reviews or national security strategies for evidence of this, or recall James Woolsey's February 1993 comment that, with the end of the Cold War: "We have slain a large dragon but we live now in a jungle filled with a bewildering variety of poisonous snakes. And in many ways, the dragon was easier to keep track of". Still, there are grounds for agreeing with Prime Minister Keir Starmer's statement in announcing Metreweli's appointment that the UK, "is facing threats on an unprecedented scale", and that, "the work of our intelligence services has never been more vital." Given the nature of these threats, Metreweli's CV explains her appointment; first and foremost, the expertise in technology, but also the operational roles in the Middle East and Europe, and cross-community professional experience – increasingly important in a world where old distinctions between 'foreign' and 'domestic' threats have given way to a more complex, 'intermestic', national security agenda.

Her predecessor as Chief of SIS, Sir Richard Moore, gave what amounted to his valedictory speech in Istanbul in September 2025. This was part of a significant trend in UK intelligence whereby agency heads deliver public speeches outlining the work and priorities of their agencies and assessment of the threat landscape. These are particularly welcome given the absence of a formal, published, annual threat assessment (as in the United States), or public evidence sessions in front of the UK's legislative intelligence oversight body, the Intelligence and Security Committee of Parliament, whose relationship with the agencies and executive branch has been strained over recent years. Moore himself gave a number of these speeches during his tenure, but it was his predecessor, Sir Alex Younger who broke significant ground with a speech at St Andrews University in December 2018, in which he talked in terms of the "fourth generation espionage" required to tackle the "degree of interconnectedness between nations, peoples and systems today, the ubiquitous nature of information, and the exponential pace of technological change, [which] are making the world dramatically more complicated."

At the same time, the Director of GCHQ, Jeremy Fleming, was giving significant and reflective speeches on the work of his organisation and the threat environment it faced: for example, discussing the concept of a "Cyber Power" and speaking openly about "offensive cyber" operations. Principles of accountability and ethical conduct tended to be emphasised in these speeches, reflecting the immediate post-Snowden context and need to rebuild trust and so assert the legitimacy of the activities and approaches being outlined. In a subsequent speech, the October 2022 RUSI Annual Security Lecture, Fleming focused on, "what I believe is the national security issue that will define our future", asking: "If China is the question, then what is the answer?". For Fleming, "when it comes to technology, the politically motivated actions of the Chinese state is an increasingly urgent problem we have to acknowledge and address. That's because it's changing the definition of national security into a much broader concept. Technology has become not just an area for opportunity, for competition and for collaboration, it's become a battleground for control, values and influence."

Moore's September 2025 Istanbul speech focused on the threat and challenges posed by Russia. He also outlined a new way in which the traditional human dimension of the craft of spying was being supported by technology. Moore set out how, "those men and women in Russia who have truths to share and the courage to share them" could now, "reach us securely online via our new dark web portal, Silent Courier. Our virtual front door harnesses the anonymity of the dark web so that anyone, anywhere in the world can make secure contact with MI6. So, contact us today via Silent Courier and choose a different future for yourself, for your family and for your country."

At the same time, Moore discussed SIS's other three priorities – China, Iran, and counter terrorism – making it clear that Silent Courier was not simply a resource to be considered by those inside Russia. As Moore explained: "Anyone, anywhere in the world with access to sensitive information relating to terrorism or hostile intelligence activity, can use the new portal to contact MI6." The challenges posed by China, as a rising global power, were more complex, and Moore's depiction of a country that "in many respects straddles that dichotomy of opportunity and threat" captures well Western state dilemmas. As he put it: "We, in the UK, want a respectful and constructive relationship with China. But China needs to stick to the established rules of engagement and non-interference that it publicly promotes. I hear the concerns of my colleague, Director MI5 Sir Ken McCallum, about Chinese interference in the UK; and we, in the UK, will be robust in defending our freedoms, our way of life and our economic security."

Yet, that same month, a political row broke out in the UK after the Crown Prosecution Service (CPS) abandoned the prosecution of two men, one of whom was a former parliamentary researcher, charged under the Official Secrets Act with passing information to an "enemy" (both men denied the charges). Reportedly, the CPS dropped the case because it could not secure a government witness statement to confirm that China was indeed "a threat to the national security of the UK", as per the requirement of the legislation. Was this due to government back-tracking and a preference for labelling China a "challenge" but not an "enemy", as it sought to develop UK-China trade relations? Or was it a decision reached by the CPS without any governmental pressure? A high-profile blame game ensued. Either way, the wording of the relevant legislation at the time was not helpful and did not reflect the complex world of contemporary national security. That China did pose a threat to the UK was a well-established reality for MI5, SIS, and GCHQ – as shown above.

At the same time, developments over recent months have begged questions not just of when, in the contemporary world of big power competition underpinned by 'deniable' conduct in the cyber realm, a foreign state represents enough of a challenge or threat to be labelled an 'enemy'. Questions of what constitutes a 'friend' in intelligence, security and alliance terms have also been raised: for example, by the implications of the Trump Administration's 'America First' approach for Five Eyes co-operation and intelligence-sharing (for example, with regard to the Russo-Ukrainian War), and by claims that Hungary has operated a spy network in Brussels, casting doubt on its reliability, or sense of shared purpose, as an EU member state.

While the intensity today is different, and the land war in Ukraine is certainly an exceptional state of affairs, competition and the pursuit of advantage in the international system are enduring and inevitable facts of life. We live in an era in which major revisionist powers are challenging and disrupting the status quo, emboldened by, and fully utilising, the potential offered by new technologies. In this context, challenges and disruptive activities invite countermeasures, which also have ramifications for the international environment, impacting on targets' perceptions and future behaviour and so contributing to intelligence's own version of the security dilemma. Hence, while UK intelligence highlights (and prosecutes) Russian human intelligence collection methods and warns against the threat posed by China, SIS publicises the possibilities presented by Silent Courier. This is the highly competitive, complex, and unstable international security environment that Blaise Metreweli faces as the new Chief of SIS.

Mark Phythian
Emeritus Professor of Politics
University of Leicester
UK

mp249@le.ac.uk

JOHN A. GENTRY

The cultural politicization of intelligence

Expert article • 3928

The politicization of intelligence products by intelligence officers or consumers long has been seen as inappropriate and unwise. It biases intelligence analyses, increases chances of major intelligence errors, and endangers policy-making. In recent years a new variety of politicization has emerged: the purposeful injection of ideology into intelligence agencies that alters organizational cultures and introduces new sources of analytic error. The most prominent example is the diversity, equity, and inclusion (DEI) policies of U.S. Presidents Barack Obama and Joe Biden, but evidence is growing of similar influences in Canada, the United Kingdom, and other European NATO countries.

Obama and Biden engineered politicization by issuing ideology-based executive orders that mandated DEI-related policies in federal agencies and appointing senior executives of intelligence agencies, such as CIA directors John Brennan and William Burns, who used command emphasis and bureaucratic incentives to embed DEI into agencies' organizational culture, thereby influencing routine thought processes and actions. Means included promulgating formal policies, embedding DEI principles in employee rating standards, establishing offices dedicated to monitoring compliance with executive orders, and publishing The Dive, an initially classified magazine designed to tell employees how to think about people, organizations, and issues in ideologically correct ways. Aims and processes were publicly clear and were explicitly designed to change organizational cultures.

DEI is a major problem for Western democracies because it is an action arm of "critical race theory," which is a product of the so-called Frankfurt School of what often is called "cultural Marxists" who aim, like Karl Marx but in different ways, to overthrow Western democratic governments and civilization, and replace them with Marxian utopias. DEI often is disingenuously disguised as a means to promote social justice.

Considerable evidence shows how DEI policies damage intelligence workforces and output. By many accounts, U.S. intelligence officers in recent years were hired, promoted, assigned, and given awards based on membership in large, visually identifiable demographic identity groups, not ability. DEI policies negatively affected interpersonal relations within agencies, damaging the cooperation important to do intelligence work. In the Obama/Biden years, opponents of DEI policies feared they would be punished by supporters of DEI and were careful about speaking candidly with colleagues. Brennan urged CIA personnel to be politically active in defense of DEI policies. The surge in leaks, including disinformation, in 2016-2021 and in 2025 reflects politically motivated employee actions against President Donald Trump.

We have less information about how these biases affect the quality of intelligence provided to national leaders and their effects on decision-making. One clear case is Obama's insistence that terrorism of the sort practiced by Osama bin Laden and al-Qaeda be called "violent extremism," with no mention made of possible connections to Islam. This preference is now embedded in U.S. intelligence culture, biasing terrorism-related analyses. Surely there are other examples, but they are difficult to identify. Indeed, when such views are seen as worthy, they are perceived as truth, not biases. Other Marxian ideological biases damaged Soviet intelligence analysis for decades.

In his second term, President Trump has attacked what he calls the "weaponization" of intelligence against him by the "Deep State," including by revoking Obama- and Biden-era executive orders and investigating persons such as Brennan. But his intelligence agency heads have not yet made significant efforts to change agencies' organizational cultures. The Deep State is fighting back, duplicitously claiming that Trump is politicizing intelligence, thereby employing the time-honored intelligence operators' technique of "projection" by claiming others are doing one's own actions. Trump has not clarified whether he wants to restore the old ethic of apolitical public service or seek retribution against political enemies, aiding his critics. This conflict merits close monitoring.

This history has three major lessons for Europe. First, beware of injecting ideology into agencies' organizational cultures because it generates analytical biases and flawed intelligence. DEI has often been pushed deceptively. It is important to recognize the divisive nature—and intent—of this agenda. Second, short of a major purge, it is difficult to remove such biases once established. Hence, prevention is the best policy. Third, intelligence services should monitor the information they receive from intelligence partners for ideology-based biases. Even close allies maintain their own perspectives on some issues, which now are more important than ever.

John A. Gentry
Adjunct Professor
Institute of World Politics and the School of Defense and Strategic Studies
Missouri State University
USA

PETER GILL

Intelligence and authoritarians: a duty to disobey?

Expert article • 3929

Important questions are raised currently about the stability of the relations between security intelligence agencies and their parent 'liberal democratic' governments. Populist electoral movements have already given rise to illiberal authoritarian nationalist governments in, for example, Argentina, Brazil (2019-23), Czechia, Hungary, India, Israel, Slovakia and the United States and lead in the polls in France and Germany.

It is not clear that all these governments have clashed with their intelligence agencies, but there are examples of this occurring. The most obvious is the United States where it was suggested that Gina Haspel, when appointed CIA Director in 2018 would be the first director who ever had to confront the problem of what to do when the president of the United States was a threat to national security because of his relationship with Vladimir Putin.[1]

Emboldened by his re-election in 2024, Trump appointed the inexperienced Tulsi Gabbard as the Director of National Intelligence (DNI), who then applied loyalty tests to potential recruits relating to their voting record and belief about the 'stolen' 2020 election. Gabbard fired the top two officials of the National Intelligence Council after their analysis challenged arguments that the Venezuelan government directs the Tren de Aragua gang, which had been Trump's rationale for invoking the Alien Enemies Act. In 2025 Gabbard revoked the security clearances of 37 former and serving officials (effective dismissal for those still serving) where the common factor was their involvement in the 2017 assessment of Russia's interference in the 2016 election. In the same year, the FBI forced out three senior officials who had either been involved in investigating the January 6, 2021, Capitol Hill riot or resisted White House efforts to identify other agents who were.

In Israel in April 2025, under pressure from PM Netanyahu, Ronen Bar announced that he would resign as Director of Shin Bet. The Supreme Court granted a temporary injunction and Bar submitted an affidavit to the Court (part public and part classified) in which he said Netanyahu demanded that he make false claims of security risks in order to extricate the PM from his corruption trial, that Bar obey him rather than the Supreme Court in the event of a constitutional crisis and that Bar take action against anti-government protesters. Also, in 2025 forty-one officers within the IDF Intelligence Directorate wrote to Netanyahu saying they would refuse to take any further part in the Gaza offensive, for example, selecting bombing targets.

In Germany the domestic security intelligence organisation Bundesamt für Verfassungsschutz (BfV) had already classed Alternative für Deutschland (AfD) as right-wing extremist and so incompatible with the free democratic order in three eastern states and in May 2025 this was extended nationally. This determination, which survived a court challenge from AfD, permits increased covert surveillance of AfD by informants and interception of communications etc. AfD were second in federal elections in February 2025 with 21% of the vote and have 152/630 seats in the Bundestag, therefore it is not unrealistic to imagine them as part of a future ruling coalition in Germany and the consequent potential for a clash between professionals and government.

The role of domestic agencies is to protect the regime against national security threats. It was only after 1945 that a few countries, mainly the victims of Nazi occupation, introduced legislation that provided a legal (rather than solely pragmatic) basis for agency actions and basic oversight structures. It was the 1970s before more liberal democratic countries followed suit, mainly in response to scandals of excessive surveillance of citizens by internal agencies. Following the end of the Cold War and the attempt to democratise Eastern Europe and the former Latin American military dictatorships, legislation mandating agency powers and oversight became widespread. These laws tended both to empower the agencies and to restrict them in certain areas but one key aim was to make security organisations more accountable to elected ministers. Paradoxically, this democratic principle now provokes the question of how agencies defend democratic principles that are under attack from elected authoritarian governments.

Democratisation continued into the new century but since 2008 has ground to a halt for several reasons: economic, reflecting the impact of the financial crash on incomes and social including the increasing fears around immigration both in the US and Europe. As a result, populist proponents of various forms of illiberal democracy have prospered and even if they have not won power their impact on governance has been significant. There is an extensive literature on what is described as 'democratic backsliding' in general but little analysis of its effect on security intelligence agencies. Perhaps this is because they are assumed to be such reliable bastions of support for governments whatever their policies, but it is the very centrality of the agencies to the survival of governments that requires specific consideration of how they deal with trends towards illiberal governance.

Any illiberal government depends on loyal security organs to stay in power, but we cannot assume that all the agencies involved in security governance act together or speak with one voice: 'bureaucratic politics' may rule. Technological changes in the twenty-first century have enhanced the agencies' capacity for mass surveillance through their symbiotic relationship with the corporate suppliers of communications, Internet and social media in an overall structure that might be described as surveillance corporatism. While these agencies will be a tool of authoritarian governments, they may also be their victims. So, if constitutional checks and balances are being eroded through the actions of elected authoritarians, how will, or should, security intelligence agencies react?

On the face of it, the answer is simple: from an instrumental perspective bureaucrats act neutrally to implement the policies of the executive power, but authoritarian leaders view the bureaucracy as part of the 'swamp' and seek to change it into a loyal extension of their power. To the extent that these governments see themselves as opposed by varieties of 'undesirables' - socialists, eco-warriors, Islamists, migrants – leaders will define the agencies' role in traditional ways: the surveillance and disruption of groups who may resist or take action, however peaceful, against the government of the day. As such, the agencies have more often been viewed as potential threats to liberal democracy.

In many countries no doubt this simple answer still pertains but we might consider an alternative institutionalist perspective in which bureaucrats are 'guardians of state institutions and protectors of the democratic way of life'[2] Officials cannot be value neutral and purely instrumental but are responsible for defending the principles and institutions of liberal democracy including constitutionalism, the rule of law and the public interest.

But, have the changes in law, governance, recruitment, training, working cultures and oversight of the past half century produced internal security agencies which will not simply do the bidding of ministers but will push back against them when they believe their requests/orders are illegal or unethical? Even if intelligence officials believe that a policy is mistaken or likely to be counterproductive, though not actually unconstitutional, they are, to quote the well-worn aphorism, obliged to 'speak truth unto power'. In practice, that can be difficult, but how much stronger is the requirement if an executive proposal is seen as unconstitutional? Might the agencies become less the tools of authoritarians' rule by law and more the defenders of rule of law?

It is possible to identify an escalatory ladder of resistance: ignoring demands, submission of critical reports, whistleblowing, active disruption and culminating in resignation which might all be legitimate if based on a proportionate response to the executive, but the serious difficulties and potential costs facing resisters are undeniable. Even if resisters identify what is to them an illegal use of executive power, it is likely to be characterised by authoritarians, not as legitimate defence of the institutional order, but as confirming their claim that they face the opposition of a 'deep state'. As the earlier examples show, executives and their loyalist agency directors may simply dismiss resisters or take disciplinary action against them therefore, although resisters may find there is some protection to be had in group solidarity, resistance may cost them dear. But if officials see that the rule of law and accompanying liberal order are at stake is there not a duty to disobey?

[1] Tim Weiner, *The Mission: the CIA in the 21st century*, Willaim Collins, 2025, p.313.
[2] Michael Bauer,'Administrative responses to democratic backsliding: When is bureaucratic resistance justified?' *Regulation and Governance*, open access 2023 p.7 (18:4, 2024, 1104-1117); see also Cüneyt Gürer and Elena Walczak, 'Democratic Backsliding and Security Governance, *Connections*, 23(4) 2024, pp9-31; Kutsal Yesilkagit et al, 'The Guardian State: Strengthening the public service against democratic backsliding, *Public Administration* Review, 84, 2024, pp. 414-25.

Peter Gill
Visiting Professor
School of Criminology, Sociology and Policing
University of Hull
UK

pgill806@gmail.com

GRETA E. CREECH

The tetrahedron of trust: Navigating institutional distrust in Western intelligence

Expert article • 3930

Western intelligence services function within a tetrahedron of competing demands for trust and distrust. On one side of the tetrahedron, a mission to protect populations from external and domestic threats require significant levels of trust between intelligence officers, allied partners, and their respective institutions. The stakes are high, and the cost of failure can be unimaginable. Collaboration in judgements free of partisan influence are norms simultaneously intended to mitigate intelligence failures and increase public confidence in national intelligence services. A second side of the tetrahedron requires that those groups also navigate healthy levels of skepticism toward each other to prevent the unimaginable. Classification and compartmentalization structures are institutionalized skepticism paradoxically designed to build trust, at least in the system. In the ideal, that system works primarily because it is counterintuitive. A third side of the tetrahedron is no less important: public access. Democratic voters must traverse competing entitlements to access data without being relegated to outsiders lacking a "need to know." The paradox of secrecy is the third side. Public trust in people they never see engaged in activities they cannot know about is fragile but necessary.

Political polarization and broadly held institutional distrust in the West forms the dark underbelly of the tetrahedron. At the same time, the decline in trust is uneven in appearance. In the Baltic Rim, approximately 80 percent of Latvians distrust government institutions due to political instability, scandals, and growing income inequality. Lithuania and Estonia show less entrenched distrust, though both face challenges from economic inequality and, in Estonia, entanglement with tensions between ethnic Estonians and Russians. Distinguishing between concerns over middle-class abandonment versus 500 years of history can be a challenge. In Finland, distrust is linked with immigration and welfare chauvinism. In Germany, institutional distrust intertwines with debates over immigration and national culture that often blur ideological boundaries.

To what degree growing distrust may be affecting the national intelligence services across the Baltic Rim is unknown. Beyond a reallocation of resources to prepare for potential extremist unrest, some might argue the effects are limited because intelligence officers are a unique class and unperturbed by wider sociopolitical forces. However, that assumption lacks data because the question has not been explored in research. Additionally, the standard profile of those most likely to distrust institutions is the lower-middle-class, less-educated, and rural voter—distinctly different from the workforce inside many intelligence services. However, new research involving 143 countries indicates that rising distrust crosses class, income, and cultural lines.[1]

Those working in intelligence organizations are expected to challenge their analytic assumptions regularly to provide national policymakers with the best actionable intelligence they can. However, they are often less adept at challenging assumptions about themselves and their institutions. Intelligence officers are just as likely to fall victim to cognitive bias as workers in other fields; like everyone else, overcoming false assumptions takes work and will.

The first step is to ask the question. National intelligence officers do not compartmentalize their lives. Work and home lives are mutually constitutive. Thus, they are not siloed from scandals, fears over falling behind, and the social pressures from issues driving institutional distrust within the wider public. Depending on agency rules, intelligence officers may have online social media accounts exposing them to the same disinformation narratives, poits of anger, and other nefarious content as the broader public. If so, they can also be subject to adversarial cognitive warfare efforts in ways that they and their institutions may not realize. Research suggests that even those trained to analyze disinformation and conspiracy narratives are ultimately affected by them.[2] The effects are typically more emergent and less overt, which can have the most insidious impact because no mitigating measures are available to address them. Thus, loyal citizens and even institutional leaders might come to distrust their own institutions before realizing the dynamic is under way.

U.S. intelligence agencies have never been immune from complex sociopolitical environments. Rather, they have historically embraced policy neutrality as a core value to insulate themselves from efforts by some to weaponize intelligence for political gain. Their efforts have not always been successful. Nevertheless, the widespread uncertainty and ambiguity within the intelligence environment challenges the accuracy of assessments enough without analysts having to participate in a "game" focused more on political advantage than security. That distinction between political power and security vanishes when policy debates become so entwined with psychological safety that leaders view having an advantage as security for the country.

The U.S. has become a live-action role play for this phenomenon. Congressional overseers across the two-party aisle promote narratives suggesting that the intelligence community cannot be trusted. Members of the left-leaning Progressive Caucus in the U.S. Congress have accused U.S. intelligence of using its surveillance authority to avoid congressional oversight.[3] In March 2025, intelligence analysts whose assessments contravened Trump Administration positions were accused of politicization and fired.[4] Administration allies in the intelligence community characterized the leaks as the work of "deep state criminals."[5] The American public is also unsure. Gallup research from 2022 found that approximately half of those surveyed held favorable opinions about the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA)[6] —which is also to say that half did not.

The controversies extend beyond questions of politicization into one more basic. Could institutional distrust undermine Western intelligence services from within by seeping into the mindsets of the men and women who work there? If so, distrust would become self-reinforcing by validating the phenomenon that led to the failure to begin. The result would be to apply destructive pressure to all sides of the tetrahedron simultaneously. We cannot know until we ask the question, but the stakes are too high to adopt blinders.

[1] Viktor Valgarðsson et al., "A Crisis of Political Trust? Global Trends in Institutional Trust from 1958 to 2019," *British Journal of Political Science* 55 (2025): 1–42, https://doi.org/10.1017/S0007123424000498.

[2] Ruth Spence et al., "The Psychological Impacts of Content Moderation on Content Moderators: A Qualitative Study," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 17, no. 4 (2023), https://doi.org/10.5817/CP2023-4-8.

[3] "CPC Chair Jayapal Stresses Fight to End Warrantless Surveillance of Americans Will Continue," Government, Congressional Progressive Caucus, April 24, 2024, https://progressives.house.gov/2024/4/cpc-chair-jayapal-stresses-fight-to-end-warrantless-surveillance-of-americans-will-continue.

[4] Charlie Savage, "The Latest: Leaks Investigation: Suspect in Leaked Documents Expected in Court in Boston," *The New York Times,* April 14, 2023, sec. U.S., https://www.nytimes.com/live/2023/04/14/us/leaked-documents-pentagon.

[5] Sarah Fortinsky, "Gabbard Refers Intel Leaks to DOJ, Blames 'Deep-State Criminals,'" Media, *The Hill*, April 23, 2025, https://thehill.com/regulation/national-security/5264296-gabbard-refers-intel-leaks-to-doj-blames-deep-state-criminals/.

[6] Gallup, "Government Agency Ratings: CIA, FBI Up; Federal Reserve Down," Commercial, Gallup.com, October 5, 2022, https://news.gallup.com/poll/402464/government-agency-ratings-cia-fbi-federal-reserve-down.aspx.

Greta E. Creech
Ph.D., Assistant Professor of Intelligence & Security Studies
The Citadel (Military College of South Carolina)
Charleston, South Carolina
United States

gcreech@citadel.edu

NEIL RAWSTHORNE

The democratisation of intelligence

Expert article • 3931

Building upon the UK's flagship foresight publication of Global Strategic Trends[1] there is the recognition that the global security environment is subject to a set of powerful, interacting drivers. These include intensifying competition among major powers, the growing influence of regional and non-state actors, demographic shifts, technological innovation, climate change, and increasing inequality. Each act both independently and in combination with others, accelerating or counteracting trends in ways that are often unpredictable and contradictory. The result is a future operating environment that is more volatile and contested but also more interconnected and ambiguous than ever before, defined by complexity, uncertainty, and rapid transformation.

Technological change is therefore both a driver and a disruptor within this environment, where boundaries between state and non-state authority are anticipated to become increasingly porous. This trend is being driven by the proliferation of open-source information, the commercialisation of intelligence services, and the widespread availability already of advanced technologies such as sensors, AI, and data analytics with quantum and ASI on the horizon. All of which are transforming military capabilities and the very character of conflict through the democratisation of intelligence, which refers to the increasing accessibility of intelligence capabilities—collection, analysis, and dissemination—beyond the exclusive domain of nation-states. The advent of commercial satellite imagery, open-source intelligence platforms, and powerful analytical tools has widened the playing field. Corporations, non-governmental organisations, activist groups, and even individuals can now access and exploit information that was once the exclusive preserve of national intelligence agencies. Defence planning in the future operating environment must therefore account for the influence and potential partnership—or opposition—of such non-state actors, including commercial and third-sector entities.

The abundance of data and the proliferation of information sources through such democratisation present both opportunities and challenges. On one hand, the availability of open-source and commercial intelligence can enhance situational awareness and enable more informed decision-making. On the other hand, the sheer volume of information increases the risk of decision paralysis, confirmation bias, and the inadvertent or deliberate spread of mis- and disinformation. This will have profound implications for defence policy and alliance structures, where the need for verification and trust in intelligence will remain in tension with the desire for speed and agility, as actors seek to exploit fleeting opportunities in a rapidly changing environment. In turn, there will be significant consequences for the security and conduct of operations and the protection of sensitive information both now and in the future.

Forces will need to be designed for agility, redundancy, and the ability to operate in environments where information is contested, resources constrained and attribution difficult. In response the line between state and non-state authority will continue to blur, as states outsource functions to commercial actors with independent capabilities who can provide cheaper, more appropriate and timelier rebuttal and surge capacity. The rapid advancement and diffusion of core AI systems across all domains will enable this further, with the ability to trawl, process and aggregate a myriad of data sources, both structured and unstructured, and draw insights that would have been beyond previous human capability. Constraints will be more through ethical and legal considerations (such as privacy and GDPR legislation) than technical limitations which less scrupulous actors/regimes will capitalise upon. Although arguably ceding power to private entities, such an approach enables states to better focus critical specialist resources on the intelligence capability demanded by governments to underpin national security decisions at the highest classification.

In summary, the democratisation of intelligence and the growing influence of non-state actors present both challenge and opportunity for future security. The combination of such information proliferation along with wider accessibility through AI systems is set to reshape the integration and interoperability of defence and security. Whilst fundamentally the principles remain unchanged, the speed and efficacy of an increasing suite of information tools offers the promise of enhanced situational awareness, faster decision-making, and more effective coalition operations. Perversely it also introduces new risks related to fragmentation, trust, and control as well as the spread of unverified and mis-information – with the need still for assured national assets with specialist tradecraft.

[1] Global Strategic Trends 7th Edition – Out to 2055, UK Ministry of Defence 2024.

Neil Rawsthorne
Head Strategic Foresight
Defence Futures and Force Design
UK Ministry of Defence
UK

JOONAS WIDLUND

Strategic intelligence in a democracy

Expert article • 3932

The 2019 intelligence legislation package introduced legislation on strategic intelligence to Finnish law. The package included legislation on civilian intelligence, military intelligence, the use of network traffic intelligence in civilian intelligence, and intelligence oversight. Before the enactment of the 2019 legislation, Finland was one of the few remaining countries in the European Union without specialised intelligence legislation. The need for intelligence legislation in Finland was based on the changes in the global security environment, and on the increased importance of the cyber environment in the context of national security. The enactment of the legislation also served to show how ubiquitous a tool intelligence has become in liberal democracies.

The goal of intelligence is to achieve a decision-advantage using the foreknowledge that well-timed and high-quality intelligence information can yield. Modern strategic intelligence is characterised by an expansive field of acceptable targets: strategic intelligence no longer focuses on the military and espionage activity of other states alone. The new types of asymmetric threats and hybrid activities carried out by both state and non-state actors have become key targets of strategic intelligence along with global terrorism and serious international organised crime. The line between internal and external security has faded as societies have undergone digitalisation, resulting in the critical functions of the state becoming dependent on digital systems and networks. This has created new vulnerabilities that can be exploited with very little resources by hostile actors.

With the importance of foreknowledge in countering the new types of threats, it is not surprising that democratic states have come to adopt strategic intelligence as a part of their security apparatus. There is, however, an inherent tension between intelligence and democracy. Intelligence is defined by secrecy, lack of transparency, challenges related to accountability and oversight, and the special nature of intelligence agencies compared to other parts of the government. Intelligence also has power implications, as it centralises power through information control to the executive. In contrast, democracy is based on openness, transparency, predictability, and accountability, as well as decentralised power through the separation of powers.

Because of this inherent dissonance between intelligence and democracy, democratic states must find a way to control and minimise the risks intelligence poses to democracy. The key to this is the process of democratisation of intelligence. Establishing a credible independent intelligence oversight system and the juridification of intelligence – creating a legal basis for the intelligence agencies and their intelligence powers – are key components of the democratisation process. Oversight is necessary in order to ensure the legality and accountability of intelligence activities, and juridification makes intelligence visible and a part of the legal system, as it is not democratically acceptable that intelligence boils down to secret activity carried out by secret organisations. Democratisation of intelligence is a process that describes the relationship between a given state's core values – democracy, rule of law, and human rights – and its intelligence apparatus. As such, it is entirely possible for democratisation to regress, if any of its elements are weakened.

Rule of law is currently under pressure in Western democracies, and a portion of the pressure stems from the unstable global security environment and the intensifying securitisation caused by it. Feelings of insecurity can lead to the notion that the less constraints the state's intelligence apparatus has, the more effectively it can guard national security. After all, the authoritarian states causing insecurity are not known for caring about the democratic legitimacy of their intelligence services. This line of thinking contains a grave misconception about the nature of democratically legitimate intelligence. First of all, the democratic principles and rule of law prevent the intelligence services becoming too autonomous and unfocused. Secondly, the principles help to ensure that the personnel of the services are qualified and well-trained. Thirdly, democratically legitimate intelligence helps maintain societal trust towards the authorities by ensuring accountability and providing legal safeguards. Societies without trust are fragile: this is why many authoritarian and totalitarian states eventually crumble from within. Intelligence services in a democratic state are not tasked to only protect the survival of the state, but protect the survival of the state as a liberal democracy, and in this task, the principles and oversight of democratically legitimate intelligence are a strength, not a weakness.

Joonas Widlund
D.Sc. (Admin.), Postdoctoral Researcher
School of Management, Public Law
University of Vaasa
Finland

JOHANNES KOPONEN & NATHANIEL GILKEY

Acting before geopolitical risk materialises

Expert article • 3933

In global trade, geography has always set the stage but today information decides the performance. Naval theorist Alfred Thayer Mahan's 1890 insight that power rests on command of trade routes still applies, yet the nature of command has shifted. More than ever, resilience is built not only via command and control but also via successful and precise risk prediction and mitigation at scale.

To illustrate the change, imagine a typical case: The leadership team at a Finnish high-technology manufacturer followed early reports of rising tension near a set of industrial towns in western Ukraine, an area known for producing wiring harnesses used across the automotive and electronics sectors. When fighting later intensified, several factories were forced to shut down. Inside the company, the news triggered a series of reasonable mitigation actions.

Crucially, the interpretations about the impacts were correct. But they were reached after the disruption was already unfolding.

This reveals a central weakness in how organisations today understand external geopolitical risk. The limitation is rarely a lack of intelligence or analytical skill. People inside organisations routinely make sophisticated, multi-dimensional sense of events. The real constraint is timing. Many organisations still form their situational understanding after the event, when costs have already begun to accumulate.

Unlike traditional analytics systems that rely on fixed parameters, artificial intelligence (large language models) can help to recognize emerging patterns in unstructured sources. Artificial intelligence is a poor forecaster, but it excels in inference: at connecting context, linking a customs regulation update in one country with freight delays elsewhere, or identifying sentiment changes that may precede price shifts. Their strength lies not in replacing human judgment but in extending its horizon. When combined with existing logistics and sensor data, they enable early identification of developing issues.

It is understandable that companies historically responded to geopolitical risk reactively. But today, with the aforementioned tools, the probabilities of such disruptions and their likely operational impacts can be estimated far more precisely than most assume. Prediction markets, structured inference systems, and large language models now make it feasible to assign auditable probabilities to emerging developments—such as policy shifts, port slowdowns, sanctions, and regional protests—before they fully materialise.

This shifts organisational sensemaking from explaining what has already happened to evaluating what is becoming more likely. Instead of multiple interpretations emerging only once disruption is visible, the organisation can observe a common probability signal as it changes. A shared probabilistic frame becomes a shared language.

Our work at Aie (whyaie.eu) applies this principle: we calculate comparable probabilities for external risks affecting specific supplier groups and sourcing categories, enabling organisations to judge alternatives on a common scale.

For the Baltic Rim, where supply chains are exposed to chokepoints in energy, shipping, and cross-border logistics, this shift is strategic. A shared pre-event situational picture allows companies to reroute shipments, hedge exposures, and adjust commitments before avoidable crises occur.

The next phase of trade resilience will depend on how effectively Baltic rim nations combine physical and informational infrastructure. Ports and ice-class vessels remain essential, but essential are also systems that interpret global supply risk signals in real time. Investing in predictive capacity is not a technological luxury; it is a strategic necessity, akin to coal, radar, or meteorological intelligence in earlier eras of maritime modernization.

As global trade faces new volatility, the Baltic region stands at the frontier. Geography defines potential; insight defines power. Predictive capabilities, supported by artificial intelligence inference, are becoming the operating doctrine for resilient trade. Just as radar once extended the vision of navies, predictive capabilities extend the vision of economies, turning uncertainty into a manageable variable rather than an unknown unknown.

Johannes Koponen
CEO
Aie (whyaie.eu)
Finland

johannes@whyaie.eu

Nathaniel Gilkey
Senior Geopolitical Analyst
Aie (whyaie.eu)
Finland

JAN GOLDMAN

Covert operations and hybrid warfare

Expert article • 3934

Espionage activities in the Baltic Rim stand as both a symbolic and practical battleground in the contest for strategic advantage between Russia and the West. Its significance is rooted in geography, history, ethnic composition, and its status as a borderland between NATO, the European Union, and the Russian sphere of influence. With the war in Ukraine raging on, we can see a step up in Russian covert operations in support of hybrid warfare.

Historically, one of the most significant Western clandestine operations of the early Cold War was Operation Jungle (1949–1955), run by the British MI6 in collaboration with US-backed West German intelligence, which sought to insert resistance agents into the Baltic states to provide material support to indigenous anti-Soviet groups and gather signals and human intelligence. Nevertheless, Operation Jungle encountered formidable Soviet counterintelligence, which was led by the KGB, successfully penetrated, captured, or turned most agents inserted by the West, often transforming them into double agents and feeding disinformation back to Western handlers. Undercover agents were cultivated and even sent as "false defectors" to infiltrate anti-Soviet organizations and Western intelligence services.

Today, as part of its information warfare and propaganda campaign against the Baltic States, Russia has intensified its efforts to sow fear and disrupt institutions. With social media platforms such as Telegram and TikTok playing a key role in the propaganda campaign, the government targets the political process, historical narratives, NATO membership, and support for Ukraine. Information warfare is further enhanced by AI-driven misinformation and deepfake technologies. In Apil 2025, NATO held an held an emergency meeting following a series of coordinated cyberattacks on critical infrastructure in Lithuania, Latvia, and Estonia attributed to Russian state-backed actors. The attacks targeted government networks, energy grids, and digital communication systems, causing service disruptions and exposing vulnerabilities in regional cybersecurity frameworks.

In addition to non-violent subversion, Russia has been using covert operations to attack the Baltic Rim States. For example, it has been reported that thirteen Estonians attacked the Interior Minister's car, while in Latvia, pro-Russian activists targeted national security sites, vandalized public spaces in Riga, and attacked the Museum of the Occupation of Latvia. This, in addition to a July 2024 incident where incendiary devices hidden in packages caused a fire at logistics hubs in Leipzig, Germany, and Birmingham, United Kingdom. The parcels were reportedly shipped from Lithuania. The destabilizing potential of non-violent and covert actions as a method of weakening NATO and EU influence in Russia.

Another tactic in Russia's hybrid warfare strategy is to use GPS jamming. These tactics have been ramped up since its war in Ukraine. As a result of Russian jamming, aircraft near Baltic Rim airports are losing their GPS signal, which endangers passengers and crews and undermines communications. Meanwhile, the Baltic Sea has seen an increase in reports that Russia has conducted sabotage operations and targeted critical undersea infrastructure. Its shadow fleet has been scraping the ocean's seabed to cut internet and power cables.

The result has been to significantly heighten tensions in the region, strain diplomatic relations, and increase the risk of a military confrontation. Without a doubt, this atmosphere of uncertainty and mistrust could potentially escalate into broader conflicts if left unchecked, destabilizing the entire region and beyond. Without a doubt, the Baltic Rim States need to stand firm against external pressures from Russia, and their resilience and commitment to collective security are crucial for preserving peace and preventing further escalation throughout the rest of Europe.

Jan Goldman
Professor of Intelligence and Security Studies
The Citadel
Military College of South Carolina
USA

jgoldma1@citadel.edu

MELISSA GRAVES

Minutes to trust: Baltic hybrid defense

Expert article • 3935

For most of the last century, deterrence was measured in missiles and minutes to launch. In this one, it may be measured in minutes to trust; namely, the time it takes a democracy to rebuild a shared picture of reality after disruption.

When the Balticconnector gas pipeline was damaged on 8 October 2023, authorities announced "external activity" within two days. By 24 October, investigators retrieved an anchor from the seabed and publicly linked it to the Hong Kong-flagged NewNew Polar Bear. The physical footprint was limited in area, though the operational outage lasted months. Those sixteen days between incident and attribution allowed Russian-language media to establish alternative narratives that official statements could not fully displace. The technical response was excellent, but the information response was too slow.

Recent subsea-cable faults and GNSS interference over the Baltic region show the same dynamic: open-source communities detect disruptions first; governments validate later. The interval ranges from hours to days depending on classification requirements and attribution confidence. Adversaries exploit that gap.

Inside crisis cells, the friction is human. A controller wants another data point. A lawyer needs clearance language. A minister asks whether markets will panic. No one wants to be the official who spoke too soon. Delay is rarely a failure of will but rather the compound interest of reasonable caution repeated across an entire system.

The problem is structural. Open-source indicators such as flight-tracking anomalies, power-grid fluctuations, and social-media reports often provide the earliest signals. Yet governments wait for classified confirmation before speaking publicly, creating a verification gap that can stretch from hours to days. Speed requires acting on open-source signals; caution demands waiting for intelligence validation. Every hour of delay between initial detection and authoritative statement presents an opportunity for adversaries to establish competing narratives. There is no protocol fix for this tension between operational security and information speed.

Meanwhile, adversaries have adapted their responses to democratic response rhythms, timing their counter-narratives accordingly. In recent cable incidents, alternative explanations emerged within hours of disruption. These accounts do not need to be believed. They only need to create enough ambiguity to delay cohesion.

Taiwan faces similar pressure from Chinese information operations, where authorities must balance speed against accuracy while competing with state media flooding multiple platforms simultaneously. Taiwan's information-resilience model combines government coordination with agile, civil-society fact-checking and media-literacy networks, enabling verified information to circulate quickly through trusted, non-government channels.

The lesson mirrors Baltic experience: governments cannot outpace networks, but they can build trusted relationships in advance that accelerate coherence recovery. This is a democratic vulnerability, not a Baltic anomaly.

The Baltic states and Finland have built sophisticated hybrid-defense architecture through NATO STRATCOM COE, CCDCOE, and the Hybrid CoE. What is missing is not capability but rather tempo. Having the right answer matters little if it arrives after alternative narratives lock in.

Minutes to trust can be traced across phases: detection to internal confirmation, confirmation to allied notification, legal review, political clearance, public release. Recent exercises and real-world incidents show internal detection-to-confirmation can range from under one hour to half a day or longer. Each phase contains chokepoints. Each can be measured, stress-tested, and shortened.

Most hybrid disruptions trigger commercial sensors before government ones, seen in aviation dashboards, telecom fault systems, and satellite analytics. These observers see first, often hours before official confirmation. Building trust with them in advance transforms private technical data into a public-defense capability. This requires pre-negotiated protocols, pre-cleared templates, liaison channels with operators, and trusted relationships with infrastructure journalists.

Fortunately, much of this architecture now exists. Cross-border procedures aim to align initial messaging as rapidly as possible after incidents involving unclassified commercial data. The real record is mixed. Political-risk calculations differ across capitals, especially when economic equities are involved. Domestic political pressures can complicate rapid disclosure. Allied coordination remains a work in progress.

A practical step would be to treat minutes to trust as a readiness metric—tested through periodic simulations that measure the time from disruption to coordinated public statement. Track the longest phase. Identify chokepoints. Publish anonymized findings. Transparency about preparedness is deterrence itself. Yet few governments track these metrics systematically, and no alliance-wide comparison exists in unclassified form—a blind spot that limits learning across borders and allows adversaries to calibrate their timing against institutional rhythms.

Minutes to trust does not prevent hybrid operations. It limits their effectiveness. When coherence recovers faster than confusion spreads, gray-zone probing loses strategic value. For the Baltic states, the next confrontation may unfold not across kilometers of territory but across seconds of coherence that determine whether alternative narratives lock in before truth does.

The question is whether democracies can close that window fast enough to deny adversaries the ambiguity they need to obscure truth.

Melissa Graves
Dr., Associate Professor and Chair,
Intelligence and Security Studies
The Citadel
United States

mgraves2@citadel.edu

TONY INGESSON

Biotechnology and hybrid warfare

Expert article • 3936

Recent advancements in biotechnology and AI have resulted in a reawakening of fears of biological warfare, ranging from new deadly viruses engineered as weapons of mass destruction in shady labs to conspiracy theories about "ethnic bioweapons" which according to these narratives would target exclusively Russians or Han Chinese individuals (depending on the origin). The creative minds behind these latter scenarios seem to be unconcerned by the fact that ethnic bioweapons on this scale are extremely improbable, due to the genetic diversity of large human populations. Fears of a non-discriminating lab-engineered bioweapon virus may not seem as obviously far-fetched, but fail to take into account the practical (or rather, impractical) aspects of biological warfare.

A key obstacle to overcome is to create a stable organism. A pathogen can be expected to mutate and change as a result of different environmental pressures. A disease that is extremely lethal tends to burn itself out quickly, since killing off the host population is a poor strategy for long-term survival. Some of the most lethal diseases known to mankind, such as Ebola or its close relative Marburg virus, tend to cause far lower casualty numbers than more mundane diseases like malaria or cholera. The regular influenza cycles regularly kill twenty to sixty times more people every year than even the worst multi-year Ebola outbreak ever documented.

Despite the inherent difficulties in deploying biological organisms for warfare purposes, there is a long tradition of attempts to weaponize viruses and bacteria for warfare purposes. It was a major focus of research in several countries during the previous century. Ultimately, biological warfare had little to show for all these efforts. While the Japanese military was able to kill large numbers of civilians in China during World War II, they did so by using a natural pathogen (plague) and in the end the excessive casualties among the Japanese themselves demonstrated the impractical nature of large-scale biological warfare. Later, during the Cold War, the Soviets discovered that their attempts to engineer new and more deadly variants of anthrax resulted in organisms that were actually less capable than their natural predecessors. As it turns out, natural selection over thousands of years is actually quite hard to beat when it comes to pathogens.

Another obstacle to large-scale biological warfare is the difficulty in controlling biological weapons. As the Japanese learned the hard way, those who are unable to control their pathogens are quite likely to suffer the same fate as their intended victims. As a result, most of the pathogens selected for biological warfare tend to either be treatable using antibiotics (such as anthrax or plague) or to have a fairly limited capacity for spreading quickly and uncontrollably as long as basic health and safety protocols are implemented (Ebola and Marburg virus fall into this category).

The only real advantages associated with biological warfare tend to favor covert deployment, such as sabotage or disruption. Naturally occurring pathogens can be difficult to trace to deliberate use, delayed action makes it easier to exfiltrate operatives before anyone notices anything, and the ability of pathogens to reproduce enables them to in a sense operate autonomously. Operations of this kind have happened before. German agents in the United States, before it entered World War I, used glanders and anthrax to infect horses intended for the Western front. Similar operations were staged by agents operating on behalf of Germany in Finland against Russia during the same time period (1915-1916).

While modern technology opens up new possibilities, the organisms that have already been fine-tuned by natural selection over the course of millennia are already perfectly adequate for hybrid warfare purposes. Rather than causing mass casualties through disease, their real potential is for sabotage and disruption. Contaminating a water supply can be accomplished with typically non-lethal organisms like salmonella or cholera. Even if this has relatively limited potential to cause disease, the cost of decontamination and the resulting societal disruption can easily be significant. Livestock or plants used for food production can also be targeted. Coordinated campaigns using multiple attack vectors simultaneously could potentially become a huge burden, in particular if synchronized with other forms of attack.

Contemporary narratives tend to be focused on the risks associated with new technologies, but when it comes to biological warfare, we should not forget the lessons from the past. Talking about how to protect our water and food supplies may not be as appealing as discussing sci-fi scenarios involving AI and genetic engineering, but it is arguably far more important.

Tony Ingesson
Assistant Professor, Intelligence Analysis
Department of Political Science
Lund University
Sweden

CHAD BRIGGS

Lessons for hybrid & disaster risk intelligence

Expert article • 3937

The Baltic region now serves as a prime example of a hybrid threat environment, where the lines between conventional warfare and irregular tactics are increasingly blurred. Baltic and Nordic states have recognized these developments better than most, and it is no coincidence that the European Centre of Excellence for Countering Hybrid Threats was established in Finland in 2017. Yet as Russian aggression against Ukraine has illustrated, traditional intelligence assessments have struggled to keep pace with the broad spectrum of emerging security risks. Lessons from strategic disaster intelligence, a subset of broader energy and environmental security (EES), may provide some guidance.

While EES at first blush may appear to focus on natural hazards and physical processes, its development always required acknowledging and engaging with the PMESII spectrum (political, military, economic, social, information, infrastructure). Work on EES in the US Air Force overlapped closely with counter-insurgency (COIN) and irregular warfare (IW) expertise, and then provided a bridge to the wider scientific community. What emerged was an unclassified approach to anticipating emerging risks, drawing upon community expertise to identify and evaluate weak signals for early warning. Disaster intelligence relied on vulnerability analyses, identifying critical nodes and stress-testing systems not with just one source of pressure, but using scenarios where a constellation of varied risks would hit simultaneously.

While the initial concern had been force protection and operational disruptions from natural hazards, the USAF EES work incorporated emerging threats from cyber, disinformation, and cognitive warfare. The resilience of systems was not just a static quantity, but part of a dynamic system which itself was often deliberately targeted. Resilience targeting has been a key component of hybrid and cognitive warfare, with new technologies allowing it to be deployed at scale not just in Ukraine, but across Europe and North America.

The essential need is to move beyond a traditional "threat-centric" view to a more holistic and dynamic view of security as a system. This involves mapping critical infrastructure, including finance, energy, health, ecosystems and social/political communities. Such critical nodes are precisely what hybrid warfare, particularly the gibridnaya voyna as practiced by the Russian Federation, target and attempt to exploit in asymmetric and deniable attacks. After the initial 2014 invasion by Russian forces into Ukraine, Russia and proxies carried out distributed and persistent attacks against banks and hospitals, with the goal of fostering mistrust in the legitimacy of the Ukrainian government and financial system. The attacks were most vividly seen in the NotPetya cyber worm in 2017, which originally intended to attack Ukrainian health and financial institutions, spread and caused billions of dollars damage to logistics companies and hospitals worldwide. Ultimately resilience targeting strategies attempt to break down trust, which leaves targeted communities fractured and passive against an outside adversary.

Disaster intelligence also highlighted the necessity of formalized 'dark reports', where known unknowns are analyzed. Deep analyses of what is not known about a system involves identification and measurement of different uncertainties, the reasons for existing or future data gaps, and the implications for risk assessments of these blind spots. Based on experiences of the Royal Navy during WW2, earlier efforts relied primarily on HUMINT and expert judgement. New computational resources now allow for more formal and real-time modelling of both uncertainties and missing elements of early warning models. The dark reports allow for greater peripheral risk vision, and help avoid underestimation of the probability of extreme risks.

While new technical applications exist, creation of scenarios and wargames are still necessary elements of expert pattern recognition and response. The process of scenario creation helps to establish plausibility from decision-makers, especially when clustered around improbable combinations of probable events. Both institutions and individuals find it difficult to carry out multihazard risk assessments, when synergistic effects create conditions that overwhelm orientation and response. The disaster intelligence tools had to approach such risk clusters as given, and to rely on the emergent properties of group assessments to overcome analysis and decision paralysis. So for example, what if a cyberattack disables the ports of Helsinki and Tallinn coinciding with a coordinated disinformation campaign blaming NATO, a paralyzing ice storm, and a sudden influx of migrants at the Belarus-Poland border? We need to ask such questions well in advance.

Chad Briggs
Professor
Asian Institute of Management
Philippines

cbriggs@aim.edu

ADRIAN HÄNNI

Intelligence and strategic communication

Expert article • 3938

At first glance, intelligence and strategic communication seem to be irreconcilable. After all, the activities of intelligence services are considered fundamentally secret, while communication requires at least a certain degree of openness and visibility to be understood by its audience. In fact, intelligence services have begun to lift the "veil of secrecy" somewhat in the 21st century in favor of strategic communication. For example, they hold press conferences, organize open days, and post videos on social media. This public communication serves primarily to strengthen the legitimacy and acceptance of intelligence agencies among increasingly critical domestic publics. In addition to this form of open communication, however, intelligence services sometimes also send strategic messages directly through covert action.

In recent years, intelligence scholars have begun to acknowledge this potential of covert action. Austin Carson and Keren Yarhi-Milo published a pioneering study on covert action as a signaling tool to external actors, whether allies or rivals. Based on case studies from the Cold War, they developed a theoretical framework that explains why various forms of secret political actions, including covert aid programs and secret military strikes, are devised as meaningful symbols of their originators' resolve and why state actors "find covert communication both intelligible (the basic intended message is understood by perceivers) and credible (the message is believable)." Signaling in secret is possible, Carson and Yarhi-Milo argue, because covert action rarely ever takes place in absolute secrecy. Rather than merely see this partial observability as an inconvenience that must be minimized, state actors can exploit it as a signaling opportunity.

Expanding Carson's and Yarhi-Milo's framework, I introduced a first general model on signaling through covert action that distinguishes three forms of messages: internal signaling, peer signaling, and public signaling. These three distinct forms correspond to three types of audiences: Internal signaling is directed towards members of the own intelligence community or the country's political leaders. A typical case are the assassinations of Soviet intelligence defectors by the KGB during the Cold War. This lethal violence had motivational elements of hate and revenge, and at times was aimed to prevent a defector from doing damage by betraying secrets. However, the primary objective of these operations, at least since the 1960s, was to maintain a credible deterrence against further defections from the own ranks by sending a warning to potential future turncoats in the Soviet intelligence and security services that "traitors" will be punished. "A traitor is his own murderer," was the message addressed to the members of the intelligence services, aiming to deter further defections by spreading fear.

In turn, the audience of peer signaling is a group of strategic allies or rivals. Such an audience was targeted by the Mossad's assassination operations against Palestinian terrorist leaders. Mossad counterterrorism chief Shimshon Yitzhaki explained this rationale after his service had poisoned Wadi Haddad, the mastermind of the Popular Front for the Liberation of Palestine–Special Operations Group, leading his slow and agonizing death in East Berlin's Charité hospital in early 1978: "These stories of suffering have an effect of their own. They spread out and reach the ears of other terrorists, get into their minds, cause them awe and terror, disrupt their judgement, change their behavior, make them make mistakes." Peer signaling is also often directed towards rival or allied intelligence services.

Public signaling finally targets a wider public audience. Examples are, arguably, the (attempted) "theatrical murders" of FSB defector Alexander Litvinenko and former double agent Sergei Skripal by Russian intelligence services in 2006 and 2018, respectively. Another illustrative case are the Mossad's assassination operations against Nazi war criminals between 1960 and 1989. As part of the decade-long hunt, the Israeli intelligence service shot and killed the Latvian Nazi aide Herberts Cukurs in Uruguay in 1965. The Mossad commando mistreated the body of the "Butcher of Riga", who was responsible for the death of more than 30'000 Jews in Riga, and left documents about his crimes as well as a letter of confession in the form of a verdict, signed by "Those Who Will Never Forget". The case of Cukurs also shows that an intelligence assassination can signal to more than one target audience. While butchering the "Butcher of Riga", the Mossad not only sent a message to Holocaust survivors and the global public but also engaged in peer signaling to the Nazi war criminals still on the run.

Adrian Hänni
Dr., Senior Researcher
Leibniz Institute for Contemporary History (IfZ)
Munich-Berlin
Germany

haenni@ifz-muenchen.de

RUBÉN ARCOS

Intelligence and anticipatory communication

Expert article • 3939

The liberal international order and our European liberal democracies have been facing and face a number of threats and challenges that need science-based informed decisions, principled democratic governance, strong institutions, international cooperation based on shared values and determination to act upon them.

At the same time, democratic deliberation on how to address public issues affecting our European societies and how to protect us from and counter those threats, global risks and challenges similarly require public awareness and informed public opinions. That is not possible if our societies cannot count with a pluralistic information environment where news, opinions, science-based analyses, as well as legitimate persuasive communication practices can circulate free from manipulations. Securing the infosphere is key for ensuring that our societies conduct the necessary democratic debates on how to address public issues, including those related to security and foreign policy, where legitimate political disagreement can be expressed and controversies can be solved based on evidence and argumentation.

Disinformation and foreign information manipulation and interference (FIMI) are top tier security threats in themselves, but also, very importantly, because they corrode our democratic systems inhibiting the capacity of our societies to make informed decisions on a number of many other policy areas, including security and defence.

Analyses and assessments on disinformation and FIMI, also as part hybrid threats and warfare, are key for informing the decisions and enabling actions aimed at countering the hostile activities of state and non-state actors with this regard. Intelligence on the covert hostile influencing activities and malign perception management efforts by foreign authoritarian actors and their proxies targeting policymakers, opinion leaders and constituents is key for informing preparedness, prevention and coordinated responses.

While the detection of manipulative patterns of coordinated behaviour and reaction to the already disseminated foreign disinformation and propaganda by threat actors, in the form of content fact-checking and debunking are the usual practices –that is to say, once the harmful narratives, conspiracy theories and disinformation is already out there– anticipatory intelligence and anticipatory communication are critical to address proactively these threats.

I understand anticipatory communication as the deliberate communication processes and communication activities performed in anticipation of events, likely developments, emergent issues or of potential actions by hostile actors, that aim to exert influence on information, knowledge, attitudes and behaviours of stakeholders and on the strategic and the information environment, in order to deter, neutralize and counter the aims of hostile adversaries. Anticipatory communication has a strategic intend and is informed by rightful information, intelligence, threat analyses and assessments, indications and warning, forecasting and foresight.

Anticipatory communication and strategic communication (that purposeful communication processed aimed at achieving goals and objectives according to a strategy, either deliberate or emergent, using symbolic communication and significant behaviours, though not necessarily anticipatory) practices are important capabilities to develop and instruments against hostile information-led influencing.

Anticipating emergent and latent issues –such as economic, historic, political, societal, or any other domain associated vulnerabilities of our democracies– likely to be weaponized in future endeavours by threat actors is key for proactive preparedness and planned coordinated efforts, complementary to coordinated responses. Foresight approaches may identify factors driving future disinformation scenarios and assess likely manipulative narratives that could be weaponized against European members states and EU partners and allies abroad. Crowd forecasting methods may be used for predicting future political developments abroad and hence inform the strategic planning of positive communications. Table-top exercises and wargames can be used for exploring courses of action against disinformation under plausible threat scenarios, the disruptive potential a new technology, or for gaining insights on the potential behaviour of adversaries.

Anticipatory analysis and the assessment of FIMI risks is key for orienting the behaviour of our European democratic systems.

In order to operate with full capabilities under an anticipatory policymaking approach and mindset against FIMI and disinformation, our systems also require an expert reservoir of knowledge (i.e., subject matter, technical, thematic expertise including on countries or regions of interest on issues likely to become the focus of disinformation and information manipulations) ready to be used, particularly under crises and emergencies contexts when surge capacity is needed.

Rubén Arcos
Associate Professor
School of Communication Sciences
University Rey Juan Carlos
Spain

Visiting Professor
Department of EU International Relations and Diplomacy Studies
College of Europe
Brugge
Belgium

Visiting Professor
School of Management, Social and Health Management, Preparedness and Resilience Research Platform (PREP)
University of Vaasa
Finland

ruben.arcos@urjc.es

FILIPPA LENTZOS & GEMMA BOWSHER

CBRN disinformation as strategic weapon

Expert article • 3940

Foreign information manipulation has become a defining element of modern conflict. In Russia's war on Ukraine, as well as in persistent pressure campaigns around the Baltic Sea, disinformation serves strategic aims that go far beyond propaganda. It seeks to fracture public trust, obscure accountability and compromise policy coherence across the Euro-Atlantic area. This informational dimension now demands the same analytical rigour as more traditional security threats.

In both theatres, disinformation operates through adaptive "narrative families" that exploit local sensitivities. Themes of NATO aggression, Western decadence, or the historical treatment of Russian-speaking minorities are recycled to sow division and fatigue. At their core, these narratives aim to erode trust in institutions and scientific expertise. Nowhere is this corrosion more consequential than in the field of chemical, biological, radiological and nuclear (CBRN) security.

The CBRN disinformation nexus has become a distinctive and dangerous subset of the broader information threat landscape. False claims of "military biological laboratories" in Ukraine or insinuations of chemical provocations are not spontaneous conspiracy theories but part of an orchestrated narrative system. Such stories trade on scientific complexity and public anxiety. They gain traction by blending technical terms with selective or misleading imagery. The narratives are then amplified through state media, proxy outlets and diplomatic channels, even reaching arms-control venues. The messaging aims to weaken trust in international treaties and verification processes, and the narratives have been expanding in speed, scale and sophistication since 2022.

Disinformation campaigns that target CBRN issues deploy a distinct set of tactics, techniques and procedures tailored to the technical nature of the subject. While clone-site operations are a recognised tool in broader information warfare, clear evidence that fully fledged clone domains have been a primary vector for CBRN falsehoods is limited; CBRN claims most often spread through state-affiliated media channels, Telegram and other closed messaging networks, pseudo-expert commentary, and the selective re-use or manipulation of genuine scientific imagery and documents. Malign actors make deliberate use of scientific language and fragments of technical data to create the appearance of insider knowledge, then accelerate reach through coordinated amplification — automated bot networks, sympathetic influencers, and cross-platform seeding that repackages content quickly into local languages.

Increasingly, synthetic media and AI tools are used to produce realistic laboratory scenes or fabricated expert statements that complicate verification. The aim is to distort the information environment. By shortening the time from initial claim to mainstream exposure online and in social media, these operations complicate institutional responses, and create ambiguity that outlasts any single debunking effort. Countering these practices therefore requires both rapid response and anticipatory measures involving pre-emptive public explanation, tighter infrastructure and sustained support for fact-checking and scientific communication.

Monitoring this activity has become an analytical discipline in its own right. The CBRN Disinformation Tracker launched in 2025 under the G7 Global Partnership initiative to counter CBRN disinformation provides a structured way to catalogue incidents and measure reach. EUvsDisinfo offers complementary trend data. These datasets collectively map an ecosystem in which malign actors exploit the intersection of science communication, crisis reporting and geopolitics.

In the near-term, the CBRN information threat environment will become more complex. Artificial-intelligence tools are lowering the cost of producing persuasive scientific forgeries. Adversaries are likely to integrate these into election-period influence campaigns, combining local political narratives with global security scare stories. Another risk lies in "crisis piggybacking," where genuine incidents such as legitimate laboratory accidents are instantly reframed through pre-positioned disinformation assets to validate older falsehoods. For the Baltic Sea region, which hosts dense research and energy infrastructures, such manipulation could have tangible consequences for public order and emergency response.

Responding effectively requires more than debunking. For instance, authorities must pre-empt the narrative space. Public communication about CBRN research and preparedness needs to become proactive, offering clear explanations of laboratory work, how CBRN safety is governed, and who audits compliance oversight. Equally important is for analytical units to adopt shared metrics for disinformation and its impacts and to report them routinely for visibility across borders. Foresight and scenario-planning can incorporate information manipulation into CBRN crisis exercises.

Resilience also depends on the media and scientific communities. Fact-checking organisations in the Baltics and Ukraine operate under severe resource pressure and legal intimidation. Targeted funding, cybersecurity support and coordinated rapid-alert mechanisms would help sustain their role as early-warning sensors.

Ultimately, disinformation in the CBRN domain is not only about words or images. It challenges the epistemic foundations of trust, fracturing the relationship between citizen, science and state. For the Baltic region and for Ukraine, where resilience has become a strategic asset, countering such manipulation is integral to national security. Intelligence and foresight professionals must therefore treat CBRN disinformation as both a present operational threat and a future risk multiplier. The capacity to measure, anticipate and neutralise these campaigns will be as decisive for stability in the Baltic Rim as traditional defence measures on land or at sea.

Filippa Lentzos
Associate Professor in Science & International Security
King's College London
United Kingdom

Gemma Bowsher
Dr., Senior Research Associate
King's College London
United Kingdom

IIKKA PIETILÄ

Approaches for identifying vulnerabilities in the cognitive domain

Expert article • 3941

The Baltic Rim states confront renewed geopolitical pressure and hybrid threats, while managing the social effects of increasingly distorted information space, digital interconnectedness, and intensifying individualization. The contemporary socio-technological era is shaped by fluid identities, continuous connectivity, and accelerated flows of produced, curated, and mediated information contents in a plethora of platforms and services by various individual, commercial, and state-related actors.

Although democratic institutions remain formally intact, representative democracy is increasingly strained in its legitimacy among younger generations. Many perceive institutional politics as remote and detached from their lived and mediated realities. Among other factors, this disconnect introduces vulnerabilities for societies deep within the cognitive and information domains.

As the psychological and communicative foundations of democracy erode, attack vectors multiply and branch into the fine-grained details of individual and group identities. External influence operations and internal polarization infiltrate the very pathways through which meaning and belonging are constructed.

Digitalization thus presents a double-edged sword. Well-designed infrastructures and channels can boost transparency, expand inclusion, and strengthen legitimacy enhancing resilience against manipulation through belonging and cohesion. However, poorly designed systems and lack of facilitation may instead accelerate fragmentation, emotional contagion, and adversarial identity formation thus exposing exploitable vulnerabilities at the cognitive and information domains.

The core challenge lies at the intersection of cognition, communication, and security. To strengthen regional democratic resilience, we must ask: how are exploitable vectors at the cognitive and information domains of warfare to be identified, modeled, and countered in practice in the current socio-technological era?

Ideology and Identity as Cognitive Capital. Rather than viewing ideology and identity merely as targets or vulnerabilities, they should be understood as cognitive capital—reservoirs of narrative, motivation, and cohesion. A robust cognitive security posture depends in addition to shielding on nurturing resilient identity architectures capable of absorbing narrative stress without splintering.

The Citizen-Centric Socio-Cognitive Model (CCSCM)[1] offers a framework for understanding how cognition, social structures, and mediated environments interact in shaping societal participation. CCSCM enables describing citizens through the internal, activity, and external layers, which are permeated by various influence vectors that reside in the information domain. CCSCM highlights the feedback loops between individual sense-making, collective identity, and institutional communication.

CCSCM suggests that citizens are socio-cognitive agents, situated at the confluence of internal processes, social interaction, and various medias and systems. Ideological and identity variance, under this view, is not chaotic noise but cognitive diversity, the substrate of pluralistic yet integrative reasoning and deliberation.

Synthetic aperture polling analogy: Multi-Lens Sense-Making. To mitigate the vulnerability implications and threats through informed decisions and contingencies, polling and public sensing in information space must evolve beyond static snapshots. A more potent analogy is synthetic aperture sensing: just as a SAR satellite builds high-resolution images through multiple passes at varying angles, so too must citizen sentiment be probed through shifting framings and perspectives without neglecting the temporal domain.

By varying moral, emotional, pragmatic, and value as well as identity-based lenses, one composes a synthetic aperture in the cognitive and information domains, generating a layered image of societal perception. This enables early detection of latent fractures or emerging alignments before they harden into damage such as polarization or apathy.

Citizen Intelligence as a Democratic Resilience Tool. An emerging frontier in this field is CITINT (Citizen Intelligence)[2] i.e. intelligence activities performed by individuals, NGOs, and civil networks. This represents a shift in issue ownership: intelligence has become distributed and participatory rather than state-centric. CITINT can be viewed through the CCSCM lens.

At the internal layer, where activities such as information appraisal and consolidation, and identity formation reside, the CITINT activities contribute to developing cognitive faculties that in bigger picture strengthen resilience and decrease the susceptibility for external influences.

At the activity layer, citizen involvement in data collection and interpretation strengthens agency and supports individuals to resist manipulative narratives. Moreover, at the activity layer, citizens move from passive sensing and content consumption to active engagement, for instance in curating, analyzing, and publishing information.

At the external layer, institutional systems and platforms mediate how citizen-generated insights are evaluated and integrated, and how the feedback loops are implemented, and how – if at all – the CITINT activities are facilitated.

In effect, CITINT can function as both a barometer for developments in the information domain, and as instrumentation for empowering the citizens. In the Baltic Rim context, building integrated infrastructures where citizens, institutions, and technologies co-produce understanding can be a promising path forward. Rather than outsourcing vigilance, citizens can be empowered as custodians of cognitive resilience and co-actors in the information and cognitive domains of defense.

Possibly the resilience of Baltic Rim democracies will increasingly be won or lost not in parliaments or military domains, but in the cognitive terrain of perception, meaning, knowledge, identity, and control of narrative. The challenge is strategic and resides at cognitive and information domains: how to secure the democratic mindscape in an environment where beliefs and meanings constitute the operational terrain?

The CCSCM provides a scaffold for integrating cognition, participation, and mediation. Combined with CITINT, it points toward an ecosystemic model of cognitive security rooted in proactivity, inclusion, and shared agency.

If the Baltic Rim states adopt orientations of this nature, they may function as a prototype for democratic durability in the age of contested meaning. The task ahead is not simply to oppose distortion but to design societies capable of shared understanding: societies that know themselves in complexity, together. Especially in areas where nations and individuals partially share identities, but have significant cultural, historical, or societal differences, models and frameworks that aim for cohesion, constructiveness, and integration should be explored to facilitate common resilience.

Embedding such frameworks for cognitive and information domains within Baltic policy practice would not only safeguard democratic integrity but also provide a replicable model for enhancing cohesion and resilience.

[1] CCSCM as presented in Pietilä, I., Kortesuo, K., Pohjalainen, U., & Tuominen, M. (2024). Shift in intelligence issue ownership: Conceptualizing CITINT – Intelligence conducted by citizens. Frontiers in Political Science.

[2] CITINT as presented in reference in first footnote.

Iikka Pietilä
PhD
Finland

JOUNI MÖLSÄ

The new strategic resources: Trust and antifragility

Expert article • 3942

Artificial intelligence is often discussed as a technological upgrade, something that accelerates workflows or improves decisions. This view is too narrow and increasingly risky. The deeper transformation, and its impact on societies, is cognitive. AI operates inside the same information environment that shapes attention, emotion and judgment. When that environment becomes distorted or overloaded, democratic societies risk losing the capability that underpins self-governance: the ability to think clearly under pressure.

The Baltic Rim is one of Europe's most contested cognitive spaces. Modern information manipulation rarely aims to break infrastructure. It seeks to weaken interpretation. Influence operations exploit emotional triggers, overload and algorithmic visibility rather than factual disputes. Under these conditions, people do not necessarily believe in falsehoods; they begin to doubt everything. Democracies cannot function efficiently in a climate of permanent uncertainty.

Generative systems accelerate the volume and speed of content beyond human cognitive limits, often drawing on material already biased or manipulated. Polluted inputs become polluted outputs, and the boundary between deliberate influence and accidental distortion grows thin.

This is why trust becomes a strategic resource. Drawing on Henrik Rydenfelt's Sitra essay 'Data, valta ja demokratia' (2024), three forms of power shape how societies make meaning: data power — control of what is collected; knowledge power — authority to interpret information; and information power — the ability to guide visibility and attention. When these come under simultaneous pressure, trust becomes the stabiliser that holds democratic judgment together.

The Baltic Rim's high-trust societies have long benefited from a reciprocal social contract: institutions assume citizens can handle complexity, and citizens assume institutions act in good faith. This creates a trust asset that becomes critical when information environments destabilize. But trust is not self-renewing. It erodes when media ecosystems weaken, when AI obscures provenance or when citizens feel cognitively overloaded. Strengthening trust therefore requires more than technical safeguards. It demands a strategic shift in how the region approaches information security.

A first step is to treat information resilience as part of the region's core security architecture. Media systems—local journalism, public service broadcasting and diverse news ecosystems—function as a cognitive grid that allows citizens to share a common reality even under pressure. When parts of this grid weaken, adversarial narratives fill the gaps.

Second, the region should adopt transparency as an operational principle. Clear labels for AI-assisted content, public model cards for automated systems and verifiable origin metadata reduce the ambiguity that hostile actors exploit. Societies that can explain how information is produced retain credibility even during rapid change.

Third, cognitive resilience must be strengthened at scale. This does not mean teaching citizens to detect every falsehood. It means cultivating reflection, perspective-taking and emotional regulation, the skills that help people evaluate information under stress. Combined with transparent institutional practices, these habits form a population-level defense.

To advance these goals, the Baltic Rim can draw on the theory of antifragility. Whereas resilience describes the ability to recover, antifragility describes systems that grow stronger through stress. Applied to information security, this means using pressure and failures as learning tools rather than destabilizers.

Antifragility begins with open error-handling. When institutions correct mistakes transparently and quickly, they remove a key vector for manipulation and strengthen trust. It continues with regular stress-testing of information workflows—red-team exercises that expose weak points in verification, editorial judgment or crisis communication. Each rehearsal builds capacity.

It also means creating redundancy in meaning-making. Multiple independent newsrooms, cross-border collaborations and alternative distribution channels ensure that no single point of failure can distort public understanding. If one channel is disrupted, others compensate.

For the Baltic Rim, adopting trust and antifragility as strategic principles transforms cognitive security from a defensive posture into a long-term advantage: the ability to absorb pressure, learn from it and emerge more coherent, more resilient and more autonomous. AI is not only a technological question; it will reshape how societies form understanding and judgment.

Jouni Mölsä
Leading Expert
Change Agency Ellun Kanat Oy
Finland

jouni.molsa@ellunkanat.fi

PHILIP M. BAXTER

Strengthening intelligence for the AI era

Expert article • 3943

Artificial intelligence (AI) is rapidly becoming ubiquitous in society and on the battlefield, and is poised to do the same in the intelligence analysis space. The emergence of large language models as active collaborators in a broad array of tasks over the last several years has left governments and companies scrambling to leverage AI models as quickly as possible. While we have not yet achieved artificial general intelligence (nor the independent, sentient systems portrayed in film), the rapid advancement of machine learning and large language models (LLMs) techniques is simulating systems that appear intelligent enough to their users. This has accelerated the adoption of these tools across an ever-growing set of missions, as well as making their application to a range of existing data types possible.

In Ukraine, artificial intelligence has been used for processing data from the battlefield to make targeting operations more efficient. For example, the AI-powered software GIS Arta system is used for rapid targeting of enemy artillery. In Israel, AI models like "The Gospel" and "Fire Factory" assist in identifying and tracking human targets and automating strike recommendations. In the United States, investments are being made into better understanding and deploying an LLM to support intelligence analysts in their workflows, performing tasks such as identifying logic gaps or masking the identity of sources to increase the distribution of analytical products. Businesses are similarly seeking to advance their corporate intelligence and consumer engagement by deploying machine learning techniques on their available data (resulting in the generic "AI-enabled" branding) or to engage with customers. While noteworthy challenges persist in these developments, such as AI hallucinations, inability to explain the logic of how an output was achieved, data verifiability, and protections against malicious data injection, among others, these systems are rapidly sought out and implemented.

Setting aside the morality and ethical issues of these systems, two issues will persist regardless of how much the underlying algorithms improve. The first is the impact of cognitive offload by analysts onto artificial systems, eroding over time the analytical rigor of the analyst. Early research already suggests that heavy reliance on these tools can impede the development and maintenance of critical thinking skills. As such, policymakers will need to walk a tightrope. These tools cannot be ignored; their integration will be a requirement given the work of other countries to also utilize the advantages provided by these tools. However, as these tools expand and become more ubiquitous in the analyst toolbox, they will have a negative effect on the capacity of the analyst. Tool development and deployment will need to be selective and deliberate, providing support to the analyst while not replacing their critical capacities.

Second, data will start to emerge as the next major hurdle in AI. Currently, AI tools are applied to existing datasets or layered onto existing sensors to enhance processing capacity. The "low-hanging fruit" has been the focus given their easy accessibility. To continue to extract the full value from AI, deliberate strategies will need to be implemented to generate data specifically for AI models. For example, in the conflict in Ukraine, sensors were deployed to capture data from specific areas to increase situational awareness of movements throughout the country. This deliberate planning made the AI tools currently deployed feasible. As intelligence agencies implement these tools, they will be able to utilize existing data streams, but will also need to identify methods for collecting or transforming data with the AI requirements in mind. Without strategic planning, the AI tool ecosystem is more likely to resemble a hand-carved woodworking shop, an assortment of bespoke tools for individual tasks, rather than a consolidated platform of integrated data, more akin to an automated manufacturing line, where each component feeds into the next through shared interfaces and a single governing workflow.

Artificial intelligence tools released to the public over the last several years have captured our imaginations and spurred a new age of AI exploration and integration. However, we are quickly approaching the end of the low-hanging data that has enabled rapid deployment throughout society. We will also face challenges in implementing these tools while maintaining a vibrant analytical workforce. With deliberate planning and the right investments, the next generation of AI can supplement human judgment rather than distorting it.

Philip M. Baxter
Assistant Professor of Intelligence Analysis
James Madison University
United States of America

JAMES L. REGENS

Artificial intelligence is transforming the character of war

Expert article • 3944

Although the nature of war remains constant over time, innovative technology deployed at scale disrupts the military status quo and ultimately can transform the character of war. The cutting-edge technology's use tied to an effective strategy and tactics is a game-changer revolutionizing maneuver, enhancing mass, improving precision or facilitating surprise to achieve strategic, operational or tactical advantage on the battlefield. This shift in the character of warfare typically triggers a cycle with the innovation spreading to other adopters, some militaries lagging behind or failing to adopt, and spurs efforts to win a new race for technological dominance.

Basil H. Liddell Hart's observation — reflecting on lessons learned from World War I —that "… the only thing harder than getting a new idea into the military mind is to get an old idea out" aptly characterizes the technology innovation cycle in the context of warfare. It encapsulates the tension between actively embracing new technologies and prolonged reliance on older, less effective capabilities. Addressing this reality ensures integrating new technologies and military strategy can lead to real-world advantages.

Just as technological breakthroughs like tanks and airplanes in World War I or radar and aircraft carriers in World War II revolutionized warfare in the past, artificial intelligence (AI) is the latest new technology capable of remaking the character of war. Its conceptual roots go back to British code breaking work at Bletchley Park in World War II. Building on that experience, the convergence of breakthroughs in high performance computing, more powerful microchips, and the volume of big data availability over the past decade has fueled burgeoning recognition that AI promises to revolutionize warfare by fusing not just synchronizing mass and precision to dominate the battlefield.

Leveraging AI's functionality significantly enhances military capabilities, fundamentally alters the nature of missions, and impacts operations. For example, during Operation Desert Storm in 1990-1991, the state-of-the-art for military-embedded AI had matured enough so the DARPA-funded Dynamic Analysis and Replanning Tool (DART) was used for logistics scheduling. By 2002, AI was being used on the battlefield for a drone to autonomously navigate and provide situational awareness to special operations teams. Since then, the US military has expanded its reliance on a mix of static AI systems that use fixed rules or algorithms for deterministic tasks such as imagery analysis and dynamic AI systems. Dynamic AI systems are advancing rapidly and can learn, adapt, and respond in real-time to changing circumstances, data, and user interactions for applications to more complex tasks like target generation, surveillance, intelligence, and decision support.

Viewed retrospectively, a central challenge in warfare over the past 25 years — from counterinsurgency to conventional battles — has been synthesizing and interpreting vast amounts of real-time data to detect, characterize, track, and target threats faster than adversaries can adapt. With the sheer volume of information available, making sense of it all becomes overwhelming. Success in such dynamic environments hinges on the ability to observe, orient, decide, and act (the OODA loop) more quickly than the opponent. This is possible because dynamic AI systems offer a solution to the challenge of information overload created by the exponentially increasing volume and velocity of digital data.

In essence, AI-embedded military systems facilitate solving the problem of leveraging quantity and quality of strike power — especially as asset stocks decline by use or are degraded by enemy actions in high-intensity wars of attrition. This is a real not hypothetical problem. The protracted Russia-Ukraine War, the short but intense 12-Day Israel-Iran War, and periodic US strikes against the Houthis in the Red Sea demonstrate consumption rates for equipment like artillery munitions for ground strikes or drones, missiles and air defense systems for aerial operations is staggering.

To place this in perspective, the US launched more than 150 Terminal High Altitude Defense (THAD) interceptors at incoming Iranian targets during the brief 12-Day Israel-Iran War — more than 25 percent of existing US inventory and more than three times the annual purchase rate. Similarly, US naval operations against the Houthis in January 2024 used more Tomahawk missiles than the Navy bought in 2023.

Simultaneously solving the problems of having adequate inventory on hand, stockpile replacement/surge capacity and an effective real-time integrated system for threat identification, classification, tracking and targeting is critical. Failure to develop and deploy accurate and reliable AI-based systems at scale creates a major capability gap even if the first two problems are addressed. As a result — unless all three problems are resolved satisfactorily — the likelihood decreases the US, its NATO allies, and regional partners deter or win future high-intensity wars of attrition — especially with a pacing competitor like China — or respond to threats to North American Continental Defense, in NATO's Far North, and its Eastern Front.

Successfully bridging these capability gaps matter for navigating the current and future strategic landscape. The US, its NATO allies, and regional partners like Japan and Australia face a significant resource allocation challenge coping with four major adversaries — China, Russia, Iran, and North Korea — across three main theaters — Asia, Europe, and the Middle East. These known adversaries are increasingly cooperating, amplifying their collective threat to the West. Inevitably, new and unforeseen threats also will emerge.

The integration of AI into the complex geometry of multi-domain operations — encompassing air, land, sea (surface and subsurface), space, information, and cyberspace — is driving a transformative leap in the speed, precision, scope, scale, and effect of military actions. The sheer magnitude of AI's prospective impacts explains why America and China's competition to dominate AI military use applications — particularly in areas like air defense, unmanned systems, command and control, logistics, intelligence, and situational awareness — mirrors their rivalry over dominance in commercial applications. Paralleling the US-China efforts, investing in developing and deploying military-embedded AI is a priority for numerous countries including Russia, Israel, Ukraine, UK, Japan, Finland, Poland, Estonia, Germany, and France. Ultimately, the pace and scale of integrating functioning AI systems into military capabilities not simply the sophistication or technical quality of those applications will determine which armed forces have sufficient technological dominance to deter or win wars. This advantage will help determine the winners and losers in a tumultuous geopolitical landscape.

James L. Regens
Co-Founder and CEO
Audax Concepts
United States of America

Regents Professor Emeritus
University of Oklahoma
United States of America

KATHLEEN M. VOGEL

AI and bio-threat assessments

Expert article • 3945

Within the past few years, policy officials and experts have pointed to potential new security threats from the convergence of artificial intelligence (AI) and advances in the life sciences and biotechnology. For example, AI is being incorporated into biological design tools to design new biological components and chemical molecules; some worry that these new tools could be used to design new types of biological weapons. Automated and AI-enabled cloud laboratories have been identified as a possible concern for remote, on-demand bioweapons production in the future. Others have pointed to the rapid advancements in and diffusion of large language models (LLMs), which could upskill a wider range of actors with the information to work with dangerous pathogens and launch bio attacks. At the same time, some are advocating for the use of AI to counter bioweapons threats. In July 2025, US President Donald Trump called for the creation of a new AI-enabled verification system to identify suspect activities in contravention to the Biological and Toxin Weapons Convention (BTWC). These varying perspectives show a divergence in opinion on the risks and benefits of the current and future AI-biotech convergence. We are still in the early days of these technological developments. AI can be a concern for bioweapons development but that possibility remains distant. What is clear now, however, is that the reality of this AI-biotech convergence is complicated and will take some time to study and sort out. One area that we can examine where there is present utility (and known concerns) is AI for bio-threat assessment.

Regarding the BTWC, AI systems can be very useful in gathering and analyzing data required in reporting under states parties obligations to the convention, and in confirming the accuracy of data collected. AI tools could also be used by states parties to gather and analyze a larger trove of data regarding potential suspect facilities. For example, AI systems could be used for rapid data mining of scientific publications and other open source and government data (e.g., procurement and financial records; emissions, effluent or energy data; video surveillance and satellite imagery data; patent information) to identify indicators of illicit research activities. AI-enabled systems could also be used for disease surveillance to gather and quickly process data on outbreaks indicative of possible biological attacks and provide early warning capabilities and fast dissemination of information to public health officials and members of the public on preventative or protective measures that could be undertaken. In spite of various beneficial applications of AI for bio-threat detection, it is important to remember that AI systems work with data that can be quantified or made codified; they are not useful for evaluating the tacit dimensions of weapons work that have been shown to be important in former bioweapons programs of state and non-state actors. AI systems are also limited in their ability to infer intent, i.e., a state or non-state actor's motivation to develop and maintain a biological weapons program.

In addition, AI-systems have limitations and vulnerabilities that could be overlooked or exploited to generate flawed information. For example, AI tools can be used to spread misinformation and disinformation, as has been observed with Russian accusations of suspected biological weapons activities occurring by the United States and their allies and partners (with no concrete evidence that confirms illicit activity). AI systems are vulnerable to data poisoning, in which nefarious actors could corrupt the data used by these AI systems leading to inaccurate conclusions. AI systems are also subject to hallucinations, in which a LLM reports data or makes conclusions that are nonsensical or inaccurate. Accuracy in LLM outputs rely heavily on the integrity of the data used, therefore, missing data, inaccurate data, and corrupt data can lead to error-laden outputs that can mischaracterize the threat. Thus, the outputs of AI-enabled biothreat assessments are only as good as the inputs.

Now and into the future, we need to carefully consider the strengths, weaknesses, and limitations of AI-systems for bio-threat assessment. The most powerful adoption and use of AI is in human-machine teaming, which captures the strengths of both and modulates the limitations of both. To date, most attention in bio-threat assessment is currently focused on the AI technology itself. This is a known problem of focusing on a technological fix to address problems, rather than doing the harder work of thinking holistically about how to skillfully use the strengths of both humans and machines to provide better data and assessments about threats emanating from the convergence of AI, the life sciences, and biotechnology. We need to think carefully about how to use AI systems for human benefit in bio-threat assessment now and into the future.

Kathleen M. Vogel
Professor
School for the Future of Innovation in Society
Arizona State University
USA

kathleen.vogel@asu.edu

STIG STENSLIE

Digital Beijingology: Towards an AI-driven intelligence methodology for analysing Chinese politics

Expert article • 3946

At the Norwegian Intelligence School in Oslo, we are leading an innovative research and development project that combines traditional approaches to understand Chinese leadership, decision making, politics with methods from computer science. The goal is to develop a new type of intelligence methodology for understanding closed, authoritarian regimes where classic political intelligence analysis is enhanced with AI-powered tools – a "Digital Beijingology".

At a time when not only Xi in China, but also Putin in Russia and other important leaders, rule through increasingly personalistic and closed power structures, the need for methodological innovation to understand politics in closed, authoritarian regimes is more urgent than ever.

While for Norway Russia poses a direct security challenge, with a military presence in our immediate vicinity, digital threats, and information operations aimed at Norwegian interests. China is a more complex actor – both a challenge and a potential partner.

In the face of such regimes, both a revitalisation of classic methods – often referred to within intelligence circles as Kremlinology or Beijingology – and an embrace of new technologies are required for intelligence to provide decision-makers with a better understanding of threats and opportunities.

Closed regimes and hidden exercise of power

In closed, authoritarian regimes, there is neither transparency nor independent institutions that can provide reliable information about political decision-making processes. Instead, intelligence analysts focusing on such regimes must read between the lines – interpreting signals in speeches, cadre movements, language use, and symbolic politics to understand what is happening behind the scenes. This is not least true in Xi's China, where collective leadership has been replaced by personal concentration of power, and in Putin's Russia, where information control, propaganda warfare, and an unclear balance between state and security services make understanding decision-making processes demanding.

Such regimes are "hard intelligence targets". Access to decision-makers is non-existent, strong security awareness makes covert intelligence collection difficult, and information is leaked mainly when it serves the regime. Nevertheless, the West – and Norway – must understand these actors, not only to assess their threat potential and intentions, but also to identify spaces for cooperation, conflict prevention, and crisis management. It requires an intelligence service that combines the best of the old and the new: an analytical discipline rooted in a deep understanding of political culture, and a methodological framework that fully exploits new technologies.

Leadership analysis as a core task

To understand closed, authoritarian systems where power is concentrated around individuals, leadership analysis becomes a core task. Xi and Putin are not just presidents – they are ideological shapers, strategic architects, and ultimate decision-makers in regimes that cultivate loyalty and personal power. Understanding these leaders' psychological profiles, symbolic self-presentations, and decision-making patterns is crucial to explaining and predicting politics. It is equally important to understand the basis of leaders' power and how they exercise it.

Leadership analysis, however, needs to renew itself. In the past, the field has been criticized for being speculative and person-centred, but in the current situation, it is on the contrary necessary to delve deeper into how personality, ideology, and strategic rationality are woven together in authoritarian institutions and decision-making processes. This requires not only biographical and cultural insight, but also a methodological framework that can combine qualitative assessments and systematic data analysis.

Artificial intelligence and big data

Developments in artificial intelligence, large language models, and big data analytics are opening new possibilities for analysing closed, authoritarian regimes. Where humans can only read a limited number of documents, machines can analyse an infinite number of texts, identifying discursive and sentiment shifts, and patterns in language use that point to changing priorities or internal tensions within the regime.

Our R&D project at the Norwegian Intelligence School explores how digital methods, network analysis, machine learning, scraping, sentiment analysis etc support the analysis of leadership, decision making, and politics China and Russia. The goal is to strengthen analysts' ability to capture subtle signals that are otherwise easily overlooked, such as subtle shifts in political language use, changes in power relations or the emergence of new centres of power within the regime.

Such AI-driven Kremlinology or Beijingology is not as a replacement for human judgment, but a powerful reinforcement of analytical capacity.

A new chapter for intelligence analysis

The revitalisation of intelligence analysis of closed, authoritarian regimes is not about choosing between technology and expertise but about combining them. It is about developing an analytical approach where classical political analysis, psychological understanding of leaders, and machine learning work together. It is also about building bridges between academia and intelligence – between theories of authoritarian systems and practical methods for analysing them.

By combining academic immersion in Chinese and Russian political culture with new digital methods, our R&D project seeks to develop a methodological framework for the intelligence analysis of the future. This will have value far beyond academic research – it will strengthen intelligence's ability to inform decision-makers in a world where power is concentrated in a few hands, and insights must be drawn from dispersed and fragmented sources.

Conclusion

The need for intelligence that can penetrate the dense veils often surrounding authoritarian regimes is greater than ever. Xi's China and Putin's Russia challenge not only Western security, but also our ability to understand political systems that do not follow open, democratic logics. To meet this challenge, our project seeks to combine the best of two worlds: new technology that makes it possible to analyse large amounts of data, and classic leadership analysis that provides deeper insight into personal power structures and decision-making processes. Only in this way can we ensure that intelligence continues to deliver its core value: insight into the hidden – in support of wise and informed decisions.

Stig Stenslie
Research Director
Norwegian Intelligence School
Norway

Professor
Oslo New University College
Norway

SARITA BLOMQVIST

New challenges for OSINT and journalism: Fighting fake news in the age of AI

Expert article • 3947

In the spring of 2023, while teaching media literacy to Finnish students as part of YLE's Uutisluokka project, I showed them a viral image of the Pope in a Balenciaga coat - one of the first AI-generated photos to go viral and fool global audiences. At the time, spotting the telltale signs of synthetic imagery was still easy. Yet it was already clear that the kids in the classroom as well as the next generation of journalists would face a verification challenge far beyond what traditional tools could handle.

Two years later, that prediction has already materialized. Artificial intelligence is reshaping the practices of both open-source intelligence (OSINT) and journalism as well as the reality we consume online. It was quite early in 2025 when I spotted an eye-opening conversation on Facebook. Someone had shared a video of a whale being cleaned by divers with a caption "There's still goodness in the world". Except this goodness was artificial. I have to admit that though to my eye it was clear that the video was fake it was still quite realistic. The only thing giving it away as AI, was that the debris falling off the whale seemed to disappear into nothing instead of falling off the back of the animal. What was exceptionally alarming to me in this example was that people seemed to want to believe it was true and fighting that sort of belief is difficult. Since then, we have seen videos after videos of newsworthy events that are completely or partially artificial: videos from Israel bombing Syria or the Texas floods. Now everytime I open any given social media app I'm bombarded with AI generated videos and pictures. It's so common and normal that even the White House publishes AI content consistently and universities across the globe battle with AI generated papers. In Finland AI is so common that a well-established photography company thought it to be acceptable to edit the faces of kids in school photos so much that they lost freckles. Of course, the parents didn't think it was, because they spotted the AI.

The amount and the scale of AI content might be alarming, but what has kept me sleeping well at night is that the human eye has been quite good at spotting it. Even if we can't put a finger on what exactly is the problem, something seems a little off when watching AI generated visual content. A former colleague of mine shared an AI generated deepfake video of himself and it was so good that in his words only his family and friends spotted that something wasn't quite right. Spotting AI generated visuals is getting harder by the day and the amount of time and effort it takes is increasing.

What I find most problematic, is that especially in social media, we rarely take the time to really look at a picture or a video. It's easy to be critical when someone asks you: Is this AI? But most of us are not hardwired to be critical all the time. Critical thinking acquires energy and our brains do almost anything to save it. And the general public receives almost no information let alone training in how to recognise AI generated content. We still believe what we see even though our reality online is being altered faster than ever before and in ways we can't quite yet fathom.

To most of us AI generated content is just harmless entertainment. But it can, is and will be used to shape our worldviews. AI is making it easier and faster to generate fake news and simultaneously it's getting harder to spot what's AI and what is real. We might be lightyears away from singularity or even generative AI but we are approaching the moment in time when it becomes impossible to believe what we see.

According to Derek Bowler, the Head of Eurovision Social Newswire at the European Broadcasting Union, AI generated content could be undetectable from a visual perspective already in 2026. This means that by the time you are reading this article we might have already gone beyond that point. And when that happens, using AI to generate audiovisual propaganda, disinformation and content for criminal purposes or even information warfare becomes tempting to say the least. This is when we can see fake news like never before and don't even know about it.

According to Mr. Bowler, there are mainly three reasons why people currently make and share AI generated videos of news events. Firstly, they simply want to be a part of a conversation. This can lead to harmful misinformation but is not done on purpose or maliciously. Secondly in social media engagement is currency. Some of these AI videos get loads of attention. Especially in X and in Tiktok people make money this way. The third reason is to purposefully generate false information to mislead or maybe even cause harm or disruption. AI is now also used in OSINT, which is the method we use to fight fake news, investigate events or determine facts based on content published online or mainly in social media. Fact-checkers in the Nordic countries are integrating AI tools into their workflows to support tasks such as monitoring, data analysis, translating or just simply doing the work faster by automations. However, AI is not the best way to detect AI. According to Mr. Bowler, every time an AI detection tool is updated or a new one is created the technology has taken a leap forward hence making the content it's supposed to help flag as AI is better than the detection.

This is where traditional OSINT methods and tools become helpful. Of course, AI can't be detected with reverse image search but things like geolocating and satellite images can be helpful in some cases. The most helpful tool is the person or preferably the persons doing the research. Human judgement, ability to doubt and contextual interpretation are often the best and the only weapon against disinformation and misinformation even when it comes to AI generated content. Looking for context, on-site reports and comparing information from reliable sources should help create doubt. Together with knowledge on how and when misleading content is created and what signs to look for both within and outside the content, we get professionals equipped to assess and handle complex situations. The problem is that many newsrooms have put their efforts into creating and using AI tools in producing and scaling journalism instead of educating and training their people to do research.

"AI is scaring newsrooms. In general, there's a lot of newsrooms, particularly in public service media, who are getting up to speed with AI as a tool to use for output and for workflows. The biggest problem is that many newsrooms have largely ignored the field of verification and they're waiting for a tool to come along that tells you everything you need to know. That tool will never exist. From that perspective, it's leaving newsrooms in a position where they may not be able to actually deal with the levels of misinformation and disinformation that's out there", Derek Bowler says.

Together with the increasing quality another concern of mine is the increasing amount of AI content. Throughout the years we have seen state backed entities creating vast amounts of false information and content especially when it comes to conflicts like the one in Ukraine. With the help of AI the amount can and probably will skyrocket. Especially in state-controlled media environments or even highly polarised environments this can lead to false information dominating or overtaking the whole society. This means that the false narrative is so overpowering that there's no room or possibilities for fact checking. This is concerning from a European perspective because effective collaboration acquires us to have a shared reality with our allies. Upholding our own democracies or EU level decisionmaking on complex and emotional matters requires discussion based on facts without alternative facts taking over. Scientific research as well as institutional journalism and traditional media outlets have been a way for citizens and decisionmakers of democracies to share facts and a basis for reality. But we no longer get our news only from traditional sources that base their stories in research. In the UK 20 %, in Denmark 12 % and in the US 34 % of people say social media was their main source of news in 2025. And like I already pointed out, you can't really use social media without being exposed to AI generated content.

Misleading or false AI content is not the only issue we are facing when it comes to news. According to the World Economics Forum's Global Risk Report 2025 the use of AI chatbots as a news source or as search engines is emerging with 7 % of people getting news this way on a weekly basis and when we talk about young people under 25 the amount rises to 15 %. At the same time, according to Reuters Digital News Report 2025, more than half the public across the markets the report covers say they are concerned about what is real and what is fake when it comes to online news. According to Reuter's survey most check the validity of content through an outlet they consider trustworthy. One might think that what people think is a trustworthy outlet is something like institutional journalism or government sources or research and some do, but many find search engines like Google to be that and some of them use LLM's like ChatGPT like search engines. 13 % said they don't know how to verify content at all.

In a digital world controlled by algorithms that are fuelled by AI, upholding democracy becomes a challenge. The most effective algorithms already manipulate our worldviews and have taken away our ability to make informed decisions. We have seen this happen on a large scale during some elections. Social media can quickly suck a person into a realm of dis- and misinformation even without them noticing: our emotions are easily manipulated and we believe what we want to believe if we are not vigilant. Combined with our tendency to believe simple explanations and latch on to the narrative that is repeated to us over and over again, we are vulnerable in front of massive amounts of AI generated information the algorithm has pushed for us. I was involved in debunking fake news and fact checking during the COVID19 pandemic and I saw first hand what disruption of our realities and facts can mean for governments, societies, communities and individuals In order for our democracies to work effectively the majority needs to be able to separate truth from fiction.

Moving forward we need to educate our decisionmakers, journalists and the public in media literacy in the age of AI. We failed to do that when social media took over. Based on my experience I'd say we can't afford to do that again. Disinformation, misinformation, propaganda and hybrid warfare affect us all. As we are witnessing the disruption of information and power and increasing polarisation on a global scale, all of us need the basic knowledge in how to verify content.

Public trust has always been the basis of the news business but I'd say it is becoming even more important so newsrooms should not take implementing AI lightly. Use of AI in news ŕooms should be well justified and as transparent as possible. My question from day one has been, how can we write, enhance and illustrate news with AI and still say that AI generated content done by content creators rather than journalists is not a good thing. Like Derek Bowler said, trust should not be placed in tools only. And last but not least democracies in the Baltic region and in Europe need to work together. We face the same challenges when it comes to security. AI fuelled algorithms that amplify AI generated content based on AI generated information are a security threat. We need to be prepared for AI generated content when the next elections come no matter where the elections are held. We haven't been prepared before and now the challenges we are facing are greater than ever and will continue to grow.

List of sources

Outsourcing, Augmenting, or Complicating: The Dynamics of AI in Fact-Checking Practices in the Nordics: https://journals.sagepub.com/doi/10.1177/27523543241288846
Reuters Digital News Report 2025: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025
Economics Forum Global Risk Report 2025: https://www.weforum.org/publications/global-risks-report-2025/
Interview with the Head of Eurovision Social Newswire at the European Broadcasting Union Derek Bowler in 2025

Sarita Blomqvist
Ecosystem Facilitator
M.A. Journalism
Dimecc Oy
Finland

sarita.blomqvist@gmail.com

BRAM SPOOR

OSINT in NATO's Multinational Corps Northeast

Expert article • 3948

This article looks into the use of open source intelligence (OSINT) within NATO's Multinational Corps Northeast (MC NE). It is based on the author's PhD research for which 56 respondents from the corps were interviewed on their intelligence work, including their use of OSINT.

MNC NE is the command for NATO ground troops in Poland, Estonia, Latvia, and Lithuania. While the Russian invasion of Ukraine has put the alliance on alert, it remains in peacetime condition as long as Article 5 is not invoked. Therefore MNC NE is not fully manned or equipped and has a limited operational mandate that restricts intelligence collection activities. As a result, respondents in all echelons of the corps fell back on collecting intelligence from open sources. Most of this collection took place on the internet and includes news sites, blogs, fora, social media or websites of relevant organizations such as Institute for the Study of War or Bellingcat. In doing this, the respondents faced several challenges.

First of all, the technical access. For security reasons there was a limited number of computers that have access to the open internet. And in many cases the connection was limited in bandwidth, thereby affecting search activities. Secondly, there were no specific open source collection tools available within MNC NE. Meanwhile, many relevant tools are available that facilitate structuring, focusing, and automating the collection of open sources as well as facilitate access to the deep and dark web. Thirdly, open sources in the Russian language posed significant problems. Most staff did not master the Russian language to the extent that they could easily collect and interpret open sources that are in Russian. There was general agreement that this lack of Russian language capabilities hampered collection efforts. The fourth challenge is the magnitude of open sources that are available. For many respondents this resulted in sheer information overload making it very difficult for the respondent which sources to select and focus on.

While these challenges are of a more practical, or circumstantial, nature the problem runs deeper. Intelligence staff had little knowledge of, and experience with, conducting OSINT. Almost none of the respondents had followed an OSINT course or training, although these are widely offered. An additional point of concern is the invalidated nature of the open source information. As one section head remarked: 'The main challenge of the operating environment is the confirmation of a piece of information that is open source.' Many respondents pointed to the limited collection mandate. This made it difficult for them to verify information from open sources.

Furthermore, respondents argued that the F6 system, that is used to grade sensor reporting and judge the credibility of the source (score between A-F) and reliability of the information (score between 1-6), is difficult to apply to open sources. For a sensor report the source is either the sensor itself (e.g. observation, imagery) or a human source (signals intelligence or human intelligence). However, when determining the source for an online news article, the F6 system leaves room for interpretation. Is the news company the source or the medium? If the article is based on several sources, some cited from other media, what is the source then?

The F6 system is especially difficult because Russian disinformation is often tied into existing phenomena and real news facts. This is difficult to unravel and understand as it is, let alone to use the F6 system against. Several respondents even questioned the use of open sources as it was. One respondent, reflecting on the information value of social media mentioned by many respondents, stated: 'Social media is only about extremes; every nuance is filtered out by algorithms. It's a common mistake to think that social media is an actual reflection of the world and of people's perceptions and ideas.'

The reliance on open sources, the lack of OSINT training and experience, and the problems with determining the reliability of information had severe consequences. Given these difficulties, it is not clear whether the use of open sources at the corps was mere collation of publicly available information, or if it entailed some form of analysis or enrichment that turns it from aggregated information to proper intelligence. This had the risk 'of importing propaganda, misinformation, and disinformation', as one divisional lieutenant-colonel stated. In particular in the context of the current information war, respondents considered this potentially harmful. This danger is real, as Varzhanskyi shows.[1] Using the concept of reflexive control he studies how in the Russo-Ukrainian war disinformation is used to influence open source information and intelligence to ultimately influence the opponent's decision-making. While the respondents are aware of this danger, their working circumstances are certainly not optimized to prevent this.

[1] Illia Varzhanskyi, "Reflexive Control as a Risk Factor for Using Osint: Insights from the Russia–Ukraine Conflict," *International Journal of Intelligence and CounterIntelligence* (2023).

Bram Spoor
Assistant Professor of Intelligence
Netherlands Defence Academy
The Netherlands

PETER DE WERD

Military OSINT: low-hanging or forbidden fruit?

Expert article • 3949

From an intelligence perspective the Cold War never ended. While the term for Russian intelligence and influence operations, 'active measures', was replaced with terms like 'measures of support', their primary intelligence targets – the United States, NATO and China – have remained the same. Today, as Sweden and Finland have joined NATO, Russia actively engages in a further escalating hybrid campaign of espionage, subversion and sabotage. New technologies and the changing information landscape have introduced new vulnerabilities in our digitally dependent societies. As NATO officials warn, the threats to free public debate and critical infrastructure are part of a growing pattern the West is not sufficiently prepared to counter.

Hybrid threats place new demands on military intelligence, requiring a wider focus and a revaluation of traditional collection priorities. Of course, secret electronic and signals intelligence on adversarial military activities are still crucial. Yet, the focus potentially widens to the total defence of society, and collection includes more and more open source intelligence (OSINT). The democratization of digital technology has significantly expanded the relevance of publicly available information. Online reporting demonstrates how investigative journalists and citizen collectives can expose and map the extent of Russian sensitive activities. For example, identifying the systematic spying at sea by 'shadow fleet' ships, by utilizing public AIS signals and intercepted Morse code messages, or going out to sea to film antennas and armed guards. Other private initiatives debunk Russian disinformation and influence operations, or gather information on military tactics and evidence of war crimes on the Ukrainian battlefield.

A tension exists between the speed and availability of public information and what military intelligence bureaucracies can process and deliver. The increasing relevance of open sources has led to a growth of OSINT units within European militaries and the development of new OSINT training programs. In addition, for example in the Dutch military, some informal grassroots OSINT initiatives by individual service members and small groups have emerged, to gather relevant publicly available information themselves. These initiatives are driven by a sense of urgency, the lack of operational and tactical intelligence on Russia to model military exercises, or more personal motives to develop online investigative skills. Service members partly conduct these activities in their own time and as private citizens, bringing what they find into their work context. This information is then sometimes even transformed into formal products and reporting. Despite appreciation of 'grassroots products' from some military commanders and peers, military intelligence professionals also have raised concerns about the validity and quality of information, and lack of control. Perhaps these local and informal activities are unavoidable – or even useful to some extent. Yet, many military commanders lack the understanding and overview to effectively guide these practices.

Acknowledge grassroots practices, address legal gaps, and improve safeguards

Developing and organizing new practices of military OSINT is essential. However, their regulation requires strengthening. At present, the blurring of military intelligence and different forms of public information makes already existing challenges more prominent. These include the need to create adequate mechanisms for mitigating mistakes, and considering risks, necessity, proportionality, and subsidiarity of collection. When does gathering information become unauthorized violation of privacy or systematic surveillance, for example?

A key underlying problem, in several European countries, is the legal gap that exists. Current laws regulating intelligence services and the armed forces have restraints in terms of scope, and limits to authorizing military OSINT activities. In addition, the European Convention on Human Rights, the General Data Protection Regulation, and other conventions, safeguard the protection of fundamental rights such as privacy of citizens. The current hybrid conflict increases the need for OSINT collection activities. Yet, for military units, these are now often only regulated in legal frameworks designed for deployment in times of war, during out of area missions, or in 'peacetime' when seconded to the intelligence services for a specific assignment.

To improve armed forces readiness and training in the Netherlands, a new Defence Readiness Act has been submitted to Parliament. The current draft would allow for military units to create an adequate 'information position' on the relevant operational environment, and to train for this by collecting information – including personal data – from open sources. In line with earlier evaluations, the Dutch Ministry of Defence is also further developing its privacy organisation and broader institutional oversight. A challenging task, given the extensive size of the armed forces compared to national intelligence services, and one that becomes even more complicated as new information technologies develop, or if informal grassroots OSINT initiatives proliferate without improving safeguards.

Compared to the Netherlands, the governance system in Finland seems more robust. The defence intelligence agency and the service intelligence units all reside under the control of the Defence Command Chief of Intelligence – with expert and parliamentary oversight. Still, OSINT is approached as a distinct collection discipline, referring to sources such as social media, official statements and documents, as well as research literature. The diplomatic work of Defence attachés, while formally considered a form of human intelligence, also involves openly collecting such official reporting and monitoring the media. In day-to-day reality the distinctions between formal military intelligence collection, informal grassroots OSINT practices by service members, and other investigative initiatives in civil society could prove blurred. Hence, addressing gaps in national legal frameworks with regard to military OSINT, while investing in professionalism and safeguards, should be a priority for European military and intelligence leaders.

[1] E. van der Meulen and P. de Werd, "Exploring grassroots knowledge production: Towards internal crowdsourcing for military intelligence," in *The Art of Scaling: Organising Swift Adaptation to Cope with Crises and War*, ed. H. Zijderveld et al. (Leiden: Leiden University Press, 2025), 239–60.
[2] For example see C. Ruckerbauer and T. Wetzling, *Zügellose Überwachung? Defizite der Kontrolle des Militärischen Nachrichtenwesens der Bundeswehr* (Berlin: Stiftung Neue Verantwortung, Oktober 2023).
[3] https://puolustusvoimat.fi/documents/1948673/2014902/PV_sotilastiedustelu_raportti_EN_2025_web.pdf/c0125ed9-1467-23e7-e7b6-a7891c4fb5fe/PV_sotilastiedustelu_raportti_EN_2025_web.pdf

Peter de Werd
Associate Professor Intelligence and Security
Netherlands Defence Academy and
Radboud University
The Netherlands

STEPHEN COULTHART

Lessons from Ukraine: How OSINT networks are changing war

Expert article • 3950

Open source volunteer research networks

Open source research networks (OSVRNs) have been active well before the Ukraine–Russia war. The first OSVRNs emerged shortly after new internet technologies—such as the iPhone and Facebook—enabled users to create and share more digital content. OSVRNs are composed of individuals, sometimes operating independently and sometimes with institutional backing, who collaborate to apply their skills and expertise to extract the "so what" from publicly available information. These networks are defined by their use of open source information—data in any format (e.g., social media, videos, satellite imagery) that can be accessed by anyone without restriction, whether free or commercial, in a legal and ethically acceptable manner. However, there are gray areas: in many definitions, open sources also include hacked or "breach" data.

The skills required to exploit open source information—known as "tradecraft" in the intelligence profession—include source validation, operational security awareness, advanced search strategies, and report writing, among others. Individuals involved in OSVRN range from self-taught amateurs to full-time professionals. Well-known and long-standing OSVRN include Bellingcat, the Digital Forensics Research Lab, the Conflict Intelligence Team, and Forensic Architecture.

Lessons learned from OSVRN in the Ukraine-Russia war

Lesson #1: The 'Half-Life of Secrets' is Accelerating – and OSVRN are helping to lead the way.

In 2015, Peter Swire of the think tank New America wrote: "Modern computing means that leaks can occur at scale and be transmitted globally, while pervasive sensors and [actors] outside of government can detect many activities that were once secret." He likened the rapid erosion of secrecy to radioactive decay, describing it as a "half-life of secrets." In recent years, the growing availability of open source information has made it increasingly difficult for governments—or anyone, for that matter—to keep secrets. A frequently cited example came in 2018, when an Australian security studies student identified military bases using data from the Strava fitness app.

The war in Ukraine marks a new chapter in the decay of secret state activity, with OSVRNs leading the way. OSVRN can now analyze conflicts more effectively than just five years ago, due to the explosion of available data. When the conflict began in 2021, global data production stood at about 70 zettabytes; by 2025, that number had doubled to about 150 zettabytes (or 150 trillion gigabytes). About half of this data consists of context-rich videos.

These networks also benefit from an expanding range of data sources that help lift the fog of war. For instance, Russian mechanized units have used unencrypted radio communications, which civilian groups intercepted—and, in some cases, disrupted by transmitting their own messages. The proliferation of small, low-cost satellites—miniaturized versions of traditional ones—has further enhanced visibility of the battlespace. Anyone with a credit card and an internet connection can now purchase high-resolution satellite imagery. These trends are likely to accelerate, opening even more opportunities for OSVRN to pierce the fog of war.

Lesson #2: OSVRN are shifting from observers to more active participants in conflict.

A core function of OSRVN has been to investigate and document war crimes—most notably in Ukraine, through their reporting on the Bucha massacre. These networks also engage in counter-messaging campaigns aimed at challenging government propaganda.

The war in Ukraine has shown how these networks activities now directly affect the battlefield. Analysts outside government tracked Russian troop movements before the invasion, demonstrating the value of open sources for strategic warning. According to Ryan Fedasiuk of the Center for a New American Security, this was open source information's greatest contribution in the months leading up to the war. OSVRN have also taken on humanitarian roles. Like efforts to evacuate Afghan civilians in 2021, OSVRN groups helped rescue trapped students in Ukraine's early days of conflict, marking a shift toward a more operational use of open sources.

Finally, OSVRN are shaping the cyber battlefield. While hacktivist groups are not traditional OSVRN, many depend on open source information. The IT Army of Ukraine, for instance, disabled web cameras to deny Russian forces OSINT access, while Russian-aligned groups such as Gamaredon and Fancy Bear have used open sources to craft phishing campaigns and conduct surveillance.

Lesson #3: The value of open source information is creating new ethical challenges for OSVRNs –sharpening old ones.

The Ukraine–Russia conflict has brought to light a wide range of ethical tensions. Three key issues stand out. First, these networks become more relevant to the battlefield, their potential to cause harm increases. Civilian analysts, for instance, may inadvertently release information about noncombatants—as has occurred in cases where the families of Russian soldiers were exposed. Second, open source information and analytic reports can have dual-use implications. An OSVRN operating on one side of the conflict might disclose information that could be exploited by the other, creating ethical dilemmas about the appropriate level of transparency in wartime.

Finally, these network's activities can put their own members at risk. Russia, for example, has launched cyberattacks against members of Bellingcat. Because these individuals operate outside of government structures, they lack the counterintelligence protections typically afforded to official personnel. This raises an open question: to what extent are OSVRN willing to expose their members to potential harm in pursuit of their mission?

During the preparation of this work, the author used GPT-5 to improve the clarity of human-written text.

Stephen Coulthart
PhD, Associate Professor
University at Albany
USA

Scoulthart@albany.edu

GIANGIUSEPPE PILI

The satellites are cast – geospatial gntelligence in an era of open source intelligence

Expert article • 3951

Magis homines movet umbra, quam res – Gaius Julius Caesar

Geospatial intelligence (GEOINT) is not a discovery of the war in Ukraine; it played major roles during the Cold War, when satellites were sent into orbit and were used for Earth monitoring and early warning detection systems. However, after the second invasion of Ukraine by the Russian Federation in February 2022, GEOINT played an irreplaceable role on both sides of the battlefield, and the asymmetry in space capability determined different strategic approaches, even at the policy level. One of the most fundamental capabilities that the West shared with Ukraine was, indeed, GEOINT access and remote sensing data exploitation.

The contemporary battlespace and the configuration of the actual force are shaped by the wide availability of sensors which send back data, even partially analysed, to the Command & Control centres and commanders. Ukraine was able to strike deep into Russia and the Black Sea through drones maneuvered far from the point of impact. Most of the Intelligence Surveillance and Reconnaissance (ISR) is conducted by continuous data collection from drones (Imagery Intelligence, IMINT), ground sensors and satellites. They are all fused together in platforms that allow a shared situational awareness of the battlefield.

It is indeed this sensor and data availability that brought further AI integration into sensor-equipped vectors (e.g., Unmanned Aerial Vehicles (UAVs) and possibly Unmanned Surface Vehicles (USVs)). The quantity of data exhausted any human capacity to analyse and exploit them. As a result, machines were trained and reinforced to digest even more extensive collected data. The war in Ukraine did not show a revolution in firepower production, as not even a single new platform was designed and, at best, legacy weapons evolved in non-industrialized ways. For example, there was no evolution in tank design, and cope cages were improvised coverages against drones so as not to change the original platform. No visible changes in artillery designs are recorded, and, indeed, the Armed Forces of the Russian Federation imported even older North Korean artillery.

However, what did change was the level of precision striking at all levels and the speed of recalibration from the moment of fire and of battle damage assessment, from artillery munitions to First-Person View drones (FPVs), including the Russian adaptation of FAB aerial bombs. These technical developments, or the lack of, can be explained by three factors: the need to maintain the highest level of lethality, the industrial limitations that constrain the overall productivity of new military platforms, and the explosion of cheap sensors able to monitor Earth from space and from air.

GEOINT not only impacted the battlefield, but also the way the general informational ecosystem works. Especially in Western countries, GEOINT is now available to Open Source Intelligence (OSINT) units and traditional media alike. This has had a major influence on the general understanding and perception of the war in the public debate which, in turn, shapes political decision-making. OSINT analysts were able to track illicit movement of oil and weapons between North Korea and Russia; they were able to disseminate information about civil rights violations and illicit use of chemical weapons.

This was possible because access to space was cheaper and more broadly available at the disposal of researchers. This goes far beyond satellite imagery but includes telecommunication and internet connections, as Starlink and Russian and Chinese equivalents are showing. The European Space Agency disseminates medium-resolution satellite imagery and remote sensing data from a wide variety of sensors daily for free. This empowered a much broader information ecosystem which can track the movements on the battlefield. For example, analysts check Russian military presence in the Mediterranean Sea, monitoring the straits through these sensors along with human or imagery intelligence. Information shapes the battlefield and vice versa the battlefield influences politics. Hence, the war in Ukraine reminded the spectators and all parties involved that the cognitive domain and the information space are objects of war as much as anything else. Visible changes on an open-source map can shape the narrative at the ground level, thereby determining political action.

The war in Ukraine is the first conventional war between two states of the contemporary age. This level of Earth monitoring and remote sensing to such a scale and the jeopardy of European and Euro-Atlantic security create the conditions for a different appreciation for GEOINT influencing the battlefield and the policymaking via OSINT sharing and dissemination.

This double-loop is enabled by space access and an informational space widely shaped by GEOINT products through OSINT capability. Although the war in Ukraine has not ended just yet, this ecosystem will survive the frontlines to stay in the present and future of Western societies.

Giangiuseppe Pili
Ph.D., Assistant Professor
Intelligence Analysis Program, School of Integrated Sciences
James Madison University
Virginia, USA

piligx@jmu.edu

ROBERT DOVER

The impact of large language models on intelligence

Expert article • 3952

Information science used to concern itself with how to make meaning from scarce data. In intelligence that meant paying attention to its provenance and how to process it accurately. The era of AI and large language models now means that information science is about how to deal with an abundance of information. The field is also challenged by the speed at which information is collected and how to use and trust machine assessment of information without deskilling analysts: the role of the analyst is also changing to one of identifying where the machine is making errors. The field has yet to come to a mature way of understanding how to avoid being 'gamed' or manipulated, and so even the most sophisticated systems are highly vulnerable to manipulation by adversaries.

LLMs are, however, powerful pattern matchers. Effective LLMs are good at identifying outliers, – which has obvious intelligence applications. They can shape research questions and engage in feedback loop dialogues with human analysts to refine assessments. This sort of dialogue can then also impact upon an LLM's future assessment. The way that an LLM builds and layers understanding is, therefore, a discipline in its own right.

Public and open LLMs are good at drawing together publicly available OSINT. Closed LLMs obviously need to be fed curated data to do the same work. If either open or closed LLMs are used effectively, they can radically enhance a horizon scanning function by focusing in on where, for example, terminology is layered and where it shifts (over time and geographical space). The further development of multimodal models has extended the layering to imagery, multiple languages, video and audio feeds. This can make an LLM a highly sophisticated assessor of imagery intelligence, audio intercepts and the written word, in a joined-up configuration. At its core LLMs are making probabilistic assessments, and therefore the analyst needs to express an identified measure of confidence in the underlying intelligence and in the prompt engineering, the model and its output.

LLMs are currently most usefully deployed in intelligence as a means by which to enhance and augment the productivity of intelligence analysts, rather than in replacing them. In human intelligence (HUMINT) the work of LLMs is in examining transcripts, finding falsehoods and linking to patterns. They do not yet replace the art of handling, which remains a uniquely human to human relationship.

Could I, for example, train an LLM to think in a Finnish way?

If I tried to emulate Finnish culture, by training my LLM on Finnish language, literature, idioms, the Finnish education system, and other local Finnish particularities, and get my the LLM to 'think' and respond as a Finn? In this way, I might be able to test and forecast how various narratives might be received in the Finnish population. In doing so I might be able to speculate about Finnish-specific deception weaknesses or be able to create realistic Finnish red teams in electronic desktop exercises.

But is it possible to boil down the essence of what it is to be Finnish in this way? There are significant dangers of stereotyping, of over or under-reading what we believe to be essential texts or cultural artefacts and missing the myriads of sub-cultures available in a country. To get close to doing something useful we would need a multitude of Finnish models across ages, educational attainment, and regions, and try to calibrate these through real-world evidence collection. Even then capturing enough complexity and nuance would be incredibly difficult.

What a Finnish cultural emulation LLM might be able to achieve is an increased degree of empathy in the analyst. In turn this would reduce the mirroring biases we see in intelligence assessment cadres. Such an emulator LLM should only ever be seen as a simulator to help develop and work-through hypotheses (the human and machine working together), rather than as a replacement for the all-source intelligence mix.

So, how do we ensure LLMs are used effectively in intelligence? The answers are not going to be ones promised by AI companies. Using LLMs in intelligence will require large human labour inputs and careful standard operating procedures. Some have described trust in LLMs to require 'provenance by design', a reworking of privacy or security by design. Each phase of the assessment has to be attached to a testable action log, and assessments need to be stress tested through counter-poisoning techniques and enhanced triangulation. Rather than LLMs being a black box in which prompts are entered and outputs result, there must be transparency over the way that the LLM weighs its evidence and how it changes its responses due to different prompting. It is through a quite classical epistemological approach of examining falsifiability that analysts can then spot the gaps and suggest responses through their chain of command to them.

To take advantage of LLMs, without compromising intelligence tradecraft, agencies must focus strongly on the provenance at all stages of a model's use. Far from degrading the intellectual capability of analysts, effective use of LLMs will require a greater level of skill in method and discrimination in evidence capture and usage. But labour saving, it will not be. Not in the short to medium term.

Robert Dover
Professor, Dean of the Hull University Business School
University of Hull
United Kingdom

r.m.dover@hull.ac.uk

OLLI TEIRILÄ

Dynamics of intelligence-media relationship

Expert article • 3953

Intelligence's relationship with publicity, especially the media, has gone through a multitude of phases in the past century. Even when tensions have prevailed, the relationship has had its range of benefits, at least in open and democratic societies. However, the intelligence-media relationship faces new contemporary challenges. The media-sphere is becoming more fragmented as traditional media houses are challenged by the content flows of social media and a wide variety of blogs. Additionally, the trust in so-called mainstream media is being increasingly questioned by a multitude of actors. The phenomena have their effects also on the intelligence-media relationship. Understanding the nature of the relationship is paramount for both actors, and for the information-seeking public as well.

In the 1900s, especially in newspaper-rich Britain, the intelligence-media relationship was often full of tensions when media, under a dominant oversight paradigm, sought to reveal scandals and wrongdoings of the intelligence community (IC). After the 9/11 terrorist attacks, intelligence communities took a more collaborative approach towards the media, albeit very cautiously. However, incidents such as the misuse of intelligence in the preparations for the 2003 Iraq War, led to new tensions in the relationship. Media's readiness to discuss intelligence matters has progressed over time changing the relationship as well. Additionally, the media-driven public discourses have also influenced changes in oversight mechanisms and accountability within the IC. Media's own oversight or self-control over what to publish is also a notable aspect of the relationship. More thorough media coverage and interaction with the community can be seen as a shift to "legitimacy through regulated publicity" paradigm.

Conforming to the new paradigm, the mutually shared transparency gives legitimacy embraced by the IC and, additionally, accountability as well. In theory, the community needs publicity and transparency for legitimacy derived from public understanding. The government, for its part, seeks to regulate and control the publicity concerning the "Secret State". In addition to other motives, media uses the publicity to further public knowledge and understanding of what, in the end, remains partially secret and unknown. This three-way balancing act works at best to keep intelligence failures or abuses from becoming existential threats to society. But only, if the three are not entangled in a hostile confrontation but interacting through understanding of mutual benefits.

The future trends of the dynamic intelligence-media relationship have two key variables: the nature of publicity and the IC's reaction to it. The media's role may range from offering constructive criticism to focusing on sensational events and failures. Similarly, the communities may choose to become more open, engaging in public discourse, or they may opt for increased secrecy and withdrawal.

In the context of modern governance, complete secrecy within the IC seems unlikely due to the emphasis on transparency. A closed-off community with minimal interaction and questioning media could lead to a precarious standoff. Both parties would probably face frustration rather than benefits. The most probable trajectory for the media-intelligence relationship is one of moderate progress. The media will maintain their slightly skeptical stance, while the IC will gradually assume a more active role in public discussions. Although certain aspects of intelligence operations will always remain classified, extensive coverage of intelligence-related matters is likely to persist. Declassification and publishing of intelligence and intelligence assessments before and after Russia's attack on Ukraine is an example of contemporary publicity for intelligence.

The digital age has ushered in an era of unprecedented amount of available information. With the rise of social media, citizen journalism, and alternative news sources, distinguishing facts from fiction has become a daunting task. Multitude of voices, with a multitude of objectives, challenge the information available to people on a constant basis. Maintaining public trust in both intelligence agencies and the media is paramount to the success of both actors. Recent controversies, ranging from intelligence failures to allegations of media bias, have eroded this trust. Rebuilding and sustaining faith in these institutions will require a concerted effort to enhance transparency, accountability, and integrity in their operations. The 2020s promise to be a pivotal period for the relationship between intelligence communities and the media. As they confront a rapidly evolving information landscape, while also navigating emerging technologies and geopolitical uncertainties, their collaboration will be indispensable.

Intelligence communities need to come out and tell their story. Otherwise, someone else will do it.

Olli Teirilä
Major, PhD
Finnish Defence Forces
Helsinki
Finland

HARRI MÄKI-REINIKKA

Building comprehensive security – Finland as a model for EU preparedness

Expert article • 3954

Finnish model of comprehensive security is a strategic framework that forms the foundation of Finland's resilience, emphasizing a whole-of-society approach to safeguard critical societal functions against a wide range of threats. These threats include not only traditional security risks like terrorism and cyberattacks but also natural disasters, severe weather events, civil unrest, food and water disruptions and migration waves.

The model integrates collaboration among public authorities, businesses, organizations, and citizens, ensuring preparedness and response capabilities under all circumstances, rooted in normal-time legislation and arrangements.

Finland's model has gained international recognition, discussed in regional organizations around the Baltic Rim and in the Nordic and Arctic contexts. The EU is seemingly moving to a wide preparedness strategy under the next multiannual financial framework.

Key features of the model include broad threat recognition, which addresses both human-caused (like hybrid attacks) and natural threats (climate-related crises), whole-of-government approach where security and preparedness are embedded across all public policy and legislation, with effective inter-agency communication. The model includes also whole-of-society engagement involving private companies, NGOs, cultural institutions and citizens, fostering bottom-up resilience alongside top-down measures.

Finland's model has gained international recognition as Finland is a global leader in resilience and preparedness, creating opportunities to share expertise, technologies, and services with other nations and organizations.

After recent global crises like the COVID-19 pandemic and Russia's brutal and illegal invasion of Ukraine, Finland can position itself as a hub for resilience solutions, attracting interest from governments and organizations seeking to enhance their own security systems.

The model emphasizes public-private partnerships, which drive innovation in areas like cybersecurity, critical infrastructure protection and crisis management tools. Finnish companies can provide technologies and services developed for resilience, such as secure communication systems, disaster response equipment or data analytics for threat detection.

Finland can offer consulting services, training programs and capacity-building initiatives to other countries or regions looking to adopt similar resilience models. This includes sharing best practices for whole-of-society preparedness, citizen engagement, and cross-sector coordination.

By promoting the resilience model, countries can build stronger diplomatic and trade relationships among like-minded nations prioritizing security. This open doors for businesses in sectors like defense, technology, and infrastructure.

Finland's advocacy for an EU-wide preparedness strategy, as outlined in President Niinistö's report, positions Finnish expertise at the forefront of EU policy. In March 2024, European Commission President Ursula von der Leyen tasked former Finnish President Sauli Niinistö with drafting a report on enhancing the EU's civilian and military preparedness. The resulting 165-page report, "Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness", was released on October 30, 2024. It builds on the Finnish model of comprehensive security and proposes an EU-wide framework to address modern threats.

The report emphasizes moving away from reactive crisis management to proactive preparedness, addressing interconnected crises like pandemics, the war in Ukraine, climate impacts and hybrid threats. The report encourages also the EU to adopt an all-hazards approach inspired by Finland's model. The EU should prepare for all types of threats—natural, human-caused, civilian, or military—through an integrated framework.

Key recommendations in the whole-of-society approach focus engagement of governments, private sectors, NGOs, and citizens in resilience-building. Same time it is important to promote active citizen involvement through risk education and preparedness communication to enhance societal resilience without causing alarm.

There are eight core areas for resilience outlined in the report including cross-sector coordination, situational awareness, civilian-military cooperation and public-private partnerships. Civil protection authorities are pivotal in bridging national and sectoral divides.

The report proposes a unified legal framework to standardize roles and responsibilities across governance levels for rapid, harmonized emergency responses. It aims to embed "preparedness-by-design" in all EU regulatory frameworks and operations, promotes stronger collaboration with the private sector to leverage innovations, especially against hybrid and cyber threats and encourages joint cross-border procurement to enhance resilience capabilities.

The report calls for at least 20 percent of the EU budget to be allocated to security and crisis preparedness, a significant increase given competing priorities like climate neutrality (30% of the budget through 2027). It also proposes the Securing Europe Facility (SEF) to consolidate funding for civil security, protection, and emergency response, linking research with operational deployment and advocates for stronger foresight, intelligence-sharing and efficient crisis decision-making processes across the EU.

Expert article • 3954

The report raises up the need for assertive EU diplomacy to address hybrid attacks and scale up defense efforts. It recommends to prioritize fortifying infrastructure to withstand disruptions, including cross-border training and public education initiatives.

The report acknowledges that the EU lacks shared strategic culture, small egalitarian society, and high institutional trust. In member states it is now time to prioritize security over diverse national priorities and narrow the distance from citizens, which may hinder effective public involvement.

Hopefully EU's complex political system and varying member state priorities do not limit implementation of the ideas presented in the Niinistö's report. By leveraging the model countries can enhance their economic and diplomatic influence while contributing to global security.

Harri Mäki-Reinikka
Ambassador (Defence, Energy, Logistics and Digitalization)
Ministry for Foreign Affairs
Finland

JUHA VAUHKONEN

The strategic importance of Finland's neighboring regions and the growing security challenges

Expert article • 3955

Russia's brutal and unjustified invasion of Ukraine in February 2022 led, to put it bluntly, to the withdrawal of Russian troops from this area, from our vicinity, more or less completely, with the exception of the Kaliningrad enclave, of course. From a purely military perspective the situation was excellent. The threat of Russia's aggression against its neighbouring countries with traditional, conventional military means became quickly very unlikely.

Nevertheless, one need only look at a map to see that this northern region is extremely important to Russia. The Greater St. Petersburg area, including the city itself and its ports, is a significant logistics hub for the export and import of Russian goods and commodities. Forty percent of Russia's foreign trade passes through the Baltic Sea and it is Russia's most important route for oil exports. The isolated Kaliningrad enclave is supplied via the Baltic Sea, either by sea or by air. Its lifeline is very thin. Alongside St. Petersburg and Kaliningrad, the strategic importance of the Kola Peninsula from the perspective of Russia's strategic deterrent is undeniable. The key capabilities of the Russian nuclear first strike capabilities are located in the Kola region.

For the reasons stated above it is Russia's strategic interest to secure the use of the Baltic Sea in all situations. Especially for its Northern Fleet the entire Arctic region means unrestricted access to the Atlantic via the northern sea routes and it is clear that the region's importance will continue to be emphasized.

Russia was undoubtedly a military power in the Arctic before the outbreak of the war. The Russian leadership announced major changes to the armed forces in December 2022. Aspiration to restore that role and the influence that it brings with it will most probably be emphasized in its foreign and security policy.

According that announcement the size of the armed forces is planned to increase in the coming years, which will include changes in the force structure and the establishment of new forces. Build up of infrastructure for its future military deployment and military infrastructure along Finland's eastern border is already visible.

The war in Ukraine will end, someday. Then the troops that left here will return to their homes, which will in no way be the same as when they left. Finland and Sweden are members of NATO, and all the Nordic and Baltic countries have bilateral defense agreements with the United States.

During the war, the border against NATO has doubled to 2,556 kilometers, and the Baltic Sea has become, in practice, even if the term is unfortunate, NATO's inland sea. The NATO countries in the region will significantly increase their defense spending in the coming years, not to mention the contingency measures launched by the alliance. The threshold for attacking again a smaller neighboring country has risen dramatically... and the Northeast Passage continues its inevitable thawing. I will return to this briefly later.

Direct military threat from Russia is currently very low, but the expansion of the war in Ukraine cannot be ruled out and, notwithstanding the foregoing, no conventional attack at a later date. We must prepare, in any case, for the threat of a large-scale attack. Broad scale influencing is already a reality. Russia considers itself to be in a systemic conflict with the West, and it seeks to influence, in particular, the unity of NATO and the European Union, as well as the commitment of the United States to European defence arrangements. Russia remains a valid threat that requires continued preparedness, the strengthening of our military power and capabilities, and, on the other hand, the continuous improvement of the crisis resilience of our civil societies as a whole.

Russia's dealings with other countries have always been based on lies, blackmail, threats, and empty promises. Why would anything change now? We already know that Russia is prepared to take greater political and military risks to achieve its goals. It will continue its malicious and evil deeds despite the war, and especially after it.

Russian intelligence activities in Finland have increased, and I would assume this is also the case in other countries in the region. Russian military intelligence service has sought to update its intelligence methods to better reflect the changed operating environment. The methods are more diverse and partly improvised than before. This can be seen, for example, in the increasing use of proxies and intermediaries and in more straightforward information gathering.

It goes without saying that intelligence in digital networks remains significant. In addition to these, the Russian intelligence services have the ability to carry out sabotage and disruption of critical infrastructure. We have experienced cyberattacks, seen link masts fall, airspace violations conducted in a grossly blatant manner, GPS-jamming, drones harassing airports, etc etc. It is good to keep in mind that Russia has the readiness, if necessary, to increase the intensity of its operations and to target also military targets or critical infrastructure largely and security of supply as well.

In these changed circumstances, the enemy is not always necessarily a recognizable "little green man or woman". Identifying the opponent and verifying their identity is quite challenging from the "ones and zeros, the "guys and gals" in the community, whether it be a work or friend community where the person has been "one of us" for years, not to mention those faceless calculating agents who, using deviousness and secretive tactics, get those foolish but useful people to talk out of turn. War is now being waged in the realms of cyber and disinformation, as well as in the more traditional "cloak and dagger" environment. It is important to be aware of this and recognize it. The Russians have been among us for a long time. I dare say that they are very familiar with our transparent societies and our legislation, which they also know how to exploit for their own purposes. And we have brought this situation upon ourselves.

Expert article • 3955

Finally, very briefly about the thawing of the Northeast Passage.... the Arctic region holds probably more than 10% of the world's undiscovered conventional oil resources and some 30% of its undiscovered conventional natural gas resources. In addition to oil and natural gas, the Arctic region possesses significant metal deposits and fish resources. China is already preparing its merchant fleet and Navy to face the conditions of Arctic waters and the challenges they bring, but above all, to enable the exploitation of the natural resources offered by the region in a larger scale and to secure this and other national interests in this region as well.

It doesn't really fit with the Russian image of a great power that China would come with a barrage of merchant ships and naval forces into areas it considers its own, or at least to which it thinks it has a pre-emptive right. Even if the strategic partnership between Russia and China were to endure beyond the war and the burden of history, it would of course be reasonable to raise the question of how prepared we Europeans are for the day when Chinese intelligence ships and aircraft begin to operate in our nearby waters and airspace, not to mention any overt hostile actions that we may also encounter. It is good to remember that Panda is a bear too.

Juha Vauhkonen
Rear Admiral (ret), Defence Command Chief of Intelligence (2021-2023)
Finland

OUTI SALOVAARA

Finland's eastern frontier – where democracy meets totalitarianism

Expert article • 3956

Can business ever bridge the divide between democracy and totalitarianism that lies between Finland and Russia?

This question came to my mind while writing my nonfiction book Ruble Princes (Ruplaruhtinaat), published in the summer of 2025. It explores the real estate deals and business activities of wealthy, influential, and well-connected Russians in Finland.

When Finland in 2000 opened its property market to buyers from outside the European Economic Area, Russians quickly and unexpectedly became the largest group of foreign purchasers. For affluent Russians, Finland was a nearby, stable, safe, efficient, and friendly country.

Before long, however, the real estate purchases and business ventures of these "luxury Russians" began to attract negative attention. Some of the properties they acquired were located in strategically sensitive areas, certain buyers' backgrounds raised suspicion, and their business operations often seemed to involve money of unclear origin. Such property transactions were increasingly viewed as a potential security threat to Finland.

In 2020, buyers from outside the EEA were required to obtain permission from Finland's Ministry of Defence before purchasing property. In July 2025, property purchases by Russian and Belarusian citizens were banned altogether. By then, however, Russians had already acquired thousands of properties across Finland—particularly in the southeast and eastern parts of the country.

As a journalist, I have investigated Russian property deals and business activities since the early 2000s. Among the buyers I found, for example, executives from the gas and oil giant Gazprom and Russia's state television, IT tycoons with KGB backgrounds, and even an Orthodox oligarch reputed to have been Putin's personal masseur.

The grand business plans of these wealthy Russians ended, time and again, in disappointment. Promised investments never materialized, and loss-making enterprises were kept alive with funds channeled from Cyprus or the Virgin Islands. Wages and contract payments often had to be recovered through legal action.

These Russians showed little inclination to adapt to Finnish values, principles, or ways of doing things. They rarely spent time with native Finns or spoke Finnish. Instead, they used Finland as a base for financial transactions, a safe haven for assets, a support for their home-country businesses, and a destination for leisure. EU residence permits and citizenships facilitated their children's education and employment in the West. Western journalistic practices were alien to them—critical questions about the origins of their funds were met with silence or threats of lawsuits.

In my book, I describe the world of wealthy Russians as a vast spider's web of power, business, and money flows stretching across Russia and beyond, with the Kremlin at its center. The closer one gets to the middle of the web, the better the positions available in companies, ministries, municipal administrations, universities, customs offices, schools, museums, foundations, associations, and other organizations – either state-controlled or nominally private – under Kremlin influence. And the closer one is to the center, the more one can siphon from the Russian taxpayers' purse. Russia is not called a kleptocracy for nothing.

Unlike Finns, Russians have learned through history that honesty, trust, and adherence to laws and rules do not lead to success. These wealthy and ruthless Russians were received by an open, trust-based Finland, a society that naively believed all newcomers would adopt Finnish values and the principles of a rules-based state. Like the rest of the European Union, Finland steadfastly believed it was fostering Russia's democratization, even though everything Russia did proved otherwise. For the Kremlin, preserving and rebuilding the empire and achieving geopolitical goals regarding its neighbors have always taken precedence over all else.

From the Kremlin's perspective, small nation-states have no right to independent decision-making—they are merely parts of great-power spheres of influence and vassals of the strong. Russia seeks to influence its neighboring states through affable intermediaries, whose charm has even drawn former Finnish prime ministers into the company of Kremlin insiders – lobbying for Gazprom's Nord Stream gas pipeline or sitting on the board of the Sberbank bank.

Russia does not seek international trust, dialogue, or interdependence that might prevent crises. It seeks only to build dependencies on Russia – while simultaneously eroding and destabilizing democracies.

The more wealthy and influential Russians are networked into Finnish society through business, property ownership, cultural connections, or political ties, the more effectively Russian authorities can influence Finnish society, including the shaping of public opinion. At worst, this could lead to an unlawful and improper erosion of Finland's sovereignty.

Finland must reconcile its own democratic and rule-of-law principles – such as openness and non-discrimination – while protecting itself from exploitation by a neighbor representing opposite values, whether through espionage, murky business dealings, or various forms of hybrid influence.

When Russia's war of aggression in Ukraine eventually ends and Western sanctions begin to ease, Finland's eastern neighbor will be an even more totalitarian state than before. How, then, will Finland ensure its own interests and security in business and other dealings with Russia, when that was already difficult in the past?

Outi Salovaara
Master of Social Sciences, Master of Science (Economics and Business Administration),
Independent Journalist
Finland

MARKUS LAINE

Police as the first responder for threats to national security

Expert article • 3957

The operating environment of the Finnish police – like that of other security authorities – is undergoing a major change. Hybrid influencing targeted at Finland is increasing as internal and external security issues overlap each other. The operating environment has been particularly influenced by the return of large-scale and long-lasting warfare to Europe. Changes in the external security environment, in particular Russia's war of aggression, are also reflected on the internal security of Finland, and the police must prepare for new and diverse security threats. Events affecting critical infrastructure in Finland and the surrounding areas have attracted extraordinary attention recently. During this century, the police have encountered completely new areas of responsibility, such as terrorism and war crimes, cybercrime, pandemics, instrumentalised migration, hybrid influencing and the street gang phenomenon. To combat the new threats, the police have been given more intelligence powers, such as the Civilian Intelligence Act and the Criminal Intelligence Act, which is still under preparation. The exchange of information between authorities is also being streamlined.

The police in Finland are the authority responsible for internal security, but at the same time the police are also the first responder in the prevention of several external security threats. The police are an authority of high-level operational response, providing security services every hour of the year. The police are constantly prepared to respond to all threats to internal security throughout Finland. Especially in sparsely populated areas and sea areas, co-operation with the Finnish Border Guard is highlighted. The goal of Finland's security policy is to safeguard territorial integrity and to prevent Finland from becoming involved in a military conflict. A well-functioning and effective police force plays a significant role in reaching this goal. The police are the main source of operational response capabilities in the face of unclear threats as long as they have not been identified as military threats.

If Finland was to encounter unforeseen hostile military activity by a foreign state, the situation would probably require the immediate use of police powers as a first response to counter the threat. Both legally and operationally, it is clear that the Finnish Defence Forces together with the Border Guard are responsible for the military defence of Finland and for safeguarding territorial integrity. This is emphasised in the sea areas and airspace, where the military authorities have a high level of readiness to counter a military threat. However, the unconventional threats that are characteristic of the changed security environment may be unpredictable to such an extent that the police have the responsibility to perform the first response to the incident, especially when operating in the inland of Finland. By virtue of the Finnish Police Act, the police are tasked with safeguarding the legal and social order, protecting national security and maintaining public order and security. In addition to its own duties, the police are also the regional surveillance authority as referred to in the Finnish Territorial Surveillance Act, and are responsible for safeguarding territorial integrity.

If an unidentified and heavily armed troop appears at a rural wilderness airfield somewhere in Finland, a citizen first reports it to the general emergency number, and the nearest police patrol is alerted to the scene. No matter whether it is a question about foreign soldiers not wearing insignia of a foreign nation or an organised crime group, it is clear that public order and security are seriously endangered. In co-operation with the Defence Forces, the police will attempt to identify whether the situation primarily falls within the competence of the police or whether it is a task for the Defence Forces. Under normal conditions, the police are responsible for carrying out the assignment until the situation is identified as hostile military activity, for example. It should be noted that the efforts of the police as a first response authority may continue in that type of situation for a long time.

On the basis of legislation concerning executive assistance, the police have the opportunity to receive executive assistance from the Defence Forces and the Border Guard. The instrument of so-called demanding executive assistance enables the police to use the equipment and capabilities of the Defence Forces. In the changed security environment and in particular in unclear demanding internal security threats, this means that the police are able to utilise even heavy weapon systems and other capabilities intended for the use of military force even before the situation is interpreted to be a military threat.

Particular attention must be paid to the Åland Islands in the southwestern part of Finland. This is an autonomous and demilitarised area, which means that the Finnish Defence Forces are not present in the area under normal circumstances. Important energy, telecommunications and sea connections run via the Åland Islands, and according to the estimates made by authorities, the risk of hybrid influencing in Åland has increased. It is important to pay particular attention to the special status of the Åland Islands and to the threats against the area in the co-operation conducted between the Finnish police, the Åland police and the Finnish Border Guard so that the authorities have an immediate and effective response capability to counter threats detected in the area, such as threats against critical infrastructure.

Finally, it should be noted that there may be a high threshold for interpreting threats or influencing measures against Finland as military threats. This may mean that the police have a longer-term and more extensive responsibility for assignments that suggest military activity. Tasks that clearly fall within the competence of the police, such as the pipeline and cable breaks that have been encountered in the Baltic Sea, have also been demanding and long-lasting by nature. Duties related to countering hybrid operations and new threat scenarios require a high level of preparedness, capability and sufficient powers from the Finnish police. Intelligence is a key component in preventing and combatting threatening situations. The measures taken by the authorities will not be timely and sufficiently effective without an early warning, an adequate conception of the current situation and an assessment of the development of the situation. The direct and close exchange of information has been the strength of the Finnish authorities for decades. This approach can be used to ensure that all competent authorities have a correct conception of the current situation and that they are prepared to counter the threats also in the future.

Markus Laine
Police Lawyer, Head of Legal Affairs
Southwestern Finland Police Department
Finland

PETER SUND

Internal Security Policy of Finland – examination of its impact on industries

Expert article • 3958

The recent government report on internal security describes the operating environment of internal security and defines the priorities and objectives of internal security policy for the coming years. This article examines the potential impact the policy approach to the Finnish industries, especially from the perspective of digital society. Although being key topics in the context of the internal-external security nexus, protecting civilian population in major disruptions and emergencies as well as protecting the society from hostile information influence is not discussed here.

Internal Security in a changing operating environment

The policy outline recognizes, but understates, the nation's economic prosperity having an important and multifaceted impact on internal security. Finland depends on foreign trade and exports. Equally important is that our democratic governance and welfare-state model rely on economic prosperity. Crime, social instability, political dissatisfaction, and insecurity rise sharply when economic prosperity stumbles. Similarly narrow view is taken on technological transformation, suggesting technological solutions often arise from cooperation between authorities. Conversely, most of the technological development is borne by companies and public-private partnerships produce effective solutions to challenges identified by authorities.

Priorities and objectives: Countering espionage and organized crime

The policy outline notes that cybercrime, particularly property and fraud offenses, has grown significantly and is evolving rapidly. But the scale and societal impact of the phenomenon is underscored by recent findings: according to the 2025 Digital Security Barometer (DVV), about 60% of citizens are concerned about cyberattacks and digital fraud, and nearly 40% report declining trust in digital security. Similarly, a survey by the biggest telecommunications company Elisa corporation found that over 90% of Finnish large enterprises believe cybersecurity threats have increased in recent years. The scale of serious cybersecurity incidents processes by authorities in Finland underscores the daily impact to the society. Despite these observations, the policy outline lacks proposals to address such a clear and significant challenge.

Instead, it reiterates previously examined needs for broader criminal intelligence powers.[1] From industries' perspective, expanding criminal intelligence powers based on "internal security threats" would again undermine the very values that internal security is created for. If "internal security purposes" were used as an independent basis for exercising intelligence powers, internal security threats would need to be defined precisely and narrowly. For example, broad definition of cybercrime covers a range of offenses from fraud to espionage, with severity varying from minor victim-based crimes to aggravated offenses. Legally, these acts differ greatly in culpability and cannot be treated as equivalent grounds for coercive powers. Moreover, a significant portion of Finns annually fall victim to some form of cybercrime (e.g., scams, malware, phishing) — phenomenon so widespread that society no longer fully recognizes its scope.

In contrast, success lies in enforcing criminal liability through enhanced pre-trial investigation and prosecution measures, including international—especially European —cooperation. Internal security and economic security are closely linked in countering industrial espionage and related economic crimes, which together erode domestic industry. Acts of vandalism, sabotage and general danger crimes harm industrial operations and profitability, causing direct damage and indirectly increasing public anxiety and reducing consumption and investment willingness. Conversely, terrorism cannot dismantle Finland's constitutional order or significantly weaken companies' competitiveness or delivery reliability. Yet substantial and growing resources have been allocated to responding to terrorist threats, particularly to the state intelligence service—raising questions about prioritization of societal benefits. Such policy remains inadequate regarding protection of corporate assets, economic conditions for business, and security of supply.

Protecting critical infrastructure

The policy outline suggests that in serious cybersecurity incidents, competent authorities lead case management within their mandates. In Finland, nearly all critical infrastructure is connected to digital systems. De facto, responsibility for cybersecurity lies primarily with companies and communities, as they form most of society's infrastructure and economic structure and possess the legal, administrative, and technological capabilities to implement measures. Companies and communities identify anomalies in their ICT systems, investigate causes and impacts, and eliminate adverse effects as well as recover from incidents. Cybersecurity is thus a daily commodity maintained by data holders where information systems reside. The reliability of systems managed by these entities ensures not only their own operations but also effects to external parties thus providing collective resilience.

[1] See Police Criminal Intelligence Legislation Development Needs, Ministry of the Interior Publications 2023:19.

Peter Sund
CEO
Finnish Information Security Cluster (FISC),
Technology Industries of Finland
Finland

peter.sund@teknologiateollisuus.fi

TOMMI KOIVULA

On Finnish intelligence culture

Expert article • 3959

Being "intelligence-savvy" has not, at least historically, been one of the virtues of Finns. One reason may lie in the characteristics of Finnish society, which has been traditionally composed of small communities, a homogeneous population, a strong culture of trust, and, until recently, a widespread belief that Finland is a relatively uninteresting and remote country.

Historical experience may also explain the often cursory Finnish view of intelligence. For decades, intelligence – whether civilian or military – was characterized by its distance or even isolation from large segments of Finnish society. In the first decades of Finland's independence, state intelligence organizations were often seen as aligning with political ideologies: in the 1920s and 1930s, they were associated with right-wing politics; during the late 1940s, they leaned left; and their activities were often viewed as serving domestic political purposes.

Later, during the Cold War, Finland voluntarily limited its intelligence activities to countering internal security threats and gathering intelligence domestically. This approach was primarily driven by the Finnish foreign policy leadership's desire to avoid jeopardizing relations with the Soviet Union. Ironically, intelligence activities by major powers were often quite active in Helsinki during the Cold War. Nonetheless, the "low profile" of Finnish intelligence during those days – and for several years afterwards – also contributed to the notion that Finland's intelligence services have, until recently, maintained a relative distance from the Finnish public.

Perhaps for these reasons, the term "intelligence" has, for decades, been met with some reservations in the academic world as well. For example, when the University of Jyväskylä launched the first nationally significant master's program dealing with intelligence analysis in 2017, the term "intelligence" was deliberately omitted. Consequently, the program is still titled Security and Strategic Analysis to this day.

However, something resembling an emerging "intelligence culture" has developed in recent years. Several external factors have driven this new awareness of intelligence, such as intensifying geopolitical and economic competition, highly publicized cases of corporate espionage, hybrid and information warfare campaigns directed against Finland, and the new possibilities and threats posed by modern technology – many of which have had an impact on Finland as well, not to mention Finland's membership in the European Union and NATO.

On their part, the intelligence agencies – particularly SUPO, Finland's civilian Security and Intelligence Service – have taken successful steps to become more publicly visible. This shift was partly driven by the Civilian Intelligence Act and the Act on Military Intelligence of 2019, which granted new responsibilities and powers to the services, as well as the establishment of a new parliamentary committee on intelligence. These developments have led to increased public interest in the topic.

Moreover, academic study of intelligence is rapidly diversifying in Finland. Traditionally, the universities of Helsinki and Turku have been the main centers for research on intelligence history, while the National Defence University focused on the needs of the armed forces and military intelligence. However, new players have emerged: in addition to the University of Jyväskylä mentioned earlier, the University of Vaasa now offers programs related to legal and administrative issues in intelligence, and Tampere University has introduced a part-time professorship in national security, among other initiatives.

An important development is the first full professorship in intelligence studies, which was launched at the beginning of 2025 as a joint academic chair between the National Defence University and the University of Turku's Future Studies Center. This new position helps create a critical mass around Finnish intelligence studies, gives the field greater visibility, and promotes international cooperation.

There has also been thematic diversification within the field. In addition to historical studies, recent research projects have focused on economic intelligence, privatization of intelligence, public-private partnerships, parliamentary oversight, administrative perspectives, critical intelligence studies, and the relationship between intelligence and the media – just to name a few.

This new interest in intelligence has already begun to yield results. In recent years, several doctoral dissertations and many master's theses have been produced on the subject in various Finnish universities. Some academic textbooks have been published too, as well as podcasts and non-fiction books aimed at a broader public. Still, much work remains. For example, there are no academic journals dedicated to intelligence studies in Finland, and only a small group of scholars publish internationally on the subject.

Nevertheless, awareness of intelligence is rapidly growing in Finnish society. It may be fair to view the recent developments as steps from childhood to early adulthood in Finnish intelligence culture.

Tommi Koivula
Professor
Department of Warfare
Finnish National Defence University
Finland

ANTTI AINE

Legal resilience and intelligence

Expert article • 3960

In Western democratic states governed by the rule of law, protection of individual rights is of fundamental importance. Law determines the legal status of individuals and creates a framework for the exercise of their rights. In a state governed by the rule of law, authorities must act within the limits of their defined tasks and respective powers. Concurrently, authorities should have sufficient powers at their disposal so that they can safeguard the fundamental security interests of society. The tension between the protection of individual rights and the sufficient powers of the authorities is crucial to legal resilience.

The tension between the protection of individual rights and the sufficient powers of the authorities is also reflected in intelligence legislation. Several relevant examples can be mentioned. The legal conditions for the use of information obtained through intelligence methods in criminal investigations has recently been raised in Finland. The assessment is related, on the one hand, to the protection of confidential communications guaranteed by Article 8 of the European Convention on Human Rights and, on the other hand, to the possibilities of the authorities to investigate and solve serious crimes. Another example is the targeting of intelligence methods to premises used for permanent residence and falling within the scope of domestic privacy. A third example concerns the legal conditions on the basis of which intelligence collection methods may be used without the knowledge of their targets.

The legal regulation of intelligence requires a continuous reconciliation of the legal status of individuals and the fundamental security interests of society. The consideration is holistic in nature. Changes in the security threats to society lead to consideration of the possibilities of maintaining a balance between the rights of individuals and the security interests of society. The review can be carried out on at least three parallel levels with mutual interfaces.

In a state governed by the rule of law, it is essential that the use of powers related to intelligence is legally and politically controlled. This requirement also applies to the development of the conditions for the use of powers. In states governed by the rule of law, the legal conditions for intelligence are typically discussed in connection with the preparation of legislation. It is obvious that national legislative solutions may differ from each other. An example of a very thorough process is the drafting of legislation on civil and military intelligence in Finland. The Finnish Parliament and its committees played a central role when the detailed content of the legislation was decided in 2019. The parliamentary review focused in many respects on the relationship between the rights of individuals and the relevant determination of the powers of the authorities. The legal assessment was based in many respects on the provisions of the European Convention on Human Rights and the case law of the European Court of Human Rights.

The application practices of intelligence legislation are also central to the balance between the protection of individual rights and the fundamental security interests of society. The framework for evaluation is legal. The application of the provisions typically requires discretion, in which case the decision-making practices have their own significance. The principle of conformity with the law in public governance requires that the legality of the public authorities' activities be overseen. This assessment may be based on the authorities' internal oversights of legality. Control may also be exercised by independent institutions, such as the intelligence ombudsman. Courts play a central role when granting an authorisation for intelligence collection methods. It is essential that courts have sufficient expertise in intelligence activities in addition to knowledge of the legislation.

It is justified to discuss questions related to intelligence in academic research. The balance between individual rights and society's security interests is a relevant topic of legal research. Legal research can support the interpretation and application of individual provisions. In addition, legal research can systematise the relationships between different parts of the legal regulation of intelligence and maintain the coherence of law. However, questions related to intelligence can be elaborated in various research contexts. It is highly valuable that these questions have been discussed in different scientific disciplines (for example, social science and military sciences). Interdisciplinary projects have high potential in intelligence research, because parallel perspectives can help to create the conditions for structuring social phenomena and their regulatory possibilities.

The balance between individual rights and adequate powers of authorities is central to Western democratic states governed by the rule of law. This balance must be continuously maintained as society and its security threats change. This requires well-functioning intelligence legislation, effective application practices and dynamic intelligence research.

Antti Aine
Professor
University of Turku, Faculty of Law
University of Helsinki, Faculty of Law
Finland

WESLEY WARK

Canadian intelligence at a cross-roads

Expert article • 3961

The Canadian intelligence system today stands at a crossroads. Its birth stems from the experience of World War Two and a consequential, post-war debate over Canadian intelligence requirements. Over the course of the following seventy years, Canadian intelligence has evolved with two main missions in mind: domestic security; and membership in an intelligence partnership now known as the "Five Eyes," linking Canada with the United States, the United Kingdom, Australia and New Zealand.

For much of the Cold War the domestic security mission focused on counter-intelligence: efforts to thwart Soviet, Warsaw Pact, Chinese and Cuban spying in Canada. Canada was tutored early in that endeavour by British intelligence. It was always a battle of unequals, as adversarial embassies and consulates were stuffed with spies posing as diplomats. But with the end of the Cold War, the domestic security mission swung, at first slowly, and then, after 9/11 dramatically, to a counter-terrorism mission. The objectives were to thwart violent extremist activities within Canada and to ensure there was no spill-over across the Canada-US border. This required close cooperation with US domestic security agencies, especially the FBI.

Canada's membership in a tight-knit intelligence club was central to the construction of its intelligence system after 1945. The signing of a signals intelligence sharing agreement with the United States in 1949 (CANUSA), with the agreement of the UK, was a major expansion in the direction of what would become the Five Eyes, with the addition of Australia and New Zealand in the early 1950s. Canada would go on to develop a signals intelligence capacity with an Arctic-focussed mission, build a small, open-source intelligence agency, and begin to produce strategic threat assessments, initially with a focus on the Soviet threat to North America, all with an eye to making a contribution to the intelligence partnership such that it would secure Canada's place. Canadian intelligence capabilities were always far smaller than either the United States or the UK, and often did not reach those of Australia.

The cross-roads that Canadian intelligence now faces are a product of fundamental disruptions to its twin founding missions. On the domestic security front, the threat of violent extremism remains, but concerns over cyber espionage impacting on Canada's economic security and on its critical infrastructure now are of greater moment. At the same time, tensions with the United States over its economic policies and their impact on the closely intertwined Canadian economy, and threats of US annexationist efforts have made security cooperation with the United States more challenging.

Canada's long-nurtured membership in the Five Eyes now also faces challenges and future uncertainty because of the policies of the Trump administration. While the Five Eyes partnership remains unique and is unlikely to implode, concerns about intelligence sharing and the politicisation of US intelligence have eroded trust and forced Canadian officials to confront the degree of dependency involved in our membership in the Five Eyes and the overwhelming reliance Canada has on the US intelligence community to help it fill out a global picture of threats.

The cross-roads moment that Canadian intelligence now faces involves two imperatives. One is the effort to shift resources from a primarily domestic security mission to a more global intelligence capacity. This will require new foreign intelligence capabilities beyond our long-established signals intelligence function. The other is the need to expand and diversify our intelligence partnerships to reduce our singular reliance on the Five Eyes and on the US intelligence community, in particular. On both of these fronts, the objective is to achieve more sovereign capacity and autonomy for Canadian intelligence in what the Canadian Prime Minister recently dubbed, the "age of disorder."

As the Canadian intelligence system reorients itself to new geopolitical and geo-economic realities the expectation is that Canada will increasingly look north, to the security of the Arctic, and will look for new and expanded intelligence relationships with the Nordics in particular. Canadian intelligence will be twinned with new defence capabilities in the Arctic and a reassertion of our NATO role as a Northern flank state.

Wesley Wark
Dr., Senior Fellow
Centre for International Governance Innovation
Canada

Fellow
Balsillie School of International Affairs
Canada

wwark@cigionline.org

SVEN FELIX KELLERHOFF

Capital of spies in the Cold War and today

Expert article • 3962

If anyone could judge, it was Hans-Georg Maaßen. „Berlin is the European capital of spies", said in 2013 the then head of the Bundesamt für Verfassungsschutz, responsible for countering espionage in the Federal Republic of Germany. Maaßen was not talking about the past, about the time of German division, when the hottest front in the Cold War ran right through Berlin, but about the present, about the 21st century.

Every Berlin tourist knows where the spy quarters are in the government district, because bronze plaques hang next to their portals. At least six embassies in the city centre most likely serve as listening posts: the US mission and the British and French embassies on Pariser Platz, the late Stalinist palace of Russia on Unter den Linden, the prefabricated building of the North Korean mission on Wilhelmplatz and China's diplomatic location on the Jannowitzbrücke. On the roofs of all these buildings, Google Earth shows mysterious objects: interception antennas.

At the same time, probably no country is as naive as the Federal Republic. In the German and international intelligence establishment, a statement by long-time Chancellor Angela Merkel in 2013 initially caused astonishment, then laughter and finally pity: „Spying among friends is not acceptable", the head of government had announced after the alleged revelations about the NSA's surveillance activities. Yet everyone who is even remotely familiar with the subject knows that every intelligence service tries to eavesdrop on everything it can – at least every service except the Bundesnachrichtendienst (BND), which is either completely prohibited from doing so or faces such high legal hurdles that it is of little practical significance.

Today, Berlin is the capital of espionage due to a misguided sense of restraint, even though there are hardly any targets for industrial espionage here – simply because the German metropolis has virtually no relevant economy. Instead, there is all the more politics, administration, associations, law firms and consulting companies. Berlin is also a city where representatives of right-wing and left-wing opposition parties visit a headquarter of enemy intelligence services such as the Russian embassy, and where parliamentary staff members spy for China.

This thoroughly depressing state of affairs invites comparison with the Cold War. In the decades between the end of the Second World War and the collapse of the Soviet empire in 1989/90, Berlin was synonymous with espionage: Nowhere did the two blocs clash more directly than at the inner-city border. Until the Wall was erected, this was the „invisible front" in a very dirty secret conflict, which included not only clandestine propaganda battles but also a whole host of secret operations. In the 1950s, this more or less secret struggle was part of everyday life in both East and West Berlin. The autobiography of British double agent George Blake provides a somewhat exaggerated picture of the intelligence situation at that time: „One got the impression that at least every second adult Berliner worked for some espionage organisation, many of them for several at the same time."

This remained the case even after the 13 August 1961. Although living conditions in the former German capital had changed, and with them the conditions under which agents attempted to monitor, infiltrate or otherwise harm the other side, the formerly „invisible front" was now impossible to overlook. But fundamentally, nothing had changed: Berlin was and remained the capital of spies. From the eastern part of the divided city, the GDR's Stasi launched one attack after another on its more successful German rivals in the Federal Republic and West Berlin. The police there were systematically infiltrated, and regional politics were at least co-directed by agents of influence. Conversely, Americans and British eavesdropped far into the Eastern Bloc from the legendary Teufelsberg and the (much less well-known) USAF station on the „Amiberg" in Marienfelde, recording radio and radar signals to gain advantages for the constantly looming military conflict. In one respect, both sides were similar in this constant confrontation: whenever international interests were affected, the German participants in this risky game had no say whatsoever – both in the dictatorially ruled Soviet bloc and in the democratic West.

This decades-long power struggle ended with the reunification of Germany in 1990, but only temporarily. For Russia's shift against the West, and thus against peaceful coexistence in the world, which began in 1998, led within a few years to a new Cold War, which has become heated since the attack on Ukraine in 2022 at the latest.

Unlike a few decades ago, however, awareness of the dangers has virtually disappeared, at least in many German minds, right up to the highest levels of government. There is no other explanation for the distorted reaction of at least significant sections of the political establishment to intelligence activities: The completely normal (and in most cases even legal) gathering of information by Western, mostly American diplomats was blown up into a scandal dubbed 'Cablegate' in 2010, while actual attacks by a foreign power, for example on Germany's strategically essential energy security, were considered part of a „Energiewende". In such a mindset, even a former chancellor was ultimately able to openly act as an agent of influence for the Kremlin.

Sven Felix Kellerhoff
Senior Editor for Contemporary History
DIE WELT
Germany

kellerhoff@welt.de

KIMMO ELO

Germany's liberal democracy under pressure: China and Russia as the most active "foreign powers"

Expert article • 3963

Germany's position as the EU's most influential democratic system has made it one of the main targets for authoritarian states seeking to undermine liberal democracy. Its strong and diversified economy also attracts scientific and corporate espionage. Yet, from the perspective of political stability, the more serious concern lies in the growing attempts to destabilise Germany's liberal-democratic order. These efforts have become more visible since Russia's anti-Western rhetoric escalated into full-scale war against Ukraine. However, China's ambitions to rise as a global superpower cannot be overlooked, as they contribute to increasing pressure on European liberal democracies."

The Zeitenwende (juncture) declared by Chancellor Olaf Scholz in response to Russia's invasion also reflects a shift in Germany's security and threat assessments. An interesting loophole into this change is provided by the 2024 annual report of The German do¬mes¬tic in¬tel¬li¬gence ser¬vices (Verfassungsschutz), published in June 2025. The report highlights intensified influence operations by Russia and China, with cyber activities playing a central role. Both states possess increasingly advanced capabilities to conduct large-scale, sophisticated cyber operations, which are difficult to counter and result in financial damage and massive data breaches.

Although Russia and China share the strategic goal of weakening liberal-democratic systems and reducing the resilience of Germany and the EU, their operational approaches differ. Russia, facing extensive sanctions since 2022, has maintained high levels of activity, focusing on traditional intelligence targets such as foreign policy, security policy, EU affairs, and NATO. It seeks influence in EU energy policy and German domestic politics, targeting elections, political parties, and decision-makers to identify actors who may serve Russian interests.

Operationally, Russia has been challenged by the closure of its legal residencies. Russia has responded by intensifying intelligence gathering through contacts and open sources. It has also deployed "low-level agents" — individuals without formal intelligence training — for one-off sabotage and espionage missions. Alarmingly, Russia appears willing to use direct violence against individuals if it believes this will help it to achieve strategic goals.

China's objectives in Germany, particularly in political intelligence and influence, are similar to Russia's but pursued with greater subtlety and long-term strategy. This makes Chinese operations harder to detect. China has long been active in scientific and technical espionage, exploiting the openness of global academic networks. German authorities, like those in Finland, have begun educating e.g. researchers about related security risks. China also appears more adept than Russia at integrating human intelligence (HUMINT) with technical and open-source intelligence.

A common feature of both Russia's and China's intelligence operations is their centralised control from Moscow or Beijing, respectively. Intelligence priorities are set at high political levels, an observation being rather typical for foreign intelligence from historical perspective. For counter-intelligence, this requires activities and competences moving away from a simple identification of individual spies toward an improved understanding of broader strategic intentions. This is especially important given Europe's uncertain security environment and the unpredictability of U.S. intelligence sharing. Should the U.S. reduce its cooperation, German (and European) security assessments could face serious blind spots.

Recently, German authorities have warned about the potential misuse of democratic mechanisms by authoritarian forces. There are concerns that foreign powers may exploit parliamentary processes to gain access to classified information for strategic purposes, possibly with "useful idiots" or actively collaborating MPs. This highlights the "dual-use" risks inherent in liberal-democratic structures as well. Awareness of such systemic vulnerabilities is essential to defending liberal democracy. Undermining democracy through its own mechanisms is not just Germany's problem—it affects all European liberal democracies. The more these risks are recognised, the less room there is for abuse.

Kimmo Elo
Dr., Adjunct Professor, Senior Lecturer
Department of Geographical and Historical Studies
University of Eastern Finland
Finland

kimmo.elo@uef.fi

Currently, Dr. Elo is the leader of a subproject in the RESLIDE Consortium (2024-2027, https://reslide.fi/en/).

ALEXANDER CLAVER

The Devil's Advocate within Dutch military intelligence

Expert article • 3964

The Devil's Advocate (DA) in Dutch military intelligence serves as an institutionalized form of critical reflection and quality control. The concept was introduced within the Defence Intelligence and Security Service (NLD DISS) in 2008 to enhance analytical rigor and counter groupthink by critically evaluating analytic products and providing contrarian perspectives. It has operated independently, reporting directly to the Director, while being closely connected to operational and analytical departments. Over time, its role has expanded from reviewing intelligence products to assessing organizational processes and analytical methodologies across the intelligence cycle.

The concept of a "devil's advocate" has its origins in the Catholic Church with the Advocatus Diaboli critically examining the presented evidence in canonization cases. This tradition of structured dissent served to prevent bias and ensure balanced judgment. Within Dutch military intelligence, the DA and his team fulfill a similar purpose by challenging assumptions, testing reasoning, and exposing weaknesses in analysis. When applied with care to avoid "contrarian fatigue", or outright resistance its strength lies in encouraging alternative perspectives and reducing cognitive errors.

Academic research has convincingly shown that so-called authentic dissent – i.e. genuine critique, based upon thorough investigation rather than staged - stimulates creativity and better decision-making. The DA's goal is not to prove an assessment wrong, but to test its logic and consistency. The DA helps balance the risks of false positives (seeing links that do not exist), and false negatives (missing weak, but real signals) by ensuring analytical conclusions are robust.

From its inception in 2008, the DA and his team - small, autonomous, with full information access - reviewed finished intelligence products emphasizing transparency and learning over punishment: DA-reports are discussed with analysts to strengthen analytical reasoning. Initially, the DA conducted dozens of reviews annually, often applying other methods like scenario exercises, contrarian analyses and the introduction of competing hypotheses. These efforts aimed to instill a culture of reflective professionalism and thereby reduce groupthink and enhance the quality of intelligence analysis.

After this initial phase the DA's scope widened. It began assessing the organisation's overall self-reliance - to what extent its intelligence products relied on information provided by foreign allies - the effectiveness of analytical methods that were used, and organizational processes. The office also contributed to internal training programs and helped establish an academic intelligence curriculum at the Netherlands Defence Academy. From 2012, as NLD DISS faced budget constraints, the DA was tasked to design a system that linked (budgetary) resources to intelligence requirements. A "quantification matrix" and customer feedback cycle allowed its leadership to align input (and its quality and usefulness), throughput and output - closing the loop between what was needed, produced, and delivered. This also helped decision-making on prioritization issues.

As the DA expanded its scope into organizational assessment, tensions arose. Some departments viewed its findings as management oversight rather than a peer review mechanism. Despite this, consistent support from senior leadership guarded its existence and effectiveness. By the mid-2010s, the DA had evolved into a recognized means of quality assurance within NLD DISS. Its main challenge now became keeping access to data (systems) and maintaining its relevance in an era of increasing data complexity.

Intelligence processes today depend heavily on the automated processing of huge data streams. Traditional DA reviews - focused on written assessments - are insufficient for evaluating ICT-systems and algorithmic tooling that analyze vast datasets. The "black box" nature of AI introduces new risks of bias, false correlations, and misplaced confidence in machine outputs. Therefore, besides reviewing intelligence products and processes, the DA started to scrutinize data inputs, data models and algorithms.

Team composition and leadership play a central role in maintaining DA-quality. Cognitive and disciplinary diversity is valued for strengthening critical review and avoiding analytical tunnel vision. Leadership is facilitative rather than directive. Team members are expected to work autonomously while maintaining collective accountability – a balance that allows for creativity.

Communication is a crucial part of the DA's effectiveness. The team's work continues after the completion of an investigation: presenting findings, engaging with analysts, and ensuring that conclusions are understood and used are essential steps. Dialogue with analysts increases transparency and helps prevent resistance to critique. Formal briefings, 'roadshows', and personal discussions complement written reports. Keeping a "paper trail" supports institutional learning and accountability while also demonstrating that challenges are evidence-based and professional. Successful engagement depends on credibility, openness, and the ability to balance independence with collaboration. Transparency about methodology and criteria strengthens legitimacy and reduces defensiveness among colleagues.

Since 2008 DA concept has evolved from reviewing human judgment to overseeing hybrid analytical ecosystems where human reasoning and machine algorithms interact. The current and future DA will question what intelligence says as well as how it was produced. In a world dominated by automation and information overload its critical role - as a guardian of analytical integrity - remains vital.

The Dutch DA's development illustrates how institutionalized dissent enhances the credibility and resilience of intelligence work. By systematically questioning assumptions, it helps prevent analytical complacency and strengthens decision-makers' confidence in intelligence outputs. However, its long-term value depends on adaptability, e.g. by acquiring technical literacy to review complex, data-driven systems. This poses significant new challenges for the DA.

The Dutch experience demonstrates that dissent, when institutionalized constructively, is a sign of strength rather than disunity. By combining professionalism, transparency and independence, the Devil's Advocate system has become an enduring mechanism for learning, adaptation, and trust within Dutch military intelligence.

Alexander Claver
Dr., Devil's Advocate
Defence Intelligence and Security Service
(NLD DISS)
The Netherlands

DIETER BACHER

Austria's legacy as a Cold War intelligence hotspot

Expert article • 3965

It sounded like a classical Cold War spy story: In 2020, an Austrian businessman, Jan Marsalek, escaped to Russia in course of a fraud scandal at the German company "Wirecard". He had obviously also worked for Russian foreign intelligence: He was suspected that he had used members of the Austrian federal office for the protection of the constitution and counterterrorism (BVT) to obtain classified information on Russian dissidents in the West and on high-ranking employees of the Austrian Ministry of the Interior (BMI). More connections of the network, like a group of Bulgarian nationals in Great Britain, became known in 2024 and 2025, with the investigation still ongoing and Marsalek on the run, allegedly living in Moscow.

For an intelligence historian with knowledge on Austria, this case ideed seemed like a relic from the Cold War. In 1968, a similar case had occurred: Johann Ableitinger, a former member of the "Staatspolizei" (State Police), the forerunner organization of the BVT, had used his contacts to former colleagues to obtain Stapo information for Czechoslovakian intelligence. Several uncovered activities caused the first Parliamentary Commission on Espionage in Austria in 1969.

Both cases appear to be quite similar. They give the image of Austria as an operational field for intelligence operations, they used a similar HUMINT approach, and both informants obviously collected information on not "Austrian" targets, but topics related to other countries, with Austria just being the "place of access".

Austria had already become an "intelligence hotspot" in Ableitinger's time. With its geographical position in central Europe, intelligence stations in Austria were and are able to reach out to many other states. A factor especially relevant for signals intelligence (SIGINT), resulting in Austrian capacities of the "Goldhaube" system or suspected Russian capacities in the 22nd district of Vienna. As Austria's northeastern borders were part of the "Iron Curtain" and thus close to communist Czechoslovakia and Hungary. Secondly, Austria was and is host to several international organizations, like the UN International Atomic Energy Organization (IAEO) or the main office of the Organization of Collaboration and Security in Europe (OSCE) in Vienna – organization of high diplomatic interest and therefore interesting for intelligence gathering. And thirdly, there were nearly perfect starting conditions at the beginning of the East-West-conflict: As Austria was occupied by the four powers USA, Great Britain, France and the Soviet Union until 1955, their services had years to establish their stations here. During this time, intelligence structures were built that would shape intelligence activity until 1991 and beyond.

These conditions were recognized early. In late 1950, a member of British MI5, Sir Philip Vickery, spoke on "Austria being virtually the only highway from the West into the Satellite countries provides a unique opportunity for the collection of intelligence". A Soviet colleague of him, former GRU officer Vitaliy Nikol'skiy who was stationed in Baden near Vienna during the early 1950s stated in his memoirs that Austria provided "broad possibilities to conduct espionage from Austria not only in Europe, but also across the ocean" at that time. Austria got its image of a "intelligence hotspot" for a reason, even in professional circles.

Did Austria keep this strategic and operational importance until today? There are more recent, contradicting developments. Since 1991, the political landscape around Austria has changed considerably: Communist regimes had ended, and both EU and NATO have expanded to the East. Austria does not inherit its border position "between the blocs" anymore, the supposed "hotspots", especially since 2022, went to Warsaw, Budapest and the Baltics. To a certain point, Austria also lost its significance as a forum for diplomatic exchange. Thirdly, due to EU sanctions against the Russian economy, many economic ties Austrian companies had developed towards Russia since 1991 were also cut or at least heavily reduced. Developments that downsized both intelligence interest and access in the country.

But as the mentioned Marsalek case shows, a certain "legacy" seems to have remained. Austria is still a neutral country, but part of EU structures, host to international organizations, a waypoint and even new home to dissident groups interesting to Russian services and a place of continuing SIGINT possibilities. Austria has preserved some of its importance for foreign intelligence activities, but still under the premises to be a "collection point" rather that the target itself, with both "classical" and new approaches. Also for intelligence, a figure of speech seems quite accurate: The past is present in the present. And when it comes to intelligence history, Austria as a example can also help to understand both sides of the coin.

Dieter Bacher
Assistant and Researcher
Institute of History
University of Graz
Graz
Austria

Ludwig Boltzmann Institute for Research on Consequences of War
Graz
Austria

dieter.bacher@bik.ac.at

DAVID STRACHAN-MORRIS

The argument for an Irish Intelligence Service

Expert article • 3966

The Republic of Ireland is in a unique and very difficult security position in terms of both geography and politics. It sits on the western flank of Europe, exposed to the Atlantic, and with the main communications between Europe and continental America concentrated in its territorial waters off its southwest coast. Politically, it plays an important role in international security, with regular membership of the UN Security Council, and is at the heart of Europe through membership of the EU. Its geographic and political position have made it a regular target for probing and incursions in the physical and digital worlds but, in common with many small states, Ireland lacks the level of 'hard power' necessary for its defence. Other European small states have done what they can individually to provide for their own defence while also joining collective defence institutions. Ireland, however, is constrained by its constitution, its neutrality and the Triple Lock mechanism, all of which limit the extent to which it can build up its armed forces and fully engage in collective defence. This paper argues that if Ireland were to develop an effective national intelligence infrastructure to provide strategic forewarning of potential threats, this would considerably enhance its security by enabling more informed decisions and supporting a policy of pragmatic dynamic neutrality.

Ireland is not completely without an intelligence capability. The Irish Defences Forces and An Garda Síochána provide military and security intelligence about potential threats to the State, and its overseas interests. But useful as this is, it is insufficient for Ireland's needs. The existing intelligence services provide current and warning intelligence but are limited in their ability to provide strategic intelligence or the kind of in-depth national intelligence estimates required for decision-making on international issues. Expanding the remit of these organisations to include that task would be a mistake; it would put an undue strain on their resources and distract them from their core missions. A separate national intelligence agency, in whatever form, with a clear chain of responsibility to government (under a designated Minister), and with oversight and accountability built in from the start, will ensure that decision-makers receive the strategic and estimative intelligence they need.

An important first step towards establishing a national intelligence agency in Ireland would be to allay fears that, shrouded in secrecy, it will engage in activities that are not commensurate with Ireland's values of neutrality and respect for international rules-based order. But, by making legitimacy and trust the cornerstones of intelligence, Ireland can go a long way towards building an effective intelligence service within its established principles. Engaging with academic thought and research on these issues can provide some practical ways forward, especially if we look beyond the usual examples of the UK and the USA.

For example, since its creation, the UN has resisted a formal intelligence function and, in fact, the word 'intelligence' was even banned. The steady increase in attacks against UN missions and peacekeepers led the UN to change this position and establish an intelligence capability. Following extensive consultations with member states, intelligence leaders, academics and other stakeholders, the UN overcame objections to the creation of this function by being very explicit about its purpose and method of operation, putting clear boundaries on the activities it would undertake and providing for oversight and accountability. While it is unlikely that Ireland will limit intelligence activity to the same extent as the UN, there is a model here for establishing intelligence as a legitimate function of the state and a national intelligence agency as the legitimate organ of state to conduct that function.

In terms of trust in institutions, Ireland ranks alongside nations such as Denmark and the Netherlands, and much higher than the UK, with the 2023 OECD Survey on Drivers of Trust in Institutions showing very high public trust in the police, the courts, and the civil service. The Netherlands, Norway, Denmark, Sweden, and Finland, all of which are also considered high trust societies, have developed and enhanced their intelligence agencies without suffering a loss in public trust and there is a growing body of work from those states that Ireland can draw on and from which it can take important lessons. None of these countries is perfect and all have had their intelligence scandals, but they provide useful lessons to learn from and frameworks for thinking about how intelligence fits into the relationship between state and society, and how intelligence agencies in these societies interact with the rest of the international system.

Good intelligence is essential for strategic warning and effective decisionmaking. By being clear from the outset about the role, activities and purpose of intelligence, and learning from societies and organisations with similar values, Ireland can – and should – establish an effective intelligence service that will enable it to navigate the complex contemporary security landscape.

David Strachan-Morris
Dr., Lecturer in Intelligence and Security
School of History, Politics and International Relations
University of Leicester
United Kingdom

SIR DAVID OMAND

The enduring value of secret intelligence

Expert article • 3967

Human intelligence has always had survival value, to reduce ignorance of what might be over the hill, assessing whether the rustle in the trees ahead is most likely the hunters' lunch or whether they will end up being a predator's lunch. Also of proven value is secret intelligence – information that people who may mean harm do not want to be known, both concerning their hostile intentions and their capabilities to cause damage. Such information has to be stolen, against the wishes of the holder, preferably without their knowing that their secrets have been exposed. Obtaining such secrets is the timeless business of intelligence officers, now as an organised activity of the state under the law, exploiting all the marvels of modern digital technology as well as the traditional tradecraft of the spy.

Equipped with such intelligence, the State can better fulfil its traditional and fundamental duty of protecting its citizens and helping protect those of friendly nations. It can help map out diplomatic routes to resolve or moderate disputes (such as the role played by satellite observation in Cold War nuclear arms control), expose hostile intentions (as the US and UK intelligence communities did before the Russian attempt to overthrow the government in Kyiv in 2022), and guide sound investment in defence and security on the basis of knowledge of adversary capabilities (as the United Kingdom has just done in its 2025 Security and Defence Review).

The same anticipatory logic applies to other threats, including terrorism, weapons proliferation and serious and organised international criminality including narcotics and illegal migration. It also applies to the new vectors of cyber threat that are emerging in the digital world we now depend upon for everyday life and economic activity. Every aspect of the world is now described in numbers, including text, images, video, speech, sensor data and geo-location, DNA and health data, financial transactions and our Internet use, and data from our cities, our homes and our wearables. These key strings of numbers can be easily stored, retrieved, searched, manipulated and denied to us. A key characteristic of modern inter-State sub-threshold warfare is that it takes place in this digitised world, such as we see in the wave after wave of cyberattacks that Russia has unleashed on Ukraine. And from the discovery of Chinese State penetration of US critical national infrastructure with the planting of 'trojan horse' malware intended to provide the capability to disrupts in the event of a China/US crisis.

To use secret intelligence for defence against such threats a number of stages have to be passed successfully. There have to be sufficient data points that can be collected in the first place to form the necessary situational awareness of what is being faced. There have to be sufficiently sensitive sources and methods able to access and report both secret and open information. And to detect when an adversary is trying to use deception and fake information to mislead. The intelligence analysts need to be able to explain adequately what is going on, for example whether the massing of forces by an adversary is for intimidation or is a prelude to attack. With good situational awareness and a sound explanation of what is being seen then the analysts can move on to provide estimates of how events may unfold in the coming weeks or months The resulting intelligence estimate has then to be conveyed honestly to the policy makers and Ministers in terms they can understand, with any warnings sufficiently forceful to get senior attention. And, finally, the government must want and be able to act on the warning in sufficient time.

One stage where experience shows this process is most likely to go wrong is the failure of the analytic process to explain correctly the information being gathered. For example, the indications that Israeli military intelligence is said to have picked up before the devastating Hamas attack of 7 October 2023, including a plan for such an attack and training and reconnaissance, appear to have been explained away by senior intelligence officers since they assessed Hamas as having neither the capabilities not the intent to conduct a major attack on Israel. That fateful misreading of the intelligence was probably influenced by a second likely cause of failure, when powerful policy makers overestimate the success of their policies, for example that Hamas could not pose that kind of threat since Israeli Cabinet policy towards Hamas governing in Gaza was designed to eliminate that risk. Just because the likelihood of an event is assessed as low does not mean it cannot happen, as the world has so often discovered. Contingency planners must work on the basis of the reasonable worse case not always the most likely estimate. Which is why I have always argued for secret intelligence assessment to be complemented by horizon scanning for serious longer-term developments to provide strategic notice of what might come to challenge us, and the comfortable assumptions we can too easily make.

Sir David Omand
Visiting Professor
War Studies Department
King's College London
United Kingdom

david.omand@kcl.ac.uk

Sir David Omand is Visiting Professor in the War Studies Department, King's College London after a career in UK defence, intelligence and security including Director of GCHQ and UK Security and Intelligence Coordinator.

JOONAS SIPILÄ

Intelligence producer–consumer relationship

Expert article • 3968

The relationship between the intelligence producer and the intelligence consumer forms the cornerstone of an effective intelligence system. Intelligence, in its broadest sense, is not merely the collection of source material, be it data or information, but the transformation of that information into insights that inform and support decision-making. This process hinges on a dynamic partnership between those who produce intelligence – the intelligence organisations – and those who consume it, such as policymakers, military commanders, or corporate executives. The nature of this relationship directly influences the relevance and impact of intelligence on decision-making and, in the end, strategic and operational outcomes.

For the intelligence to achieve its function, the intelligence produced must reach the consumer, it must be delivered and accepted. Delivery refers to the implicit part of the process where intelligence has to be received by the appropriate persons in order for it to inform (e.g. warn) the decision-makers. Intelligence may not reach decision-makers for a multitude of reasons ranging from organisational culture not conducive to relaying unwelcome information, messages being misdirected or screened out by staff prioritising them incorrectly, to agenda overload or unclear formulation that obfuscates the central message.

The consumers must also accept the intelligence provided as truthful. Timely and actionable analysis is difficult to produce and even correct process does not mean much if the results are deemed irrelevant by the end-user. The consumers of intelligence as customers are in the position to deny the validity of results or completely ignore them. Warning or other information produced by intelligence services does not exist if the customer does not receive or accept it.

For the message to be accepted, it is crucial that the decision-makers share the same fundamental understanding of the politico-strategic environment. In addition, the decision-makers have to, in general, trust the intelligence community and the analyses that it provides and be receptive to the information provided. If there is a lack of trust in the correctness of analyses in general or suspicions of partisan interests, it will be significantly harder for the message to be accepted.

From a decision-maker's point of view, intelligence organisations are only one of the providers of information. The intelligence received must be actionable and timely, but above all useful from the point of view of the decision-maker. Needless to say, each decision-maker, organisation and analyst has a differing view on what actually is relevant and thus desirable. There does not exist a yardstick that would objectively measure what is relevant and what is not. A perception of an intelligence producer that the customer does not pay attention to or does not want to receive the intelligence, even though deemed important by the producer, might simply indicate that the intelligence producer has misperceived the need of information.

At its core, the producer-consumer relationship is defined by communication and mutual understanding. Producers should understand the consumers' priorities, objectives, and operational context in order to provide intelligence that is not only accurate but also relevant and actionable. Conversely, consumers should be able to articulate their requirements clearly, providing feedback and guidance to shape collection priorities and analytic efforts. When this dialogue is strong and the producer and consumer have a shared understanding of the world, intelligence becomes a highly useful tool – constructively supporting timely decisions and reducing uncertainty. When the relationship is weak, misunderstood or, in extremis, antagonist, intelligence risks becoming irrelevant, or even misused and harmful.

Trust is a central element in this relationship. Consumers must have confidence that the intelligence they receive is as objective and free from bias or political influence as possible, while producers must trust that their assessments will not only be used, but used responsibly and not distorted to fit preconceived agendas. This balance requires integrity, transparency, and professionalism on both sides. In a sense, the value of intelligence is in direct relation to the way it is used; its importance is born out of the interaction between the producer and consumer. This underlines the need for facilitation and dedicated intermediaries that help to bridge the gap between the producer of intelligence and its consumer.

Joonas Sipilä
PhD, Research Director
Defence Command Finland
Helsinki
Finland

SASKIA POTHOVEN

Intelligence producer–consumer relationship

Expert article • 3969

Defence intelligence has (rightfully so) been characterised in the past as the "neglected handmaiden" but is arguably gaining importance in recent years due to increasingly complex and wicked international problems. The threat of war in Europe since the Russian invasion of Ukraine in particular necessitates a closer working relationship between different national defence intelligence actors. When looking at the Netherlands, we can see that the Dutch defence and military intelligence network is in transition, as the Ministry of Defence is increasingly shifting its focus from wars of choice to wars of necessity. Whereas for the past 25 years, the intelligence authority was centralized at the Dutch Defence Intelligence and Security Service (MIVD or DISS), the operational commands of the armed forces are now rebuilding their military intelligence capacities for both peace and wartime, including the expansion of analysis and fusion capacity and the acquisition of ISR (intelligence, surveillance, reconnaissance) assets such as the MQ9 reaper drone. As a result, the intelligence sections of the operational commands are turning into intelligence producers themselves, whereas in the recent past they almost exclusively consumed intelligence disseminated by DISS or international partners.

These developments necessitate a reconceptualization of the traditional dichotomy of intelligence producers and consumers. The debate on the relationship between intelligence producers and consumers has been going on for more than half a century, with two predominant schools of thought - based on a predominantly Anglo-Saxon and civilian context - that continue to lead the discussion. The traditionalists, following Sherman Kent, prefer distance in the relationship between intelligence producers and their clients, whereas the activist approach following Willmoore Kendall and Robert Gates advocates for close interaction instead. Although they differ in their views on how intelligence producers and consumers should relate to one another, both schools generally portray the relationship between intelligence producers and consumers as hierarchical and dichotomous, with mutually exclusive roles and norms. As a result, the roles of intelligence producer and consumer are often considered as strictly separated both in academic literature as well as in practice. In the Dutch defence intelligence network, this view has translated in the often-heard statement "we provide the weather forecast, but we do not tell if they should bring an umbrella". In other words: it is the task of an intelligence analyst to tell the 'objective' truth, but they should refrain from any advice on what to do with the information.

Practice however shows us that the relationship between different (defence) intelligence entities is often much more layered and networked than this dichotomous portrayal would suggest, creating the need for a "team of teams"like approach to national defence intelligence cooperation. Defence intelligence agencies often have an interdependent relationship with the intelligence branches of the armed forces: depending on the level and type of product, they can be producer and consumer at the same time. An armed forces intelligence branch might for example receive a strategic intelligence product from a defence intelligence agency and use this as input for its own intelligence product intended for the operational and tactical level. The other way around can also be the case, as defence intelligence agencies become intelligence consumers when they use (raw) intelligence collected by ISR assets of the operational branches of the armed forces.

We should therefore consider Dutch defence intelligence – and potentially other national intelligence networks as well – as a network of intelligence "prosumers": intelligence entities that both produce and consume intelligence while working towards a common goal. By going beyond the traditional dichotomy, the notion of intelligence prosumerism can help us gain more insight and understanding in the complex and multifaceted nature of (defence) intelligence relationships. Furthermore, as current regulations concerning intelligence services and the armed forces often limit the information gathering possibilities of the armed forces especially when they are not formally employed, cooperation between the service and the armed forces is often complicated by legal restraints. Recognizing that national defence intelligence cooperation is often more multilayered than the traditional producer-consumer framework suggests can therefore also lead to legal and policy frameworks that are better connected to the realities of day-to-day practice and create a closer working relationship between different national defence intelligence actors.

Saskia Pothoven
PhD, Researcher
Netherlands Defence Academy and Leiden University Institute of Security and Global Affairs The Netherlands

JYRKI ISOKANGAS

The paradigm shift of intelligence and the challenge of buzzwords

Expert article • 3970

Intelligence does not have an unambiguous definition. According to Sherman Kent (1949), intelligence consists of knowledge, the organization that produces knowledge, and the activities of this organization. In the Finnish Ministry of Defence report from 2015 "Guidelines for Finnish Intelligence Legislation", the task of intelligence was defined as information collection aimed for increased understanding of changes, threats, and opportunities. With intelligence analysis, intelligence organizations produce early-stage information that enables proactive measures and preparedness. The definition emphasizes two aspects: intelligence must predict future developments, and these predictions must be actionable enough for mitigating threats and utilizing opportunities.

The task of strategic intelligence is relatively clear, but we are on the threshold of a paradigm shift—or perhaps have already crossed it. The main reason for the change is the digitalization of societies, which has led to an exponential growth of information, faster information dissemination and routinely used artificial intelligence. As a result, national intelligence services do not have exclusive rights to strategic intelligence. Digitalization enables intelligence as a business, as well as the collection and analysis of information as a leisure activity. Although some key intelligence systems are still exclusively used by intelligence services, practically anyone can collect or purchase information from open sources and analyze it, with the help of artificial intelligence, if necessary. Even national intelligence services engage in such activities. As a result, digitalization has brought new, more visible actors to the field of intelligence. Intelligence services have been encouraged to open their activities. The availability of open-source information has supported this increased transparency.

Digitalization has created new intelligence actors, but the more significant change has taken place in the operational environment. Beyond the traditional domains of land, sea, air, and space, nowadays cyber, information and cognitive domains have emerged as new types of environments. These emerging domains enable the use of novel and adaptable tools for influencing societies. Therefore, current buzzwords include e.g. *hybrid influence*, *information warfare*, and *cognitive security*. The key development is that warfare, or just hostile influence are no longer dichotomy; between war and peace exist several different levels. After Russia's annexation of Crimea in 2014, we have not been in a state of peace, but neither are we at war—at least not from the perspective of the traditional definition of war. However, our societies are constantly subjected to hostile actions, especially in these new domains.

The main task of intelligence is to anticipate future developments and support decision-making regarding appropriate own actions. In the traditional domains of land, sea and air, development of a threat usually requires time and different types of force preparations. Ideally, strategic intelligence can identify these preparations, have ample time to monitor the development and ultimately provide an early warning for decision-makers when the threat reaches a certain level. Assessing future developments and providing early warnings are no easy tasks, but capable intelligence has prerequisites for success. The time a threat takes to develop also provides an opportunity to manage or even prevent undesired development through one´s own actions. Intelligence has a substantial role in supporting proactive decision-making and operations.

However, in cyber and information domains, we have largely accepted a position where we do not anticipate but merely react to the threats. Clearly, these domains are significantly more challenging than the traditional ones. Situational awareness or predictive intelligence analysis cannot be executed solely by intelligence services. Private enterprises and the third sector have a key role. However, instead of trying to fix the problem, we have elevated resilience as an additional buzzword. When discussing hybrid threats, politicians regularly repeat the phrase "we must be prepared for everything," even though a simple thought experiment makes it clear that it is not possible to prepare for everything, even if we had unlimited resources. Resilience is an important part of any kind of defense, but it cannot be the first line of defense. It is the last lock when everything else has failed.

The problem is significant. Currently, we are unable to establish a comprehensive situational awareness in the cyber domain, even less so in the information or cognitive domains. Therefore, we do not have the strategic intelligence capability to predict hostile cyber, or information operations directed at us, nor the ability to support own proactive decision-making regarding countermeasures. This stems in part from the absence of mandated authorities and their capabilities, the heterogeneity of actors, and the tendency to interpret these emerging domains as separate entities, shaped by the currently popular buzzwords. The cyber and information domains should be considered as a whole, and preferably together with the traditional domains. An emerging threat in a domain may be detected for the first time in another domain. Russia's large-scale attack on Ukraine in 2022 was observable in the information and cyber domains long before Russia began military deployment to the Ukrainian border.

Intelligence should be collected and analyzed from all domains. Ideally, situational awareness and predictive strategic intelligence analysis are carried out in cooperation with various actors. The key buzzword at the time of writing might be *multidomain operations*. Until another buzzword surpasses it – hopefully it is *multidomain strategic intelligence*.

Jyrki Isokangas
Colonel (ret.), M.Sc. (cybersecurity),
University Teacher
University of Jyväskylä
Finland

jyrki.t.isokangas@jyu.fi

Photograph by Petteri Kivimäki.

JAMES J. WIRTZ

The key to intelligence success

Expert article • 3971

Much has been written about intelligence failure, so much, in fact, that scholars are criticized for selecting on the dependent variable. That is, the intelligence studies literature generally explains the causes of failure, while ignoring what leads to success. This creates methodological issues that can hide what separates failure from success when it comes to avoiding strategic surprise attacks or other unwanted faits accompli.

Intelligence failure is rooted in the process of producing warning and analysis for officers and officials, which is commonly referred to by the term "intelligence cycle". Much can go wrong in this process. Intelligence collection requirements might be mis-specified, the raw data collected might be planted as a deliberate deception, or relevant data might never be collected. Data also could remain hidden or unrecognized until too late, buried in the information tsunami created by the digital revolution. In terms of analysis, a Pandora's Box of cognitive biases, organizational pathologies, and personal motives can sidetrack timely and accurate estimates, especially if the intelligence-policy consensus of the moment cannot account for emergent threats. Because stratagem and the gambits it enables are incredibly risky, they are often viewed by analysts as too "hare-brained" to be taken seriously, even when accurate evidence of some looming event is detected. It is also difficult to convince skeptical leaders that the opponent is undertaking a potentially self-destructive diplomatic or military initiative.

Despite the array of problems that bedevil analysis, scholars generally agree that accurate information, useful assessments, or even timely finished intelligence and formal warnings exist within the "intelligence pipeline" before instances of surprise and intelligence failure. For instance, the Director of U.S. Central Intelligence noted that before the 11 September 2001 terror attacks, the "system was blinking red": analysts and law enforcement knew that Al-Qaeda cells were active in the United States and that some sort of operation was imminent. Nevertheless, they failed to translate this foreboding into timely action; they failed to bridge the chasm between intelligence analysis and effective policy response.

Bridging this gap between analysis and response is the critical factor that separates failure from success; intelligence analysts and managers must take responsibility before the moment of crisis to build a bridge to those who must act on warning. National intelligence communities must undertake four actions to bridge this chasm between warning and response.

First, intelligence assessments must fit strategic requirements. Strategies that require warning weeks or months before untoward events are doomed to failure if intelligence analysts can only provide a few days or hours of warning. Although this intelligence-operational synchronization should be the responsibility of intelligence professionals, strategists occasionally should consider if their expectations about warning are getting ahead of intelligence realities. Strategy must be synchronized with intelligence.

Second, intelligence professionals and officials need to agree on who receives warning, who will recognize the warning for what it is, and who will take appropriate action. Too often, officials and officers are unaware that they need to act in response to warning. Before the Japanese attack on Pearl Harbor, for instance, assessments were disseminated to officials in Washington and Oahu, but everyone seemed to think that someone else recognized and understood the big picture and would respond appropriately. Disaster looms when intelligence producers and consumers simply assume that "someone else will take this for action."

Third, the bridge between analysis and response is built on trust. Intelligence managers build trust with officials by explaining the strengths and limits of intelligence, while intelligence consumers build trust by discussing strategic objectives and requirements to build a common operating picture with analysts. Effective collaboration occurs when everyone is aware that everyone understands the threat and what is needed to defeat it.

Fourth, intelligence consumers must understand that specific event prediction is rare. Instead, they are likely to receive indications & warning intelligence, which is a general assessment indicating a movement from a routine day-alert peacetime posture, when the ability to undertake operations is limited, to a generated-alert posture, a time when the ability to undertake operations is increasing. Officials sometimes prefer to wait to see what materializes under these circumstances. Nevertheless, by the time things become cut and dried, it is generally too late to take effective action.

Bridging the gap between intelligence producers and consumers, between warning and response, is the key to intelligence success.

James J. Wirtz
Professor of National Security Affairs
Naval Postgraduate School
Monterey, California
USA

jwirtz@nps.edu

KURT F. JENSEN

Foreign intelligence: One perspective

Expert article • 3972

Foreign Intelligence collection is performed in different ways, depending on resources, national requirements, and levels of risk acceptance. Non-clandestine information collection using human sources or intelligence collectors gathering open information are options with minimal risks and costs. Much information can be secured relatively openly. Such information, while correct and valuable, is not always supported by documentary evidence. Its strength is that it often reflects interpretations and observations.

The prime goal of foreign intelligence is understanding of the international environment, together with warnings and contextual interpretations of evolving events. Warnings are not predictions but highlight emerging trends, attitudes, changes, and new issues. Such information, when merged with all-source material, becomes intelligence. Intelligence analysis, separate from collection, should exist in close and active proximity to collection operators and work closely with the foreign ministry, since diplomatic information-gathering is an important facet of intelligence collection. Analysts with depth of knowledge, understanding of, and experience with a subject can prepare valuable assessments, even when some details are not available.

Intelligence assessments are a valuable tool for decision-making, explaining situations, clarifying emerging issues, and putting context to information while interpreting the material through the cultural, historical, ideological/religious perspectives of the actors on the other side. Analytical organizations where rotationality is a constant factor diminish the understanding and interpretation acquired from lengthy and intimate knowledge of a country, a leader, or a region.

Much information is accessible in published material which can be secured through various strategies. Social media is a treasure trove and can be managed through AI. Travellers, including tourists, businesspeople, technical experts, academics, journalists and others observe and hear things during visits abroad, and can be debriefed. Refugees from denied areas can be of significant intelligence value depending on their education/training or employment experience. Casual conversations with visa applicants can elicit valuable information. Trained debriefers can often elicit more information than a person is consciously aware of possessing. Coercion should never be an option in seeking information.

Intelligence gatherers are often posted as diplomats. However, intelligence gatherers go beyond conventional diplomats to focus more narrowly on individuals with possible knowledge of or access to subjects of national security interest. There are often persons with access to parts of the targeted information, but not within targeted institutions, and not aware that their knowledge is sensitive. Such persons may be frank in their discussions. An approach to such persons can be facilitated by demonstrating innocence or naivete, or simple seeking explanations of complex issues. Many questions should be asked in such approaches, most of which should be innocuous. Local security personnel may interrogate the contact. The contact must respond freely and frankly, to underscore the innocent nature of the meeting. With many questions asked by the diplomat, many on non-sensitive subjects, it is less likely that the source will recall anything more than queries from a diplomat with little knowledge of local events or circumstances.

There are additional strategies to securing information. Observation is one – walking through an industrial park, attending conferences, and checking out harbours is easy. Persons with access to information about denied areas can be approached at a social level. Travel to provincial areas of a nation can facilitate casual intercourse with persons less sensitive about secrecy, often when accompanied by a good meal.

Training in human behaviour and the reading of body language eases the diplomatic intelligence gatherer's task. An open 'diplomatic' inquiry approach may not necessarily gain access to a well-placed critical source but imposes few risks and can be very revealing. Understanding people and how truthful and comfortable they are, is critical to successful information gathering. Interpretation of non-verbal body language can guide the 'diplomat' to home in on valuable information or detect negative responses from interlocutors.

Intelligence organizations must understand their roles. They 'tell truth to power' providing contextual data which should be understood by policy makers. Intelligence organizations are only one source of information used by policy makers. Policy outcomes reflect many strains of input some of which may be rated more significant than the intelligence input.

Kurt F. Jensen
Dr.,Adjunct Professor
Carleton University
Canada

kurt.jensen4657@gmail.com

KIRA VRIST RØNN

Whole-of-society approach to foreign espionage

Expert article • 3973

Re-introducing the threat from foreign espionage

Foreign espionage from mainly Russian and Chinese actors constitutes one of the main threats facing many Western societies. Espionage is the act of covertly gathering information about a counterpart - information that is intended to be kept secret - with the aim of obtaining military, political, economic decision advantages on a given topic. This threat has re-gained relevance in recent years, with rising conflicts and geopolitical tensions most evidently in the wake of Russia's full-scale invasion of Ukraine in 2022.

Most Western (and especially the Nordic countries) are valuable targets for foreign espionage due to their geographic location, membership of NATO, military support to Ukraine and their technological developments.

Counterespionage has traditionally been a core task of governmental intelligence services with the aim of providing expert knowledge and support to decision-makers when forging security. Responding to recent developments in the threat landscape, intelligence observers have however begun to articulate a need for intelligence to become more inclusive and interactive. A central aspect of such an inclusivity is increased cooperation between central actors that usually do not cooperate.

Inviting civil society actors to cooperate in counterespionage aligns with current European Union strategies emphasizing *a whole-of-society* approach to security. *Civil society actors* are for example private companies, governmental authorities, and individual citizens. In such approaches, various actors across society are requested to work together to obtain common solutions to shared and often complex security issues.

In their attempt to safeguard our democratic societies, intelligence services have increasingly begun to reach out to civil society actors when identifying and counteracting security threats and in this sense, they apply a whole-of-society approach to counterespionage.

However, it remains unclear what a whole-of-society approach to counterespionage entails, how it is practiced, and what the societal implications of the approach would be.

What is a whole-of-society approach to counterespionage?

Generally, the whole-of-society approach entails the inclusion of a variety of stakeholders in order to tackle pressing threats with the aim of obtaining societal resilience, better situational awareness and more efficient responses.

In the Nordics, intelligence services have primarily reached out to civil society with the aim of establishing awareness on the side of the public via one-way communication in for example yearly risk assessments aimed at the public. This awareness-approach stands in contrast to the United States' (US) (and to some extend the British) post 9/11-approach. In these settings, governmental intelligence services often ask civil society to chip in and co-produce intelligence with information on suspicions activities - so far mainly related to the threat from terrorism in campaign such as "if you see something say something".

Engaging civil society in counterespionage is not an entirely novel practice. During the Cold War, Nordic intelligence services launched campaigns asking citizens to be aware of (mainly Russian) spies – see i.e., the Swedish campaign "The Swedish Tiger" or campaigns like "Keep your piece of the puzzle". After the recent reemergence of foreign espionage as a main threat, a range of new initiatives have been launched.

Recent examples include campaigns asking individual citizens to provide information about suspicious espionage-related activities for example in connection with larger events; engaging university employees and funding bodies in safeguarding against foreign espionage within academia and recruiting civil society actors to help safeguard national interests via more or less formalised partnerships.

Balancing between appropriate pro-action and stereotyped suspicion

The **potentials** of this approach are most often understood as the assumed ability to build better situational awareness, safeguard societies against foreign espionage and build societal resilience. Since such whole-of-society campaigns are a rather new phenomenon in the Nordic context and more broadly in the EU, the increased inclusion of civil society actors also comes with risks. These are for example, the risk of "responsibilising" civil society actors by including them in security policies and turning them into security actors. This type of governing "*through* civil society" potentially renegotiates the relationship between state and its citizens. Security then risks turning into a duty, rather than a right, for citizens. Additionally, there is a risk of creating stereotyped countermeasures favouring exclusion and instilling a sense of suspicion across groups in society. The Danish Security and Intelligence Service was for example accused of promoting racist and discriminatory practices by a large group of university employees when launching their latest campaign concerning knowledge security and the risk of espionage at universities in Denmark ("Is your research at risk?").

These highly inclusive and co-producing approaches to civil society have an intuitive appeal since they aim to include and empower civil society actors and potentially establishes societal resilience via cooperation, inclusion and interaction between all stakeholders. However, they also come with risks which have not been conceptualized or critically assessed in the intelligence literature on counterespionage. In the wake of 9/11 security scholars addressed the increased focus on citizen-led intelligence collection and the risks following along such initiatives e.g., unwarranted and broad suspicion across society and vague risks factors.

Counteracting foreign espionage is an intersectoral endeavour and a cornerstone for reducing malicious, interconnected, antagonistic threats aimed at our societies. However whole-of-society approaches should be guided by cautions eye to the potential democratic and societal implications.

Kira Vrist Rønn
Associate Professor
Department of Political Science and Public Administration, Center for War Studies
University of Southern Denmark
Denmark

kroenn@sam.sdu.dk

MARTTI LEHTO

Intelligence and espionage in the cyber world

Expert article • 3974

Today, information is online and therefore subject to intelligence and espionage. National cyber intelligence involves government agencies and national security organizations collaborating to collect and analyze information from public and non-public sources on cyber threats, adversaries, and capabilities to protect a nation's critical infrastructure and interests. The aim of intelligence activities is to produce early-stage information for policymakers and military leaders that enables threats, risks and changes to be influenced and prepared for and hardening national defense systems.

Cyber espionage can be defined as activities that obtain secret information (sensitive, private or classified) from private individuals, competitors, groups, governments and opponents to achieve political, military or economic advantage using illegal methods on the Internet, networks, software or computers.

The distinction between cyber intelligence and cyber espionage is ambiguous, as the use of illegal methods has not been comprehensively and unambiguously defined. Cyber espionage, particularly when organized and carried out by nation states, is a growing security threat.

The most common targets of cyber espionage include large corporations, government agencies, academic institutions, think tanks or other organizations that possess valuable IP and technical data that can create a competitive advantage for another organization or government. Targeted campaigns can also be waged against individuals, such as prominent political leaders and government officials, business executives and even celebrities.

Common cyber espionage tactics

Most cyber espionage incidents are classified as advanced persistent threats (APTs). An APT refers to a sophisticated and sustained cyberattack wherein an intruder discreetly gains access to a network, with the objective of extracting sensitive information over an extended timeframe. Such attacks are meticulously orchestrated to target specific organizations and are designed to circumvent existing security protocols for prolonged periods.

Executing an APT attack necessitates a greater level of customization and sophistication compared to conventional cyberattacks. Such adversaries are often well-resourced and comprise highly skilled teams targeting organizations of substantial value.

Cyber espionage can target individuals

A cyber attacker uses vulnerabilities in a system to penetrate a target. A vulnerability can be any weakness that allows damage to occur or can be used to cause damage. Vulnerabilities can exist in systems' SW/HW, organizations processes, and human activity.

Most cyber espionage operations incorporate some element of social engineering to elicit action or obtain necessary information from the target to facilitate the attack. Phishing attacks are a common form of social engineering. In this type of attack, the attacker attempts to act as a trusted actor in order to obtain personal information. These techniques frequently exploit psychological factors such as excitement, curiosity, empathy, or fear to prompt rapid or unconsidered responses. As a result, individuals may be deceived into disclosing personal data, engaging with malicious links, or downloading malware.

Everyone working in a significant position and handling important information should appreciate that they may become a target of the intelligence operations of a foreign power. State-sponsored operators may also focus their cyber espionage campaigns on private individuals and public servants.

One consequence of Russia's military actions in Ukraine has been the increased emphasis on cyber espionage, particularly as conventional human intelligence activities have become more challenging for Russian operatives. Nevertheless, the value of human intelligence remains significant. As essential intelligence can now be collected more efficiently through information systems, the focus of human intelligence efforts can be directed with greater precision.

How to prevent cyber espionage?

Numerous cybersecurity and intelligence solutions are available to help organizations gain deeper insights into threat actors, their attack methodologies, and the tactics they routinely employ.

Implementing robust security measures is essential for protecting sensitive data and networks from cyber espionage. Key tactics include endpoint security, which involves proactively detecting and neutralizing threats before they escalate, as well as monitoring for unusual activity during an attack. It is important to regularly audit an organization's cyber-physical systems. By conducting vulnerability assessments and penetration testing on a consistent basis, organizations can identify and address security gaps.

Equally critical is employee training; regular training sessions are necessary to raise awareness about cyber threats such as phishing and social engineering. Ensuring that employees understand how these attacks work helps foster a culture of cybersecurity awareness. This empowers staff to recognize and report suspicious activities, acting as a frontline defense against potential breaches.

Martti Lehto
Research Director
Faculty of the Information Technology
University of Jyväskylä
Finland

martti.lehto@jyu.fi

KALLE SALMINEN

Intelligence at the edge

Expert article • 3975

Europe's security landscape has been fundamentally reshaped. Russia's war in Ukraine has forced nations to reassess how information is gathered, shared, and acted upon. In the Baltic and Nordic region, countries approach this differently, but the overall direction is the same: improving resilience through cooperation, practical innovation, and the ability to adapt quickly.

Traditional centralized systems were effective in slower, more predictable contexts, but they are too rigid for today's fast-moving crises. Modern operations require flexible, shorter decision cycles where relevant information reaches the right people at the right moment. Command structures remain essential, but the way decisions are supported is changing.

Across the Baltic Rim, new capabilities are emerging. Digital twins allow operators to test responses before crises occur, while extended-reality environments enable safe rehearsal of complex scenarios. Remote-operation systems reduce risk by allowing critical assets to be inspected or controlled from secure locations. Combined with secure communications and positioning, these tools help build a clearer shared picture.

Today's challenge is no longer access to information, but the sheer volume of it. No human can handle the volume, speed, and diversity of modern data flows without assistance. This is why distributed decision-support nodes, operational "brains" capable of fusing sensor data, legacy systems, and field inputs, have become essential. Human-in-the-loop AI strengthens judgment as a tool rather than replacing it. In many European organisations, legacy systems are still the backbone of daily operations, which makes reliable integration, not replacement, critical. Integrated digital environments, including metaverse-style operational spaces, help filter what matters and present information in a way that people can act on efficiently. Platforms such as ProVerse illustrate how data fusion, visualisation, simulation, and remote operations can be brought into one environment to support these decisions and provide a shared visual and spatial understanding that traditional systems cannot offer.

Equally important is secure cross-border interoperability. Nordic, Baltic, and Central European partners increasingly need systems that can grant temporary, role-based access to operational data, allow shared situational environments when necessary, and still safeguard national autonomy. This kind of permission-based cooperation makes it possible for systems to operate independently day to day yet connect within a common environment when the situation requires it.

These developments support a wider European objective: building technology-independent, interoperable systems that reinforce sovereignty and trust. The challenge now is to turn promising pilots into capabilities that last.

Edge intelligence is already becoming routine in exercises. Shared standards, regular training, and transparent evaluation help civil, and defence actors work together when a real crisis occurs. Preparedness brings clarity and calm, helping leaders and communities act with composed steadiness when it matters most.

That same trust must extend to the systems we build. Technological sovereignty and ethical responsibility remain essential. AI and automated systems should be transparent, auditable, and under human control. At the same time, Europe cannot allow long bureaucratic debates to slow the development of capabilities that are urgently needed. Innovation and responsibility must advance together by building systems that are safe, but also fast enough to keep pace with a changing world. Europe should not settle for following others but aim to set the direction and provide a genuine tactical advantage for its own region.

By 2030, the Baltic Rim could show how smaller nations can act together with purpose, supported by technologies that shorten the distance between sensing and response. With continued progress in cross-border digital infrastructure and AI-assisted decision support, the region can demonstrate a practical and democratic model for resilience.

Ultimately, intelligence at the edge builds on human judgment. It gives people the tools and information they need to make more informed, faster, and safer decisions. In the end, Europe's strength will rest on its ability to connect insight with action, responsibly, decisively, and together.

Kalle Salminen
Executive Chairman
ProVerse Interactive
Finland

KLAUS ILMONEN

Corporate statecraft – divided fealties

Expert article • 3976

Introduction: An evolving world order

A more volatile political environment has affected the relationship between states and corporations and their respective roles in comprehensive security. As modern societies increasingly rely on critical infrastructure provided by private corporations, states are viewing corporate policy from the perspective of strategic state interests, reflected in EU policies on strategic autonomy and economic security[1], for example. With their growing impact and international reach, corporations, on the other hand, have become less accountable to individual states and political actors in their own right. Corporations are integrating political considerations in managing corporate affairs while states are looking for means to align corporate enterprise to serve strategic state interests, leaving corporations to struggle with divided fealties and states with increasing security concerns in a fractured world order.

Corporations as political actors

Corporations have a central role in serving the complex demands of modern societies, including functions vital for strategic state interests from telecommunications to healthcare. Corporate enterprise increasingly includes social and political elements that affect society directly and that are beyond the scope of public authorities or formal political institutions. Importantly, corporations are accountable to their key stakeholders, and do not necessarily subscribe as citizens of any single state, nor do they always owe fealty to the interests of the state.

On the international level, reliance on institutional frameworks has decreased[2] with continued global power rivalry. Global governance has also become disaggregated with a broader variety among participating actors. Individual states are less able to shape the conditions for corporate enterprise and corporations are finding they must take responsibility for their security environment independently to protect their infrastructure, their intellectual property and their value chains.[3] Corporations have emerged as important political actors, both domestically and internationally, sometimes at par with states in matters related to corporate affairs.

The securitisation of the economy

Globalization and international economic integration have resulted in global value chains and economic interdependencies that have raised national security concerns. Access to foreign raw materials, technology and know-how can be restricted and "weaponized" for strategic purposes, for example. Economic factors have become an increasingly important aspect of global power rivalry, as rival blocks seek relative strategic advantages by pursuing or maintaining access to critical assets – and by denying access to others – through protectionist policies, by promoting national production and by restricting exports or foreign investments.[4] The securitisation of the economy is changing the division of labour between states and corporations as corporations have become important actors for comprehensive security.

States recognize that the pursuits of increasingly multinational corporations are not necessarily aligned with state interests and are struggling to integrate corporations in comprehensive security arrangements. Commercial assessments may result in business pursuits that compromise state interests – such as transfer of strategic products, technology or know-how to rival powers. The effects of corporate enterprise on state security can be seen as a corporate externality warranting policy responses. The EU, for example, has taken significant steps to strengthen its strategic autonomy and resilience through regulation and policy initiatives related to the central role of corporations in national security priorities. Importantly, mandatory regulation has in many cases been applied in tandem with favourable industrial policy and commercial arrangements in efforts to mobilize corporations to serve state interests in a pivot towards "strategic capitalism".[5]

Towards corporate statecraft

In a less-structured international framework, corporations cannot rely on states or existing institutional frameworks alone but need to manage their interests independently. New tools are needed to integrate political aspects of the corporate enterprise in corporate management. Corporations must manage fundamental political and regulatory changes as a part of their strategies and business models. Corporations will need to strengthen their resilience to geopolitical changes, assess their role with respect to strategic state interests and to societal expectations, and build competitive business models and strategies adapted to an evolving operating environment.

As political actors, corporations may apply tools of statecraft in their interaction with states and other political institutions. Corporate statecraft can be seen as a part of corporate strategy related to interactions regarding the political aspects of the enterprise. Relationships between corporations, states and other political actors are characterized, in many respects, by asymmetric interdependencies. Formally, corporations are subject to laws and other political decisions of sovereign states. However, in many cases, states are dependent on corporations for investments and revenue, as well as matters of strategic importance, such as research and development and critical infrastructure. A key element of corporate statecraft is the management of these interdependencies.

Corporations can be expected to maximize their influence on political decision-making in matters critical for their business, while seeking to insulate their business from the impact of political decisions. The promise of significant investments, for example, may be used to ensure favourable treatment over the long-term. Corporations may also look to diversify their operations geographically to avoid exposure to a single jurisdiction and to promote competition with regard to political decision-making affecting their business. Altogether, to hedge for political risks, it may well be in the interests of corporations not to be overly exposed to any single state. Some corporations have already sought to ringfence operations in China, for example, in order to build supply chain resilience and to manage regulatory requirements. Corporations may seek to increasingly decentralize business models so that they can adapt to varied political and regulatory requirements. In this regard, corporations may also deliberately seek to build a political identity independent of state affiliations.

Conclusions: Divided fealties in a new international (dis)order

In an era where states and corporations would need increased mutual reliance and cooperation, they are being driven apart as they remain affixed in roles based on a political order that has come to pass. In their pursuit to redefine their respective roles, states and corporations are well-advised to manage their interdependencies by finding synergies and long-term common interests. Importantly, corporations are increasingly accountable to their key stakeholders with political and security needs directly linked to the state. Thus, corporations may find alignment with state interests as they approach the political implications of their enterprise based on the long-term welfare of key stakeholders.[6] States, on the other hand, may seek to strengthen incentivises for corporations to contribute to state interests by industrial policy and by creating competitive business environments.

The political challenges of states and corporations are not subsiding. Geopolitical developments have resulted in the erosion of established international state-centric institutions and frameworks, and the emergence of a less structured and more multifaceted political environment. This allows new actors to emerge on the international arena, including multinational corporations, who will be better able to form international interaction to serve their interests.[7] In the current geopolitical environment, multinational corporations are increasingly in a position to set "their own conditions and destinies".[8] In this regard, comparisons have been made to historical periods preceding the dominance of nation states when the international stage was shared with "merchant-republics, wealthy oligarchs, and early joint-stock-companies".[9] In a potential return to a pre-mercantilist order, both state security and corporate statecraft will be of considerable importance.

This article relates to a pending research project on the evolving role of private corporations in comprehensive security in Finland and the EU.[10]

[1] European Commission High representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy"*, JOIN(2023) 20 final, Brussels, 20 June 2023.
[2] Tuomas Tapio, *Geotalouden Paluu [The Return of Geoeconomics]*, 2018, pp. 142-150.
[3] George Haynal, *Corporate Statecraft and its Diplomacy*, 9 Hague J. of Dipl. (2014), p. 393-419.
[4] Anthea Roberts, Henrique Choer Moraes and Victor Ferguson, *Toward a Geoeconomic Order in International Trade and Investment*, 22 J. of Int'l Ec. L 655-676, 657 (2019).
[5] Henrique Choer Moraes and Mikael Wigell, The Emergence of Strategic Capitalism, FIIA Working Paper 117/2020.
[6] Oliver Hart and Luigi Zingales, *Companies Should Maximize Shareholder Welfare Not Market Value*, J. of L., Fin. and Accounting, 2017:2, 247-274.
[7] Milan Babic, Jan Fichtner and Eelke M. Heemskerk, *States versus Corporations: Rethinking the Power of Business in International Politics. The International Spectator*, 2017: 4, 20–43.
[8] Colin Reed, *Developing a "Corporate Foreign Policy": The Urgent Need For Boardroom Geopolitics Strategies*, Encyclopedia Geopolitica, 3 November 2022.
[9] Reed (2022).
[10] See Klaus Ilmonen, *Geopolitics and Corporate Law in the EU*, Law & Geoeconomics, 2025:2.

Klaus Ilmonen
Attorney, LL.D., Finland, Partner
Hannes Snellman Attorneys Ltd.
Helsinki
Finland

Professor of Practice
Hanken School of Economics
Helsinki
Finland

klaus.ilmonen@hanken.fi

DARREN E. TROMBLAY

Beyond spy-versus-spy: Counterintelligence as information warfare

Expert article • 3977

There is a significant disconnect between intelligence and geopolitical literature that results in counterintelligence being a little-understood discipline. Intelligence literature often focuses on the tactical, spy-versus-spy aspects of counterintelligence. Meanwhile, geopolitical literature, while often not giving intelligence its due, gives counterintelligence even less attention. Counterintelligence, however, is nothing less than information warfare that has implications for strategic decisionmaking.

Counterintelligence, at its core, is the manipulation of an adversary or competitor's information environment. This manipulation takes two distinct forms: cutting off access and introducing information.

Cutting off access prevents hostile intelligence actors from gathering information that addresses collection requirements. This deprives a service's respective government inputs to decision making. Cutting off an adversary's flow of information takes two primary forms. The first is disrupting operations, whether human or cyber that are exfiltrating data, through counterespionage (the law enforcement aspect of counterintelligence). Second, preemptive security measures can disrupt an adversary from even initially gaining access to sensitive information.

The other objective of counterintelligence is to manipulate an adversary's decision-making through the clandestine introduction of information. Specifically, manipulation exploits adversarial intelligence collection activities by facilitating their answering of requirements, but on the target's terms. U.S. double agent operations, starting in the Second World War, fed hostile intelligence actors both true and deceptive data that Washington wanted them to receive, with the intent of eliciting a certain decision. The Soviet Union (and its Russian successor) employed "active measures" to disrupt Western decision-making by creating controversy around policy decisions.

While counterintelligence has historically focused on government or government-adjacent (for instance, the defense industry) information, the contribution of the independent private sector to elements of national power, especially since the end of the Cold War, has broadened the counterintelligence playing field. State-affiliated companies have become practitioners of economic espionage, the theft of trade secrets, against foreign competitors.

Theft is not the only way counterintelligence plays out in the private sector. In one instance, a Chinese telecommunication company specifically sought to create turmoil in a foreign competitor. This attempt to sow disruption, which could impact decision making, conceptually the same as Soviet active measures. Counterintelligence could theoretically impact the private sector through the distortion of information. For instance, a company, seeking a competitive advantage could corrupt research and development through malicious cyber activity.

Academia has also been a counterintelligence battleground. East German intelligence, for instance, infiltrated a high-profile U.S. think tank, with a recruited agent, in the mid-1970s. The Soviet KGB attempted to do similarly. Such penetrations had the potential to facilitate both collection and influence. China has explicitly targeted the academic sector to effect knowledge transfer, which can support scientific decision making, through its talent programs.

Counterintelligence, therefore, does not exist in a hermetically sealed world of spies and spycatchers. Information warfare - affecting an adversary or competitor's decision making by restricting or allowing the flow of data - is at the center of the discipline. Although historically centered around government information, counterintelligence increasingly plays out in other venues, as entities beyond government contribute, independently, to elements of national power.

Darren E. Tromblay
MA, MS

Darren E. Tromblay is an independent author, having published a variety of books and peer reviewed articles on aspects of national security, with more than two decades in the U.S. intelligence community as an analyst and historian. He is a member of the International Journal of Intelligence and Counterintelligence editorial board.

KRISTIAN GUSTAFSON

Structured intelligence analysis for the modern military

Expert article • 3978

Intelligence analysis has always demanded disciplined thinking, yet for much of its history it has relied heavily on intuition, personal judgement, and the craft knowledge of experienced analysts.[1] As the modern security environment has grown (arguably) more complex—characterised by ambiguous indicators, rapid tempo, and deliberate adversarial deception—the limits of intuition have become increasingly evident. Contemporary military decision-making requires assessments that are transparent, defensible, and able to withstand both scrutiny and uncertainty. The strongest argument for structured analytical techniques (SATs) is therefore straightforward: they impose rigour, reduce avoidable error, and provide commanders with a clear understanding of how an assessment was reached. In an environment where decisions carry operational and strategic consequences, structured analysis is not simply a methodological preference; it is a professional obligation.

Much of the momentum toward more formal analytical methods emerged from repeated historical failures. Intelligence organisations throughout the twentieth century often relied on gifted individual analysts or ad hoc processes.[2] Failures especially around the 2003 invasion of Iraq cast long shadows in intelligence structures in the US and UK, leading to direct political pressure to formalise analytical standards and processes. The lack of effort at structuring assessment may lie behind the disastrous failure to predict the fall of Kabul to the Taliban in 2021.[3] Its rigorous application may be the reason that US and UK analysts successfully predicted the full-scale Russian invasion of Ukraine in 2022, whilst equally sophisticated states such as France and Germany—and even Ukraine's own government—refused that analysis.[4]

These episodes demonstrated that even highly experienced analysts are vulnerable to cognitive shortcuts, institutional pressures, and mirror-imaging. Structure became necessary not because analysts were unskilled, but because the task itself was uniquely difficult: data are fragmentary, adversaries are deceptive, and outcomes are rarely certain. The military profession long ago recognised parallel needs in planning, adopting structured tools such as the UK Combat Estimate, the American MDMP, or the NATO 6-step Operational Planning Process to discipline tactical and operational thinking.[5] Despite SATs becoming a standard, the Intelligence Communities of NATO countries have so far failed to implement a common and shared structured approach to intelligence analysis.[6]

This is unfortunate, as the challenge to all modern states is underlined by the nature of intelligence problems. Analysts rarely work with complete or reliable information; instead they must draw inferences from partial signals, "essentially geared to penetrating those areas in which concealment and deception are endemic."[7] Under these conditions, intuition alone is vulnerable to well-documented cognitive biases. Confirmation bias, for instance, leads analysts to overweight information that supports their existing beliefs. Anchoring can cause them to cling too closely to initial estimates, even when new evidence emerges. Availability bias encourages overreliance on vivid or recent events.[8] These are not moral failings but predictable features of human cognition. Structured techniques—such as key assumptions checks, analysis of competing hypotheses, indicator & warning matrices, decision-tree analysis and red-teaming—exist precisely to mitigate these vulnerabilities. They force analysts to articulate reasoning, challenge assumptions, and examine alternative explanations systematically. And they are well developed now: analyst handbooks proliferate in government, and Pherson & Heuer's Structured Analytic Techniques for Intelligence Analysis provide strong handrails for new analysts. [9]

For military users who may be less familiar with these techniques, the value lies in what they make visible. A structured assessment provides clarity about what is known, what is uncertain, and how confidence was derived. This transparency supports better command decisions. When a commander receives an intelligence estimate built on explicit assumptions, clearly defined indicators, and a documented evaluation of alternative hypotheses, they can judge the robustness of the assessment and its relevance to operational planning. By contrast, an unstructured "expert judgement" product may be compelling on the surface (it might offer a good "story") but offer no way to evaluate whether it is sound.[10] The issue is not that intuition is worthless—indeed, seasoned analysts often generate valuable insights—but that intuition without discipline cannot be audited or defended.

Time pressure, a defining feature of military operations, further strengthens the case for structure. The "time problem" in intelligence arises not only from the need to detect signals early but from the human struggle to recognise significance while events are still unfolding.[11] Commanders and analysts alike are prone to hindsight bias: once an event has occurred, it seems obvious in retrospect, leading organisations to believe they "should have known." Structured approaches help counter this by generating explicit indicators in advance, enabling the identification of weak signals before they coalesce into unambiguous threats. They also create shared frameworks that help commanders interpret ambiguous situations without assuming that intelligence can predict events with certainty.

Critics have sometimes argued that structured analytical techniques do not reliably increase the accuracy of intelligence assessments.[12] Such a view mirrors some initial overenthusiasm at the effectives of SATs, and just as much misunderstands their primary purpose. SATs are not diagnostic tools in the medical sense; they are thinking tools. Their central value lies in improving the quality, transparency, and defensibility of reasoning. Even if accuracy improvements are modest or context-dependent, the discipline they impose reduces the risk of catastrophic misjudgement, particularly in high-consequence military environments. They also facilitate organisational learning. A structured assessment leaves a traceable record that can be reviewed, compared, and revised as events develop, as happens for example within the UK Cabinet Office with formal reviews of intelligence products. As we learn from Tetlock and Gardner[13], feedback is crucial to improving the accuracy (or, more specifically, the "Brier Score"[14]) of analysts, and auditable analysis allows professional reviews of intelligence products to help improve the individual analyst and improve processes within government.

Structured techniques also enhance communication between analysts and military decision-makers. Intelligence is only useful if it is understood, and misunderstandings between producers and consumers are common. Analysts may believe they have conveyed nuance, uncertainty, or conditional assessments, while commanders may perceive confidence or precision that was never intended. The adoption of probability- and confidence-based language, including frameworks such as the Professional Head of Intelligence Assessment (PHIA) scale, helps bridge this gap.[15] It provides a consistent lexicon for expressing uncertainty,

enabling decision-makers to integrate intelligence assessments into planning processes more effectively. This author's recent primary research into UK national intelligence products, conducted along with government, found that structured reasoning paired with structured communication, results in intelligence that is more actionable, more reliable, and more attuned to the needs of its military audience.[16]

SATs are not designed to replace judgement; they are designed to discipline it. Creativity remains essential in identifying novel patterns, generating hypotheses, and anticipating adversary behaviour. Structure simply provides a scaffold that ensures creativity does not drift into speculation. The two are complementary, not contradictory. In fact, many of the most innovative analytical leaps arise from structured activities—such as red-team exercises or alternative futures analysis—that deliberately force analysts to consider perspectives they might otherwise overlook.[17] Even properly designed and structured wargames can be treated like an analytical tool with clear benefits in situational understanding and a clear framing of options.[18]

For modern military organisations facing agile adversaries and complex operating environments, the adoption of structured analytical methods is therefore not simply best practice but operational necessity. Uncertainty cannot be eliminated, but it can be managed. Bias cannot be removed, but it can be mitigated. Adversarial deception cannot be wished away, but its effects can be constrained by disciplined reasoning. Structured methods achieve this by making thinking explicit, exposing assumptions to challenge, and enabling effective dialogue between analysts and commanders.

Perversely, many seem to be rushing past structured analysis and shoving it aside in favour of the unproven promise of Artificial Intelligence. Whilst AI can already automate routine, time-consuming tasks such as summarising reporting, processing imagery, or handling large data streams, it remains poorly suited to the core challenges of intelligence work: ambiguity, uncertainty, and adversarial deception.[19] AI systems depend on large quantities of reliable data and struggle with the fragmentary, contradictory, and deliberately manipulated information that defines real intelligence problems. They also "hallucinate," importing or inventing false information in ways that analysts may not immediately detect, and cannot at the moment clearly lay out their reasoning. Because intelligence assessments ultimately require synthesis, and the ability to judge intent—capabilities AI cannot replicate—AI should be treated as an aid to human reasoning, not a substitute for it. Its promise is significant, but its peril lies in assuming that computational pattern-matching can replace the experienced human analyst, structuring their thinking in an auditable way in making sense of a deceptive and adversarial world.

Ultimately, structured analysis should enhance trust. Commanders do not need perfect intelligence; they need to understand the basis of the assessments on which they must act. After all, command decisions will rest on the commander's judgement, not that of the perhaps quite junior analyst. But when an intelligence product shows its workings (highlighting evidence, assumptions, gaps, dissenting interpretations, and the rationale for its conclusions) it empowers military leaders to make more informed decisions. In critical, time-pressured combat situations, this transparency is not optional. It is the foundation of intelligence professionalism.

[1] Kenneth V. Strong (1970), *Men of Intelligence: A Study of the Roles and Decisions of Chiefs of Intelligence from World War I to the Present Day*. London: Cassell.
[2] Secretary of State for Foreign and Commonwealth Affairs (2005) "Review of Intelligence on Weapons of Mass Destruction: Implementations of Its Conclusions" London: Her Majesty's Stationary Office.
[3] Kristian Gustafson (2024) 'Kabul, 2021 - The Taliban Overtakes Kabul', in Gronning, BEM. and Stenslie, S. (eds.) *Contemporary Intelligence Warning Cases Learning from Successes and Failures*. Edinburgh: Edinburgh University Press. pp. 236 - 258. ISBN 10: 1-3995-3191-3.
[4] Kristian Gustafson, Dan Lomas, Steven Wagner, Neveen Shaaban Abdalla & Philip H. J. Davies (2024) *Intelligence warning in the Ukraine war*, Autumn 2021 – Summer 2022, Intelligence and National Security, 39:3, p. 404, DOI: 10.1080/02684527.2024.2322214
[5] NATO (2019) AJP-5, "Allied Joint Doctrine for the Planning of Operations"
[6] Lars C. Borg & Kristian C. Gustafson (2025) "Teaching Structured Analytic Techniques across Nations: Same, Same but Different", *International Journal of Intelligence and CounterIntelligence*, 38:3, 843-861, DOI: 10.1080/08850607.2025.2479991
[7] Michael Herman (1992) *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press, p. 118.
[8] Richards J Heuer (1999). *Psychology of Intelligence Analysis*. Langley, Virginia: Centre for the Study of Intelligence, CIA.
[9] Randolph H. Pherson & Richards J. Heuer Jr (2019) *Structured Analytic Techniques for Intelligence Analysis* (Third Edition). Washington DC, CQ Press.
[10] Philip Tetlock and Dan Gardner (2015), *Superforecasting: The Art and Science of Prediction*. London, Random House Books, p. 72.
[11] David Kahn (2006) "Surprise and Secrecy: Two Thoughts", *Intelligence and National Security*, Vol.21, No.6, December 2006, p.1060
[12] Martha Whitesmith (2022), *Cognitive Bias in Intelligence Analysis*. Edinburgh: Edinburgh University Press, pp. 5-6.
[13] Tetlock & Gardner, pp 180-182.
[14] Jeffrey A Friedman (2019), *War and Chance: Assessing Uncertainty in International Politics*. Oxford: Oxford University Press, pp 76-77.
[15] UK Government, PHIA Probability Yardstick, see https://www.gov.uk/government/publications/explaining-uncertainty-in-uk-intelligence-assessment/explaining-uncertainty-in-uk-intelligence-assessment Accessed Nov 2025.
[16] Kristian Gustafson (2025) "Analytical Confidence Rating Framework Project 2025", UK Professional Head of Intelligence Analysis.
[17] Peter C. Bishop and Andy Hines (2013) "Framework foresight: Exploring futures the Houston Way", *Futures*, Vol 51, pp. 31-49.
[18] Eric M. Walters (2021) "Wargaming in Professional Military Education: Challenges and Solutions", *Journal of Advanced Military Studies*, Volume 12, Number 2, 2021, pp. 81-114. 81-114
[19] Zachery Tyson Brown (2024) ""The Incalculable Element": The Promise and Peril of Artificial Intelligence", *Studies in Intelligence* Vol. 68, No. 1.

Kristian Gustafson
Dr., Reader in Intelligence & War, Deputy Director
Brunel Centre for Intelligence & Security Studies
UK

Dr. Gustafson has conducted consultancy and advisory work for the UK Cabinet Office, and the MOD's Development, Concepts and Doctrine Centre, including an integral role in developing UK Joint Intelligence Doctrine.

MAGNUS ANDERSSON

Improving operational intelligence analysis

Expert article • 3979

The craft of operational intelligence analysis has never been more important than now. Although technology has the potential to significantly improve intelligence analysis, a human intellect still has to critically assess the findings and make up their mind whether or not to believe in and act upon them. Operational analysis, in criminal intelligence, is the craft of discovering and describing what has happened or is about to happen within a case. This is done by critically assessing, cross-referencing and presenting all-source intelligence and evidence about events, places, people and activities, it is a modern version of Sherlock Holmes' mystery solving craft.

Operational analysis is similar to the historian's methodology. Both tell a story about how events unfold based on an evaluation of sources and an interpretation that forms an explanation. The story's plausibility is assessed in two dimensions, its coherence and the reliability of each story element. Operational analysis result in a specific and detailed nongeneralized explanation about a narrow slice of reality, which is necessary for a successful warning or a conviction in court. But both create understanding and insight by learning about how events happened.

Operational analysts should become proficient learners since effective learning applies to both gaining understanding about the details of a case and gaining skills in specific analytical techniques. Learning is done through active recall and spaced repetition. Operational analysts practice active recall and spaced repetition when working with data in a case by creating visualisation charts, discussing the elements of the case and writing summaries of the findings. Here analysts can improve by using the Feynman technique in their work. When using it, you: 1) break the topic down into small parts and retrieve them from memory; 2) write about each part in simple terms or visualise them; 3) review what you have done and identify gaps in your understanding; and 4) revise your output. Importantly, it is done as if you are going to teach someone else. Experiments show that you learn better by using these steps and, as an operational analyst, you have an output that is ready for immediate dissemination. And what is dissemination but a way of teaching someone about the specifics of a case and why they should believe the conclusions. In intelligence and investigations, the technique should be complemented with the use of references during the writing process.

We learn by actively working with a material, that is why visualisation charts and written atomic notes about parts of a case should be a core task in analysis. Writing notes is usually done during meetings, but it should also be done as analytical case notes. Analytical notes can be indexed and linked into a Zettelkasten system or a wiki which both organically link notes together. Over time these will grow into complete analysis reports. Atomic notes and short memos are what you write using the Feynman technique. Notetaking can also be used to capture that which has not been registered in intelligence platforms, such as key information only found in a colleague's memory.

There are techniques in how to take notes and learn, such as the Cornell Method where you divide the page into different areas to be able to categorise the note's content. By categorisation and the use of an index you instantly collate the information you are working with. Many analysts use a notebook where notes are compiled in a chronological 'catch-all' function as the work progress. A complementary way is to use a compendium notebook, i.e. a case or topic specific notebook and apply the Cornell Method in it.

Notes don't have to be written text. In fact, visualisations such as maps, link, event, flow and activity charts are representations of atomic elements. Thinking exists on a scale between verbal and visual. Verbal thinking is words formed in our head, while visual thinking is either spatial visualisations of forms or object-visualisation where thoughts appear as an image or a movie scene. In experiments comprehension is improved significantly with the addition of pictures even for verbal and auditory learners, which emphasise the importance of visualisations to improve understanding and thinking. That is why visualisations should be at the centre of learning and analysing the details of a case and teaching them to a decision maker.

These techniques can be done in conjunction with or independent of technology and are timeless in their use. They are your personal complement to intelligence software platforms. With operational intelligence analysts being knowledge workers, these techniques should be at the forefront of their skill set and they are fairly easy to implement. By applying them you improve your personal knowledge management system in order to tell the operational story about how a crime was or is about to be committed.

Magnus Andersson
Intelligence Project Manager
Swedish Police/Police Intelligence Division
South
Sweden

Ph.D. Student
Department of Political Science, Intelligence Studies
Lund University
Sweden

magnus.andersson@svet.lu.se

TALLAT R. SHAKOOR

Escaping the intelligence cycle straitjacket?

Expert article • 3980

Introduction
The intelligence cycle is a theory of how an intelligence organisation is supposed to work. For many, it is considered a universal concept that any intelligence organisation, with respect for itself, must make the cycle the centrepiece of its intelligence doctrine. However, the intelligence cycle is neither a universally valid model nor a valid metaphor for the work carried out inside state intelligence organisations.

A Cold War solution to Second World War problems
The cycle has been around since the end of the Second World War. Initially, the cycle was an attempt by two American officers, Davidson and Glass, to enlighten American commanders on intelligence principles and rid them of their 'contempt for intelligence'[1] to avoid the intelligence failures of the Second World War. Secondly, Davidson and Glass proposed a cycle as the model of what they saw as the universal principles of intelligence.

In practical terms, the cycle or an accustomed version is prevalent in the American, British, and NATO doctrines. Furthermore, if we move to the European continent, we find the intelligence cycle, even in the doctrines of the intelligence services of the Scandinavian welfare states. Taking a concrete example, I want to zoom in on the Danish example of a state intelligence organisation, where we find that the intelligence cycle is not applied.

Black swan…
If a theory is falsified in just one instance, it is disproved. The late Karl Popper, a German philosopher of science, made the dictum that *any* theory must be challenged. Popper famously stated, "No number of sightings of white swans can prove the theory that all swans are white. The sighting of just one black one may disprove it".[2] By that same token, if the intelligence cycle is seen as a universally applicable and relevant concept, it only takes one example to disprove its universal relevance.

Although the Danish intelligence national community pays public homage to the' universal' intelligence cycle in both the security and foreign intelligence service, the intelligence cycle is not used for all intents and purposes. Instead, something else is in play. It is much less exotic and makes the Danish Defence Intelligence Service much more integrable with the rest of the Danish central administration. It is New Public Management. As I have shown in my dissertation and elsewhere, looking for direction vis-à-vis the intelligence cycle in the DDIS, we find, in its stead, a dialogue between the national customers and the DDIS, structured within the theory of New Public Management. So what? So what if organisations claim to follow a time-worn ideal and do something more innovative and more up-to-date? What difference does it make?

"To improve is to change…."
'To improve is to change; to be perfect is to change often,' were reportedly the words of a cigar-chomping British wartime prime minister.

In her most recent book, American intelligence scholar Amy Zegart argues that three significant challenges - a tech-shaped dynamic threat landscape, a tsunami of data on a more level playing field of state, and privately collected intelligence, and the ever thornier dilemma of secrecy and transparency - face the American intelligence community.

I agree and would extend the argument even further. *All states* face their brand of multifaceted, dynamic threat picture in a global, multipolar, global security landscape that includes hostile actors on international, transnational, state, non-state, geographical, and environmental levels. *All states* must stay on an eye-to-eye level with technological developments to exploit them and protect their citizens from attacks prompted by that same technology. Also, new, hybrid forms of conflict have become the new normal. To be able to face these challenges, *all national intelligence organisations* need to be reflexive about how they meet these challenges. Of course, all intelligence organisations are different. The challenges might be the same, but they are taken down, interpreted, and met in very different ways. There is no one-size-fits-all solution.

These facts point to, in my opinion, that a necessary first step for intelligence organisations is to acknowledge that one of the heirlooms, or flotsam, of the Cold War – the intelligence cycle, initially a solution for mid-20th-century intelligence problems – has turned into a conceptual straitjacket, preventing new and dynamic solutions for 21st-century problems from appearing.

Building reflexivity
Rather than seeking outdated, universal models, national intelligence organisations must establish in-house centres of excellence tasked with staying abreast of the general yet uniquely packed set of challenges that every national intelligence organisation faces. These centres of excellence should be advisors to intelligence leadership and national customers in helping organisations and customers understand what global challenges will mean for them and advising how these challenges could be understood and perhaps acted upon within a national political framework and with limited resources. This is particularly important for small states, which have less influence in shaping world events and, therefore, must be more agile and dynamic in their approach. To improve is to change; to be perfect is to change often.

There is no place for heirlooms from the Cold War or for Cold War flotsam.

[1] Davidson and Glass, *Intelligence is for Commanders*, 1948: x.
[2] Popper, *The Logic of Scientific Discovery*, 1935.

Tallat R. Shakoor
PhD, Senior Consultant
Danish National Police
Denmark

PÄR ANDERS GRANHAG

The Scharff technique for eliciting human intelligence

Expert article • 3981

I assume we agree that all wars are battles for information, and that even if cold wars lack the actual combat, they are still about information – to get to the status and the intentions of the opposing side. Some argue that we have entered a new era of cold war. Modern national security work utilizes sources such as geospatial intelligence, signals intelligence and social media intelligence, but the most critical information often comes from human sources: human intelligence (HUMINT). The science of today is so far passed earlier wars with respect to technology; there is little to learn in terms of reconnaissance, weapons and defense systems. Interrogation, however, is unchanged since antiquity – it is about the dynamics between two persons competing for information. Here I will give an example of how psychology might assist in collecting HUMINT. It is obvious that psychology always is an integral part in recruiting human sources, but for this short note I will focus on the actual interaction between an intelligence officer and a source of some kind – I will talk on the issue of elicitation.

Elicitation is a particular way of collecting information; the first part of the concept is to gently gather new information, the second is to collect it without revealing what you're after, and the third part is to leave the source with the impression that he or she didn't contribute with anything new. Elicitation and traditional interrogations coincide only with respect to the objective of obtaining new information. But even for this part they are different – elicitation is about advanced psychology and subtle ways of gathering information, whereas traditional interrogations typically are about primitive psychology and ways of forcing out information.

I have spent 20 years studying a master of elicitation: Hanns Joachim Scharff (1907-1992), who worked as an interrogator for the German Luftwaffe during WWII. Many sources speak to that Hanns Scharff was very successful at his job and he is often portrayed as a legendary interrogator - but his approach is typically sketchily described. Scharff never used coercive or harsh methods, instead he was quick to appreciate the value of learning about his prisoners' counter-interrogation tactics (CITs). In essence, he tailored his own strategies and tactics in the light of his prisoners' CITs. Broadly speaking, Scharff used his knowledge on his prisoners' CITs to develop general strategies to engage his prisoners in meaningful conversations, and to tailor specific tactics to elicit small pieces of information (for example, he was a master in terms of using claims to elicit information). Together with my colleagues I have conducted three waves of research on the Scharff technique; the first was about conceptualization and proof of concept. For the second wave we examined the effectiveness of the Scharff-technique in different contexts, for example the sources' level of cooperation and to what extent the technique can be used for small cells of sources. For our third wave we trained different professional groups in the technique, for example intelligence officers and police handlers. All in all, for these scientific tests the Scharff-technique has lived up to its reputation – the technique outperforms more standard and commonly used elicitation techniques. I have on request given presentations on Scharff's technique in many different countries, and for high profile organizations such as the MI5, Defence Intelligence (UK), NYPD Intelligence Division, LAPD Major Crimes Division and the FBI.

Pär Anders Granhag
Professor of Psychology
Department of Psychology
University of Gothenburg
Sweden

pag@psy.gu.se

WŁADYSŁAW BUŁHAK

Illegals – Lessons from Polish and British archives

Expert article • 3982

Among HUMINT techniques, the illegal method tends to be the most effective during times of hybrid or full-scale war, making it particularly relevant in the current global climate. This method involves conducting intelligence operations in enemy territory without using official cover, such as diplomatic status, and ideally without any visible contact with the nation carrying out these activities (the Western term for that is "non-official cover").

Illegals typically use documents that express a nationality different from their true one, and they may impersonate others, both living and deceased (impostors). The idea has even become a recurrent scheme in popular culture, exemplified by the TV series "The Americans." It is well-known that Russian intelligence employs this method, particularly in the context of the war in Ukraine, partly as a response to restrictions on Russian diplomatic missions or other official representations in many EU countries. In the internal hierarchy of the Soviet security apparatus and its Russian successors, "illegals" are viewed as an elite group within the espionage profession.

While this type of operation is often attributed to Soviet and Russian intelligence, it is also important to recognise that the Israeli intelligence services may have been the primary users of this kind of method. Within the former Soviet bloc, the East German Stasi intelligence, the HVA, led in this regard. Nonetheless, the KGB and its successors, in fact, executed significant operations of that kind, with notable examples including the cases of William Fischer (also known as Rudolf Abel) and Konon Molody (also known as Gordon Lonsdale).

From a scholarly perspective, understanding this method is a salient aspect of studying intelligence or security. In this context, access to in-depth archival data is crucial. For example, the extensive British counterintelligence files on the already mentioned Lonsdale affair are available at The National Archives in Kew. Concurrently, the Polish Institute of National Remembrance (IPN) has made similar documents from 1945 to 1990 available for research. These documents contain information on case officers (handlers), illegal agents and residents, liaisons and couriers. They also include original Soviet manuals and data concerning specialised training programs in Moscow for future handlers of illegal agents. Moreover, most importantly, the plans and reports stored in the IPN archive enable the reconstruction of the entire system of similar operations against the West.

The system was complex, encompassing precise plans of espionage operations abroad and a dual system of illegal residencies (stations). One type operated directly in adversarial countries, such as the USA, Great Britain, FRG, France, Switzerland, and Italy. The second type functioned as liaison posts in neutral or less significant countries, intended for communication and coordination. The commercial fleet played a vital role in supporting these operations through illegal communication methods, drawing parallels with the contemporary Russian "shadow fleet." The system also utilised sailors, international train conductors, and airline stewards as couriers and liaisons.

The Polish example demonstrates that the method in question was complicated to implement due to both trivial budgetary and human limitations. The romantic times when anyone would devote their entire life to the communist idea passed with the revelation of the system's crimes in the late 1950s. A trivial problem for illegal agents is loneliness, functioning in a relationship imposed by the service or the need to hide a double life from their partner (resulting in jealousy). Otherwise, other problems typical of single people arise (alcohol, stimulants, casual sexual relations), leading to an increased risk of exposure. A significant problem was also the headquarters's control over the agent, which had been dormant for years. Moreover, the aforementioned reliance on frequent travellers also posed risks, as all such individuals are often under heightened suspicion from law enforcement for potential illicit activities beyond espionage, like smuggling.

Consequently, American opponents of Soviet 'illegals' coolly stated in one of their internal reports that, ultimately, the activities in question 'are complex, time-consuming and probably overestimated'. According to the Americans, the enormous costs of such intelligence operations are in no way commensurate with the importance of the successes achieved. The Americans also pointed out that, in fact, the activities of Soviet' illegals' rarely went beyond (also for mundane reasons) beyond simply 'surviving' in the West. From the Western services' perspective, it was their theoretical 'mobilisation' potential in the event of war that is dangerous, rather than their actual information or penetration capabilities.

Władysław Bułhak
Dr hab., Senior Lecturer/Researcher
University of Warsaw
Institute of National Remembrance
Poland

w.bulhak2@uw.edu.pl;
wladyslaw.bulhak@ipn.gov.pl

MELINA J. DOBSON

Rethinking US insider disclosures

Expert article • 3983

Debates about whistleblowing in the intelligence world remain fraught because there is no settled understanding of what a whistleblower is. Despite legal guidelines, the terms used to describe insiders who disclose wrongdoing carry political weight and shape public perception as much as the facts themselves. Whistleblower, leaker and dissident are often used interchangeably, yet each signals different motives and consequences. This ambiguity obscures the actions of those who come forward in the public interest and complicates any attempt to protect them.

Insiders in intelligence agencies work in an environment defined by secrecy and trust. Access to confidential material allows them to carry out their duties, but it also places them inside a closed circle whose members are expected to uphold absolute loyalty. When an individual raises concerns about wrongdoing, they challenge the norms that bind this community. Such disclosures usually follow a period of moral and personal conflict. Fear of retaliation, financial insecurity and the risk of losing a career are central to the dilemma faced by insiders who consider speaking out.

Legal provisions intended to protect those who raise concerns have often proved unreliable or unsuitable. The successful 2023 US Security and Exchange Commission Whistleblower Programme, for example, excludes intelligence personnel entirely. Within the intelligence community, formal reporting routes exist, but those who use them remain vulnerable if internal authorities decide that the issue raised does not qualify for protection. Individuals may be exposed to administrative or professional reprisals with no means of enforcing their rights. This lack of a credible safeguard discourages insiders from acting, even when they hold evidence of serious misconduct.

When internal mechanisms fail, some choose to make unauthorised disclosures. These actions divide opinion. Some see them as irresponsible breaches that endanger national security, while others view them as last-resort attempts to expose wrongdoing that would otherwise remain hidden. The line between a disclosure made in the public interest and one driven by other motives is not always clear. This blurred distinction has, at times, seen individuals treated as security threats even when they sought to expose malpractice rather than cause harm.

A further complication arises from the inconsistent enforcement of secrecy laws such as the Espionage Act. Some insiders who revealed questionable or unlawful practices have faced severe penalties, including charges intended for espionage. Yet senior officials who mishandled classified information in more serious ways have received limited punishment. These disparities raise concerns about the influence of status and political convenience on legal outcomes. They weaken trust in the fairness of the system and deter potential whistleblowers from coming forward.

Support networks have developed to assist those navigating these risks, yet even specialists disagree on how to define whistleblowing in national security settings. Some legal clarity has emerged through the Protection of Intelligence Community Whistleblower Act (2014), but debate continues over whether its scope is sufficient. Some argue that disclosures to the press can be justified when internal processes fail, while others insist that communication outside approved channels automatically undermines legitimacy. These contrasting views reflect the broader uncertainty surrounding the issue and the difficulty of applying consistent standards to complex, high-risk environments.

Crucially, the question of whistleblowing in intelligence organisations is not only about definitions. It concerns power, accountability and the tension between secrecy and democratic oversight. Whistleblowers take considerable personal risk to reveal matters that may have serious implications for public trust and the rule of law. While reckless disclosures must be prevented, there must also be a credible path for insiders who act responsibly and in the public interest. Without this, wrongdoing may remain concealed and institutions may become less resilient, not more secure.

A more constructive approach would recognise that disclosures are an inevitable feature of secretive systems. Rather than concentrating solely on whether a leak is right or wrong, the emphasis should fall on understanding its context, motives and consequences. Clear legal standards that recognise proportional, public-interest disclosures would help differentiate principled actions from harmful ones. Protecting those who expose genuine misconduct ultimately strengthens national security by reinforcing ethical conduct, improving institutional integrity and ensuring that secret power remains subject to democratic scrutiny.

Melina J. Dobson
Dr., Lecturer in Intelligence Studies
Centre for Security and Intelligence Studies (BUCSIS)
University of Buckingham
UK

melina.dobson@buckingham.ac.uk

JENNIFER A. DAVIS

Supporting women in intelligence leadership

Expert article • 3984

Intelligence leadership is at its strongest when it brings together diverse perspectives from many experiences, yet most intelligence leadership is still heavily male-dominated. While progress has been made on this front, women are still heavily underrepresented in senior leadership positions. Recently, there have been dramatic steps forward, including a number of women appointed to leadership roles as agency heads, but this progress has been uneven and sporadic. By recognizing that female leaders bring essential and valued skills to the intelligence enterprise that contribute significantly to security and stability, the field of intelligence becomes stronger and more effective. Only by continuing to expand opportunities for women in intelligence leadership, will intelligence organizations be best positioned to respond to today's complex and evolving threats.

Numerous works have been written about the impact that women in the SOE and OSS had during World War II, the contributions of female codebreakers at Bletchley Park and Arlington Hall, and during the Cold War. Some excellent recent research concerns the impactful role that CIA analysts had in the search for Osama bin Laden after September 11th, and the vital intelligence female analysts and case officers such as Cynthia Storer, Barbara Sude, Gina Bennett, and Jennifer Matthews provided in the fight against al-Qaida. These successes show the impact that women bring to intelligence teams, and their contributions to mission success in a wide variety of analytic and operational roles.

Recently, there has been a dramatic improvement not only in the recognition of women as intelligence operators and analysts, but also their impact as leaders. These include the selection of a number of Agency Directors, including Gina Haspel, Director of the Central Intelligence Agency (CIA), Letitia "Tish" Long, the first woman to head a U.S. Intelligence Agency when selected as Director of the National Geospatial Intelligence Agency (NGA), and both the former and current Directors of National Intelligence, Avril Haines and Tulsi Gabbard. Other notable female leaders include Greta Bossenmaier, Canada's National Security and Intelligence Advisor, and in the United Kingdom, Anne Keast-Butler, the first female head of GCHQ, and Blaise Metreweli, the first female head of MI6. Recently, Major General Ann Lena Hallin was selected as the first female Director of Military Intelligence and Security in Sweden, and Michelle Johnson currently serves as the first female Deputy Chief of Staff for Operations and Intelligence at NATO Headquarters. These women have shown remarkable skill and leadership, rising through the ranks in traditionally male-dominated industries, and finding ways to "speak truth to power" on difficult issues such as foreign terrorism, hybrid threats, and complex and evolving geopolitical realities concerning security threats in Europe and beyond.

Unfortunately, many of these women also faced traditional obstacles against women in leadership; their progress reveals not the absence of barriers, but their ability to overcome them. In many Western agencies, the number of women working in intelligence agencies at entry and mid-career levels are roughly equivalent to the percentages of women in the workforce or society as a whole. However, this drops off dramatically at upper leadership levels, where women often make up only 10% of executive leadership. Most research indicates there is no single reason why women are underrepresented in senior leadership, but a series of related potential factors.

One CIA study identified three key ways in which women can be empowered for future intelligence leadership roles. First, the report found the importance of mentorship in developing potential future executive leaders among female employees. Secondly, they recommended current leaders work to align mission needs with employee goals in a more organized and deliberate manner. Finally, they recognized the importance of greater organizational and workplace flexibility, to help employees balance work/life decisions throughout their careers. These findings also mirror those from business and executive leadership studies, which have found the importance of mentorship in developing current and future female executive leaders and opportunities for leadership with greater work/life balance.

Intelligence operates at it strongest when it can example complex problems from a multifaceted perspective, incorporating as much strategic insight and experience into its perspectives. By finding ways to improve recruitment of intelligence leadership from a variety of roles and careers, building and improving professional mentorship, and finding opportunities to empower a broad variety of leadership perspectives from both men and women, the field of intelligence will be a stronger, more agile, and dynamic workforce best able to see the complex world of geostrategic problems from all multiple angles.

Jennifer A. Davis
Associate Professor, Intelligence Analysis
James Madison University
United States of America

Davi32ja@jmu.edu

NIKO MAKKONEN

Intelligence studies as a developer of intelligence and intelligence culture

Expert article • 3985

This article examines the role of intelligence studies in the development of national intelligence culture and state-level strategic intelligence. The two main theses presented in the article are: 1) intelligence studies can be purposefully used as a means to develop intelligence and intelligence culture, and 2) intelligence studies can utilize perspectives of science studies in this activity.

Intelligence and science have several similarities. The core task of both is to produce analyzed knowledge. In addition, science and intelligence, as concepts, refer to the activities in which this knowledge is generated and the institutional structures in which this activity takes place. Intelligence and science also have several differences. One of the most significant is the secrecy, which is a fundamental characteristic of intelligence. Also, the goals and methods often differ significantly. Therefore, intelligence is often considered more of an art than science.

The relationship between intelligence and science is multidimensional and partly problematic. Intelligence and scientific research can be each other's subjects, but they can also share same research objects. This relationship becomes even more complex in a framework that includes science studies and intelligence studies, which consider science and intelligence as their own research objects.

Intelligence studies approaches intelligence in a similar manner that science studies approaches science. This means that intelligence studies can be the subject of science studies. This kind of four-dimensional framework offers interesting perspectives for research. Among them, one can distinguish approach aimed specifically at developing intelligence and, more broadly, the entire intelligence culture. This approach known as instrumental approach emphasizes the practical benefits and utility of research activities. The importance of science studies and the philosophy of science for the development of science have been immense. Could intelligence studies do the same for intelligence and intelligence culture?

Research in intelligence studies can be divided into descriptive or normative research based on its nature. Descriptive intelligence studies can, for example, describe intelligence and intelligence culture, as well as their history and future. The normative research emphasizes the design science nature of intelligence studies. In general, the task of design science is to formulate technical norms, i.e. conditional recommendations and instructions for action.

As with intelligence itself, intelligence studies can aim to achieve a comparative advantage over opponents. In this case, the secrecy associated with the nature of intelligence is also strongly reflected in the nature and possibilities of intelligence studies. In this context, questions related to the ethics and morality of science become relevant. They are particularly emphasized in what intelligence studies aims to achieve and how its results are utilized.

Three examples of possible research goals and themes based on the main theses of the article are presented below:

1. One goal of intelligence studies can be to provide general public with public scientific knowledge about intelligence. By popularizing this knowledge, it can be further refined into a form that is more understandable and accessible to the general public. Scientific knowledge deepens civil society's understanding of intelligence and increases trust in it. This strengthens the national intelligence culture.
2. Science is characterized by being progressive. Progress can be viewed, for example, from a cognitive and institutional perspective. Instrumental science studies on intelligence studies can produce knowledge about how intelligence studies has developed as a tool for developing intelligence itself. The goal can also be to investigate means that promote intelligence studies. The fascination of this perspective is that a similar approach can be applied not only to intelligence studies but also to intelligence itself. How does intelligence progress, and how can it be promoted?
3. One of the tasks of intelligence studies can be to serve as a practical design science, which task is to produce scientific knowledge for conducting effective intelligence. Intelligence can then be seen as a skill that can be developed through intelligence studies. Design science produces recommendations and instructions for action. In intelligence studies, these may concern, for example, the use of intelligence as an instrument in state security policy or internal effectiveness of intelligence.

The changing international security situation highlights the importance of states' strategic intelligence and, more broadly, a strong intelligence culture. Academic intelligence studies can play a significant role in the development of intelligence and intelligence culture.

Niko Makkonen
Lieutenant Colonel
Finnish Defence Forces
Finland

GORDAN AKRAP

Strategic intelligence and education

Expert article • 3986

In the last ten years, there have been numerous discussions in the academic and professional community about how, in what way, and by what methods and means modern security challenges (hybrid threats including AI) can be most effectively countered. Ultimate goal of hybrid threats is to shape the information environment of the attacked audience; influence their cognitive processes and thus the decisions that are made. If the information attacker cannot influence the content of the decision that the target audience (TA) makes, the attacker will try to influence the timing of those decisions. Either to make decisions too early or too late. If attacker wants to be successful, must carefully monitor the entire process of managing the information environment as well as the results of its actions. The efficiency of the entire process is based on information, knowledge and intelligence. The better and more reliable the information collected, processed and delivered and delivered on time, the greater the chances that the target set in the attacker's plans will be better realized.

It can be concluded that in the gravitational centre of a hybrid attacker is intelligence. Depending on the level of goals set, it can be strategic, but also operational as well as tactical. It is important to note here that tactical intelligence can also achieve effective results in the strategic domain. A good example of this is the fact that Croatia managed to eavesdrop on the telephone communications of Serbian President Milošević by tactical means during the Croatia's Homeland War. This was for strategic decision-makers in Croatia from crucial importance. The intelligence we collected enabled an in-depth understanding of the content and manner of decision-making content and time on the aggressor's side and created the preconditions according to which Croatia, slowly but surely, began to achieve a state of information supremacy during the War.

Intelligence is upgraded knowledge. We recognize strategic intelligence as one of the key components of achieving a state of information supremacy. Better and deeper knowledge of the context of processes of the adversary (political, informational, military, cultural, social, economic, security, international) decrease the amount of intelligence that we need to understand the threat, and to be able to plan defensive and, if necessary, offensive countermeasures against a hybrid attacker. This brings us to the centre of this opinion. Given that in the gravitational centre of the attacker's plans, their realization, monitoring of effectiveness and making corrections is the intelligence, and response of the defence system, should be like that.

The starting points of defence activities are:

- the ability to acquire strategic intelligence that should indicate early warning signal, identify planners, authors and implementers;
- possible vectors of attack(s),
- the timing of the launch of one or more attack vectors;
- ways and models of increasing the effectiveness of the attacker's actions.

That brings us to education. How can we start new, or enrich existing, study programs with the study of Intelligence and Security Knowledge? How to reconcile the need to educate future experts for the needs of modern and future conflicts and wars with the need to adhere to the necessary levels of secrecy that the intelligence communities require?

Intelligence and Security studies should produce specialists who will:

- be without prejudices,
- know the doctrines, strategies, plans, intentions and abilities of the adversary and who will observe him through the lens of the adversary and not through his own lens,
- be able to read the information between the lines.
- be able to recognize and isolate the necessary and useful information content (signal) from the huge amount of available (dis)information (information noise),
- have the ability to think critically,
- be able to communicate with the power of arguments and not with the argument of power,
- be able to make decisions in situations of incomplete information security and under stress, learn from them, quickly identify possible errors and correct them,
- be able to actively collaborate with other experts at national and international level;
- not give in to the political correctness because political correctness is detrimental to the effective planning and operation of any defense system (it prevents the proper, accurate and reliable recognition of threats and the identification of their causes), and
- have the knowledge, will, time and ability to recognize and deal with the causes of security problems and not only with their consequences.

An analysis of conflicts and wars from the end of the last century to the present day clearly shows that no one will be able to win any conflict and war if remains alone. Without partners, friends, allies. Anyone who loses the ability to create and effectively use strategic intelligence, as well as those who do not constantly develop the existing educational programs and technology associated with it, will be an easier victim for a hybrid attacker. This will weaken not only its defense capabilities as well as societal resilience, but also those international associations of which that country is a member.

Gordan Akrap
Associate Professor, Vice Rector
Dr. Franjo Tuđman Defense and Security University
Zagreb
Croatia

Gordan.akrap@sois-ft.hr

TOBBE PETTERSON

Joint Nordic-Baltic intelligence research

Expert article • 3987

It is sometimes claimed that there is a gap between academic intelligence research and intelligence practice; that despite significant similarities between the two, there are fundamental differences that create a divide. The similarities are primarily methodological, the research process and the intelligence process are essentially the same, and concepts such as triangulation are accepted and important – while the major differences concern transparency and driving forces; in academia, openness is fundamental, while secrecy in intelligence practice is both necessary and part of the culture. The existence and significance of these differences are open to debate, but regardless of whether they are real or constructed, they have influenced how research is conducted, or not conducted, and how practice uses, or does not use, research to support operational activities. The full potential has simply not been realized in the same way as in other disciplines; compare with medicine, where research and clinical practice go hand in hand.

Academia-practice collaboration also varies between different countries; in the US and in the UK, there is a well-established organized collaboration, but in the Nordic and Baltic countries this is not as developed; although some collaboration does take place, it is more on an ad hoc basis. For example, there is academic intelligence education based on research at the universities of Jyväskylä and Lund as well as at the defense colleges and police academies in the region. At these, as well as at in-house research institutes, such as the research department at the Norwegian Intelligence School in Oslo, academic research is conducted that is at least partly relevant to practice. However, this is a fragmented field with a random relevance to practice rather than a response to real needs in the practice. Contributing to the fragmentation has been the need for an interdisciplinary approach to achieve intelligence relevance, something that requires coordination within academia, more than when a single scientific field is sufficient. In addition, the closed culture of the field has made it difficult for individual researchers to know how they could contribute to practice relevance. Nor have there been any structures on which to base cooperation, with the exception of the defense and police academies and various individual initiatives, such as the Intelligent Intelligence collaboration platform in Sweden and the Scandinavian Intelligence Hub network in Denmark.

Today the solution described above is obviously no longer sufficient. To meet societal challenges, there must be a better match between academic research and intelligence practice—the gap must be reduced, and a different more collaborative mindset must be created. It is likely that ways forward can begin to be built by both academia and practice working together to find relatively simple solutions to what may be perceived as a contradiction; for example, increased transparency while maintaining the need for confidentiality can be achieved through dual publication, where different types of reports for academia and practice based on the same results are created. Practice can also make it easier for individual researchers to find relevance, perhaps in the form of crash courses for researchers, where the practice and the challenges are presented.

For a small scientific field in a relatively small region such as the Nordic-Baltic region, more than just a change in mindset is required – a structure must be built. This both involves finding a research infrastructure that can handle sensitive information and some form of organizational structure – a joint research environment where researchers and practitioners from the various Nordic-Baltic countries can meet. One possibility is to look at the existing and previously mentioned collaboration initiatives in Sweden and Denmark; the former with a national focus, the latter with a Scandinavian. Could these serve as a role model for a larger Nordic-Baltic initiative? In order to make such a initiative effective, in addition to traditional joint research applications to, for example, the EU's Horizon program, it is likely that a division of labour will be necessary: Perhaps the path to success lies in carefully coordinating the contributions of different universities, with one taking primary responsibility for a practice relevant sub-area of intelligence research and another university for another. In the joint environment, ongoing research can then be discussed and results disseminated, and of course multinational research groups can play an important role.

Exactly how a joint Nordic-Baltic initiative should be created is open to discussion but given the security policy situation and the importance of intelligence activities for society, the most important thing is not to find a perfect solution from the outset, but to get the work started now.

Tobbe Petterson
PhD in Intelligence Analysis,
Head of Innovation
Swedish Armed Forces Intelligence and
Security Centre & Lund University
Sweden

SUVI HEINONEN

Seismology improves situational awareness

Expert article • 3988

Seismology is a branch of science that most people associate primarily with earthquakes. However, seismic waves are generated from a variety of sources beyond tectonic activity such as industrial accidents, mining operations, explosions, and traffic. Whatever might be the cause of seismic wave, it can be recorded by instruments called seismographs.

For decades, the international seismological community has played a key role in monitoring nuclear tests, particularly underground detonations. The physical characteristics of an explosion differ from those of a natural earthquake, which results from two blocks of the Earth's crust slipping past one another. In contrast, an explosion releases energy outward from a single point source. These differences in physics produce dissimilar seismic waveforms, allowing seismologist to distinguish between earthquakes and explosions.

A notable example of seismology's broader utility occurred on September 26, 2022, when an underwater explosion caused a gas leak in the Nord Stream pipeline near the Danish island of Bornholm. The first blast, at 02:03 Central European Time, was automatically detected and classified as a likely explosion by the Danish and Swedish national seismic networks within a minute. The same rapid detection applied to the second explosion at 19:03 UTC. These seismic waves traveled through the bedrock and were detected with seismographs thousands of kilometers from the source.

Seismographs are also recording explosions related to the war in Ukraine that Russia started 2022. In April 2025, the destruction of an ammunition depot in Russia's Vladimir region generated seismic events of magnitudes 3.4 and 3.2. Estimating the explosive yield from seismic magnitude is more complex for surface blasts, as much of the energy escapes into the atmosphere or contributes to fires rather than generating seismic waves traveling through bedrock. Nonetheless, seismological data provides reliable and uncompromised information about large explosions, offering a cost-effective and robust method for monitoring vast regions using civilian infrastructure that is nearly impossible to spoof or jam.

The Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) maintains a global network of stations capable of detecting seismic events larger than magnitude 4 anywhere in the world. For instance, North Korea's six nuclear tests between 2006 and 2017 were clearly recorded also in Finland by the FINES station, part of the CTBTO's International Monitoring System (IMS).

Russia withdrew its ratification of CTBT agreement in 2023 and in November 2025 Russia has floated the possibility of nuclear tests after US president comments on starting testing nuclear weapons. Geopolitical tension in Europe is apparent, and national and regional seismic networks provide additional valuable tools for real-time situational awareness. We need to work to ensure that our capacity to detect violation of CTBT is optimal both technically and in terms of communication and collaboration, both nationally and internationally, especially within NATO.

Traditionally, seismograph stations have been located on land but recent advances in fiber-optic sensing are revolutionizing the field. Laser pulses sent through standard telecommunication fiber-optic cables can detect changes in strain caused by seismic events. This technology enables monitoring along hundreds of kilometers of undersea cables with spatial resolutions down to a few meters. Detected strain changes may result from explosions, passing submarines, or even large marine animals. Fiber-optic seismology offers a promising tool for tracking strategically important activities, such as the movements of so-called "shadow fleets" in the Baltic Sea.

Planning seismic networks with a regional strategy—rather than within national silos—will enhance detection effectiveness regardless of main interest being on monitoring natural earthquakes or man-made explosions. For defense and civil authorities alike, seismic network forms a powerful tool to create accurate, real-time situational awareness across the Baltic region and information gained from these networks can support timely decision making. The existing seismic station network and related cutting-edge expertise can be utilized as part of overall security protocols of NATO countries.

Suvi Heinonen
Director, Institute of Seismology
University of Helsinki
Finland

OLLI-MATTI MIKKOLA

Energy transition as a strategic intelligence issue

Expert article • 3989

Energy has always played a central role in geopolitics - and will continue to do so in the future. The energy transition is a response to climate change, but the shift from fossil fuels to low-carbon and electrified societies also transforms geopolitical dynamics. The energy transition is reshaping the strategic landscape in such a way that intelligence analysis must adopt a new approach to energy-related issues to provide decision-makers with successful early warnings.

Global investment in clean energy is almost double that in fossil fuels. Natural resources, technological capabilities, and political will to either advance or hinder the change are reflected in states' geopolitical choices, which are driven by control over regions and resources. Fossil fuel-based geopolitics is now accompanied by the geopolitics of renewable energy.

The ideal of the energy transition is a gradual global phase-out of fossil fuels. In practice, not all states and governments are willing to do this voluntarily. Achieving global consensus on the timeline and order of the phase-out is challenging: which countries should lead the way, and for whom would it be economically or politically most feasible? This ambiguity makes the energy transition a complex geopolitical battleground.

Energy transition on the great powers' chessboard

China is the clear leader in renewable energy investments. China controls significant parts of the renewable energy value chains: the demand, ownership and refining of many critical raw materials are concentrated there. This gives China a significant competitive advantage and enables it to establish geoeconomic dependencies in various areas.

The United States' current policy relies on oil and gas, and President Trump opposes the green transition. However, internal power relations in the US may change, which could also alter attitudes toward the energy transition. In any case, the US' role as a major producer of fossil fuels does not support the decisive phase-out of fossil fuels.

Russia aims to prolong the fossil fuel era as long as possible, even though the long-term sustainability of its oil-revenue-based economic model is questionable. Its governance is built on power structures created by fossil energy. A potential decline in oil revenues poses a significant threat to the regime's future. However, Russia cannot avoid the impacts of climate change and environmental issues indefinitely.

The European Union invests significantly in clean energy, making it a key actor in the geopolitics of renewable energy. Russia's invasion of Ukraine was a catalyst for changes in the energy policy. The REPowerEU plan, published by the European Commission in 2022, promoted the adoption of renewable energy, diversified energy sources, and improved energy efficiency. However, a complete decoupling from Russian energy is still ongoing and some states inside the EU oppose the development.

New value chains create new dependencies

Unlike fossil energy, renewable energy can be produced to some extent in nearly every country. This allows states to diversify their energy sources and reduce dependence on fossil fuels. However, the adoption of renewable energy requires the use of critical minerals and rare earth elements, whose deposits and processing capacities are geographically concentrated. Thus, the geopolitical dimension of renewable energy is also built on dependencies – though under different drivers than in the fossil era.

As a result, new flows emerge between states in areas such as critical raw materials, hydrogen and clean technology expertise. Some states or regions may become more self-sufficient, but renewable energy value chains also create new dependencies that must be carefully identified. This transformation is reflected in changes in the routes and volume of trade and investment, as well as in potential geopolitical ambitions to control new areas and resources as seen in disputes about Eastern Ukraine or Greenland.

Towards new analytical frameworks

As states recalibrate their energy systems, the distribution of strategic resources, economic dependencies, and political influence will evolve in unpredictable ways. These dynamics demand that strategic intelligence analysis play a central role in guiding national security and foreign policy decisions.

Intelligence services must develop robust analytical frameworks to monitor how states' capabilities and intentions shift in response to energy-related changes. This includes defining precise indicators for multiple scenarios in which global power relations may be reconfigured. The ability to anticipate such shifts is essential for maintaining strategic stability and ensuring informed policy responses.

The energy transition becomes a basic element of strategic early warning taxonomy. It will shape threat perceptions, alliance structures, and economic resilience. Policymakers must therefore integrate energy foresight into intelligence processes to remain active in a rapidly changing global landscape.

Olli-Matti Mikkola
Senior Scientist, PhD
Natural Resources Institute Finland
Finland

OSSI KETTUNEN

Arctic tensions – can they be controlled?

Expert article • 3990

Tensions in the Arctics experienced a thaw when the Soviet Union collapsed. However, the interests of the great powers in the Arctics had nevertheless been preserved. As early as on 1992 Foreign Minister of Russia Andrei Kozyrev stated: *"The territory of the former Soviet Union cannot be considered a zone where CSCE norms would be fully applied. This is a post-imperial region where Russia must defend its interests by all possible means, including military and economic means."*

This serious message was also reflected in the Arctic when Russia drew up a military development program on 2009. Accordingly, it began to renew bases in the Arctic region, build new ones, and deploy the latest radar and missile equipment to bases on the shores of the Arctic Ocean. It also renewed its strategic forces: SSBN fleet, heavy surface ship units and developed new types of missiles. The U.S. recognized the lines of development and began to respond militarily to the changes. The volume of the exercises has increased in the Arctic and the U.S. has developed six new Multi Domain Task Force (MDTF) organizations, one of which was to be stationed in the Arctics. MTDF is the fire power unit and consists of HIMARS Battery, Mid-Range Capability Battery, Long Range Hypersonic Weapon Battery and sophisticated signal and intelligence companies and support units.

The U.S. brought the threat of China to the international political debate in 2019 in a speech given by Secretary of State Mike Pompeo in Rovaniemi, Finland, when he clearly stated China making a greater threat than Russia. The changed assessment was verified in the U.S. National Defense Doctrine in July 2024, which put China ahead of Russia in the defense policy program. The change also had an arctic dimension, on which Deputy Defense Secretary Kathleen Hicks made a statement: *"The Arctic region of the United States is critical to the defense of our homeland, the protection of U.S. national sovereignty and the preservation of our defense treaty commitments."*

China's strategic partnership with Russia has created a new, even more demanding need for military intelligence in the Arctic. China's entry there is nowadays viewed with suspicion and reservations, and its support for projects to strengthen Russia's infrastructure is being closely monitored. The strategic partnership and the war in Ukraine have increased the need for the U.S. to develop cooperation with the Arctic allies. Its manifestations include the re-ratification and conclusion of bilateral defense treaties (DCAs) with countries in the region. The implementation of the DCA has started already in Finland in August 2025 when the Ministries of Defense of the U.S. and Finland made arrangements for the construction procedure.

Strategically, the Arctic forms an important area for countering ballistic and cruise missiles launched by China and Russia. Regionally, it increasingly includes not only Alaska, Greenland and Canada, but also Norway, Sweden and Finland. Their inclusion gives NATO a new strategic advantage. The association of Finland and Sweden to NATO will provide an opportunity for a completely new missile defense structure and intelligence. The use of both manned and unmanned electronic reconnaissance aircrafts has increased. As an example, in September 2025 the large surveillance drone came from Sicily flying back and forth over Finland before it continued north across the border into Norway flying at high-altitude (53,000 feet) collecting vital data. In the Arctic, it also manifests itself in increased military exercises. Finland takes part in about a hundred international exercises of different levels and types each year. An example is the international exercise *Nordic Response 24* held in March 2024, in which a total of approximately 20,000 soldiers from 14 different countries participated.

The distribution of natural resources is becoming an increasingly important factor in the Arctic. The U.S. is dependent on special raw materials from China, which are needed especially in the electronics industry. Add to that China's ability to produce advanced military material 5-6 times faster than the U.S., the competitive situation is problematic for the U.S. A further problem arises from the slow opening of mining operations in the U.S., where it takes an average of 29 years to open a mine for production, which is the second slowest process in the world. Therefore, USA's desire to acquire mines that produce various rare materials is inevitable. This can be seen in USA's efforts to exploit natural resources of Greenland and Canada.

For Russia, European countries and the United States, the Arctic means a common future. The utilization of the region's natural resources will become current over the span created by global warming. The Arctic is part of the global economy and strategic goals. We have been able to resolve conflicts of interests in the region without armed conflict for decades. Are we ready to continue with these geopolitics? What does it require from the Arctic states? At least it is time for the wakeup call.

Ossi Kettunen
Colonel (ret), a member of the Finnish Society of Military Science
Finland

ossi.kettunen@gmail.com

TEEMU NAARAJÄRVI

The complexifying China challenge

Expert article • 3991

During the last decade, the China-policies of the EU and many of its member states have changed significantly. When in the mid-2010s China was still largely seen as an enormous economic opportunity, already in 2019 the EU defined it simultaneously as a partner, a competitor, and a systemic rival. After Russia's full-scale attack to Ukraine in February 2022 and China's increasingly apparent role as an enabler of Russia's military action, the relationship between China and countries supporting Ukraine have soured even more. But there are other aspects of China that have played a role in the shifting attitudes toward it. At the same time, cutting links to it is still off the table.

China has been conducting and continues to conduct espionage against other nations all over the world, also in the Northern Europe. While China itself denies any wrongdoing, there are enough both classified and public examples to prove the contrary. Moreover, China uses its intelligence apparatus not only to collect information, but to influence other nations and individuals in them.

While Chinese espionage is not a new phenomenon, in the last decade China has furthered its own legislation to strengthen the role of intelligence and security authorities both domestically and abroad. Several new laws have been formulated and even more existing laws amended to promote a comprehensive interpretation of national security. This has, for example, raised concerns of unwanted technological transfer to China in the forms of industrial and research cooperation.

At the same time, China continues to increase its geopolitical clout. While its goal is most likely not to become a superpower like the post-Cold War Unites States, it promotes its global interests increasingly assertively and is today only realistic challenger to the U.S. dominance in the world affairs. Combined with the Chinese de facto support of Russian war of aggression in Ukraine and the fact that so many countries seem to have no qualms with that speaks loudly of the changing world order and the role of China in that change.

China's biggest leverage internationally grows from its economic power. While it is the top exporter in the world, its domestic market is also massive and very attractive to foreign companies. Moreover, the dependence on the Chinese exports has increased all over the world. China knows this and uses both its exports as well as market access as political tools. Especially in the case of rare earth minerals the link between a given country's disposition to China and possibility to import coveted minerals is clear, and not new. For example, in 2010 China imposed restrictions on the export of rare earth minerals to Japan. While the move was later ruled to be in contradiction with the WTO rules, the signal was clear: China was both able and willing to use export restrictions to protect its own interests. In the latest occasion of this particular power, China informed the world of the new export restrictions in late 2025, a move forceful enough to push even the United States to look for a negotiated solution in its trade disagreement with China. While the Chinese screening mechanism for rare earth exports was delayed, the message was again heard all over the world. Moreover, the rare earth minerals are much more coveted on global scale today than 15 years ago.

Political considerations apply to Chinese foreign direct investments as well. In the mid-2010s the Chinese investments to Europe went largely to big European economies such as Germany, France, and the United Kingdom. Finland, too, was named as a major destination of the Chinese FDI, but while the figures were admittedly impressive, they were linked to very few individual deals, such as the sale of the online gaming company Supercell to Chinese Tencent with 8.4 billion euros in 2016. It was more or less at that time when the more critical discussion on the risks related to Chinese investments began in Europe, and it has continued to this day. Today, it is not only that Chinese investments to Europe are on lower level than in the past, but they are also distributed differently: for example, Hungarian automobile industry has become a major destination of Chinese FDI in Europe.

In conclusion, it is clear that in the context of China, countries as well as unions and alliances need to prepare themselves for a continuous balancing act between economic gains and security risks for the foreseeable future. While the economic cooperation with China is still necessary and lucrative, it is good to remember that it often comes with additional baggage.

Teemu Naarajärvi
PhD, Head of Strategic Analysis
Finnish Security and Intelligence Service
Finland

DHEERAJ PARAMESHA-CHAYA

Perils of India's 'intelligence-free' grand strategy

Expert article • 3992

As of this writing, India's relations with the United States have reached its lowest in the last couple of decades. This has surprised many who were bullish about Indo-US ties. The tariffs imposed by President Donald Trump on Indian imports, reasoning that India's buying of Russian oil is sustaining Moscow's war machine, are viewed by contemporary observers as undoing decades of diplomatic hard work on both sides. One of the key factors driving the relationship was the 'China' threat, which the present US-India animosity seems to have obscured, resulting in New Delhi trying to mend relations with Beijing. Although popular opinion tends to blame Trump's miscalculations for the current state of Indo-US affairs, an objective historical assessment reveals that no country has surprised and antagonised India as often as the United States. This article, therefore, argues that India's grand strategy requires a readjustment of its strategic intelligence priorities to lend it a degree of predictability in its foreign relations.

At the grand strategic level, India assumes a great power status and desires significant influence in global politics. Absent written documents, this strategy is largely reflective of its vast geography, large population, and a civilisational identity. There is, however, a fundamental disconnect between this strategic aspiration and its intelligence institutions. In fact, the roles of its national security institutions have never been articulated, leaving them merely responding to emerging crises. For instance, India's foreign intelligence organisation, the Research and Analysis Wing (R&AW) was created in 1968 only after the wars of 1962 and 1965 with China and Pakistan, respectively. Since then, agency has focused on India's immediate neighbourhood, primarily Pakistan and China, and the Indian Ocean Region. However, in achieving India's grand strategic objectives, it has been the US that has consistently been an impediment but has received no attention from India's foreign intelligence.

The list of US surprises to India's national security is indeed long. The earliest dates to 1954-55 when Pakistan entered the US led alliance systems. An alarmed Indian leadership directed the Intelligence Bureau, R&AW's predecessor, to monitor US arms sales to Pakistan and its impact on Pak defence capabilities. The next surprise came a decade later when US defence supplies to Pakistan provided the impetus for Pak's military adventurism in 1965. In 1971, the entry of the USS Enterprise into Bay of Bengal significantly altered New Delhi's thinking about the US' presence in the Indian Ocean, leading to a short-lived trilateral intelligence cooperation between India, France, and Iran. During the 1980s, the US' covert war in Afghanistan allowed Pakistan to sponsor terrorism in India whilst acquiring nuclear weapons – both ignored by Washington. All this while, India focused its intelligence capabilities only on Pakistan, instead of the US that was sustaining Pakistan's actions that were threatening regional security. Later, during the War on Terror, India trusted the US to be a reliable partner. Yet, when the 2008 Mumbai Attacks occurred, it was again betrayed by a lack of unequivocal support from the US and its English-speaking allies against Pakistan.

Beyond these episodes, there is a fundamental incompatibility between Indian and US grand strategies that has remained consistent since the 1950s. For instance, when India approached the US during the mid-1950s for food assistance, it was held to ransom by a demand for changes to India's foreign policy. Prime Minister Jawaharlal Nehru had refused to barter India's "self-respect or freedom of action" even for something it desperately needed. Where Washington's grand strategy was clearly a derivative of material power, India's grand strategy emerged from abstract notions of freedom and self-respect. Fast forward to the current crisis, and it is the US' penchant for coercion that is fundamentally at divergence with India's preference for self-respect and freedom of action. Therefore, the strategic orientation of the two countries makes 'surprise' an inbuilt feature in their bilateral relations. This realisation has seeped well into India's counterintelligence logic. Consequently, India's nuclear tests were well shielded from US intelligence coverage; and American spies operating in India have been regularly targeted and neutralised. The same consciousness, however, has not extended to India's foreign intelligence. Hence, moving forward, India must recognise that achieving its grand strategy requires not only partnering with the US, but also truly 'knowing' it. The latter requires India to transform its intelligence-free grand strategy to one that reorients its foreign intelligence to the right targets.

Dheeraj Paramesha-Chaya
Lecturer in Intelligence
School of Criminology, Politics, and Law
University of Hull
UK

SAJAL KABIRAJ

Asian science espionage in Europe: Is it a narrative or wake-up call?

Expert article • 3993

Scientific Espionage is defined as the act of using scientific personnel, exchange researchers, and dual appointments, as well as technology, to obtain information and expertise about the plans, future innovation and activities especially of a foreign nation or a competing company, usually through illegal means. The primary aim of scientific espionage on behalf of foreign states is to acquire information in order to be a step ahead in terms of knowledge or to fill existing research gaps in knowledge with the aim to compete for profits.

A 2023 report published by Bundesamt für Verfassungsschutz has outlined preventive steps which can be implemented to mitigate risks of non-approved outflow of scientific flow of data, information, and expertise. The report assumes that institutions of higher education and scientific research institutions in Germany can probably be at the risk of espionage activities using various techniques to gain access to privileged data, expertise and unauthorised information. Methods for science espionage are ever evolving in the age of Artificial Intelligence (AI). The various methods for science espionage includes both explicit and implicit methods. The focus is more on acquiring explicit scientific knowledge as it can be easily conceptualized, formalized, codified and prototyped for usage and adaptation in different scenarios. European institutions must also evolve, placing purpose at the core of research and scientific discovery and use AI tools to enhance learning through structured social learning and human interaction. Embracing AI for combating enhanced cybersecurity threats of espionage requires training of European scientific personnel in the use of AI and Big data and Networks of Cybersecurity. The EU general data protection regulation (GDPR) is a good initiative in this regard. There is also a need for inculcating values and respecting security protocols and the message should be clearly conveyed to the partners, who often don't seem to understand the norms due to lack of familiarization with rules based systems in Europe. Orientation weeks explaining the details to visiting researchers and scientists at the beginning of the co-operation could go a long way to deter practices unacceptable in Europe. At the same time, scientific personnel must deter themselves from honey pot attractions and should not fall prey to lure and lust.

Scientific espionage in the long term poses a threat to Europe and its dominance as an economic and scientific player. Trust and confidence building measures in joint scientific could go a long way in preventing IP theft, loss of patents, image and profit. Bild, the German tabloid newspaper recently reported that Volkswagen might be forced to halt production at key plants soon due to a shortage of semiconductors following the Dutch government's seizure of chipmaker Nexperia. The Netherlands cited risks to EU's technological security, prompting Beijing to retaliate by banning exports of Nexperia chips from China. Rare earth metals, tariffs, supply chain disruptions, geo-political tensions, are current concerns that face the semiconductor supply chain. Narratives set by the West for the East, especially models and assumptions need to be adjusted at the scholarly research level so that industrial manufacturing and jobs are not impacted. This is a question of many for the complexities involved in understanding scientific espionage which can lead to a catastrophic situation.

China's phenomenal rise can be attributed as a result of structural reforms leading to innovation, discovery, speed of deployment and agility. It represents a tectonic shift in knowledge acquisition as a national culture to progress. China is setting global milestones in chemistry, AI, material sciences through gradual capacity building and research ecosystem in universities.

Scientific innovation in Asia comes from looking outside the box, and sometimes from looking deeper inside it. While some broad inventive ideas might be borrowed from Europe, it necessarily cannot be termed as scientific espionage. Dynamic tidal lanes in Beijing are changing the way traffic flows by adjusting direction based on traffic demand, easing congestion during peak hours. It is an example of innovation merged with practicality of lean thinking. Europe Innovates, Asia Imitates seems like a forgone narrative. In AI and Smart Cities, companies like SenseTime and IFLYTEK have succeeded in integrating vision, speech, and data into daily life from education to traffic flows.

Europe values process, ethics, branding and planning, while Asia values iteration, speed, experimentation and agility. Scientific espionage can be avoided by willing to learn from each other, co-operate and compete based on principles of mutual respect and trust.

Sajal Kabiraj
Dr., Principal Lecturer of Strategy
Faculty of Business and Hospitality Management
LAB University of Applied Sciences
Lahti
Finland

RYAN SHAFFER

Learning intelligence from Africa: Insights from the Nigerian intelligence literature

Expert article • 3994

African intelligence studies literature is an important and growing body of work that should be studied by scholars throughout the world. Though Africa appears to be establishing intelligence studies programs recently compared to Europe and North America, this should not imply African intelligence studies lacks rigor, capability and insight. For decades, scholarship about Africa has repeatedly highlighted and acknowledged the complexity and advances in Africa, perhaps notably with Basil Davidson's (1914–2010) landmark The African Genius. Similarly, this article argues for understanding African intelligence studies literature on its own terms and objectives. While intelligence studies education in Africa is not without deficiencies, it has proved useful and is important to study its contributions. Indeed, there are important issues and lessons learned in the existing African intelligence literature that make useful additions to the international scholarship.

There is no reason to believe African intelligence officers lack skills, experience and knowledge of their craft. With over fifty countries and hundreds of intelligence and security services throughout the continent, the services consistently counter attacks and national security threats. No doubt, these institutions face challenges in the professionalisation of intelligence which have been noted by scholars, such as Dalene Duvenage. Additionally, while some African intelligence officers engage in human rights abuses to support dictatorial governments, others work daily in challenging conditions to thwart espionage, sabotage, terrorism and other national security threats that pose direct threats to life and liberty in African societies. This article seeks to understand African intelligence by looking at published works from African intelligence officers of various positions and ranks. To do this, the article will use Nigeria as a case study. This approach allows the reader to better understand the intelligence studies literature in one country rather than make generalizations about a region or all of Africa.

Drawing from published books by Nigerian intelligence officers, this article demonstrates the insightfulness of African intelligence professionals who describe capabilities, strategic planning and frameworks. Though the literature maybe challenging for scholars in Europe and North America to obtain due to the localized distribution networks of the books, there is no lack of informative writing from Nigerian intelligence officers. There are political and civil liberties restrictions in Nigeria, as Freedom House has assessed, which impacts how and what authors write about. Nonetheless, these books take approaches and make conclusions that contribute to the international intelligence studies scholarship.

Intelligence literature in Nigeria

Nigeria's National Institute for Security Studies (NISS), located in the capital, Abuja, is one of the more notable organizations in the country that publishes intelligence studies scholarship. It was founded in 1999 as a training school before becoming the Institute for Security Studies in 2008. By 2019, it became known as the NISS and describes itself as the 'foremost security training institute in Nigeria' which 'prepares high-level security intelligence professionals, as well as senior level managers for critical roles in the sustenance of national security.' Beyond offering classes for security professional leaders, the NISS publishes a journal and books devoted to intelligence and security studies topics. Currently, the institute is headed by Afakriya Gadzama, a former head of Nigeria's internal intelligence service, the Department of State Services (DSS) from 2007 to 2010.

The NISS is not the only educational Nigerian institution devoted to intelligence and security. For example, Nigeria's National Defence Academy established the Department of Intelligence and Security Science in 2019 with the mission 'to prepare students for the analytic, operational, research, and investigative intelligence process within the federal government.' Such programs aim to give intelligence and security officers a foundation for executing their work with elements of critical thinking, history, law, ethics and security knowledge.

This article draws from books published by the NISS as well as other publishers. These books describe the capabilities, frameworks and approaches taken by Nigerian intelligence officers, reflecting the country's intelligence culture. In doing so, this article demonstrates elements of professionalism, adaptability and reform throughout different periods of Nigerian intelligence.

Intelligence Literature by working-level officers

Intelligence officers in Nigeria publish different types of books for varying purposes ranging from memoir to a compilation of essays about their craft for other professionals. Farida Waziri's 2019 memoir, One Step Ahead, details her life, including work in the Special Branch (which later became the National Security Organization then the DSS) from training to intelligence collection. She described her tasks as attending public meetings to write reports about 'inciting statements and voices critical of the government' (p. 28). Waziri, who later served as chair of Nigeria's Economic and Financial Crimes Commission from 2008 to 2011, also notes how 'credible intelligence is expensive' and how intelligence collection during the 1970s was 'professionally executed' (p. 29).

Taking a different approach, Stan Olu Azodoh's 2023 monograph about information and communication technology security issues in Nigeria draws from his work as an intelligence practitioner in DSS. He notes that Nigeria has made only limited investment in technology, and the country is susceptible to cyber threats, including online security breaches. He highlights the importance of encryption and describes Nigeria's use of very-small-aperture terminals (VSAT) as an improvement in the country's information security. He notes the DSS is one agency that uses it because VSAT 'is excellent security against unauthorized access' and its transmissions 'can be scrambled,' making access 'virtually impossible without authorization' (p. 83).

Likewise, retired DSS officer Raymond Nkemdirim's 2022 collection of essays on intelligence highlights Nigeria-specific issues. As far as intelligence advancements, he explains Nigeria's 'massive acquisition of state-of-the-art technical intelligence (TECHINT) equipment' has 'ensured that' Boko Haram has been 'infiltrated' (p. 31). He also discusses Nigeria's employment of psychological operations (PSYOPS), which 'proved an effective tool in de-radicalisation and perception management operations of Nigeria's intelligence services' (p. 192).

Intelligence literature by leaders

The NISS' books are a useful forum for current and former Nigerian intelligence leaders to discuss ongoing issues and past events. Some of the books are compiled from papers written during NISS courses and the resulting publications are used to educate future Nigerian intelligence leaders. Of note, in 2022 the NISS published the anthology, Manning The Gates, which was edited by Adegboyega A. Karim and Amadu Sesay and written to honour Yusuf Magaji Bichi, head of the DSS from 2018 to 2024. One author, Brown Ekwoaba–former DSS head of training and staff development–details the significance of training and retraining by looking at training requirements of the service and highlighting different training frameworks and capabilities taught in hundreds of seminars, workshops and courses for over 4,000 intelligence officers.

Whereas, Inemesit Emmanuel–former DSS director of intelligence–describes the need to shift ways of thinking about intelligence in light of the information revolution and concludes that the skillsets used 'for counter-intelligence operations two decades ago have become obsolete' (p. 394). He further notes the importance of academic education for intelligence assessments, having analysts who are 'voracious readers of books on all subjects under the sun' and having a special unit to utilise artificial intelligence in Nigeria's intelligence community (p. 395). As for intelligence operations, G.B. Eteng–former DSS director of operations–notes the importance of utilising emerging technology and describes how the security services must broadly consider future threats shaped by decreased national revenue, increased unemployment and diminished agricultural output.

Similarly, the NISS published The Nigerian Economy and National Security, edited by Augustine Ikelegbe, Abdulwahab Muhammad-Wali and Adegboyega A. Karim, in 2015 and re-released in 2022. A chapter by Yusuf Magaji Bichi provides strategies for countering national security challenges with attention to identifying, understanding particular motivations of nefarious actors and combating the threats. He notes, for example, the importance of intelligence-led operations that employ the requisite methods and technologies to gain insight into an actors' intentions and plans. Likewise, Inemesit Emmanuel describes how intelligence is a 'major input' in policy formulation and highlights the different ways the DSS informs policymakers through daily reports, national threat outlooks, position papers, opinion polling and numerous other methods (p. 267).

Whereas, the NISS' predecessor organisation published Security Sector Synergy in Nigeria, edited by Linus N. Asiegbu and Adegboyega A. Karim, in 2013 and was reprinted in 2022. The anthology was the outgrowth of papers presented by senior intelligence leaders during the institute's Executive Intelligence Management Course. E.E Ita–then Director-General of the DSS–writes about the need for the security sector to evolve and adapt, calling for reforms that include developing a national security framework, increasing civil society participation in security sector reform and having good governance. Likewise, Folashade Adekaiyaoja, then DSS assistant director of the training directorate, discusses the importance of reform and innovation, but notes how 'communication' is key to change because 'success is unlikely to be attained if the reforms are not shaped and embraced by all stakeholders' (p. 54).

In a 2023 anthology published by NISS titled Strategic Leadership and National Security in Nigeria, Harry Erin–commander of the Economic and Financial Crimes Commission–explains that terrorist groups in Nigeria, like Boko Haram, received financial support from internal and external sources and the Nigerian government developed regulatory laws to counter this, but a multitude of factors including slow prosecutions stymied efforts. Also looking at capacity building, Kehinde Ayoola–DSS' director of technical services–calls for integrating artificial intelligence into the Nigeria's National Security Strategy and utilising it for surveillance and analysis among other issues. Additionally, Alfred Tussy Obajemu–Defence Intelligence Agency deputy director–discusses military intelligence, describing specific intelligence cells to support operations and Nigeria's defence attaché system that 'is involved in strategic intelligence collections' (p. 542).

Taking a different approach, Contemporary Security Challenges in Nigeria–a 2021 NISS anthology edited by Adegboyega Adebayo Karim, Amadu Sesay and Saleh Dauda–explores Nigeria-specific challenges by offering security assessments and recommendations. The book was written in honour of Afakirya Aduwa Gadzama, who served as Director-General of the DSS from 2007 to 2010 and worked in the agency for thirty-five years. Kabiru Sani–former DSS director of intelligence–describes how the DSS counters threats through building criminal profiles in databases to track security concerns, provides intelligence directly to consumers, neutralises subversive organisations and has liaison programmes with other agencies. Similarly, Abdullai Abba Adams–the director of State Director of Security in Gombe–describes Nigeria's response to Boko Haram with kinetic and non-kinetic responses, which includes reducing the risk of radicalisation and mitigating the risk of terrorist attacks. Additionally, Inemesit Emmanuel discusses the importance of intelligence coordination with other African countries and suggests it can be improved with better planning, capacity and demarcation of responsibilities and roles.

Conclusion

This article highlighted African intelligence professionals discussing their craft. In particular, it reviewed Nigerian intelligence officers' perspectives by looking at their descriptions about their services, work, challenges and capabilities. In doing so, it explained how Nigerian officers describe professionalism, adaptation and reform to briefly shed light on Nigerian intelligence on its own terms. One important issue that was not analysed here, but needs noted is the human rights abuses committed that have been reported by non-government organisations like Amnesty International. There is a dearth of information about abuses in the current literature from Nigeria by security service professionals, which is an important topic that needs to be written about and addressed. Nonetheless, this article has demonstrated how intelligence studies is an emerging academic field in Africa and that international scholars can learn from the emerging publicly available literature. Deeper collaboration with and incorporation of African intelligence scholars in North American and European intelligence studies literature will benefit the international academic community.

[1] Awwal Isa, *Engaging the Academy to Improve Professionalism in Nigeria's Intelligence Community*, PhD dissertation (University of Buckingham, 2014), 100.
[2] Dalene Duvenage, 'The Professionalisation of Intelligence in Africa,' in *Contemporary Intelligence in Africa* ed. Tshepo Gwatiwa (New York: Routledge, 2024), 187–205.
[3] For a review article on Nigerian intelligence-related books published by the NISS, see: Ryan Shaffer, 'Nigerian perspectives on intelligence and national security,' *Intelligence and National Security* 40, no. 04 (2025): 782–791. For examples of the scholarship in general, see: Tshepo Gwatiwa ed., *Contemporary Intelligence in Africa* (New York: Routledge, 2024); Ryan Shaffer ed., *African Intelligence Services: Early Postcolonial and Contemporary Challenges* (Lanham: Rowman and Littlefield, 2021); Ryan Shaffer ed., *The Handbook of African Intelligence Cultures* (Lanham: Rowman and Littlefield, 2023).
[4] 'Nigeria,' Freedom House, 2025. https://freedomhouse.org/country/nigeria
[5] 'Nigeria's Foremost Security Institute,' National Institute for Security Studies, 2022. https://web.archive.org/web/20220219025503/https://nissnigeria.gov.ng/about
[6] 'Department of Intelligence and Security Science,' Nigerian Defence Academy, 2025. https://nda.edu.ng/department-of-intelligence-and-security-science/
[7] Farida Waziri, *One Step Ahead: Life as a Spy, Detective and Anti-Graft Czar* (Burlington, NJ: Webcza, 2019).
[8] S.O. Azodoh, *Emerging Information and Communication Technology (ICT) Threats and Nigeria's National Security: A Practitioner's Perspective* (N.p.: NIRPRI, 2023), xvi.
[9] Raymond Nkemdirim, *Nigerian Security Challenges: A Compendium of Selected Intelligence* Essays (N.p.: Floris Global Multiventures Ltd, 2022).
[10] Adegboyega A. Karim and Amadu Sesay eds., *Manning The Gates: Essays in Honour of Yusuf Magaji Bichi* (Abuja: National Institute for Security Studies, 2022).
[11] Augustine Ikelegbe, Abdulwahab Muhammad-Wali and Adegboyega A. Karim eds., *The Nigerian Economy and National Security: Challenges and Prospects for Sustainable Security and Development* (Abuja: National Institute for Security Studies, 2015, 2022 reprint).
[12] Linus N. Asiegbu and Adegboyega A. Karim eds., *Security Sector Synergy in Nigeria* (Abuja: Institute for Security Studies, 2013, 2022 reprint).
[13] Adegboyega A. Karim and Mohammed B. Umar eds., *Strategic Leadership and National Security in Nigeria*: Essays in Honour of A.S. Adeleke (Abuja: National Institute for Security Studies, 2023), 301.
[14] Adegboyega Adebayo Karim, Amadu Sesay and Saleh Dauda eds., *Contemporary Security Challenges in Nigeria: Perspective on Peace Stability and Sustainable Development: Essays in Honour of Afakirya Aduwa Gadzama* (Abuja: National Institute for Security Studies, 2021).

Ryan Shaffer
Co-Editor
Global Change, Peace and Security
United States

MARKKU PAJUNIEMI

The Baltic Sea – A sea of war and peace

Expert article • 3995

Throughout history, the Baltic Sea has undeniably been of greater geopolitical importance than its size, and it remains at the heart of European security policy. The Baltic Sea has al-ways been a channel, not only for trade, but also for cooperation and cultural exchange. On the other hand, it is also a scene of competition, power struggles and conflicts. During Czar Peter the Great's time in the 18th century, the establishment of the city of St. Petersburg changed the strategic position of the Baltic Sea and especially the Gulf of Finland. The city was founded, not only as "Russia's window to the West", but also to challenge the position of Sweden, a rival superpower at that time. Stalin, on the other hand, once said: "The Baltic Sea is a bottle, but we don't have its cap." According to this reasoning, the Baltic Sea is an area where Russia is vulnerable to external influencing. After a period of brief openness following the collapse of the Soviet Union, the current Russian leadership has chosen to close the windows, and in the present geopolitical situation, the Baltic Sea is once again a sea of tensions.

The economic and political importance of the Baltic Sea to the eight NATO countries along its coasts is indisputable. While Russia, despite the significance of the Baltic Sea, al-so has the possibility of compensatory transport arrangements, a free access to the sea plays a crucial role especially for Finland, which is practically completely dependent on sea traf-fic. Thus, Finland and Sweden's NATO memberships will further increase the strategic im-portance of the Baltic Sea, also from the Alliance's perspective.

A considerable part of Russia's foreign trade and energy transport continues to pass through the Baltic Sea. In 2024, for example, the volume of oil transported through the Koivisto oil harbour in the Karelian Isthmus was equivalent to about one fifth of the total oil exports by Russia. Russia does neither have the capacity to store crude oil, nor, at least for the time being, enough capacity and infrastructure to transport it to the Asian market by land. From the Russian point of view, the importance of the Baltic Sea is emphasised, not only from the economic point of view, but also for the Kaliningrad enclave and St. Petersburg area. While NATO as a defence alliance does not in reality pose any threat to Russia, in the rhetoric of the Russian leadership, protecting St. Petersburg and Kaliningrad from the im-agined military threat of the West is central.

The confrontation between Russia and the West in the Baltic Sea region has escalated as the war in Ukraine continues. The war in Ukraine reflects in the Baltic Sea in increased military tensions, drone strikes and countermeasures, airspace violations and ambiguous activities of the Russian shadow fleet. NATO's deterrence to Russia's open use of military force is credible. However, Russia's means of hybrid influencing are versatile and it ex-ploits the opportunities that open up opportunistically to question the credibility of NATO.

The importance of data cables and energy infrastructure at the bottom of the Baltic Sea has been emphasised, especially for Finland and the Baltic states. At the same time, the risk of them becoming targets of external influencing has increased significantly. Attributing any damage to a specific actor is difficult. Russia's ability to utilise vessels in the Baltic Sea region as a tool for hybrid influencing remains considerable.

The presence of the Russian Navy and its measures to protect the undisturbed passage of its shadow fleet vessels will continue in the Baltic Sea. Russia has shown its readiness to ag-gressively intervene in Western attempts to control its shadow fleet's vessels, for example in connection with ship inspections. Russia's stronger action, combined with the varying condition of the vessels, the expertise of the crews and the large-scale disruption of posi-tioning systems increase the risk of an intentional or unintentional collision between Russia and the West. Russia's actions show a disregard for the damage caused to neighbouring countries. Russia also seeks to politicise the events and blame the West. At the same time, Russia's actions will force NATO to react, and it is likely that Russia's is also testing NATO's deterrence and unity.

The significance of the Baltic Sea both for the West and for Russia will remain considera-ble. The question is, however, whether the Russian leadership will at some point be ready to open the windows to Europe again. For the time being, even a slight opening of the win-dows seems unlikely. At least in the short term, relations between Russia and the West con-tinue deteriorating in the Baltic Sea region, regardless of the development of the war in Ukraine. This underlines the importance of up-to-date and high-quality intelligence analy-sis, where close cooperation between the NATO countries of the Baltic Sea region plays a key role.

Markku Pajuniemi
Colonel, Director
Finnish Defence Intelligence Agency (FDIA)
Finland

RT HON CHARLES CLARKE

Current intelligence challenges in the Baltic

Expert article • 3996

The current threatening and turbulent geopolitical situation heightens the need for strong mechanisms to acquire and assess intelligence. This needs to accurately inform governments about the challenges and potential challenges that they face and so advise them about how best to meet them.

This need, which is always there, has been exacerbated by the fundamental changes that have taken place in the last 15 or 20 years and have undermined the relative stability which had otherwise existed in Europe since 1945.

The Baltic Sea has of course often been a theatre of intelligence and counterintelligence conflict, notably during the Cold War but also before that, notably during the period of the Russian Revolution.

But the challenges now are greater, and I suggest here the five important overlying current intelligence tasks and suggest that targeting and properly assessing these fields should be the immediate priority for such work.

First of all, we need to develop the capacity to understand Russia much better than we do at the moment. Russia and its actions were much better understood just a decade or so ago, and insight has declined. That includes in regard to the current intentions of the leadership regime and any possible changes to it. Speculation is always rife about Putin himself, including his intentions, the influences upon him, his health and the effectiveness of his command over his government.

Such guesswork becomes even more extravagant when considering possible processes by which he might leave office and which individual or individuals might replace him and what are their attitudes. There is now an enormous hole in our understanding of these dynamics. This has deepened as a result of the increased isolation of Russia including from its neighbouring countries in the Baltic Sea region. We need to fill the hole in order to achieve greater predictability but that requires a lot of work.

Second, we need to understand properly current Russian military doctrine and its evolution. This is particularly important in the field of nuclear weapons and their location and possible use. But it also extends to the deployment of non-nuclear forces, land, sea and air, associated as they are with perceived threats to Baltic Sea region countries. Both Kaliningrad and the Saint Petersburg area are particularly important geographical spaces whose significance in contemporary Russian military doctrine needs to be better understood.

At sea we should understand better the significance of, and threats to, undersea communications of a variety of different types, and, on the surface, the operation of the 'dark fleet'.

The third need is to better understand Russia's significant regional military ally, Belarus. The leadership of Lukashenko, whose attitude to the Russian leadership is flexible and self-interested, always puts the stability and actions of the country into question.

Fourth we need to better assess the capacity of Russia to mobilise Russian speaking populations to support Russian foreign policy and military ambitions.

Russia uses 'hybrid warfare' to exploit ethnic and linguistic identity fault lines and weaken state legitimacy. It seeks to lay the groundwork for 'humanitarian intervention' narratives, such as those used in Crimea and Donbas.

The main techniques – designed to engineer tensions - include 'protecting minorities', amplifying their diaspora by supporting and recruiting various religious, cultural and community NGOs linked to Russia. They also try to instrumentalize migration, for example at the Lithuanian and Latvian borders and to co-ordinate 'grey-zone' activities such as cyber-attacks on municipalities as well as inflammatory pranks and falsified incidents, such as vandalism of Soviet-era monuments,

It remains very important to wind the substantial work which has already been done into an appreciation of Russia's overall approach.

And finally, we need better to understand the capacities and intentions of other major world forces, notably the United States and China, to engage effectively in the Baltic Sea region. This applies both from the point of view of deterring possible conflict in the region and of establishing what engagement, if any, might take place in the event of conflict.

There are many mechanisms for acquiring intelligence in each of these five intelligence fields and some Baltic Sea countries are already doing effective work. However, it's important to focus resources on each of these challenges and there are enormous benefits in coordinating intelligence activities across the Baltic Sea region to maximise the impact of the good work which needs to be done.

These important intelligence challenges in the Baltic Sea region urgently need attention. They are very difficult to address but address them we must.

Rt Hon Charles Clarke
UK Home Secretary 2004-2006
Baltic Geopolitics Programme
Cambridge University
United Kingdom

charlesclarke2109@gmail.com

BENJAMIN L. SCHMITT

The Baltic Rim Economies must lead the global response to "Underwater Mayhem"

Expert article • 3997

Since the onset of Russia's full-scale invasion of Ukraine in February 2022, a multitude of foreign policy and national security assumptions about the post-Cold War landscape have been shattered. Over the years, many of these assumptions resulted in a calcification of the parameter space considered for geopolitical and diplomatic policy planning across the Transatlantic community. For example, in the European energy security sphere, the two-decades leading up to Russia's renewed 2022 aggression against Ukraine saw a focus on the diversification of European energy infrastructure and supplies away from overdependence on the Russian Federation, while regulatory and legal policy aimed to erode Moscow's monopolistic practices in the European energy sector.

However, the relative level of peace across the Transatlantic community over these decades resulted in a deprioritization of focus on one of the most fundamental of all energy security threats to the region: physical sabotage of energy and critical infrastructure. Policies, technologies, and infrastructure deployment plans to deter the physical targeting and damage of energy and related critical infrastructure by malign actors, both onshore and offshore, atrophied over these years, though the threat has been a historic one.

Attempts to disrupt military communications infrastructure predate the modern era, with examples including the deliberate destruction of coastal or inland semaphore (or optical telegraph) towers during the Napoleonic wars, among other conflicts of the era. The construction of subsea telecommunications and energy connections have served strategic purposes since the mid-nineteenth century and concerns over sabotage have been a hallmark of military planners. These include concerns over cutting subsea telegraph lines that began to be introduced in European waters in the mid-1800s, as well as potential disruption of early subsea hydrocarbon pipelines, such as those developed during the Allied-liberation of Europe following the D-Day landings under Operation PLUTO (Pipeline Under the Ocean). The distributed nature of subsea pipelines and cables has traditionally made these installations difficult to comprehensively defend, and even with the advancement of technological monitoring and geospatial imagers in recent years, they are hardly immune from attack.

Since 2022, northern Europe and the Baltic Sea region have been at the epicenter of a growing threat vector – the deliberate damage of subsea hydrocarbon pipelines, electricity cables, and telecommunications links, which have driven concerns about the security of this offshore infrastructure in a region increasingly targeted by Russians sabotage operations.

In the onshore environment over this period, there have been dozens of sabotage attacks that have been investigated and attributed by national authorities around the Baltic Sea to Russian actors or non-Russian nationals recruited over social media platforms like Telegram to conduct operations to damage critical installations from rail lines, to telecommunications installations, to arson against logistical hubs used to supply Ukraine with defensive weapons. The same cannot be said about the maritime environment across Northern Europe, where the list of incidents involving the likely deliberate damage of subsea critical infrastructure has continued to grow, while attributions against any actor have remained scarce.

Given this reality, a University of Pennsylvania-backed research project – UNDERWATER MAYHEM – was launched in 2023, with the intent to perform an academic investigation of these incidents – a majority of which have taken place in the Baltic Sea itself – using open-source intelligence (OSINT) gathering methods. The objective of the study has been twofold. First, to perform an open-source investigation into the pathologies of these subsea attacks to analyze commonalities and potential trends that can be made available for policymakers and the public to better understand the threat environment and to mount policy actions to deter future incidents like these. Moreover, the study aims to assess the extent to which OSINT tools like commercial multiwavelength satellite data, open-source maritime tracking software platforms, and related open-source industrial databases, can be combined with a wide array of interviews with practitioners of national security policy, experts, and subsea military and industrial operations (e.g. professional and naval divers) to properly characterize potential offshore sabotage events.

A first research report under this project- UNDERWATER MAYHEM (Vol 01) – was published in May 2025 and focused on deep-dive case studies related to the January 2022 cutting of one-of-two of the subsea fiber optic cables linking the Norwegian archipelago of Svalbard with the Norwegian mainland in the Barents Sea, as well as the September 2022 Nord Stream gas pipeline sabotage concentrated at two sites northeast and southeast of the Danish island of Bornholm in the western Baltic Sea.

Additional case studies will be presented in a forthcoming report – UNDERWATER MAYHEM (Vol 02) – slated for publication in 2026, with case studies including a focus on the October 2023 Balticconnector gas pipeline damage (and nearby subsea telecommunications cable cuts), the November 2024 cutting of the Finland-to-Germany C-Lion1 and Sweden-to-Lithuania BCS seabed telecommunications cables, and the December 2025 subsea cutting of the Finland-to-Estonia Estlink2 electricity line and a number of adjacent telecommunications cables – each reportedly by extended anchor drags by nominally civilian ships.

The volume will furthermore probe similar incidents that have taken place in the Taiwan strait region, including the February 2023 cutting of subsea telecommunications cables connecting Taiwan to the Taiwanese Matsu islands, the January 2025 cutting of the Trans-Pacific Express telecommunications cable connecting Taiwan to the United States, Republic of Korea, and Japan, and the February 2025 cutting of a telecommunications cable connecting mainland Taiwan to the Taiwanese Penghu islands. Furthermore, related concerns with the Russian Federation's seismic exploration for oil and gas within Antarctic waters – a prohibited activity under the Antarctic Treaty System – round out the study.

As the research project continues, a number of trends are already apparent, and Baltic Sea littoral states can lead the way to deter these incidents even beyond existing prudent response actions like NATO's Operation Baltic Sentry, which was launched in January 2025 to focus on deterrence against further attacks against subsea infrastructure in the region. Just some of the actions that Baltic Sea states can take to further secure offshore critical infrastructure include: invoking NATO's Article 04 collective consultation mechanism for incidents that are able to be attributed to Russia or Russia-recruited actors (or other malign actors); increasing cross-competency coordination between public and private entities for European energy and critical infrastructure protection in the maritime space; taking steps to support the wider development and coordination of OSINT monitoring technology hardware and data analysis tools to increase the likelihood of rapid attribution against malign offshore actors; and to increase plans for strategic communications to combat disinformation campaigns that have often emanated from Russian sources following sabotage incidents.

The Baltic Sea remains a technically challenging maritime environment to protect offshore infrastructure. Therefore, a continued reorientation by policymakers to focus on physical sabotage deterrence as a principal policy objective under energy and critical infrastructure plans is merited. Not only will such a path support Baltic Sea regional security itself, but Baltic Sea littoral states can provide pathfinding experience that can aid other regions around the world as incidents of underwater mayhem continue to spread.

Benjamin L. Schmitt
Ph.D., Senior Fellow
Department of Physics and Astronomy
Perry World House
Kleinman Center for Energy Policy
University of Pennsylvania
USA

Senior Fellow for Democratic Resilience
Center for European Policy Analysis
USA

Co-founder
Duke University Space Diplomacy Lab
USA

Term Member
Council on Foreign Relations
USA

Twitter: @BLSchmitt

MIKA SUONPÄÄ

Intelligence networks in the Baltic Sea Region during the interwar period

Expert article • 3998

Between the two world wars, the Baltic Sea region became a hotbed of intelligence activity, ideological confrontation, and covert operations. Various state and non-state actors, including intelligence agencies, political organisations, and émigré groups played pivotal roles in shaping the geopolitical landscape through surveillance, information-gathering, propaganda, and clandestine collaboration.

The following short article is based on my recently-published book Infosoturit (Gaudeamus, 2025), or infowarriors, which considers the activities of a Swiss anticommunist organisation Entente Internationale Anticommuniste (EIA) in Finland and the Baltic States from 1923 until the Winter War. The EIA constructed a global network that gathered information on communism from different countries, and on this basis, produced transnational anticommunist propaganda intended mainly for media outlets and state officials.

The assassination of a Soviet diplomat Vatslav Vorovsky by two Swiss-Russian terrorists in Lausanne in 1923, triggered a politically charged trial. Concocted by the EIA's president Theodore Aubert, the defence's strategy shifted the attention from the murder to Soviet atrocities, successfully diverting the court's focus. Out of nine judges, five voted for the release of the suspects, and they were freed. Aubert's final statement at the trial was later published as a pamphlet L'Affaire Conradi, which became the ideological manifesto of the EIA.

The EIA mobilised a vast network of Russian émigrés to gather evidence for the trial, and they also had connections to state officials in different countries. One Finnish intelligence officer was invited to testify at the Lausanne trial but instead submitted a written statement detailing executions in Petrograd. His involvement, facilitated by Russian émigrés in Finland and Germany, highlighted the transnational nature of state and non-state intelligence collaboration.

In Finland, Suomen Suojelusliitto, founded in 1921, functioned as an anticommunist propaganda organisation. It cooperated with the Finnish state police (EK) to monitor the communists' activities. By 1924, they had developed a detailed surveillance strategy for mapping communist influence across municipalities. This relationship extended into the late 1920s and early 1930s, when the EK provided the Suojelusliitto with classified reports and updates on domestic and international communism. Similarly, Estonia's Kaitseliit, and the country's political police, worked closely to monitor suspected communists.

In 1925, chief officers of the state police from Finland, Estonia, and Latvia convened in Helsinki to discuss anticommunist strategies and the potential establishment of anticommunist organisations. These meetings also underscored the role of non-state actors as intelligence sources and support structures because the Suojelusliitto's president was invited to speak at the conference about international anticommunist cooperation and to discuss with state police representatives.

Russian émigrés, too, were instrumental in intelligence operations. One of them, served both the Estonian political police and the British SIS in the 1920s. Operating from the British passport office in Tallinn, he maintained a network of informants and provided military intelligence on Soviet naval and army capabilities. He also had ties to the EIA, supplying documents through the Swiss consulate. Finnish intelligence maintained a cautious stance toward Russian émigrés but recruited some of them for minor roles under strict supervision. While the EIA viewed Russian émigrés as a link to "real Russia", Finnish right-wing circles, including Suojelusliitto, were sceptical of their motives.

In 1924, the infamous "Zinoviev Letter" surfaced just days before the British general election. The conservative newspaper Daily Mail published the letter in full. Allegedly authored by the Soviet official Grigory Zinoviev, the letter called for communist agitation in Britain. The letter was later revealed as a forgery, likely orchestrated by Russian monarchist émigrés. Finnish intelligence retrospectively identified the letter as part of a broader disinformation campaign aimed at manipulating democratic processes.

By the 1930s, figures like Severin Dobrovolsky emerged as key players in émigré-led intelligence and propaganda networks. Dobrovolsky, based in Viipuri, had established a private intelligence network and collaborated with the Finnish state police. Despite ideological alignment with the EIA, his overt fascist sympathies and controversial public lectures led to his marginalization. He was executed in Moscow in 1946.

As these glimpses into the interwar intelligence history of the Baltic Sea region illustrate, intelligence-gathering networks, disinformation campaigns, and propaganda as phenomena resemble their present-day successors. However, digitalisation has radically changed the information environment during the past twenty years, thus also fundamentally reshaping the nature of information operations.

Mika Suonpää
PhD, Docent, University Lecturer in Contemporary European History
University of Turku
Finland

misuon@utu.fi

ZACHARY SELDEN

Historical legacies and the development of the Central Intelligence Agency

Expert article • 3999

The United States lacked an intelligence agency prior to World War II beyond small offices in the Departments of the Army and the Navy. Even the fabled Office of Strategic Services (OSS) that performed a wide range of intelligence gathering and analysis during WWII was disbanded soon after the defeat of the Axis powers in 1945. In 1947, however, the US created the Central Intelligence Agency, the Defense Intelligence Agency, and the National Security Agency. By the end of the 1950s the intelligence community (IC) with the CIA in a central role was well on its way to becoming a major center of power and influence within the federal bureaucracy. How do such institutions grow so rapidly with virtually no precedent?

In fact, is not entirely accurate to say that the US had no experience with intelligence prior to this massive growth of the IC after WWII. The Federal Bureau of Investigation (FBI) played a small but significant role as both a domestic and foreign intelligence service prior to the creation of the CIA. Much of the intelligence the FBI gathered, and its key personnel involved in foreign intelligence collection transferred to the CIA. This is important because institutions often follow a path-dependent development process. That is, the institutional culture that is created at the start affects what comes later. It is not that developments are predetermined, but rather patterns of action, bureaucratic practices, and institutional priorities are shaped by the past.

The FBI, however, is a particularly interesting case because its origins and development were dominated by one man, J. Edgar Hoover. Hoover was not only the Director of the FBI at its creation in 1935 remaining in the position until 1972, he was the director of the now-forgotten office that preceded the FBI known as the General Intelligence Division (GID) (later the Radical Division).

As a young Department of Justice attorney in 1917, Hoover was tasked with creating the GID, the purpose of which was to collect intelligence on groups and individuals who might harm the American war effort. Hoover and a small force of dedicated individuals collected a large database on suspected radicals, many of whom were foreign-born. After the war ended, however, the Radical Division became far more active in the wake of anarchist bombings that captured public attention. The resulting raids and deportations of left-wing radicals eventually became an embarrassment, however, and the Radical Division was closed in 1924.

Despite this unpromising start, Hoover was picked ten years later to lead the Bureau of Investigation (renamed the Federal Bureau of Investigation). Hoover brought with him many of the same personnel who had worked with him in the Radical Division, as well as the extensive intelligence database that has been collected and filed by them. Hoover maintained an extraordinary level of personal control over the FBI through his tenure that reflected his strong anti-communist sentiment. It permeated the culture of the FBI, its hiring practices, and the intelligence gathering priorities of the new bureau.

The fact that the FBI had many intelligence veterans from the Radical Division made the FBI a natural candidate for intelligence collection and analysis soon after it was founded. As Europe slid toward war, President Roosevelt asked Hoover to collect information on potential Nazi sympathizers in the US. By 1940, Roosevelt was particularly concerned about Nazi influence in South America and directed the FBI to create a foreign intelligence collection service across the Western Hemisphere known as the Special Intelligence Service (SIS).

The SIS rapidly became entrenched in every embassy in Latin America, whose agents were designated as "legal attaches" while running networks of informants. The SIS also introduced false information into Nazi networks through the targeted use of double agents. These SIS personnel stationed in embassies under diplomatic cover became in some ways the model for CIA station chiefs in American embassies.

The SIS expanded its operations into Europe after the US entered World War II and became involved in intelligence collection and analysis on a wide range of issues. With the expansion of its remit, the SIS grew as a bureaucratic force to the extent that the FBI was considered as the logical home for what would be the post-war American intelligence community. This clearly did not occur, but when the SIS was disbanded it transferred all of its files, networks, and communication systems to the newly established CIA. More importantly, however, by 1950 every CIA station chief in Latin America had previously served as an SIS "legal attache." The CIA did not simply spring into existence in 1947. Instead, it was built on a foundation that incorporated the FBI's institutional culture based on Hoover's priorities.

Zachary Selden
Associate Professor, Political Science
University of Florida
USA

JUKKA RISLAKKI

Intelligence services: Don't shoot the messenger

Expert article • 4000

An intelligence service is a mill that grinds 24/7, all year around. The orders are given by the civilian or military leadership: it has to gather and forward up-to-date, reliable and relevant information to aid the planning and decision-making at the highest levels.

The gatherers of intelligence should forward hard facts only – it is not their job to present speculation, guesswork, interpretation, or recommendation. Only the leadership that commissions the information is responsible for analysis and decisions.

Ideally this is true, but not always in real life. Intelligence officers, or spies, can leave some facts untold or present wrong or non-verified information. Sometimes they may be tempted to lie, exaggerate, or copy the information from public sources, such as newspapers. Or, they may try too hard, which can lead to their unveiling and getting caught.

On the other hand, even the best intelligence will not sway a leader who is not prepared to heed it. Stalin, probably more than any other world leader at the time, used intelligence information only to strengthen his own preconceptions and dismissed facts that were in conflict with them.

In 1941, he received, in advance, from several sources, good information, scores of warnings about the imminent German attack, ¬ Operation Barbarossa, from Helsinki, even the exact day of the assault. To him it was only disinformation.

Shaun Walker writes in his book The Illegals that in Stalin's system there was nobody left who would be courageous enough or stupid enough to express even the slightest dissent when the great Leader was wrong.

For an intelligence officer, fear of the superior and willingness to please him are deadly sins. In a country governed by an authoritarian leader, presenting unpleasant information is difficult. Often the officers avoid providing bad news because it may be fateful for the messenger himself.

Currently, the nuclear superpowers, USA and Russia, both have regimes based, above all, on mistrust. In both countries, the highest leadership does not get objective information for decision making because they have shut themselves in a hermetical bubble of terrified, lying flatterers.

The new president, Donald Trump, almost at the outset of his presidency, purged the American national security apparatus. The officers had to swear allegiance to the Chief.

Trump has made it clear that he does not fully trust his new intelligence chiefs either. He seems to trust the Russian president more than them. This has already eroded the morale of the security services.

As the intelligence historian, Tim Weiner writes: Trump is now surrounded by incompetent, inexperienced, stupid "boot lickers". "He has put the national security instruments in [the] hands of crackpots and fools." The Nobel laureate, Paul Krugman recently stated that Trump has lost touch with reality and is slipping into "a world of delusions".

There were problems of trust earlier as well. For example, six months before the 9/11 attack, the CIA director George Tenet tried to convince president G. W. Bush about the looming threat of Islamic ultra-fundamentalism. No one in the administration listened.

What about the war in Ukraine? How could Vladimir Putin, a president with intelligence service background, commit such a colossal strategic mistake, attacking with full military force in 2022? (True, the West erred too, believing that the Ukrainian resistance would hold a few days only.)

The decision to attack was made in a very small circle of Putin's yes-men. Even all government ministers did not know about it. There was nobody to express doubts or ask uncomfortable questions.

Putin and his secret service seemed to be in some kind of hubris, because many international operations had gone so well, according to plans. It was a surprise that real war followed; Putin had thought that it would be a "special operation" only.

Putin dismissed a mountain of evidence that did not fit his world view; what followed was a gigantic failure of intelligence (Shaun Walker).

The groundwork for the attack was given to the interior service FSB. Lots of money and scores of agents were sent to Ukraine – with zero results. In a corrupt society like Russia, the intelligence service is also corrupt.

The Ukrainian case can be compared to the U.S. invasion of Iraq in 2003. The U.S. Secretary of State was sent to the UN to present concocted evidence to justify the attack. According to this incorrect and faulty intelligence, Saddam Hussein secretly developed weapons of mass destruction (which was not true) and supported Al-Qaida terrorists (which was also not true), and Iraq and Iran formed an axis of evil (not true, they were adversaries).

The facts presented were of the type that pleased the President, and "the proof" was obtained by torture, which mostly does not produce solid information. George W. Bush later stated that the attack was his biggest mistake as President.

The Iraq war led to a long period of violence, chaos and streams of refugees, and to The War on Terrorism, which surpassed almost all other Western intelligence activity. It was a cruel awakening, when the West later realized that by concentrating on Islamic terrorism, it had for about twenty years neglected the potentially fatal threat of Russian and Chinese espionage.

Jukka Rislakki
Finnish journalist and non-fiction author

MIKKO VIRTA

Secret back channels in cold war

Expert article • 4001

During the Cold War, secret back channels operated through intelligence services served as vital tools for the foreign policy of state leaders. Finnish President Urho Kekkonen maintained close, decades-long connections with both Soviet and British intelligence agencies. Similar examples globally include U.S. President John F. Kennedy and German Chancellor Willy Brandt. However, in light of current knowledge, the scope and duration of Kekkonen's intelligence contacts were exceptional.

A back channel refers to unofficial communication used in foreign policy, bypassing official diplomatic institutions. Such a channel can operate either directly through a foreign power's diplomatic mission or intelligence service, or it might involve several intermediaries. A one-way or two-way channel can facilitate the exchange of information orally, through the delivery of written materials, or both.

Urho Kekkonen's close ties with foreign intelligence services apparently began in 1943 when he met Wilho Tikander of the U.S. Office of Strategic Services (OSS) in Stockholm. Through Tikander, Kekkonen could convey his thoughts directly to the West and, conversely, learn about U.S. perspectives on Finland's situation.

Kekkonen established connections with British and Soviet intelligence services, according to current information, in the fall of 1944 when he was the Minister of Justice. His first Soviet intelligence contact was the chief of Helsinki station Jelisei Sinitsyn. Sinitsyn was introduced to Kekkonen through Kustaa Vilkuna. Sinitsyn left Finland in 1945 but before doing so, transferred the contact to his successor, V.F. Razin.

British intelligence contacts included Reginald "Rex" Bosley and James H. Magill. Bosley appears to have been Kekkonen's most important contact with Western intelligence services throughout the Cold War. Their communication remained active until the 1980s, with Bosley regularly visiting Finland for political intelligence gathering.

The connection with Magill also remained close until the end of Kekkonen's presidential term. Although Magill officially resigned from intelligence work in the mid-1950s and moved into British export industry, he continued to visit Kekkonen in Finland on business trips, lobbying for everything from nuclear power plants to jet aircrafts.

Wilho Tikander's communication with Kekkonen ended in 1948 when Tikander was transferred back to the United States. Americans apparently failed to establish a direct back channel to Kekkonen thereafter. However, a roundabout connection was built in the late 1950s when Frank Friberg became the CIA's station chief in Helsinki.

Urho Kekkonen was by no means the only Cold War statesman to leverage back channels for foreign communication. U.S. President John F. Kennedy had at least two secret back channels to Moscow. One connection went through his brother, Robert Kennedy, then Attorney General, who met with Soviet intelligence officer Georgi Bolshakov over 50 times in 1961 and 1962, relaying messages between Kennedy and the Kremlin. During the Cuban Missile Crisis, Kennedy's secret channel to Soviet leader Khrushchev went through KGB Washington rezident Aleksander Fomin and ABC news correspondent John A. Scali. West German Chancellor Willy Brandt, for his part, utilized a back channel to Soviet intelligence during his new eastern policy (Ostpolitik).

Having worked for years in his youth in Finland's secret police, the Etsivä keskuspoliisi, President Urho Kekkonen understood the value of intelligence resources and how to wield them as a political instrument. Information obtained from Moscow "through the kitchen," as it were, allowed him to gauge the Soviet leadership's policies and motives, as well as assess the likely effects of his own actions.

The importance of long-standing personal relationships is highlighted in Kekkonen's dealings with both Eastern and Western intelligence services. Contact with both SIS's Rex Bosley and KGB's Mikhail Kotov was maintained from the 1940s into the 1970s. Both Bosley and Kotov spent several years in Finland, developing a strong rapport with Kekkonen. They also spoke fluent Finnish. Both advanced to high positions within their respective intelligence services; perhaps their contact with Kekkonen facilitated this. Later, they were approached when something significant occurred in Finland or when it was crucial to obtain confidential, high-level information. Personal, confidential relationships were not easily transferred to successors, and connections could be severed with personnel changes.

Soviet intelligence appears to have been a practical tool for political action for Kekkonen, whereas with Western intelligence, the primary exchange was information. The former must also be considered more significant, both for Finland and for Kekkonen himself. The KGB provided a direct line to Moscow, allowing Kekkonen to understand the Soviet leadership's intentions. Through Soviet intelligence, Kekkonen not only propelled himself to power but also fought for Finland's independence.

Western intelligence supplied Kekkonen with information on the Soviet Union, Finnish communists, and world events. Kekkonen, in turn, kept Western powers informed about developments in Finland. Starting during his premiership in 1950, Kekkonen adopted the practice of leaking information from discussions with Soviet leaders to Western intelligence services. This practice continued later as president. Based on current knowledge, there are few known instances where Kekkonen sought to arrange concrete political matters with Bosley, Magill, or Tikander in the way he did with the KGB.

Kekkonen's secret Western connections can be divided into two categories: direct and indirect. The former were more important because information flowed in both directions, allowing Kekkonen to communicate his thoughts directly to London and Washington. When operating through intermediaries, it was primarily about receiving information.

Among the intermediaries, Kustaa Vilkuna and adjutant Urpo Levo appear to have been the most important. Levo had contacts with both Americans and Britons. Information to U.S. intelligence apparently flowed also through Anne-Marie Snellman and possibly through Eljas Erkko and Marcus Wallenberg.

Western powers also provided Kekkonen with intelligence through other adjutants and the Finnish Security Service (Suojelupoliisi, Supo). The connection through Supo continued during the tenures of Armas Alhava, Arvo Pentti, and Seppo Tiitinen. Additionally, Western ambassadors seem to have provided some material while visiting the president. Through them, Kekkonen could also convey his own thoughts to the West.

Mikko Virta
Doctor of Social Sciences
University of Helsinki
Finland

BERND VON KOSTKA

Licence to Spy: Legal espionage behind the iron curtain

Expert article • 4002

The establishment of the military liaison missions goes back to the time of World War II. The plans for the subsequent occupation of Germany were discussed by the Allies – the United States, the Soviet Union and Great Britain - at that time. Article 2 of the Agreement on Control Machinery in Germany, laid the foundation for the missions in late 1944. It stated that each commander in chief of a zone of occupation would have attached military representatives, from each of the other zones of occupation, for liaison duties. This was an idea that made perfect sense from the point of view of the wartime alliance.

After the surrender and occupation of Germany in 1945, however, a good year passed by before the first bilateral agreement between Great Britain and the Soviet Union was concluded in September 1946. Bilateral agreements with the Americans and the French – the 4th occupation power in Germany - followed in April 1947. The members of these missions, 63 in total for all three western nations, had their mission houses located in Potsdam/GDR. Mission members would ideally be military 'diplomats' who would maintain contact and foster relations with the commanders-in-chief to whom they had been assigned.

However, the role of the military liaison missions soon changed with the beginning of the Cold War. Gathering intelligence in East German territory would be the most important task in the decades that followed. This was already the case in 1952 as top-secrets documents confirmed.

With the increasing importance of intelligence in the Cold War, the training of the small number of representatives each country was permitted to send to Potsdam had to be improved. Good knowledge of Russian or German was a priority. By the end of the 1950s, the three Western military missions in Potsdam were regarded as an outstanding and reliable early warning system for any possible surprise attack by the Soviet Union in Europe.

They were, so to speak, the eyes and ears of the Western powers in East Germany. For the purposes of their inspection tours, the three Western powers divided East Germany into three large operational areas A, B, and C. Each large area was allocated to a different Western power with each sending two teams to patrol its allocated area. This meant all three Western powers together had three ground teams and three air teams covering most of East Germany. Responsibility for the large areas A,B,C also switched once every few weeks. This system could only work if there was good cooperation between the three missions. They maintained telephone contact with one another almost daily and held meetings once a week to ensure they did not duplicate their efforts. Such exchange of military information could not be taken for granted, especially given that France withdrew from NATO in 1966. Yet this did not in any way impact on the bond of trust the Americans and British had developed with their French counterparts in Potsdam.

While on their inspection tours in East Germany, the members of the military liaison missions had to take notes and photos of any facts of military value. Where were units stationed? What was their strength? What equipment did they have? Were there any modifications to equipment that was already known to exist? Photographs of vehicles or aircraft were of particular interest, especially if they possessed new components. The pictures could then be sent to military specialists in the West for analysis. In some years more than 500.000 photos were taken from the mission members on their tours. There were other questions that were obviously important from a military standpoint. Were Soviet and East German ground troops on the move or was a member state of the Warsaw Pact conducting manoeuvres on East German soil?

This freedom of movement was increasingly restricted the more the missions undertook intelligence activities. Even at the outset, it had been stipulated that some areas, designated Permanent Restricted Areas (PRAs), would be out of bounds to mission personnel. The PRAs in East Germany covered approximately a quarter of the country. Also introduced were Temporary Restricted Areas (TRAs). The extent of these restricted areas varied over the decades, but it usually amounted to between 25 and 33 per cent of the total area of East Germany.

The inspection tours in East Germany were not at any stage without danger. East Germany, which gained no advantage whatsoever from the bilateral agreements between the Soviet Union and the Western powers, regarded the military liaison missions as 'a thorn in the flesh'. East Germany does not have the power to prevent the reconnaissance tours. Therefore the East German State Security (Stasi) did everything possible to make their work more difficult. There were a large number of incidents in which mission vehicles were fired on or were damaged by roadblocks or detentions. In 1984 a French mission car was brutally rammed by a military truck and the French driver died. One year later a US Officer was shot in the GDR while he was inspecting a rural area.

The missions in Potsdam played a significant role during the years of the Cold War. They could legally obtain information on East German territory and could pass it on to Western military authorities and intelligence agencies. Yet the missions were also an instrument for defusing crises. Its members were able to gain an idea not only of what the potential enemy was up to but also of what he was not up to. Furthermore, the existence of the missions ensured the Western powers were in constant contact with the Soviet Union even in times of international crisis.

Bernd von Kostka
Member of the academic staff and curator
Allied Museum
Berlin
Germany

ALEKSI MAINIO

Émigré combat organizations and Ukrainian activism in Finland in the 1920s and 1930s

Expert article • 4003

In the aftermath of the Bolshevik seizure of power, millions of inhabitants of the former Russian Empire fled the newly formed Soviet state. Owing to its geographical proximity to Petrograd (St. Petersburg), Finland became one of the main transit routes for the refugees: tens of thousands of Soviet émigrés crossed the border river running through the Karelian Isthmus to escape the country. While many continued their journey toward the metropolitan centers and émigré hubs in Central Europe, tens of thousands settled in Finland, mostly in the cities of Vyborg and Helsinki.

The majority of the refugees refused to accept the legitimacy of the Soviet rule. Political activism emerged under a variety of émigré movements, which were united by uncompromising anti-Bolshevism: the Soviet regime was to be overthrown through political propaganda, armed struggle, and, in some cases, outright terrorism. By the late 1920s, however, it became increasingly evident that the émigré combat organizations – such as the underground terrorist cells of the ROVS under General Aleksandr Kutepov – were incapable of destabilizing the Soviet power in Moscow.

Within the Soviet leadership and its expanding security apparatus, the presumed conspiracies of "White émigrés" were both feared with paranoia and exploited with cynicism. Real and fabricated "plots" and "acts of sabotage" attributed to émigrés provided convenient justification for extensive campaigns of discipline and repression inside the Soviet Union, culminating in Joseph Stalin's Great Terror and the purges of 1937–1938. Soviet intelligence also closely monitored the active operations of émigré combat groups in the Finnish territory, and official propaganda denounced Finland as a "nest of terrorists."

During the 1920s, the leadership of the anti-Bolshevik cause was largely in the hands of White Russian émigré organizations, but in the following decade, nationalistic organizations of ethnic minorities came more to the fore. Internal tensions in the Soviet Union intensified as the structural problems of the country became more apparent. Soviet Ukraine experienced the devastating famine known as the Holodomor, while elsewhere – particularly in the Caucasus – armed groups demanding national self-determination began to gather strength.

This wave of separatism swept through the émigré communities of Europe. Organizations representing the Soviet Union's minority nationalities – Ukrainians, Georgians, Armenians, and others – sought to contribute to the domestic struggles for national liberation.

The Soviet secret police, the OGPU–NKVD, reacted with even greater vigilance. Determined to contain and manipulate these militant networks, it employed highly inventive – at times almost avant-garde – methods of espionage, infiltration, and provocation. The Soviet intelligence succeeded particularly well in planting agents within Ukrainian nationalist organizations operating across Europe.

The most famous of these was Pavel Sudoplatov, born in Melitopol in 1907. Trained by the Soviet security services, Sudoplatov was tasked with carrying out a clandestine mission: to pose as a passionate Ukrainian nationalist and infiltrate the ranks of the Organization of Ukrainian Nationalists (OUN). He started his task in Helsinki, where he built his false identity as a Ukrainian Nationalist among Ukrainian OUN activists staying there.

Sudoplatov proved extraordinarily successful in playing his double role. Between 1935 and 1938, he became a close confidant of Yevhen Konovalets, the OUN's leader, who moved between several Central European cities. While carrying out underground missions for Ukrainian activists in Central Europe and the Soviet Ukraine, he received his real instructions from Moscow. In the spring of 1936, as he attempted to return to the Soviet Union via Finland, Sudoplatov was detained at the Finnish-Soviet border by Finnish border guards. Suspected of being a Soviet intelligence operative traveling under a false identity, he was taken under investigation by the Finnish security police until its main Ukrainian informant, OUN's principal representative in Finland, Konrad Poluvedka, intervened personally. Poluvedka guaranteed Sudoplatov's reliability, leading to the latter's release and safe passage from Helsinki to Tallinn.

A couple of years later, the Finnish security police discovered that Poluvedka was, in fact, one out of three or four "Ukrainian nationalists" clandestinely inserted into Finland's émigré networks by the OGPU–NKVD in the 1930s. His real identity remains unknown even today.

Sudoplatov's later career would make him one of the most notorious intelligence operatives of the Soviet era. On 23 May 1938, in Rotterdam, he presented Konovalets with a traditionally decorated Ukrainian chocolate box containing a hidden bomb. The assassination of Konovalets was not the last of Sudoplatov's violent undertakings: in August 1940, he directed the operation that resulted in the death of Lev Trotsky in exile in Mexico.

Aleksi Mainio
Associate Professor
University of Helsinki
Finland

aleksi.mainio@helsinki.fi

MIKAEL LOHSE

Juggernaut – Security Service of Ukraine

Expert article • 4004

Amidst Russia's continued aggression, the Security Service of Ukraine (Служба безпеки України, SBU) has become by far the most powerful security sector authority in the country. The SBU is almost an unstoppable force – Juggernaut – due to wartime necessity. Perhaps precisely for this reason, the SBU enjoys strong governmental and societal support. The Service's current power posture represents the consolidated position of the Government, the Verkhovna Rada (Parliament), and the Office of the President of Ukraine. A September 2025 survey showed that 78 % of Ukrainians trust the SBU, placing it as the second most trusted security authority after the National Guard. For comparison, only 14% of Ukrainians trust the judiciary.

The SBU is, by law, a public authority of special purpose with law enforcement functions, and it employs approximately 40,000 people. The Service is also part of Ukraine's intelligence community. In practice, the SBU's power is based on its triple role as a special service, a pre-trial investigation (PTI) body, and a military unit.

Counterintelligence is the backbone of any security service. The SBU counterintelligence collects data on the movement of military equipment, concentration of the's Russian armed forces, location of their bases and ammunition depots and passes this information to the Defence Forces of Ukraine for targeting and destruction. Another top priority of the SBU is the protection of state sovereignty, territorial integrity, and constitutional order. In addition, the SBU is the main authority coordinating the counterterrorism efforts of state agencies. As a special service the SBU is also occupied with the protection of state secrets, in particular, information relating to defence, economics, science and technology, and foreign relations.

The SBU conducts pre-trial investigations in several areas of crime, such as treason and other crimes against national security, terrorism and related crimes, cyber and information security offences, war and occupation-related offences, but also corruption, economic crimes and organised crime. Since the start of the full-scale war, SBU investigators have been investigating over 90,000 war crimes committed by the Russian armed forces. This array of crimes is being documented not only for Ukrainian, but also for international justice.

The main military unit of the SBU is the Special Operations Center "A" carrying out operational-combat activities and special measures. The numerical strength of this unit is at least 10,000 people during the period of martial law. It's not just about the number; it's about the fact that "A" is tier one unit among the special forces of Ukraine. The "A" fighters have already destroyed enemy equipment and personnel on an industrial scale, but the most impactful is the unit's secret operations. These operations include defeating Russia's Black Sea Fleet and striking thrice the Crimean Bridge. However, the most ingenious strike by the "A" is probably Operation Spiderweb. This covert attack targeted Russian Air Forces' long-range aviation assets at five air bases using drones concealed in and launched from trucks on Russian territory. As a result, one-third of Russian strategic cruise missile carriers were demilitarised.

The reason why SBU powers are important are negotiations on Ukraine's accession to the European Union. The overarching aim of the SBU reform is to limit its scope of functions to counterintelligence, counterterrorism, and protection of state secrets, and to bring the SBU under genuine democratic control. Let's go through this role by role.

SBU's scope of activity as a special service is typical compared to any other security service in the West. Instead, there has been more debate about whether the SBU should have PTI powers. Undoubtedly, PTI powers combined with powers and capabilities of a security service create a very powerful institution. However, the acceptability of such an institution from the perspective of accountability and the protection of individual rights depends upon the adequacy of the oversight created to prevent abuse, or overuse of power. A strong special service which is subject to tight internal control and robust external oversight, and, when using PTI powers, control by prosecutors, cannot be said to be incompatible with Council of Europe principles in general, or the European Court of Human Rights in particular. The decisive factor is therefore whether oversight is organised effectively or not. Having said that, the SBU's areas of crime are too broad, and crimes that do not threaten national security, such as smuggling and other economic offences, should gradually be transferred to the State Bureau of Investigation or Economic Security Bureau.

Where the SBU differs fundamentally from its European counterparts is in its military unit and active warfare. A domestic security service with the combat capability of one division or two brigades would undoubtedly be worrying from a human rights and accountability perspective in a peacetime context. Demilitarizing SBU is therefore essential in the long run. However, this can only happen once Russia convincingly chooses peace or is forced to do so. Until then, the SBU must maintain military strength to make Russia pay and hold at bay.

Mikael Lohse
Deputy Intelligence Ombudsman
Adjunct Professor of Intelligence Studies
Finland

LEO NIEMI

The role of geospatial data in civilian-led OSINT during the war in Ukraine

Expert article • 4005

The war in Ukraine has witnessed unprecedented democratization of intelligence. Civilian organizations now conduct sophisticated open source intelligence with the help of geospatial tools, data and analysis methods. This democratization has profound implications for how wars are documented, analyzed, and understood in real time.

Ukraine's geography significantly influences geospatial intelligence methods. The country's plains, river systems, and seasonal weather create distinct challenges. The Dnieper River serves as both barrier and logistical artery. Seasonal rasputitsa constrains military mobility and shapes operational planning. Yet the proliferation of drones fundamentally reshapes this military geography. Understanding these geographical factors through geospatial analysis provides crucial context for interpreting battlefield developments.

The Kakhovka Dam destruction in June 2023 exemplifies how geospatial intelligence illuminates infrastructure attacks. Satellite imagery documented immediate flooding and environmental consequences. This event had tactical implications for front-line positions and strategic dimensions affecting regional ecology and civilian populations.

Effective civilian open source intelligence relies on specialized collaborative networks rather than individual analysts, where technical specialists must translate complex findings into actionable intelligence. Organizations like Bellingcat exemplify how effective knowledge transfer operates within civilian OSINT communities. Their public investigation into the 2014 downing of Malaysia Airlines Flight MH17 over eastern Ukraine provided an early demonstration of systematic collaboration across technical domains within the Russo-Ukrainian war. Similar organizations have since adopted comparable approaches, each developing specialized capabilities while maintaining collaborative frameworks that enable rapid cross-verification when urgent questions emerge.

Remote sensing data, geolocated social media posts, and collaborative mapping platforms create unprecedented situational awareness accessible to journalists, researchers, and citizens worldwide. Social media platforms, particularly Telegram, play a critical role. The application has become one of the key communication channels for both Russian and Ukrainian audiences. Posts, videos, and images provide near real-time glimpses of military movements and combat outcomes. However, this abundance presents challenges in verification and operational security.

The enabling tools continue advancing. Machine learning algorithms process vast quantities of imagery and social media content. Yet AI brings new challenges as well, since it can be consciously manipulated with hostile intent under different circumstances. For now and at least in the near future, human judgment remains indispensable. Algorithms still struggle to replicate the contextual understanding required to distinguish authentic battle descriptions from sophisticated fabrications or to recognize when seemingly mundane details reveal operational patterns. Conversely, certain analytical tasks far exceed practical human cognitive capacity. Processing millions of social media posts to identify emerging patterns, or analyzing remote sensing data across hundreds of square kilometers, requires computational power that only machines can provide. The most effective approach therefore is to maintain careful equilibrium between automated data collection and human interpretation, recognizing that neither alone suffices.

Large language models exemplify this balance. Advanced models can extract semantic location information from natural language, meaning mentions of specific streets, landmarks or districts within different posts. When a local resident mentions hearing explosions near a particular landmark, algorithms employ geocoding services to convert this reference into precise coordinates, then apply geospatial filtering to identify the correct location within the appropriate oblast rather than ambiguous references elsewhere. This extracted location can then be correlated with satellite imagery and cross-referenced against other contemporaneous reports from that vicinity. In the future so called foundation models may also be capable of doing all this, without the need of having to create complex pipelines and workflows.

State authorities face increasingly complex decisions about geospatial data governance. Many nations developed open data policies premised on transparent governance and economic development, making cadastral records, infrastructure databases, and topographic datasets publicly accessible. Once released, geospatial data cannot be effectively recalled. Governments must therefore weigh whether maintaining open data access serves broader societal interests despite acknowledged security costs, or whether previously open datasets should be restricted despite questionable efficacy of such restrictions.

Leo Niemi
Analyst
Black Bird Group
Finland

leo@blackbirdgroup.fi

GREG MILLS & RAY HARTLEY

Resilience: How war is won

Expert article • 4006

In the foyer of the 'National Museum of the History of Ukraine in the Second World War' are three autonomous fast boats, one a 'suicide' vessel designed to explode as a surface mine, another carrying air defence missiles, and the third mounting a belt-fed grenade launcher.

Drones, land, sea or air, are not so much the future of war, but the present. The key question is where this technology is going – and how and when Russia's war in Ukraine might end.

On the battlefield, drones have been the most significant tactical feature, along with the ability to launch disruptive deep-strikes. The front – referred to by Ukrainians as the 'contact line' – is defined by a strip of no-man's land patrolled by reconnaissance and suicide drones. The Ukrainians alone expend around 10,000 FPV (first person view) drones daily on targets, the Russians at least this number. This no-man's land is strewn with discarded fibre-optic cables, many of the logistics routes operating under net 'tunnels' to prevent the drones from intercepting troop and vehicle movements.

This is a 'life of hell' for the soldiers, the conditions a high-tech version of the Somme more than 100 years ago, with death coming less from machine guns and artillery than with pinpoint accuracy from a silent, hovering aerial enemy.

In February 2022, few imagined a war of this type, duration and terrifying scale, drones then mostly a tool for reconnaissance or stand-off missile strikes.

But war remains as ever sui generis, with the constants only that, as General Sir Nick Carter, the former Chief of the UK's Defence Staff, reminds, it is 'inherently chaotic and uncertain, and it is about close combat between human beings'. The character of war is like the technology, circumstances and timing, inherently mutable.

Even so, the most unexpected outcome of this war is in Russia's inability, despite its numerical, nuclear and materiel advantage, to defeat Ukraine on the battlefield as much as the Ukrainians have been unwilling to surrender. People, motive, a sense of national purpose, and esprit de corps matter as much now as they did 100 years ago, perhaps more so when faced with these odds and the threat of national annihilation, at worst, or, at best, serfdom to Russian ambition.

And yet the performance of the Russian military at the outset was surprisingly poor, not least since they had taken care to assemble their forces and plan for conquest. While they have since much improved, they remain relatively hapless, perhaps because they are fighting for an imperial rather than a national cause. Their most recent summer offensive has been, in the assessment of Edward Carr writing in the Economist, 'an abject failure. Russia's tactic is to send small groups of men into the killzone. Yet, if some break through, the rest cannot take advantage of their progress. As soon as they mass, they are obliterated.'

While Russia wanted to assert its power over its neighbours, it has ended up showing the limits of that power and becoming all but a vassal to another neighbour, China, a key provider of dual-use technology from chemicals to micro-chips, and purchaser of Russian oil. If there is a victor in this war, it is Beijing, which has profited financially and undoubtedly learnt myriad lessons about Western military technologies and tactics.

The numbers inform this failure. Russian casualties hover somewhere between one million and 1.5 million men, the number of dead estimated around 25% of this figure, five times greater (probably) than Ukraine. As Carr puts it, 'Russia is advancing, but to occupy the four oblasts it claims as its own would require five more years. If the killing continues at 2025's rate, total Russian casualties will reach almost 4m.' To conquer all of Ukraine in this manner would take close to 2100, as Kateryna Yuschenko, the former Ukrainian First Lady puts it.

The resistance encountered by Russia illustrates the extent to which Moscow underestimated Ukrainian resolve founded on 350 years of resistance to Russian hegemony. As Kyiv moved to assert itself through the 2003 Orange Movement led by Viktor Yushchenko and the EuroMaidan protests ten years later, Russia fought back, attempting to impose its own presidential candidates, a failure which led to the current situation.

At home, however, so far, Putin remains unchallenged, perhaps surprisingly given the high cost in lives. He has headed off the most serious challenge to his rule in the form of Wagner's Yevgeny Prigozhin and the corruption campaigner Alexei Navalny. There appears to be no fallout, for now, at least as much as outsiders are aware, no Black Swans in sight.

If the lack of a Russian theory if victory is perhaps the most surprising aspect over the last three years and ten months, there are other unexpected turns.

Making virtue of necessity, Ukraine has delivered an army that fights tactically largely through local technology, enabled by a command control system that exploits AI and data. You still need people, if not nearly as many as has previously been the case, at least in defence. Drones are less useful in attack; this still requires artillery and armour, along with infantry.

Among other surprises is that Europe and the US have proven to have a political and security spine – Russia misreading the withdrawal from Afghanistan as a lack of foreign commitment. No one would, in 2022, have thought that Ukraine would be flying F16s, Mirage 2000s and, possibly, Gripen and Rafale, and be capable of deep-strike operations based on shared intelligence. At the same time, Europe's economy has not collapsed without Russian energy as some foretold.

The Ukrainian economy has also not collapsed, and neither has the Russian one (yet). To the contrary, the war has proven a rapid facilitator of Ukraine's economic integration with the EU despite the absence of membership, in part because of the flow of nearly six million people westwards. Despite Washington's rethink on aid globally, foreign donors remain remarkably generous on Ukraine, realising the security consequences of the second-largest country in Europe under the control of Moscow.

While Ukraine is dependent on the West, European security and dependency on Ukraine are increasing, not least because of its prowess in drone technology. Contrastingly, earlier German attempts to draw Russia in through Ostpolitik and economic interdependence, led by energy, has not stood up to the test.

It is also surprising that, despite being the imperial aggressor, Putin has been able, through a combination of fear, money, historical Soviet legacy and disinformation, to cultivate international support in convincing much of the world that the war was NATO's fault, and that Ukraine is a non-country run by Nazis.

Russia has also won allies in Africa, notably with military juntas across the Sahel. Even though in most cases this has been at local expense, it has been scarcely exploited by others. The imperial action of Russia contrasts with Ukraine's fight for self-determination, a point that seems surprisingly or perhaps deliberately lost on much of the formerly colonised world.

In this, human rights and international law have proven (again) fungible. While democracy has suffered, authoritarian populism has been given a boost. This option has been given appeal to elites by the absence of attractive Western models and calibration of benefits, and President Donald Trump's brash transactionalism has not helped.

China has in the process firmly inserted itself at the heart of global security. With Xi Jinping apparently of the view that the West is weak, a view fed by the global financial crisis of 2008/9, vacillation over Ukraine could have an impact on how Beijing acts in the South China Sea and with Taiwan.

While the threat of nukes remains, Ukraine's successful resistance has made nuclear war less likely, though the invasion itself and a Ukrainian collapse would encourage proliferation, not least in the face of a multilateral system which has been found wanting and the UN an irrelevance. The UN has been supplanted by the BRICS and G20, though this version of multilateralism is focused on regime interests rather than human security and protection. NATO, too, has been substantially strengthened and expanded, reminding of the hollow reasoning originally provided by Putin for the 'special military operation'.

And still, in spite of all of the above surprises, Russia is not (yet) interested in peace, or even trading territory for peace. Putin remains focused on dominating and turning Ukraine into something that looks rather like Belarus, as the former MI6 director Richard Moore recently commented.

Will the end also come as a surprise?

Peace is more than the absence of hostilities at a given moment. For peace to stick, there are several ground rules, as the scholar Timothy Snyder reminds us. Justice, fairness, international law, and security guarantees form part of the equation, not just territory and power. Overhastiness for personal reasons (touting for Nobel peace prizes included) can lead to unwise deals, based less on an appreciation of the relative merits, but on ego. Thus, negotiations to end the war cannot be, as Snyder terms it, a 'real estate disagreement between two men'.

Anything which neglects these aspects can only prolong the conflict.

Such a deal would fundamentally have to understand that security guarantees are not an abstraction for Ukrainians, at the heart of which are issues around sovereignty. This war came about when Russia invaded Ukraine, after all, not vice versa.

Oleksandr Lytvynenko is a KGB-trained former head of the SBU, the Ukrainian secret police and, more recently, the Secretary of the National Security and Defence Council. He doubts that, 'we will see the next aggression from the Russians. Three years for 100,000 square kilometres, 300,000 dead. They may be slaves, but they have minds. Putin will find it very difficult to return to war. So, this war is his legacy, one which demands an endgame. This explains why he is not in a hurry, as he is trying to obtain more and more for this legacy.'

Lytvynenko cites the nickname of Count Sergei Witte, who successfully negotiated the end to the Russo-Japanese War, culminating in the Treaty of Portsmouth. The treaty recognised Japan's hegemony in Korea, awarded it Russia's lease on the Liaodong Peninsula, control of the South Manchuria Railway, and the southern half of the island of Sakhalin. As a consequence, Count Witte became known as 'semi-Sakhalin'.

'Putin does not want to be "semi-Donbas",' says Lytvynenko.

Ukraine has already won this war. It continues to exist as a separate state, albeit battered and bruised. Putin has already lost since he has not rolled over Ukraine at the pace and with minimum fuss he envisaged and, in the process, turned his country into a Chinese vassal.

The question is how this all ends. Save a successful (by which read sustainable) peace agreement acceptable to all sides, and there is none in sight, there are two ways in which this is likely: Ukrainian military failure or Russian economic collapse. These are proxies, however, for an underlying equation: the stamina of Western resolve to keep supporting Ukraine versus Chinese assistance to Russia.

Is a Syrian-type collapse possible in Russia, along the lines of what Yevgeny Prigozhin's rockstar drive northwards from Rostov on Don in June 2023 threatened?

In January 1917, Vladimir Ilyich Ulyanov, better known as Vladimir Lenin, said in a lecture, 'We of the older generation [he was 46] may not live to see the decisive battles of this coming revolution.' This was delivered in Zurich while he was in exile in Switzerland, just a month before the actual revolution began in Russia, when the Tsar was deposed against the backdrop of the serial military defeats in the First World War. Lenin returned to Russia in April 1917, leading the Bolsheviks to power in the October Revolution that same year.

The same is true for the Ukrainian military, no matter the ongoing pressure and manpower shortages, that is, if Europe delivers the assistance required and Kyiv is able to generate additional soldiers, not least by incentivising recruitment and redeploying police.

This war will be won by resilience.

Greg Mills
Senior Associate Fellow
Royal United Services Institute
South Africa

Ray Hartley
Custodian
Platform for Democrats
South Africa

MICHAEL S. GOODMAN

National security challenges to 2030 and beyond

Expert article • 4007

History tells us that most big changes to national security communities occur in the wake of surprises, scandals, failures, or as reactions to large, seismic events. History also tells us that Western governments are very focussed on the here and now and that it is tremendously difficult to look to the future and plan strategically. In both cases it is easy to see why – if the system isn't broken (or doesn't appear to be broken), why fix it? It is errors or largescale shifts in focus that prompt change, but these tend to be short-lived and reactionary rather than thinking, holistically, about the future and where priorities might shift, challenges present themselves, or opportunities arise.

The purpose of this piece is to think about the future in a different way. Specifically, what are the challenges and opportunities for Western national security communities, and why is it so crucial that we think about the future in a strategic way? As the newly published UK National Security Strategy 2025 recently declared, "the world has changed" and we now live in "and era of radical uncertainty… where threats continue to grow in their scale and complexity". This short paper proposes 7 challenges that will face the national security communities moving into the future.

1) Defining the threat

State hybrid threats are the one of the biggest challenges for national security communities. Much focus is on the 'hybrid' component of what Russia, Iran and China do, from subversion, disinformation and electoral interference, through to sabotage, cyber attacks, intimidation and assassination. Tackling these issues at a tactical level is critically important, but is there enough focus on the strategic level? What activities are normal part and parcel of statecraft? So where should effort and limited resources be best placed? And is it even useful for us to separate out the parts of hybrid warfare undertaken by states like Russia, China and Iran into 'workstreams' in order to deal with them? More practically, how straightforward is it to pivot priorities to something slightly amorphous like state hybrid threats?

2) War, peace, or something in between?

Related to this is the question of war versus peace versus, what? Definitions of 'hybrid warfare' suggest it is neither war nor peace, but a state of prolonged conflict. By extension, therefore, what does 'winning' look like in the hybrid domain? Is it about completely nullifying foreign state efforts? In a utopian world the answer would be 'yes', of course, but this is unrealistic in the real world, so what can we hope to achieve? Related to which, what is the relationship between defensive, resilience building measures, and offensive, operational ones? This raises several questions: what is our risk appetite (in both a defensive and offensive way)? Is it the activity that is the 'threat', or the actor? Uncertainty is likely to become the norm.

3) Responding

Taking into account all of the above, what might be done to lessen the threat? The toolkit available to national security practitioners contains a number of weapons: from soft power tools like BBC World Service, to sanctions, the rule of law, deterrence and resilience. The last few years have seen a large number of new acts of law in the UK to counter state threats, and only time will tell whether they have the desired deterrent effect. A more resilient society will undoubtedly help, and great lessons can be learnt from countries that do this well, such as Estonia, Finland and Sweden. Perhaps deterrence is the key, whether individually at a national level or, more effectively, as part of a large coalition of states (NATO being the obvious example). These all raise the question of the response: what is the red line whereby a hybrid threat necessitates a conventional military response? Or will the future be a succession of hybrid attacks and counterattacks?

4) Appetite for risk

The classic test for governments is the Daily Mail or Washington Post test – can you justify your secret decision if it were to be on the front page of the newspaper the following day? Unscientific, but certainly an effective test to employ when considering the risk appetite of government. There is a common belief that western governments should not resort to underhand tactics to fight back, but how far can this maxim apply when we are not playing the same game as our adversaries? Related to this is the question of thinking increasingly about 'opportunities' as much as we think about 'challenges'. Increasingly, the risk appetite for governments needs to be about exploiting opportunities, but it also needs to look internally at vulnerabilities and how to ameliorate them. The focus, therefore, needs to go three-ways: assessing domestic vulnerabilities; monitoring adversary intentions and capabilities; and spotting opportunities to exploit.

5) Perspectives and the tyranny of the tactical

There is one lesson of history which should be top of our minds when looking at the current state threats: different countries approach national security in different ways. Most in the West tend to operate largely on short-term timescales, whilst the Russians and the Chinese tend to operate on a far longer timescale. There are myriad examples of where they will plan an operation over years, if not decades, in the hope that it will eventually pay dividends. The reality is that both of them play the long game in a way that the West rarely, if ever, has. The corollary of this is the thorny issue of getting policymaker receptivity when a 'threat' is slow, strategic, and not of direct importance now. How do democratic nations, with electoral cycles lasting 4 or 5 years, create strategies to counter state threats emanating from countries which plan in the far longer term?

6) Collection vs analysis

Many of those writing on contemporary security matters get fixated on the rise of open-source information, the growth of social media, the use of AI as an assessment/analysis tool, and the 'obvious' conclusion that the future will see a greater emphasis on intelligence analysis over collection. There is definitely some utility to this, though it obfuscates the reality that while OSINT can provide a huge amount, the really valuable information is unlikely to come from anything open source; the value of classified information is inherent in its secrecy. Nonetheless, it does raise the question of whether the preponderance between functions in the intelligence machinery is correct.

7) Diversity of subject

Lastly, we come to the thorny issue of diversity. Not in the sense that people might expect, but in the range of topics, thinking and approaches that government can employ. It is easy to become fixated on fire-fighting and focus on the current priorities of the day (the aforementioned 'tyranny of the tactical'), but what about those slow-burn topics that might not be significant now but absolutely will be in the future? Disease is one example, climate change another. Both require expertise and engagement with the national security community in a way that has probably not been commonplace yet.

Conclusion

It is highly likely that none of the above will come as a surprise to national security communities. The point of this short piece is to encourage people to think and write about similar experiences and encourage those within government to look to the academic community for input into this strategic thinking and to help its respective communities innovate in this new geopolitical environment.

Michael S. Goodman
Professor, Director of the King's Centre for the Study of Intelligence
Department of War Studies
King's College London
UK

PATRICK F. WALSH

Foresight Intelligence: The Five Eyes Intelligence Alliance and the Baltic States

Expert article • 4008

Foresight Intelligence means different things depending on the policy, intelligence practitioner and academic audience. Foresight Intelligence in the United States has frequently been referred as 'estimative intelligence' and in Australia the term 'strategic intelligence' is used. Semantics aside, most can agree on a few overarching principles on what foresight intelligence is and does. First, unlike 'here and now' tactical intelligence or short to medium term operational intelligence, foresight is generally focused on over the horizon threats risks and hazards where intelligence, signals and indicators and therefore pattern recognition remain difficult. What is meant by 'over the horizon' varies widely depending on the context under which the foresight intelligence is being applied. A second principle of foresight intelligence is that it exists because our intelligence communities have a duty to warn and reduce uncertainty for policy makers, so they can prevent, disrupt or mitigate emerging threats, risks and hazards.

The Five Eyes Intelligence Alliance and Foresight Intelligence

It may seem strange at first glance thinking about the Five Eyes and Baltic states foresight intelligence cooperation in the same sentence. After all, most Five Eyes countries (United States, United Kingdom, Canada, Australia and New Zealand) except for the United Kingdom are geographically distant from the Baltic states. Yet in this article, I argue the current global security environment underscores how much more the Five Eyes intelligence alliance could do with Baltic states to improve mutual understanding of emerging threats, risks and hazards.

Not all Five Eyes alliance partners have produced the same volume of foresight intelligence nor developed necessarily deep expertise in it. The United States historically has a longer tradition of producing foresight analysis then perhaps the United Kingdom and Australia. Long tradition of course does not always translate into better foresight analysis. The faulty national intelligence assessments by the US leading up to the 2003 invasion of Iraq or more recently the diverse views within the US IC about the origins of the COVID-19 pandemic show foresight analysis is not only analytically difficult but becomes more so in highly politicised environments. But the 80-year history of the Five Eyes alliance has resulted in all five countries (regardless of varying capability) developing foresight analytical knowledge and capabilities they share. While the second Trump Administration's unpredictable approach to allies including within the Five Eyes is placing some strain on the alliance at the political level, it is likely it will remain intact in the future. But the uncertain political environment in Washington where long-standing alliances have become more transactional than values based, does mean the other Five Eyes countries need to identify additional initiatives for strengthening the relevance of the alliance and their contribution to Washington. An increasingly multi-polar world also means liberal democracies have a range of other opportunities for intelligence cooperation beyond the Five Eyes intelligence alliance. In such an environment the Five Eyes needs to adapt and reinvent itself for both its member states but also to demonstrate relevance for other liberal democracies where interests intersect. In an ever increasing uncertain and volatile global security environment, one way the Five Eyes alliance can remain relevant is by sharing and expanding its foresight intelligence knowledge more comprehensively than hitherto has been the case with likeminded liberal democratic Baltic states.

Five Eyes and Baltic States Foresight Intelligence cooperation

All Five Eyes countries have deepening bilateral intelligence exchanges and cooperation with many Baltic states particularly since the Russian war in Ukraine. Three of the five Eyes countries (US, Canada and UK) also have significant multilateral opportunities for intelligence cooperation with many Baltic states through NATO. But not all Five Eyes countries have extensive intelligence cooperation with the Baltic states. Yet intersecting global and emerging security interests (e.g. Russia, China, critical infrastructure, hybrid warfare, human trafficking, global health security and human trafficking) suggest the Five Eyes alliance and Baltic states as collectives could benefit significantly from sharing foresight capabilities and knowledge. How should this be done in a practical sense? There are two broad pathways to progress this initiative. First, there is a political/policy dimension where all Five Eyes and Baltic countries underscore the political will to cooperate more broadly on sharing foresight intelligence knowledge. An example of this would be for political leaders in each country to send a senior representative of their intelligence communities to an intelligence exchange hosted by a Baltic country such as Finland, Germany, Poland or Sweden. Perhaps given Poland currently has the Presidency of the Council of the Baltic Sea States it could be hosted there. This high-level intelligence exchange would provide a regular forum for Five Eyes and Baltic states heads of intelligence to exchange foresight assessments on emerging threats risks and hazards of mutual interest and to identify collection and analytical gaps in knowledge. A second dimension to improving foresight intelligence cooperation could include a range of working level activities focused on improving practice and enhancing capabilities. On practice, a virtual foresight analytical community of practice on intelligence priorities could be co-chaired (one Five Eyes and one Baltic nation) to test key judgments and improve foresight assessments. University researchers with intelligence and defence programs and experience working with their respective intelligence agencies could also be invited to open-source forums aimed at helping intelligence analysts work on complex foresight analysis. On capabilities, heads of intelligence agencies (for Five Eyes and Baltic states) could establish a technical working group to identify ways to improve foresight intelligence collection, analysis and anomaly detection using AI and other machine learning techniques. Such measures would have tangible benefits for global security but particularly in Europe and the Indo-Pacific.

Patrick F. Walsh
Professor, Intelligence and Security Studies
Charles Sturt University
Australia

GREG FYFFE

Hypothetical futures and the polycrisis

Expert article • 4009

The current geopolitical environment, with interlocking existential crises, has been described as a "polycrisis". How do we understand the future in such a world?

Intelligence collectors and analysts focus first on the short and medium-term challenges that are of immediate concern to policy officials. However, military procurement, alliance building, and intelligence capacity development are all part of preparing for a future environment that may be two decades away.

There is always an explicit or implicit view of the future that is the focus for intelligence collection, analysis and policy. Effective planning requires a combination of processes to strengthen strategic anticipation.

Future scenarios are usually based on a limited number of drivers and trends. Complications and scenario variations multiply as the time horizon lengths. If potential drivers and significant trends are unavoidably numerous, the number of anticipated futures may expand to the point of uselessness.

The multiple existential threats of the polycrisis make it challenging to summarize future possibilities within a limited number of actionable scenarios. Too many scenarios make the future world less, not more, comprehensible.

There are multiple dimensions to the polycrisis: Russian and Chinese aggression, the US ambivalence towards alliances, climate change, potential financial crises, global immigration, potential pandemics, criminal networks, disinformation, and the rise of authoritarian populism. Critical longer-term questions arise from each of these crises.

Crises are interconnected. Bankrupt national treasuries, disease-stricken armies, and disastrous weather, have all influenced the course of armed conflicts. Systematic speculation on the course and consequences of these and other threats to global stability will help define the targets of intelligence collection and the subjects of analysis.

Formal futures exercises are useful, not because they focus on questions that no one is approaching through studies, conferences or internal debates, but because they can surface additional possibilities by using a different perspective, different questions, and different participants.

What are the alternative approaches to looking at future possibilities without generating an unwieldy number of complex narratives?

In place of using some of the standard scenario methodologies, two variations may be more promising. One alternative is to isolate a driver which historically influences events over a long timeframe. The second is to identify future states of particular interest and understand the pathways that would credibly lead to them—and the consequences that could follow.

Ideology in history is a driver that builds an impact over a long period. An interpretation of history may arise in the mind of an individual or small group, but over time dominate national and international events. What is the future of populist authoritarianism? Are there influential counter-narratives? Is there a potentially effective counter-ideology to the US MAGA movement? How do political ideologies integrate the dominance of technology?

Are there factors that can detect an incipient ideological trend and reflect usefully on the consequences for the future? Do these factors provide any focus for intelligence collection, and ultimately for policy decisions? Ideologies grow when there is an apparent system dysfunction, a theoretician, a popularizer, a target group to blame, an action plan, and a potentially large pool of supporters.

An analysis of these factors could detect in an almost invisible faction the potential for growth to a movement able to compete for national power. For already established parties, an analysis of current ideologies could be useful in understanding the potential for further popular appeal, and the implications.

The goal is to suggest how positive popular opinion trends could be encouraged and negative ones diminished. This might include a focus on security dimensions, but also domestic policy. Ideologies have impacts, and those impacts are diverted by counter-ideologies, and perceptions of potential outcomes.

A second approach to understanding future possibilities is to start with a description of a plausible and significant end-state. With specific possible futures of concern, and some agreement about the principal details, the possible pathways to that state can be elaborated, and the consequences and leverage points explored.

Building an imagined pathway between the present and the future is not easy with any method. Historical events seem to follow a predictable path when seen in retrospect. When we look to the future from our current reality, there are numerous consequential alternate futures.

There are already possible futures that are a preoccupation for engaged countries. Will the war in Ukraine end with a stalemate, partial Russian victory, or a restored Ukraine? What will the European strategic environment look like if the US retreats from its historic European commitments? A futures focus on end-states could add value to the analysis.

A series of exercises focused on either a single important driver, or on possible end states, sacrifices the variety of possibilities that flow from traditional scenario processes that incorporate multiple trends and drivers. In a highly complex world, this may be necessary to enable conversations that will generate directly useful conclusions.

Greg Fyffe
Executive Director (2000-2008)
Intelligence Assessment Secretariat, Privy Council Office
Canada

ggfyffe@icloud.com

TONI AHLQVIST

Future uncertainties, emergence and context: On interface of strategic foresight and intelligence studies

Expert article • 4010

In this brief essay I chart a selected interface between the fields of strategic foresight and intelligence studies. I view these fields through a lens of future uncertainties and argue that both of these fields need to cope with varied levels of uncertainty in a context, be it a set of future pathways or other substance matter. I argue that in both of these fields it is crucial to understand two related aspects of future uncertainties: 1) horizon of uncertainty and 2) emergence in a context.

The first connecting feature between the two fields is the need to define the horizon of uncertainty. Horizon of uncertainty refers to an analytical continuum ranging from known and projectable events to unknown entities looming on the edge of imagination. In strategic foresight, so-called "futures cone" is among the most widely known methodological frameworks for conceptualising future uncertainties, unravelling a variety of future pathways extending from probable and likely futures to possible futures, occurring only under certain conditions, and eventually landing on preposterous futures that are radically different from the present (see, e.g., Voros 2003).

However, there are also other frameworks that could be considered. For example, in a classic article Kahneman and Tversky (1982) discuss variants of uncertainty. They propose that there are two basic sorts of uncertainty: external, referring to the instances themselves, and internal, referring to a reasoning process. External uncertainty can be further divided into distributional perspective, based on multiple instances, and singular perspective, based on a single instance. Internal uncertainty can be also divided into two perspectives: reasoned perspective is based on rational arguments and evidence and introspective perspective is based on confidence. This framework opens intriguing options for assessing uncertainties in an operational environment. For example, is the event identified in the operational environment an objective novelty, that is, new in a context, or is the newness of the event based on an interpretation, that is, on an internal view? If the event seems to be objectively novel, one could firstly assess if it is based on distributions of multiple instances or just on a singular instance, and then move towards interpretations. Then again, if the event is based on interpretation, one could assess if there are rational arguments and evidence endorsing it or is it based on mere confidence, a strong hunch. After this internal assessment it is possible to move towards external assessment.

Furthermore, combination of the futures cone and Kahneman-Tversky frameworks would enable analysts to pose relevant future-directed questions and provide value-added information. Analyst could, for example, scrutinise potential future events from two perspectives, firstly evaluating the scope of future uncertainty horizon and then assessing the variants of uncertainty ranging from external to internal.

The second connecting feature between the fields of strategic foresight and intelligence studies is the need to understand emergence in a context. Both fields aim at analysing novelties, that is, new phenomena, that could catalyse significant changes in the operational environment. The operational environment is, basically, characterised by two kinds of dynamic elements: continuous trajectories and discontinuous events. Continuous trajectories spring from history, and, with varying probabilities, some of them can be expected to continue in the future. Discontinuous events are instances that disrupt the flow of continuities, something that could escalate and result in game-changing transformations. In strategic foresight, continuous trajectories are usually called trends or megatrends, and discontinuous events are called weak signals or emerging issues. But how to assess these?

This is where the context steps in. In an earlier article (Ahlqvist & Uotila 2020), we argue that when interpreting signals in the operational environment, with whatever method, it is crucial to understand the relations between the signal context and the context of the signal observer. This insight enables the analyst to differentiate between signals that are novelties in multiple contexts and signals that are novel only in one context. Thus, the analyst could find valuable information of the signal, and reduce the related uncertainty, by knowing its contextual setting. Contexts could also be purposefully moulded through a stream of artificial signals, thus producing uncertainty with intent (see Ahlqvist & Uotila 2025). This practice has become increasingly prevalent in the current geopolitical conjuncture.

To conclude, there are plethora of connections between strategic foresight and intelligence studies. Metaphorically, both fields are based on a future-oriented sensemaking process that is realised with a partial and selective present perspective, with one hand grasping for yesterday's evidence and the other hand reaching towards tomorrow's novelties that could become.

References:

Ahlqvist, T. & Uotila, J. (2025). Context moulding and the production of uncertainty: Exploring future signals in geopolitical (dis)information spaces. Forthcoming in Liuhto, K. & Sipilä, J. (eds.) Inevitable Instability in Russia: Strategic information, intelligence and foresight on Russia. Springer Nature. Palgrave MacMillan.

Ahlqvist, T. & Uotila, T. (2020). Contextualising weak signals: Towards a relational theory of futures knowledge. Futures 119, 102543.

Kahneman, D. & Tversky, A. (1982). Variants of uncertainty. Cognition 11: 143–157

Voros, J. (2003). A generic foresight process framework. Foresight 5(3): 10–21.

Acknowledgements

I would like to thank the Research Council of Finland (project numbers 353056 and 348531) and Business Finland (project number 6819/31/2023) for financial support.

Toni Ahlqvist
Professor
Finland Futures Research Centre, Turku
School of Economics, University of Turku
Finland

CHRISTOPH O. MEYER

Why intelligence-based foresight has lacked impact

Expert article • 4011

The great promise of strategic foresight is the combination of more rigorous and imaginative thinking about likely and possible futures with ways of engaging and empowering decision-makers to better prepare for and shape the future. However, this promise is at best partially fulfilled. The reasons are found either in shortcomings of the analysis or, alternatively, decision-makers' receptivity to and use of foresight. My argument is that both matter but receptivity and willingness to use are more important.

There are plenty of examples of strategic intelligence that turned out be right in retrospect. Whether these are the 1990 National Intelligence Estimate by the US about the break-up of Yugoslavia, a 2009 analysis by the EU-civilian Intelligence Hub INTCEN that correctly imagined an Arab uprising-type scenario, or the 2020 assessment of the German foreign intelligence service BND that deemed an Emirate 2.0 as the most likely longer term scenario for Afghanistan after the Trump-Administration's Doha Deal with the Taliban.

Yet there are also many cases when intelligence services missed or hugely underestimated change, where underlying assumptions turned out to wrong, or were not even scrutinised. Sometimes analysts were too focused on a single country and thus missed events and dynamics between countries and that created ripple effects. For instance, ISIS utilising instability and weak borders between Syria and Iraq or Moscow reacting to events on Maidan square. Analysts also underestimated the impact of the arrival of new communication technologies and their strategic use by social movements, authoritarian states and terrorist groups. They listened more to establishment actors in foreign security services than to the "street" in many Arab countries, forgetting the lessons of the Iranian revolution. Many Western intelligence services underestimated the deep societal and historical roots of Russian imperialism and the drivers of its revisionism. At times, analysts where more surprised about the behaviour of "friends" and "partners" than what adversaries did, including Ukraine capacity and willingness to defend itself against the full-scale Russian invasion.

However, the main reason for why intelligence-based foresight has often not met expectations lies with organisational cultures, attitudes of senior decisionmakers and public discourses. The most useful strategic foresight is by its nature disruptive to existing assumptions, policies, and political narratives. Bureaucracies and decision-makers have found imaginative and sometimes problematic ways of stopping disruptive or troublesome foresight from emerging and becoming highly visible. Foresight may expose major vulnerabilities – whether this is in defence capabilities, sources of energy or global supply chains - that decision-makers feel they do not have the money or political capital to address. They may be too focused on short-term party-management and are afraid of hostile reactions from the media and public opinion. After major surprises, decision-makers and organisational leaders in many countries have showed a lack of interest in learning the rights lessons, for instance after the 2014 Crimea surprise.

We can use strategic foresight not just to better identify and warn about threats but also to highlight opportunities for shaping a better future – and to make it more actionable in the short-term. This would mitigate warning fatigue and shift the mindset of foresight users away from managing potentially distant risks and threats towards a sense of empowerment in what they can and should do today, how they can surprise adversaries and shape a more desirable European and international order. It is about convincing decision-makers that past strategic successes can be replicated – from the policies that won the Cold War to Eastern Enlargement. This can help to energise and mobilise political supporters and convince politicians that they build a positive legacy.

The second way is to promote future-literacy among policy-communities, the media and the wider public. Currently, public debates in some European countries are dominated by self-appointed futurist, grand strategists and think-tankers who churn out future-scenarios tailored to what clients want not what they need or what the public finds exciting or sufficiently scary to attract attention. It can be hard for lay-audiences to distinguish a scenario underpinned by thousands of hours of research by experts from those produced by generalist skilled writers who can produce scenario in a couple of days supported by the latest AI tools. These give foresight as a craft and a science a bad name and create erroneous perceptions of the limits and the potential of professional future-thinking. This is why it is important for analysts to develop a stronger consensus around how good foresight looks like and to challenge poor foresight. We should seek to learn from countries like Finland who have a strong reputation for state-of-the-art strategic foresight and integrating it into the political process. This also needs to happen between European nations and within multilateral organisations like EU and NATO.

Christoph O. Meyer
Full Professor of European & International Politics
King's College London
UK

chirstoph.meyer@kcl.ac.uk

JARI KAIVO-OJA

Interfaces between intelligence research and foresight research: Promoting fruitful interfaces

Expert article • 4012

In this article, I briefly examine the interfaces between intelligence activities and foresight practices, as well as the research challenges that emerge between these research domains. It is first useful to reflect on the mutual interface between intelligence research and foresight research. The definition of these interfaces is often linked to methodological and theoretical questions, as well as to the reciprocity between the two research areas. Both research domains can be beneficial to one another: foresight research can draw upon intelligence studies, and intelligence studies can, in turn, benefit from foresight research. Ideally, this critical interaction may produce positive synergy. In poorly functioning scientific cooperation, however, such synergy can be absent or even negative. Hence, it would be valuable to consider how to strengthen the positive synergy between these two areas of research.

When reflecting on this challenge of synergy, we may, for instance, ask how various foresight methods (trend analysis, scenario analysis, weak signal analysis, wild card analysis, and multidisciplinary futures studies) could support intelligence work (e.g. threat assessment, risk evaluation, strategic signals related to comprehensive security, and preparedness). Conversely, we may consider how intelligence materials and information - whether classified or open-source - could contribute to foresight and futures research. This also raises interesting questions about the reciprocity of these scientific domains.

Can foresight research learn from traditional intelligence methodologies (such as data analyses of intelligence, information analysis, risk assessments, surveillance findings, and monitoring data and information)? Or might intelligence studies benefit from foresight methodologies (megatrend analyses, scenario analyses, weak signal detection, Delphi studies, horizontal scanning results, cross-impact analysis, etc.)? A particularly interesting unifying research field between foresight and intelligence concerns ethical, legal, and administrative issues - for example, how the oversight of intelligence activities should be organised in the future; how citizens' fundamental citizen rights should be safeguarded; or how data usage and public foresight reports could be conducted according to high ethical standards. These are by no means easy research questions, and undoubtedly more research activities are needed.

We may conclude that the interface between **foresight**, **futures research**, and **intelligence** is complex and multifaceted both theoretically and practically. Understanding this interface may help us see how futures knowledge and decision support can be integrated across different social contexts - such as strategic management, political decision-making, security policy, corporate competitive analysis, technology foresight, and systems analysis. This integrative task poses a significant challenge for each of these forward-looking research domains. Table below presents some of the key differences - and to some extent, similarities—between intelligence studies, foresight research, and futures research.

Table. Intelligence Studies, Foresight Research, and Futures Research

Research aspects	Intelligence Studies	Foresight Research	Futures Research
Research Interests	Security, survival in wartime conditions, national interests	Supporting decision-making in various contexts such as business, public administration, science, technology, innovation policy, and civil society	Exploring global, national, and local alternative futures
Research Objectives	Supporting strategic interests	Identifying, assessing, and outlining possible, probable, and desirable futures; providing practical guidance for decision-making	Identifying, assessing, and outlining possible, probable, and desirable futures
Nature of Research	Analytical, evidence-based information gathering	Usually creative, participatory, based on weak signals, scenarios, and trend analysis	Concerned with universal issues and long-term challenges of sustainable development
Time Perspective	Short to medium term (from days to a few years)	Medium to long term (3–30 years)	Long-term perspective, relevant for planetary boundaries
Primary Aim	Producing precise and timely information for decision-makers	Stimulating strategic discussion and building shared visions of the future	Refining humanity's survival knowledge through multidisciplinary inquiry
Type of Knowledge	Quantitative, evidence-based; evaluation of goals and means based on numerical data	Systemic, combining qualitative and quantitative ("Numbers and Narratives"); focused on weak signals, wild cards, megatrends, and trends	Systemic understanding of social and ecological systems; emancipatory knowledge production for media and public communication
Use of Knowledge	Strategic decision-making in governmental and administrative contexts	Application in "Quadruple Helix" interactions (government, industry, academia, and civil society)	Global actors such as UN agencies, the World Bank, the IMF, the OECD, etc.
Stakeholders	The state, corporations, power centres	Typically, "Quadruple Helix" actors	All stakeholders, actors pursuing the common good, and governments

The interfaces can be approached through four dimensions: (1) the **knowledge process dimension**, (2) the **purpose of knowledge use**, (3) the **organisational dimension**, and (4) the **institutional dimension**. Foresight activities generate strategic, future-oriented understanding (e.g. megatrends, scenarios). Intelligence, on the other hand, continuously monitors the present situation and changes in the operational environment (e.g. strengthening signals, emerging risks, and critical uncertainties). The key distinction lies in the fact that intelligence validates and updates the assumptions of foresight, whereas foresight provides intelligence with long-term frameworks and direction for analysis.

Regarding the **purpose of use**, foresight supports strategic planning and innovation, while intelligence primarily supports operational decision-making and risk management. The c**ommon ground** between the two is their shared objective: reducing uncertainty in decision-making across different time horizons. Foresight is typically conducted by research organisations, corporate strategy units, or political planning bodies, while intelligence is carried out by defence, security, and business intelligence organisations. Both rely on **networked, confidential information exchange** and shared analytical frameworks (such as risk-opportunity matrices).

A practical approach to managing these interfaces is to distinguish between **Strategic Intelligence**, **Horizon Scanning**, and **Futures Intelligence**.

- **Strategic intelligence** combines the long-term perspective of foresight with the analytical tools of intelligence, and is particularly suited for government and corporate executive decision-making.
- **Horizon scanning** functions as a joint tool for identifying weak signals and wild cards that may evolve into significant phenomena or trends.
- **Futures intelligence** merges foresight methodologies and intelligence processes, and is utilised, for example, in the strategic analyses of NATO, the BRICS countries, and the European Union.

In essence, **foresight provides direction and creates opportunities,** while **intelligence research monitors, validates, and warns.** Yet, this division of labour is not always so clear or simple in practice. Very complex interactions may emerge. For example, data and information leaks make interactions complicated and complex. The research interface involves continuous dialogue between the **possible** and the **probable** futures—a boundary that is itself often difficult to define in practice.

Jari Kaivo-oja
Research Director
Finland Futures Research Centre, Turku School of Economics, University of Turku
Finland

Docent (Adjunct Professor)
University of Helsinki
Finland

Docent (Adjunct Professor)
University of Lapland
Finland

Docent (Adjunct Professor)
University of Vaasa
Finland

Professor
Kazimieras Simonavičius University (KSU)
Vilnius, Lithuania

jari.kaivo-oja@utu.fi

LINDA RÄIHÄ

Foresight and intelligence: Sides of the coin

Expert article • 4013

In an era when strategic foresight and intelligence were not yet fully formed, one thinker bridged the two. In the atomic age that followed the World Wars, military strategist, physicist and futurist Herman Kahn reminded that deterrence requires confronting what we would prefer not to face. He argued that lasting stability is possible when societies and their leaders face uncomfortable possibilities before they become realities, thinking the unthinkable. This was not only about fear and survival but also about building trust through awareness, a security born from clarity rather than denial. Although foresight and intelligence evolved along different paths, Kahn's reasoning laid the groundwork for a fusion that enables anticipation and early action before crises unfold.

Strategic thinking in the atomic age grew out of deterrence: a tense balance between logic, fear, and the need to face the unthinkable. Kahn's call for clarity amid discomfort still resonates. His insight, forged in the atomic era, continues to shape the logic of foresight and intelligence; two sides of the same coin.

Today, the boundaries between states and enterprises have eroded. Economics, technology, and security now form one surface of that coin, turning constantly between public and private powers. Hybrid warfare and interference unfold not only in military or political arenas, but also within corporate strategy, research funding, and recruitment networks. The logic of deterrence has expanded. Power is no longer projected through weapons such as drones alone, but through data, cyber capabilities, artificial intelligence, access, and narrative control.

Technological espionage illustrates this new strategic paradigm. Though most actors operate with good intentions within structurally vulnerable systems, the modern "benevolent fool" may be a researcher, student, or employee who shares information with openness, unaware of its strategic value. Universities and research ecosystems, traditionally open by design, have become contested interfaces of soft power. The threat often arises not from malice, but from structural naivety and the lack of integrated foresight and securitization, as the Copenhagen School has noted.

Strategic intelligence anticipates developments through evidence and analysis, while strategic foresight explores broader and alternative futures. Between them lies a dynamic space of anticipation, the narrow edge of the same coin. There lies the ability to act before systems shifts to critical. This fusion enables the foresight and intelligence into a continuous, adaptive process where the intelligence cycle and scenario modelling evolve together.

Building on my recent thesis work, a dynamic foresight–intelligence framework was developed to integrate continuous data analysis, human interpretation, and scenario simulation into one adaptive system. The model showed how combining analytical precision with anticipatory reasoning accelerates and strengthens strategic decision-making. By linking risk analysis to scenario planning, the approach shortens response times, improves situational awareness, and enhances resilience in rapidly changing environments.

As the information society accelerates, static scenarios and narrow intelligence assessments fail to match its pace; their findings often arrive too late to stay relevant. A shift toward a dynamic framework built on human–machine cognition allows algorithms to process immense datasets and detect probabilities, while human judgment provides context, values, and interpretation. The result is an adaptive intelligence system capable of learning, simulating, and refining decisions in real time.

When foresight and intelligence merge, organizations and states can navigate the futures landscape more proactively, shifting from reactive defence toward anticipatory action. This integrated approach enables rapid testing of futures and detection of vulnerabilities before they manifest, turning uncertainty into an operational asset rather than a threat.

Through this approach, foresight becomes the strategic nervous system of intelligence, and intelligence the empirical grounding of foresight. Together with emerging technologies such as quantum computing and game theory, this fusion expands the prospects for real-time strategic reasoning — enabling organizations and states to simulate complex futures, detect early signals, and decide before environments shift.

Kahn's words remain relevant. Deterrence today means anticipating not atomic escalation, but systemic collapse through misinformation, cyber interference, or technological dependence. Thinking clearly about what we would prefer not to think about is still the first step, not just toward survival, but toward trust, resilience, and a new strategic fusion for the futures. Only now, clarity must arise from joint human–machine cognition under central human oversight. No need to flip the coin.

Linda Räihä
MSSc (VTM) in Future Studies
University of Turku
Finland

linda.raiha@protonmail.com

MAX STUCKI

Value from foresight in strategic decisions

Expert article • 4014

As the world grows more volatile, organisations, both private and public, have increasingly recognised the need for foresight, the systematic exploration of the future from their own point of view, to prepare for both the expected and the unexpected. As a result, foresight activities are being adopted and developed across sectors. However, in my professional experience, it often remains unclear what exactly their ultimate purpose should be. It is customary to say that foresight should inform decision making, but how that actually translates into practice and measurable value remains a challenge. When this challenge goes unaddressed, organisations sometimes close down foresight functions because they fail to demonstrate tangible results. There are ways to avoid this disappointing and needless outcome, which deprives organisations of the value foresight can generate.

First, having witnessed these struggles, my emerging understanding is that foresight is not merely another function, like market intelligence, competitive analysis, or risk management. Rather, foresight draws from all these sources and others, combining them to produce a view of the potential futures the organisation could face. In this sense, it acts as a metafunction that synthesises different information streams and uses them to generate forward-looking assessments, or futures intelligence. As a function of a different kind, it should also be treated accordingly in terms of expectations and resourcing.

A second key point is to recognise that if foresight is to inform decision making, it must do so at the point when decisions are being made, not afterwards. Once leadership has already committed to a course of action, even the best foresight-derived insights are unlikely to shift established thinking. In other words, foresight inputs should be integrated during decision making, for example when strategies are being developed. Strategies and plans should emerge from the future environments the organisation expects or might encounter, not merely from current conditions and naïve linear projections.

A third way to extract value from foresight is to use it as a corrective mechanism. Whereas organisations typically take corrective action when financial or operational data signal failure, foresight can deliver forewarnings that trigger proactive measures in the present to avoid potential dangers. This requires leadership teams to meet regularly to review and interpret the organisation's current view of the future in a structured way, and to determine what it means for operations. Doing so makes the value of foresight tangible, as it leads directly to informed and timely decisions.

A fourth observation about getting value from foresight is that organisations should share the futures intelligence they generate widely. Broad dissemination sparks new insights and encourages colleagues to engage in discussions that enrich the collective futures view with their diverse professional perspectives. If futures information remains confined to a small leadership group, which in some cases may be appropriate, such as in sensitive strategic decisions, the organisation risks losing much of its value. People remain unaware of potential changes and, more importantly, miss opportunities to think about how they could best take advantage of those changes.

Fifth, and perhaps most importantly, to generate lasting value, all foresight activities should be systematic, continuous, and guided by organisational needs and decision-making cycles. In other words, foresight should be tightly integrated into the decision-making system or framework the organisation follows, rather than operating as a separate or ad hoc exercise. To achieve this, the foresight function should have a clear mandate and direct access to those whose decisions it is meant to inform, ensuring that its insights are not diluted or delayed as they move through layers of the organisation. When foresight is embedded in this way, it becomes part of the organisation's natural rhythm of learning and adaptation, continuously scanning the environment, interpreting change, and feeding actionable intelligence into the strategic process. For such integration to succeed and endure, however, organisations must also be able to evaluate how well their foresight function performs and what value it delivers over time. Before establishing a foresight function or team, the organisation should therefore define clear deliverables and intended impacts. Linking these to measurable KPIs allows for assessment of the value derived from foresight activities. Monitoring those KPIs then enables continuous improvement, ensuring that foresight serves the organisation's evolving interests and needs.

In a world that seems to grow more uncertain with each passing day, engaging in a systematic study of change and its implications for the organisation is both beneficial and common sense. Foresight, when implemented properly, offers the tools and frameworks to do so.

Max Stucki
Senior Manager, Foresight Process
Futures Platform oy
Helsinki
Finland

STEPHEN BLANK

Russia's intelligence state and its war

Expert article • 4015

Russia is conducting a global war against the West. But this war's central theater is Europe which, from Ukraine, is under increasing attack, especially in the Baltic. This war validates Clausewitz's insight that war is a chameleon. Among the multiple forms of attack Russia has employed are attempted coups d'etats, election interference, influence operations, unceasing cyber and information attacks, arson, assassinations, attacks on terrestrial and maritime civilian infrastructure, employment of organized crime groups as Russian proxies, subsidizing of foreign political parties, and plain old espionage. Indeed, attempted coups are part of the huge expansion of Russian-backed gray-zone activities whose number has quadrupled since 2022 making this a truly global war. Moreover, some Russian military thinkers who believe that proxy wars, i.e where Russia incites natives or foreign third parties to fight for its interests, cause in their home countries, e.g by coups, may be increasing into the future.

Western observers have been unable to assign a definitive name to these attacks confirming their shape-shifting character. Nonetheless, we can discern certain commonalities in their direction, planning, and operation. Specifically, the evidence shows that these "hybrid" or "gray zone" attacks are led by, planned and conducted not by Russia's armed forces but by its intelligence agencies, both military intelligence (GRU) and its domestic and foreign intelligence agencies (FSB, SVR). Thus, whatever else they are, they are and represent intelligence wars.

This should not surprise us for Russia is and for some time has been an intelligence state where the leadership, not just Putin, is over-represented by people having known (and probably covert) links with these intelligence agencies. Furthermore, these elites have grown immensely rich and powerful by virtue of these linkages between the intelligence community and both organized crime and Russian business. Therefore, there is every reason to believe that these elites who are connected both in terms of their families and institutionally have every reason to fight to maintain their position and the system that has endowed them with such wealth and power.

In fact, led by Putin, these alumni of Russia's Soviet intelligence heritage have steadily recreated the classic traditional Russian paradigm of state power with an allegedly all-powerful Tsar ruling in the absence of any institutional or legal constraints on his power through his network of servitors (Boyars) in the classic formulation. Indeed, since these servitors of the patrimonial state where the Tsar literally owns the state receive rents, i.e. posts atop key industries, in return for their service thereby recreating the Muscovite service state where a rent-granting state is served by rent-seeking officials. Thus, corruption and criminality as well as violence and repression are pervasive. It is no accident that we see the recrudescence of the Gulag under "the organs" administration even before the war against Ukraine that has triggered a major and continuing increase in both repression and the scale of the Gulag. In line with Russian legislation the FSB has the unlimited right to interfere with any business that it chooses to engage. Thus, it has become impossible to do business in Russia without FSB approval or involvement in a firm.

Likewise, the state and the intelligence organs have propagated the myth that these organs are the true knights in shining armor defending the state against internal and external enemies. Those enemies are the reformers who alone (but with sizable foreign help) brought down the USSR in an information war launched from abroad but with the help of these alleged subversives. This mythology of the exalted intelligence officer also extends as well to Russian foreign and defense policy. This is because what Alexander Herzen termed the romance of the police is tied to an equally long-standing series of interlinked myths prevalent among the security services. These myths are that Russia alone is a true Christian state and foreordained to be a great global power, yet it is permanently under attack from external and internal enemies. Thus, pace Carl Schmitt, Russian security power starts from thew presupposition of conflict.

And since Russia is militarily technologically inferior to its enemies it must have recourse to the weaponization of every instrument or relationship of power. And outside of large-scale force majeure this campaign, like what we are seeing must be directed not only by the Tsar or its contemporary equivalent, the Presidential Administration and the intelligence community who compete for Putin's favor, resources, and standing. In this war the main front for Russia's so-called hybrid activities appears to be the Baltic region and Baltic Sea. Information warfare, influence operations, espionage, have gone on constantly for years and evidently have increased by an order of magnitude since the aggression against Ukraine began. Baltic Sea infrastructure, e.g. cables linking the various littoral states, have become prominent targets for Russian attacks. Jamming of aerial GPs has also become a permanent feature of Russian attacks across the Baltic Sea to include Finland and Sweden. An in September Russian jammers attacked EU President Ursula Von Der Leyen's plane signaling a noticeable escalation in these attacks. Russia's "shadow fleet" of third party ships carrying sanctioned Russian products have also become a persistent challenge to NATO navies in the Baltic Sea. Worse yet, "Mezhdunarodnaia Zhizn' (International Affairs), the Foreign Ministry's official journal, has just published an article calling the Baltic Sea region a "potential theater of military conflict" because NATO countries are. allegedly threatening Russia. This article not only justifies the gray zone attacks against the Baltic littoral states but justifies an escalation as well in their number and type. And since many Russian military thinkers view such attacks as preparing the ground for large-scale military engagements, we too must view them as potentially preparatory attacks for a larger war and prepare accordingly. In short, Russia's intelligence state is not just a Mafia state or criminal enterprise as many have written, it also is a permanent war state for which we must be ready.

Stephen Blank
Senior Fellow
Foreign Policy Research Institute
USA

www.fpri.org

HANNA MÄKINEN

Russia's hybrid warfare in Europe

Expert article • 4016

Since Russia's full-scale invasion of Ukraine, Europe has seen a surge in suspected hybrid operations – sabotage, cyberattacks, disinformation, and espionage – designed to destabilise without triggering open war. Hybrid warfare blends military and non-military tactics to exploit vulnerabilities and achieve strategic goals, often operating in a "gray zone" that complicates detection, attribution and response.

From Crimea to escalation of hybrid operations

Though hybrid tactics are ancient, the term gained prominence after Russia's 2014 annexation of Crimea and the war in Eastern Ukraine, where it used unmarked troops, cyberattacks, economic pressure, and disinformation to legitimize its actions. Since then, Russia has repeatedly employed hybrid methods. These include, among others, interfering elections to sow discord and undermine trust in democracy, disrupting societies and economies with cyberattacks and sabotage, and creating energy dependencies to exert economic and political pressure.

In our study published by the Finnish National Defence University, we analysed the coverage of Russia's hybrid operations in European media in the 2000s (Mäkinen & Liuhto 2025). We found that suspected cases of Russian hybrid operations have occurred with increasing frequency since Russia began its full-scale war in Ukraine in 2022, and especially since 2024. Russia's faltering war in Ukraine has led it to intensify its hybrid campaigns against the West, aiming to erode the consensus on Western support for Ukraine and sanctions against Russia. In addition, the expulsion of hundreds of Russian intelligence officers acting under diplomatic cover has forced Russia to change its way of operating in Europe.

Opinion manipulation and election interference

According to our study, Russia's hybrid warfare spans four dimensions: economic, political, societal and military. These dimensions often overlap, with for instance disinformation campaigns serving multiple strategic purposes – undermining unity in the EU and NATO, influencing public opinion and elections, and weakening support for Ukraine.

By spreading false narratives, especially via social media, Russia seeks to manipulate public opinion and election results, undermine trust in democratic institutions, and strengthen societal polarisation. The 2024 EU Parliament Elections were preceded by a major disinformation campaign that targeted large EU member states to reduce support for Ukraine and boost pro-Russian candidates. Recent examples of election interference concern Moldova's parliamentary elections in September 2025, where, along with spreading disinformation, Russia was alleged of vote-buying and protest funding, and the first round of Romania's presidential elections in December 2024, where a pro-Russian candidate surged via a TikTok campaign, leading to annulled election results.

Disrupting infrastructure and society

Media has reported about suspected Russia-linked sabotage and cyberattacks that have targeted railways, energy and telecommunication cables, and public services in Europe. In addition, GPS jamming has disrupted air and sea traffic. Though impacts have so far been limited, large-scale disruptions of infrastructure could paralyze critical sectors like logistics and finance.

Hybrid tactics can also be used to cause insecurity and instability. In 2024, hundreds of schools in Czechia and Slovakia received bomb threats, and logistics and commercial facilities in Germany, Lithuania, Poland, and the UK were targeted by arson attacks. Instrumentalised migration has also been used to provoke political and societal strain – Russia and Belarus have directed asylum seekers to EU borders on several occasions during the last decade.

Ambiguity and diverse actors

Hybrid warfare blurs the line between war and peace. It is often unclear whether incidents are state-sponsored or random acts, and proving guilt and holding someone accountable is difficult. Russia increasingly uses intermediaries and digital platforms like Telegram for recruitment, making attacks harder to predict and trace. Russia also typically denies involvement and floods the media with misleading information to further increase confusion.

Nevertheless, defending against hybrid threats requires balance. Over-securitisation can also fuel fear and undermine democracy – playing into an adversary's hands. Because Russia seeks to cause confusion and division, fostering cooperation and information sharing at national and EU levels is a key to countering hybrid influence.

References

Mäkinen, Hanna – Liuhto, Kari. 2025. Russia's shadow war: The media coverage of Russia's hybrid war against the EU in the 21st century. In Russia's war against Ukraine: Trends and lessons (Ed. Pentti Forsström). Department of Warfare, Series 2: Research Reports No. 37. Helsinki: National Defence University. https://urn.fi/URN:ISBN:978-951-25-3535-4.

Hanna Mäkinen
Senior Researcher
Pan-European Institute
University of Turku
Finland

OLGA BERTELSEN

Russian influence operations among western intellectuals

Expert article • 4017

Russian subversive operations among foreign academics, intellectuals, and politicians are corrosive not only to democracies and their values, but they make Russia's military solutions in Georgia, Ukraine and elsewhere possible. Recruitment and cooptation of the Western intellectual and political elites help Russian intelligence spread disinformation and reinforce narratives that emanate from the Kremlin. Russian intelligence professionals understand very well that whoever controls the narrative has power. They thoroughly study the vulnerabilities of target countries and prepare them for major political manipulations, using a combination of techniques, including disinformation, targeted assassinations and the like. These operations have been quite successful, and Estonia and the United States serve as the most recent and persuasive examples of the effectiveness of these techniques. Viacheslav Morozov, professor of Political Science at Tartu University, and Dimitri Simes, Russian-American author and editor, spread disinformation for years before the former was arrested by the Department of Police Security of Estonia and the latter was indicted by the U.S. Department of Justice.

With technological advancements and proliferation of social media platforms, the dissemination of false narratives as part of information warfare has become more sophisticated and difficult to detect. The dynamics and the results of these operations illuminated the fact that Western educational and research institutions constitute a vulnerability in each state and a target for Russian subversive activities. Because of their pervasiveness, it is absolutely vital to safeguard Western democratic institutions and academia and to curtail Russian influence or at least alleviate its impact. Two counterintelligence avenues appear to be effective: 1) the governments of democratic states should change laws and regulations to protect their institutions and citizens from the damaging effect of influence operations and propaganda; 2) the states should establish programs to educate broader audiences about Russian disinformation and recruiting operations and techniques. They should be free of charge or heavily subsidized by the government or local authorities.

These measures imply serious reforms in the areas of education, law enforcement, and communications capacities. Western governments need to reconceptualize their approach to alleviating exploitable vulnerabilities of their states, improving public diplomacy and enhancing societal awareness about Russia's attempt at subverting democratic societies. These efforts will help ordinary people stay alert and increase their activism, responding publicly to Russian falsehoods. The openness of Western academia by definition remains a problem and a vulnerability that encourages Russian intelligence to target expert communities, well-educated and knowledgeable. Cooperation with Russian agents of influence (including scholars) and Russian front organizations, as well as the acceptance of substantial funding from them for questionable activities, should be punishable by law. The main argument against this approach is articulated by the defenders of human rights and the First Amendment of the U.S. Constitution: Western democracies, they argue, should engage Russian academics and experts in a dialogue with foreign scholars instead of isolating them. Yet many American and European academic institutions undertook a logical step, discouraging dialogue and any ties with Russian state-sponsored educational institutions, after many prominent Russian scholars and educators signed the "Statement of the Russian Union of University Rectors" that supported Russia's war against Ukraine and called to stand behind their president and the "special military operation" in Ukraine. Notably, the European Union has terminated cooperation with Russian research institutions, suspending payments to existing contracts and ceasing new ones under Horizon Europe. The majority of non-Russian scholars argue that suspension of cooperation between Russian and Western academia is warranted and needed, at the very least until the end of the war and deconstruction of the Putin regime. Clearly, Russia's genocidal practices in Ukraine do not facilitate bridge-building activities between Russia and the West.

Interestingly, this pause in cooperation has not been ultimately translated into a pause in Russian influence operations conducted in the West. Inspired by Putin's Order # 229, Russian intelligence is as active as in the past, but it seems to rely more on the achievements and assets built at the end of the Cold War and during the first two decades of Putin's reign. In this climate and space, foreign scholars themselves should take responsibility and develop robust knowledge about foreign influence operations, which will enhance their ability to distinguish between disinformation and truth, and forge certain levels of confidence and intellectual fortitude to understand and withstand the pressure of Russian soft power. Most importantly, they have to publish studies on the topic in English to attain broader readership, as well as the accounts of their own experiences being targeted by Russian influence operations. These exposés will significantly disrupt Russian intelligence's subversive activities and degrade their networks overseas.

Olga Bertelsen
Associate Professor of Global Security and Intelligence
Department of Criminal Justice and National Security
Tiffin University
USA

bertelseno@tiffin.edu

CRAIG UNGER

America's new Manchurian Candidate

Expert article • 4018

Anyone who follows the scribblings of the Washington press corps knows all too well that journalists who probe the ties between Donald Trump and Russia are promptly dismissed by the White House as a conspiracy nuts who have been taken in by the "Russiagate hoax."

I, of course, find that deplorable.

As I've chronicled in two books—House of Trump, House of Putin, and American Kompromat—I believe Donald J. Trump is the beneficiary of the greatest counterintelligence failure in history, one that allowed the Russian Federation to install an asset of Russian intelligence in the White House as president of the United States.

That's right. Russian intelligence has its own man in the Oval Office.

My thesis is not yet widely accepted in the United States, but I'm not the only one to come to that conclusion. In one form or another, no fewer than three former CIA directors— John Brennan, James Clapper, and Michael Hayden— have all said the same thing.

But if it's true, how could that possibly have happened?

As a child in the Sixties, I was entranced by the 1962 movie, The Manchurian Candidate, in which a Communist plot did something similar. But that was Hollywood. In real life, how could that have happened? How could Russia have installed an intelligence asset in the Oval Office, thereby executing one of the most devastating attacks on American sovereignty in history— all. without firing a single shot.

As I show in my books, what took place was the result of a two-pronged attack involving both the KGB and the Russian Mafia.

The story began more than 45 years ago when Donald Trump was a young developer enjoying the fruits of his first success in real estate, the development of the Hyatt Grand Central Hotel in New York. Like any hotel, it needed hundreds of TV sets. One might think that a major outfit like Hyatt would buy the TV sets from a huge vendor like Sony or Samsung, but Trump bought them from a small operation called Joy Lud Electronics, which happened to be a front for the KGB.

That was the opening.

Moreover, the Soviet émigrés at Joy Lud were not the only operatives to reach out to Trump. In 1984, a man named David Bogatin, who was tied to the Russian Mafia, dropped by Trump Tower and plunked down $6 million (about $33 million in 2025 dollars) in cash for five condos in the building that was the crown jewel of Trump's growing real estate empire.

In so doing, the Russians were effectively laundering money through Trump real estate—because they were buying luxury condos via an anonymous corporation an all-cash transactions. (It is worth noting that the Russian Mafia, which played a crucial role in cultivating Trump, far from being an enemy of the state, is actually an arm of Russia's intelligence services.)

And so Russians began laundering hundreds of millions, perhaps billions of dollars, through Trump real estate, in effect bailing out Donald Trump from one business disaster after another. Oligarchs and mobsters moved into Trump Tower. Before long, they owned him.

And for more than 40 years, Russian intelligence began to implement one "active measure" after another through Trump, often getting him to articulate policies that aided Russia far, far more than they did the West.

Of course, having a Russian asset in the Oval Office has already dealt a devastating blow to the Western Alliance which has provided vital support for the democratic institutions, market economies, and military alliances in the West since the end of World War II. One has only to look at America's less-than-steadfast support of Ukraine in its battle against Russia's invaders. All of which leads one to wonder how strong NATO really is if the United States is no longer a reliable partner.

And, finally, one has to ask whether Trump's presidencies will mean the end of American democracy.

The answers to these difficult questions are still not clear, alas.

But the battle is not over yet.

Craig Unger
Author of several books, including *House of Trump*, *House of Putin* and American Kompromat
New York, USA

craig.unger@me.com

His most recent book is *Den of Spies: Reagan, Carter, and the Secret History of the Treason that Stole the White House*.

MIKKO PORVALI

Russian human intelligence in a new environment

Expert article • 4019

Russia's intelligence collection in Western countries has become significantly more difficult since the outbreak of its war of aggression against Ukraine. At the same time, Russia's need for information about Europe has deepened as geopolitical dividing lines sharpen. As a result, Moscow is now urgently seeking new sources of information in the West.

For a hundred years, the principal method of Russian foreign intelligence has been long-term human intelligence. Russian intelligence culture—and its celebrated successes of the twentieth century—has rested largely on effective human-source recruitment.

The contemporary importance of human intelligence for Russia is illustrated by international prisoner exchanges. In these exchanges, Russia has reclaimed from Western prisons deep-cover illegals, assassins, hackers, and arms traffickers. Western states, by contrast, have received opposition leaders, a basketball player arrested for cannabis possession, and a civic activist detained for swapping price labels in a supermarket. This disparity does not mean that Western agents are never caught, but more likely that the West relies predominantly on other methods of intelligence collection.

For Russian authorities, human intelligence is not merely one collection discipline among others. It is an organisational culture — a way in which these Russian organisations have always operated. Intelligence gathering has traditionally been organised through officers deployed to the West under diplomatic cover or false identities.

That world changed when the West unexpectedly closed ranks in response to Russia's aggression. The precursor was the 2018 poisoning of the Skripals in Salisbury. More than 150 Russian intelligence officers operating under diplomatic cover were expelled from various countries. The United States expelled 60 diplomats, the United Kingdom 24 — other states smaller numbers — but nevertheless the common front held.

When Russia launched its full-scale invasion of Ukraine in 2022, the West expelled an unprecedented number of Russian diplomats. Russia's traditional "residency" networks and human-source operations were weakened, as was access to many elite circles. Managing networks and meeting agents became more difficult. Russia's brutal conduct of the war has damaged its global reputation. Therefor it is probable that recruitment no longer proceeds smoothly even among previously sympathetic circles in politics, business, science, or the media.

As geopolitical divides deepen, Russian intelligence services cannot accept a paralysis of their collection capabilities. Lost channels and networks must be replaced — but there are very limited ways to do so.

Other intelligence disciplines will certainly be strengthened, yet organisational culture cannot be transformed quickly. Russia will continue to rely heavily on human intelligence, once its networks can be rebuilt.

Since motivating Western partners to assist Russia has become more difficult, pressure is now placed increasingly on the Russian population residing in Western countries.

Under Russian law, Russian authorities have the right to issue administrative orders to their citizens. Individuals are obliged to obey these orders regardless of the country in which they reside — or whether such orders violate the laws of their country of residence. Failure to comply is criminalised. Russia does not recognise dual citizenship in a way that would release individuals from their obligations as Russian citizens. Vulnerability is further deepened if a person has family members, property, or other interests in Russia.

Where the recruitment of Western citizens often requires identifying vulnerabilities — or actively creating them — the vulnerabilities of Russian citizens exist by default and are usually documented in state registers. These may include, for example, a parent or child living in Russia.

Western intelligence and security agencies thus face a difficult task. Everyone's rights must be respected, and no individual may be monitored solely on the basis of origin. At the same time, Western countries host large numbers of people whom Russia considers its citizens and who are, without question, more vulnerable to pressure from a foreign state than the population at large.

Western authorities must therefore proceed with vigilance and be equipped with adequate legal powers. Equally important, however, is how we treat members of our Russian-background minorities. Every discriminatory act gives grounds to Russia's claims of Russophobia or the need to defend its citizens living abroad.

Ensuring equal treatment and respectful conduct toward all individuals — regardless of minority or citizenship — is therefore essential for our national security. In this regard, the struggle for the hearts and minds of Russians living abroad is one of the most important challenges Europe will face.

Mikko Porvali
Author, Doctoral Researcher
University of Jyväskylä
Finland

JARDAR ØSTBØ

Russia is not a 'KGB state'

Expert article • 4020

Intelligence actors, activities, and culture play an increasingly important role in Russian politics and society. This must be reflected in how Russia's foreign and security policy is viewed. However, Russia is not a 'KGB state'.

The last decade and a half, the chekists (current and former employees of the security services) have strengthened their grip on power at the expense of the oligarchs and the technocrats, the two other main groups of the wider Russian elite. Intelligence methods, such as provocations, covert information gathering, information operations, and even assassinations, are parts of everyday political life. The belief in hidden motives, enemy plots, and the encirclement of Russia are at the heart of mainstream public debate. Former and current intelligence officials have increasingly privileged access to President Putin. The autocrat is said to start his workday reading intelligence briefings, with the authors competing to please him with analyses that suit (and exacerbate) his rather paranoid worldview. When comparatively more moderate voices get the president's ear, their assessments are largely brushed off.

Among the intelligence and security agencies, the FSB is the biggest and undoubtedly the most influential one. It seems clear that, for instance, the decision to go to full-scale invasion of Ukraine in 2022 in part was based on faulty or even fabricated intelligence provided by the FSB, indicating that Ukrainian resistance would be miniscule. The service also failed their mission to prepare the ground properly for regime change through provocations, covert action, and the development of effective collaborator networks. Nevertheless, the consequences for the individuals carrying the formal responsibility for these fiascoes have been minimal. Colonel General Sergei Beseda, Director of the FSB's Fifth Service, was reputedly under arrest for a while. However, he kept his post for two more years, before becoming adviser to FSB Director Aleksandr Bortnikov. In March 2025, Beseda was even one of the leaders of the negotiation team in Riyadh.

The 'special military operation', now a strange euphemism for all-out war, was initially a rather accurate term. At first, the 'full-scale invasion', as it is known in the West, was not conducted according to current military doctrine, and was not really full-scale, relying instead to a great extent on lightly armed special forces, provocation, diversionary tactics, and surprise. This reflected the chekist belief in 'special operations' as the tool to solve virtually any problem. Operational secrecy was taken to the extreme, to the extent that military commanders were kept in the dark until the last moment, with US and UK intelligence seemingly better informed than the ones who soon were to lead the operation on the ground. As the 'special operation' turned into a war of attrition, failures were largely blamed on the military leadership, with several generals, as well as Minister of Defence Sergei Shoigu and his deputy Timur Ivanov, being fired.

The present salience of intelligence actors, activities, and culture in Russian politics has led some observers to call Russia a 'KGB state'. The president spent formative years in the KGB, several of his former colleagues have gained prominent positions, and in the KGB's successor agencies there is considerable continuity as regards personnel, methods, and culture. Nevertheless, the 'KGB state' label is misleading and anachronistic. Most obviously, Russian politics and society have changed fundamentally since the fall of the Soviet Union. In the 1990s, postcommunist intelligence and security services had to find their place in a globalizing world and a predatory capitalist economy, forced to fight with oligarchs and organized criminal networks for power and influence. After initial stupefaction, the chekists found themselves exceedingly well equipped for this struggle, as they put to use the full spectrum of resources at their disposal. They were also freed of ideological constraints and political oversight. At the same time, they had to adapt to the new circumstances, forming a working relationship with, rather than all-out war against, organized crime and private business. Former intelligence officers entered organized crime and the intelligence services could use criminal methods, themselves or by proxy. The boundaries between politics, intelligence, and organized crime as regards actors, activities, and culture were blurred.

The Russian regime, personified by Putin, for all practical purposes represents a hybrid of these elements. Western decisionmakers seeking to counter, negotiate with, or otherwise engage the Russian regime should keep this in mind.

Jardar Østbø
Professor, Head of Programme for Russian Defence and Security Policy
Institute for Defence Studies, Norwegian Defence University College
Oslo, Norway

JOHN HELIN

Interpreting the Russian milblogger ecosystem

Expert article • 4021

Since the beginning of Russia's full scale invasion of Ukraine, Russian military bloggers, voenkors, have become one of the most visible Russian voices in the Western infosphere. Mostly working through the instant messaging app Telegram, their updates are routinely used by journalists, analysts, and social-media pundits. While often associated with Russian state narratives, they do not form a homogenous group. Instead they constitute a dynamic, contradictory and often quarrelsome information ecosystem where social-media commentary and participation in the war effort mix.

The voenkor landscape that emerged to the larger world in 2022 was a chaotic mix of frontline reporters, nationalist commentators, hobbyist analysts, and social-media aggregators. Over time the voenkor ecosystem has matured: some channels operate almost like miniature newsrooms with outside funding, while others are operated by single individuals relying on donations. Most are overtly pro war, however this does not mean that they simply act as propaganda mouthpieces. Many of the channels have often voiced their concerns about the way the war is being conducted.

As their influence has grown, so has the state's interest in shaping the environment. Russian authorities have spent the past two years pruning the ecosystem. The arrest of Igor Girkin, warrants on other bloggers, and even the recent branding of some pro war commentators as foreign agents, all signal a changing dynamic in state attitudes. While the boundaries remain transient, some patterns are visible: voenkors may criticise incompetence, logistics, or battlefield decisions, but challenging the legitimacy of the war or attacking political leadership is forbidden.

Those who adapt generally survive, others may face repercussions. In this sense the critical voenkors represent a form of patriotic dissent: a pressure valve for airing grievances while framing criticism as loyalty. This does not produce a unified narrative but rather a narrower band of tolerated discourse. Instead of blindly repeating state messaging, some voenkors attempt to substantiate their narratives through OSINT methods or other means, signalling good-faith engagement with the wider information space.

For example, now widely known Rybar-channel attempted to prove the Russian narrative of the Bucha-massacre via satellite imagery in early 2022, even walking back some of its claims when being proven wrong. However, these self-reflective actions have become rarer as the war has continued.

At the same time many voenkors have become de facto social-media influencers, with engagement central to their livelihoods. Like most social-media ecosystems, here too posts that provoke strong reactions are rewarded. Contradictory or emotional narratives generate engagement, incentivising grander claims, faster posting and suggestions of privileged access. These pressures shape what voenkors say as well as how they justify and present their narratives.

Given this adaptive environment, the question becomes what kind of information voenkors actually provide and how it should be used to assess the war. Despite attempts to describe the battlefield, their information should rarely be accepted as-is. This is particularly important with ideologically motivated channels. Instead they should be used to provide interpretations that reflect the specific role of each channel within the ecosystem. Voenkors are aware of these roles. Many engage in open discourse with each other, not only by reposting material but by criticising and publicly evaluating the claims made by colleagues or by the state. For observers this discourse is a useful analytical tool. The pattern of who challenges whom and who remains silent can be as informative as the original post.

Channel type also matters. Large accounts claiming to cover the entire frontline may be under closer state observation and more tied to state narratives. Smaller channels linked to volunteer units or specific sectors may have more room to operate or may offer more grounded local information. However, analysts must remain cautious. Narratives that contradict the mainstream view are not automatically more accurate. They may simply reflect the experience of a single sector or even a single unit.

For analysts and journalists in the Western infosphere, the key is to read voenkors in context. What matters is not only what they say, but why they highlight certain events, how channels react to each other's narratives, shifts in tone or anxiety, and how closely these narratives align with other available evidence. When used carefully, voenkors offer insight into the social dynamics and development of narratives around Russia's war effort. Used uncritically they become another layer of noise in an already crowded information space. Their real significance lies less in individual posts or singular details, and more in the broader trends and forces that emerge from the voenkor ecosystem at large.

John Helin
Analyst
Black Bird Group
Finland

john@blackbirdgroup.fi

RODNEY E. PEARCE

Russian medically assisted homicide

Expert article • 4022

Doctors and other medical professionals are a component of Russian Intelligence health attacks and assassinations both inside and outside of Russia. Medically disguised murders are an underappreciated concern because of their perceived plausible deniability and because of the difficulty many countries have in detecting and preventing these crimes. These methods have replaced other Soviet-era methods of removing dissidents and other victims.

During the Stalinist Terror of the 1930's through to the alleged doctor's plot in the 1950's, Soviet propagandists spread the idea that doctors in the USSR used medical treatments for diseases such as Tuberculosis to kill patients. This Soviet propaganda replaced earlier Tsarist and Orthodox Christian ideas of doctors as impartial preservers of life. The training and practice of Soviet doctors was dependent on the approval of the Soviet security services such as the Cheka and later the KGB. The Soviet security services often coopted doctors to serve them before graduating medical school.

Under Joseph Stalin, anyone in the Soviet Union was susceptible to Gulag incarceration or execution for any alleged transgression. After Stalin's death, abuse of the medical system and particularly the psychiatric system replaced these methods of repression. Soviet security services used false psychiatric diagnoses to imprison victims throughout the Soviet period. By the 1960's psychiatric misdiagnosis became one of the main methods of incarcerating dissidents. By the 1970's the KGB desired to incarcerate many more dissidents than Soviet mental institutions capacity.

Contemporary Russian intelligence services still misuse the psychiatric system to incarcerate and discredit dissenters. Shamanic protester Aleksandr Gabyshev is a recent example of a protester incarcerated indefinitely under a psychological pretense. Abuse of psychiatry by the Russian security services is less common than it was during the Soviet period, but Russia is currently in the midst of a state-sanctioned murder spree. High profile assassinations include prominent oligarchs, politicians, protest leaders, and journalists. Medical practitioners such as doctors, paramedics, and pathologists have been involved in facilitating and covering-up these murders.

Prominent opposition leader Alexei Navalny died in 2024 of what Russian government pathologists declared to be an unusual sudden death from a combination of chronic medical illnesses. Alexei Navalny's widow asserts her late husband was murdered and that Russian doctors ignored the signs of poisoning. Prominent journalist Yuri Shchekochikhin died of apparent polonium radioisotope poisoning which was claimed by attending Russian physicians to be a rare extreme allergic skin reaction. The wife, brother, and son of Russian defector Sergei Skripal all died of various supposed "natural causes" in Russia during the four years prior to the unsuccessful 2018 poisoning of Skripal and his daughter in the UK by Russian Intelligence officers.

One commonality in these murders is the manipulation of medical professionals and attempts to disguise the murders as natural medical conditions. Russian intelligence services attempt to control the victims' medical treatment and postmortem medical examiners. Poisonings often occur when urgent medical care can be obstructed such as during train or plane travel. For each widely known example, there are an unknown number of other victims whose murders have gone unnoticed.

Recruiting medical professionals are an effective way for Russian intelligence to disguise murder and this practice is unlikely to be confined to Russian territory. Murders attributed to Russian intelligence such as shootings, deaths by falling, and obvious poisonings have occurred inside Russia and around the world. Given the global spread of other less-easily disguised Russian assassinations, the disguise of murders as medical conditions is not limited to Russian territory.

Russia has the means to interfere with medical practices outside of Russia through Russian agents in medical professions and medical schools around the world. In 2022 a married couple of American doctors were caught attempting to pass sensitive information to Russian intelligence. In their legal defense, the couple referenced their family's proximity to Russian agents both inside and outside of Russia. These are not the only Russian agents in medical professions, but they are some of the only medical doctors to be caught spying for Russia.

These doctors are archetypal of contemporary Russian intelligence networks in the healthcare sector. Russian foreign intelligence has made extensive efforts to build large scale agent networks which often include family connections. These agent networks operate outside of Russia with few obvious connections to Russia. Medical practitioners in these networks both gather information and conduct active measures. Despite the high value of medical practitioners to Russian intelligence for espionage, health attacks, and assassinations, Western counterintelligence rarely prioritizes medical fields and national security checks for doctors and nurses are almost unheard of. The use of medical professionals by Russian intelligence for espionage and active measures are a warning that medical professionals and healthcare services worldwide require additional protection and that medically disguised assassinations an underappreciated danger worldwide.

Rodney E. Pearce
Independent Consultant
USA

KARI LIUHTO

Critical information needs on Russia

Expert article • 4023

Since the collapse of the Soviet Union in 1991, Russia has repeatedly arrived at major societal turning points — moments that could have redirected its development along an entirely different trajectory or even endangered the state's existence. Foresight analyses conducted over this decade indicate that Russia continues to experience lingering aftereffects of the USSR's disintegration, and some projections suggest that the country may be drifting toward instability or chaos. This highlights the importance for Western analysts of anticipating Russia's future direction.

The purpose of this column is to contribute to intelligence studies on Russia by pinpointing the most pressing information gaps that will likely influence the country's long-term development. To achieve this, the article compiles the perspectives of ten Finnish senior experts on Russia concerning these critical information needs. The empirical material was gathered through surveys and in-person interviews in January-May, 2025.

Governance: According to the experts, one of the foremost priorities is identifying the individuals who actually hold political power — particularly those operating outside the formal structures of the state. Equally significant is understanding the interconnections between dominant power clans and regional authorities. The experts express concern over the political role of the armed forces and security institutions, focusing on their internal cohesion, loyalty to the Kremlin, and the degree of competition or rivalry among the so-called 'power ministries'. Additional areas of concern include the rise of Islamic separatism and the emerging relationship between the Kremlin and a business elite aligned with the US MAGA movement.

Economy: The experts call for deeper insight into Russia's overall debt levels — spanning the public sector, private enterprises, and households. The socioeconomic situation of 'monotowns' also emerged as a central issue. These towns, whose economies depend almost entirely on a single enterprise, number more than 300 across Russia and are home to approximately 14 million people. One expert underscored the deteriorating state of Russia's strategic infrastructure as a particularly urgent concern. The ongoing war is draining the resources required to maintain the nation's highways, rail networks, and oil and gas pipelines, developments that may severely weaken both societal resilience and economic competitiveness. Another recurring theme in the interviews was Russia's artificial intelligence (AI) capacity, identified as a critical area requiring closer scrutiny. The experts also emphasised the importance of understanding the true nature of the Sino-Russian economic relationship — including Russia's dependence on Chinese goods, the scope of China's business footprint in Russia, and the depth of technological cooperation between the two countries. This focus is understandable given that by 2024, roughly 50 percent of Russia's imports originated from China. When Vladimir Putin became first time President of Russia in the year 2000, this share was only less than three percent.

Society: The experts also concentrated on the growing internal strains within Russian society. This is a particularly important topic, as many of these tensions predated the invasion of Ukraine and have likely intensified since. Long-standing sources of friction include inequality in living standards, ethnic and religious conflicts, tensions between locals and migrants, and disputes related to sexual orientation. The Russian military's expansion of youth-focused education — often bordering on chauvinistic indoctrination — has further heightened the experts' interest in understanding how young Russians perceive their own future. Rising military expenditure has come at the expense of social spending, worsening the already poor state of housing and communal services — a sector that was below Western standards even before the invasion. Experts view this as a vital area of investigation, as the system's ongoing decay may deepen public dissatisfaction. Moreover, discontented veterans returning from the war in Ukraine could, in time, form a politically destabilising force. Several experts also drew attention to the views of Russian intellectuals and cultural figures, who increasingly constitute the final bastion of public dissent in the country.

Military: In the military sphere, experts seek to better understand the real capabilities of the Russian armed forces. They highlight the importance of assessing the state of conventional weapons stockpiles and Russia's capacity to manufacture advanced systems — including hypersonic missiles, drones, and other unmanned platforms. Attention is also directed toward the progress of Russia's ongoing military reform. Given that Finland shares NATO's longest land border with Russia — more than 1,300 kilometres — it is unsurprising that Finnish experts are particularly interested in the condition of Russian military bases near this frontier. Equally, they express strong interest in the development of Sino-Russian military cooperation. Lastly, the experts underline the growing necessity of understanding Russia's hybrid operations across Europe, which have expanded markedly in recent years.

Table. A summary of selected critical information needs

Governance Kremlin power clans and their interaction Regional power clans and their views Unity and loyalty of army and security services Advancement of Islamic separatism movement MAGA-Kremlin relations	**Economy** Indebtedness and creditors Situation in monotowns State of strategic infrastructure Ability to utilise artificial intelligence Sino-Russian technological cooperation
Society Internal tensions in Russian society Militarisation of society (Youth Army) Degradation of social services Veterans of the Ukraine war Russian diaspora and its contacts in Russia	**Military** Missile and drone production Advancement of military reform Military bases in border regions Sino-Russian military cooperation Russia's hybrid war against the West

This column is based on my article published in a book "Inevitable Instability in Russia: Strategic Information, Intelligence and Foresight on Russia" (eds. Kari Liuhto and Joonas Sipilä) by Palgrave Macmillan in 2026.

Kari Liuhto
Professor of Intelligence Studies
National Defence University and University of Turku
Finland

Photograph: The Maidan Nezalezhnosti (The Independence Square of Ukraine), September 1987.

Centrum Balticum

BALTIC RIM ECONOMIES

To receive a free copy,
register at
www.centrumbalticum.org/en