human FORWARD

INTELLIGENCE

What Europe Needs To Know

Illustration ilbusca/iStock

Editorial

Dr. Rebekka Reinhard,
Editor-in-Chief

Dear Reader,

Europe is undergoing profound transformation. The year 2026 marks the moment when the governments of our continent abandoned the hope of a swift easing of transatlantic relations – in favor of greater strategic autonomy and sovereignty. This concerns not only AI-driven digital resilience, but also industrial and military resilience. One of the most essential prerequisites is access to reliable information. "We are protecting our free democratic fundamental order against its internal and external enemies" said Chancellor Friedrich Merz at the Munich Security Conference, adding: "Among other things, we will strengthen our intelligence services."

Europe is entering an era that can only be understood through an unprecedented "intelligence" culture extending far beyond the traditional intelligence-service context. The original, in part exclusive international contributions and interviews in this digital special edition therefore present "intelligence" for the first time as a holistic and urgent societal, political, economic, and technological task for Europe's future. The white paper **"Intelligence: What Europe Needs to Know"** connects domains that have so far been discussed separately in research, policy, and practice – thereby creating a novel reference framework of high practical relevance for the twenty-first century. Our aim is to contribute a humanistic approach to strategic foresight. For "intelligence" must not be regarded solely as an instrument of national security or economic risk minimization, but as an infrastructure for a free democratic society.

Whether the issue is cybersecurity or OSINT, data protection or urgently needed public-private partnerships – everywhere, a viable balance between security interests, transparency, fundamental rights, and collective self-enlightenment is decisive. We thank our top contributors from Germany, the United Kingdom, Italy, Belgium, Switzerland, and the United States for their insights and learnings.

By the way: The **Mona Lisa** on the cover is a fake – as are those on the inside pages of this publication. Would you have recognized it? Under conditions of uncertainty, what we need more than ever is rigorous source criticism and careful reconstruction of context. This applies equally to examples from art history and to political and social, economic, and technological matters.

Let's rethink intelligence. Let's reclaim humanity – and move human forward. Write to us – we look forward to your feedback!

Munich, March 2026
Let's rethink intelligence. Let's reclaim humanity – and move human forward.
Write to us – we look forward to your feedback!

Kind regards,

rebekka.reinhard@human-magazin.de
thomas.vasek@human-magazin.de
human-magazin.de
human Magazin, Dr. Rebekka Reinhard, Thomas Vašek
human_magazin, rebekkareinhard

Photo Sung-Hee Seewald

Contents

Editorial ... 2

01_Intelligence Matters

Knowledge Is Power ... 5

Thomas Vašek_ **What Europe Needs to Know** ... 6
Niccolo Petrelli *(University Roma Tre, Italien)*_ **Hybrid War** ... 13
Wolfgang Krieger *(Universität Marburg)*_ **New World Order** ... 16
Interview: Loch K. Johnson *(University of Georgia, USA)*_ **International Cooperation** ... 21
Christoph Meyer und Daniel Rainer Neumann *(King's College, UK)*_ **Reform of the Intelligence Services** ... 26
Interview: Klaus Schmidt *(Oberst a. D., BND)*_ **The Federal Intelligence Service** ... 30
Beatrice Heuser *(Brussels School of Governance, VUB, Belgien)*_ **Open Societies** ... 34

02_Insight

Advantage Through Knowledge ... 42

Interview: Jennifer E. Sims *(Stuart Street Atelier, USA)*_ **Decision Advantage** ... 43
Interview: Alana Gramm *(IBM iX)*_ **OSINT** ... 50
Simon Wunder *(Volkswagen AG)*_ **Geopolitical Risk Intelligence** ... 54
Interview: Daniela Richterova *(King's College, UK)*_ **Sabotage** ... 57
Interview: Christopher Radler-Moric *(Consultant)*_ **Corporate Security** ... 61
Interview: Ole Donner *(Consultant, Strukturierte Analyse Deutschland)*_ **Structured Analysis** ... 65

03_Technology

Own Capabilities Instead of Dependencies ... 68

Interview: Marcus Willett *(IISS, Ex-GCHQ, UK)*_ **Cyber Operations** ... 69
Armin Müller *(Central Europe Veeam Software)*_ Advertorial **AI Security** ... 77
Timo Blenk und Christina Schäfer *(Agora Strategy)*_ **Space** ... 78
Jeff Watkins *(Founder North Star Alliance, UK)*_ **Persuasion** ... 83
Interview: Frank Sauer *(Metis Institut für Strategie und Vorausschau)*_ **AI Warfare** ... 89
Richard Weiss *(Consultant, e. g. NATO Centre of Excellence COE)* und Marc Mahlke *(Consultant Cybersecurity)*_ **Cyber Threat Intelligence** ... 93
Interview: Krista Marija Läbe *(Quantum Systems)*_ **Aerial Intelligence** ... 97
Interview: Julian Werner *(Center for Intelligence and Security Studies, Universität der Bundeswehr München)*_ **Urban Warfare** ... 101
Aviva Guttmann *(Universität Aberystwyth, UK)*_ **Signals Intelligence** ... 104
Interview: Ralf Schneider und Lars König *(NetWatch)*_ Advertorial: **Threat Intelligence** ... 107

Interview with Krista-Marija Läbe, communications strategist at Quantum Systems and co-founder of the German-Ukrainian Society (Deutsch-Ukrainische Gesellschaft, DUG)

04_Governance

Controlling Power, Building Trust 112

Interview: Konstantin von Notz *(German Bundestag, Parliamentary Oversight Panel)_* **Parliamentary Oversight** 113
Interview: Luca Manns *(Universität Köln)_* **Reform of the BND** 119
Interview: Jan-Hendrik Dietrich *(Hochschule des Bundes, Berlin)_* **Militant Democracy** 122
Eva Herschinger *(Universität der Bundeswehr, München)_* **Protests** 126
Interview: Anna Daun *(Hochschule für Wirtschaft und Recht, Berlin)_* **Intelligence Culture** 130
Interview: Holger Janusch *(Hochschule des Bundes, Berlin)_* **Strategic Intelligence** 134
Interview: Esther Omlin *(Ostschweizer Fachhochschule OST, CH)_* **European Cooperation** 138

05_Ecosystem

Harnessing Europe's Strenghts 141

Brendan Kotze *(Performanta, UK)_* **Intelligence Architecture** 142
Interview: Rafaela Kraus *(Universität der Bundeswehr, München)_* **Cognitive Warfare** 148
Raluca Csernatoni *(Carnegie Europe, Belgien)_* **Cognitive Security** 152
Jim Sengl und Felix Rieger *(KI.M KI Kompetenzzentrum Medien)_* Advertorial **Media Sovereignty** 156
Interview: Larysa Visengereyiva *(Women in Defense Tech WiDT)_* **Preparedness** 158
Irina Rosensaft *(Expertin für Digitale Transformation und Cybersicherheit)_* **Collective Intelligence** 163
Interview: Dennis-Kenji Kipker *(Cyber Intelligence Institute, Frankfurt a. Main)_* **Cyber Resilience** 168
Birger P. Priddat *(Universität Witten/Herdecke)_* **Democratic Intelligence** 171

Facts

Contributors & Interviewees 177
Partners 181
Imprint 181

01_Intelligence Matters

Knowledge is power

"The strategy employed by European countries to counter Russia's escalating hostile intelligence activities has demonstrated moderate effectiveness."

Niccolò Petrelli, Italien

Illustration FierceAbin/iStock

"Have we reached a point where we must take active countermeasures?"

Martin Jäger, President of the Bundesnachrichtendienst (Federal Intelligence Service),
February 13, 2026

In the Service of Democracy

Democracies need reliable knowledge in order to remain capable of acting. In a world of digital data floods, hybrid attacks and disinformation, intelligence is becoming a central infrastructure of the open society.

The seriousness of the situation was evident in Martin Jäger. The President of the Federal Intelligence Service (BND) spoke about Russian cyberattacks, disinformation, sabotage, drone overflights, contract killings. And he chose clear words: it was Russia's leadership that was orchestrating destabilizing campaigns in our societies. In doing so, it pursued the goal of splitting NATO, installing pro-Russian governments, delegitimizing the EU: "If Russia were to succeed, the consequences would be felt everywhere."

The BND president then posed a question: " Do we simply want to continue to observe and record these developments, or have we reached a point where we must take active countermeasures?" The question also applies to the BND, Jäger added – and immediately answered his own question: „In my opinion, the service must and will become more operational."

Jäger's appearance on February 13, 2026 at the Munich Security Conference was remarkable in several respects. It is already not common for intelligence officers to speak at public events at all. Even more unusual is that a German intelligence chief threatens the Russian leadership with retaliation with hardly any circumlocution. This alone shows how dramatically the world has changed.

BND President Martin Jäger, in office since September 2025, is considered an experienced foreign-policy crisis diplomat, a man for difficult tasks whom one can send anywhere where things are burning. Among other things, he was German ambassador in Afghanistan, later in Iraq and most recently in Kyiv. In the two ›

TEXT_ ***Thomas Vašek***

Thomas Vašek is co-editor-in-chief of *human*. Previously, the trained investigative journalist was, among other roles, founding editor-in-chief of the philosophy magazine *Hohe Luft* as well as of the German edition of *MIT Technology Review.*

KEY MESSAGES

→ **Epochal rupture of the world order:** rules are losing importance, strategic uncertainty is growing – thus the need for intelligence increases.

→ **Transformation of intelligence:** in a world of data abundance, analysis and strategic interpretation of information are becoming increasingly important.

→ **Role of AI and OSINT:** AI and open sources expand analytical capabilities, but also create risks through disinformation and data manipulation.

→ **Epistemic function:** intelligence services become institutional perception and analysis apparatuses.

→ **European perspective:** Europe should coordinate intelligence more strongly, for example through a European OSINT agency.

„Good intelligence helps to make better decisions."

years of his service there, he says he experienced more than 1,000 air-raid alarms.

Jäger is not the typical administrative lawyer one so often finds at the BND. He studied ethnology, philosophy and political science. With his diverse experience – he also worked for a time for the car company Daimler – he is supposed to realign the service and lead it to the "very highest level," as Federal Chancellor Friedrich Merz has formulated as the goal.

TURNING POINT OF THE SERVICES

At the public hearing by the Parliamentary Control Panel in October 2025, Jäger indicated the direction in which he wants to change the BND. The German foreign intelligence service must become "more operational," and that means sometimes taking risks in order to obtain "valuable information." Only in this way would it remain compatible with European and international partner services, for the "hard business" of intelligence cooperation, which is based on the giving and taking of information.

What Jäger has in mind is nothing less than a cultural change at the BND. The service is to become faster, more proactive, more daring. To confront the opponent at times, to offer resistance, even to inflict pain on him when necessary. This would of course require giving the service the corresponding "means and authorities."

The direction is clear: away from mere reporting, toward a "real" intelligence service that also carries out active operations. One that might break into apartments, hack computer networks or sabotage opposing infrastructures if the legal framework allows it. All these questions are of great importance for the services' ability to act.

But it would be a mistake to limit the debate about the upcoming reform of the German intelligence services to questions of "means and authorities." What is decisive is what we expect from the services in the first place, which goals we pursue with them, in Germany as well as in the European context.

In other words: it is about strategy.

In the disruption of the world order there also lies an opportunity for the intelligence services to reinvent themselves. This is about far more than the ability to fend off hybrid attacks more effectively. Even the question of how European services can become more independent of their US partners falls short. What matters instead is how we must organize strategic knowledge in the new "world disorder" in order to safeguard our values and interests.

Intelligence services are not simply a scandal-prone necessary evil, as they are often seen particularly in Germany. We simply need them in order to remain capable of acting in a world that is becoming ever more dangerous, ever faster and more complex.

The international order of the post-war period rested in essential parts on rules, norms and institutions. States could at least roughly anticipate how other actors would react. Rules thus reduced uncertainty. They structured behavior, limited escalation and guaranteed a certain reliability in an otherwise anarchic system.

If rules no longer count, behavior becomes harder to predict. Treaties can be broken, institutional procedures bypassed. In such an environment, decisions require more knowledge. If one can no longer rely on other actors, one must better understand which goals and intentions they pursue. This does not apply only to politics.

It is this kind of knowledge advantage that "intelligence" is about. If one interprets the term narrowly, it simply means the collection and evaluation of information for governments. Good intelligence is knowledge that helps to make better decisions. Experts argue about the precise definition, for example about whether intelligence is fundamentally "secret" – and whether it is a state activity. There is broad agreement that intelligence is more than just information. Information can be anything one learns. Intelligence, by contrast, means processed, verified and appropriately prepared information that corresponds to the requirements of the respective decision-maker. Intelligence is not about absolute truth, writes the American intelligence expert Mark M. Lowenthal, but about a "proximate reality."

Modern intelligence is undergoing a structural transformation. Whereas during the Cold War information was scarce and services had to expend enormous resources and take high risks in order to obtain secret information, today the opposite is the case: information exists in abundance, from commercial satellite imagery to social-media content to leaked mobile phone data offered for sale on the dark web. Many developments – such as military movements, economic trends or social dynamics – can ›

today at least partially be reconstructed from open sources.

The increasing availability of openly accessible information is changing intelligence work. The decisive capability no longer lies primarily in collecting information, but in processing, classifying and interpreting it. Open Source Intelligence (OSINT) and artificial intelligence (AI) are at the center of this transformation.

In some respects the craft of intelligence has become easier, because data are easier to obtain. At the same time, however, it has also become much more difficult to recognize what is truly relevant in the flood of data. "Information is cheap. Processing it is expensive, and sense-making is exquisite," writes Emily Harding, intelligence expert at the Center for Strategic and International Studies (CSIS), in her article "Intelligence in a Transparent World."

Today's digital flood of data has several consequences for classical forms of intelligence work. First, their function shifts: covert methods serve less for general information acquisition than for clarifying specific questions that open sources cannot answer, such as political intentions or internal decision-making processes.

Second, the digital transparency of modern societies also increases the risks for operational activity. Individuals today leave extensive digital traces – through biometric data, travel movements or online activities – that can make covert identities and operational contacts easier to detect.

Third, the openness of the information space changes the relationship between state intelligence and other actors. Journalists, research groups, private analysis firms or civil-society networks today sometimes conduct complex OSINT analyses themselves and publish their results publicly. Intelligence services thus partly lose their monopoly over certain forms of strategic analysis.

The war in Ukraine is considered the first "open-source war" in history. Commercial satellite images, social-media data and publicly accessible sensor information made it possible even for civilian actors to observe military developments almost in real time.

Even before the Russian invasion in 2022, publicly available data made Russian troop movements visible. At the same time, the Ukrainian population itself became part of the intelligence system: smartphones, social media and civilian satellite data effectively turned society into a distributed sensor network. In addition there were commercial companies that provided satellite imagery or cyber analyses. Intelligence thus became a collective effort of state, society and the private sector.

Germany's intelligence services

Federal Intelligence Service (BND)

The BND is Germany's foreign intelligence service. It collects and analyzes information about political, military, economic and technological developments abroad that are relevant for Germany's security and foreign policy. Its findings support the federal government in security-policy decisions.

Federal Office for the Protection of the Constitution (BfV)

The BfV is the domestic intelligence service. It observes extremist activities, terrorism as well as espionage activities of foreign services in Germany. Its aim is the protection of the free democratic basic order. The Office for the Protection of the Constitution works in a federal structure together with the state offices for the protection of the constitution.

Military Counterintelligence Service (MAD)

The MAD is the intelligence service of the Bundeswehr. Its task is to uncover and counter espionage, extremism and security-endangering activities against the armed forces. In this way it protects personnel, facilities and the operational capability of the Bundeswehr.

The enormous amounts of data that accumulate at intelligence services can no longer be managed without algorithmic support. Already today the services integrate AI into their analysis and evaluation processes. What once required enormous personnel resources – for example evaluating global media flows or large image archives – can now partly be automated. AI can also combine information from different sources and thus generate situation pictures more quickly or make changes in complex systems visible.

Intelligence becomes faster, more scalable and in some areas also more precise through AI. At the BND, for example, a work unit for AI-supported analysis is supposed to help create a real-time situation picture. At the same time, however, AI also creates new risks. Faulty data or algorithmic distortions can be amplified through automated analysis processes and influence entire chains of decision-making. This becomes particularly critical in security-relevant applications in which AI systems not only analyze information but also support operational processes.

With agentic AI, the next stage of the AI revolution is already emerging. AI agents can independently plan tasks, obtain in- ›

formation and use digital tools. This shifts the use of AI from pure analytical support toward automated action systems – with unforeseeable consequences for cybersecurity.

Agentic systems can already today autonomously carry out large parts of a cyberattack, from target selection to vulnerability analysis to the exploit chain. At the same time, however, AI systems themselves are also becoming strategic targets of attack, for example through prompt injection or manipulated training data. Intelligence services must therefore learn to observe not only human actors but also artificial systems that operate independently in the information space.

For intelligence this means a double transformation. First, AI becomes the central analytical platform with which large data spaces can be evaluated, cyber operations supported and decision processes accelerated. Second, a new dependence on the big tech companies arises that develop and control the most powerful models. Intelligence capabilities are thus partly privatized.

The conflict between the Pentagon and the AI company Anthropic shows that advanced AI models are increasingly regarded as strategic infrastructure. The US government demanded comprehensive access to the company's models for military applications, while Anthropic refused with reference to risks such as autonomous weapons systems or mass surveillance. At the same time China is also pursuing the goal of making AI militarily usable.

The Anthropic case stands exemplarily for a larger dilemma. States see AI as a decisive factor of geopolitical power and want to accelerate its development. At the same time many experts warn that the technology is still immature and dangerous. In the future intelligence will therefore increasingly revolve around who has access to such high-risk systems.

Democracies are based not only on elections, institutions and the rule of law, but also on a shared epistemic foundation, that is, on a minimum of shared knowledge about reality, about risks and political options. Intelligence can contribute to this knowledge. This function becomes more important also because the information space itself has become a strategic field of conflict. Authoritarian actors deliberately attempt to destabilize democratic societies through disinformation, information overload and manipulative narratives. Such operations ultimately aim to undermine trust in any form of reliable information.

In this context intelligence can be understood as part of the epistemic infrastructure of democratic states. State analytical capabilities contribute to ensuring that political institutions remain capable of acting under conditions of growing uncertainty.

Media, academia and civil-society actors make important contributions to public knowledge production, but they neither have the same access to sensitive information nor the responsibility for collective security.

In an increasingly complex information environment, intelligence services function as an institutionalized apparatus of perception and analysis of the state. They collect, verify and contextualize information in order to provide reliable knowledge for political decisions. The aim is the systematic production of insights about risks, intentions and developments in the international environment.

Intelligence does not only have the task of recognizing threats early. It can also help make strategic opportunities visible, identify room for maneuver, and exploit situational potentials. Should our intelligence services not develop the ambition to detect such opportunities in geopolitical or technological competition? And should they not also be allowed, within certain limits, to conduct espionage in order to gain a knowledge advantage?

If intelligence is understood as the perception and analysis apparatus of the state, it can also play an important role for trust in the state's ability to act. Trust in the state arises not only from normative legitimacy or democratic procedures, but also from the assumption that state institutions can adequately recognize reality and act on that basis, across electoral periods.

This presupposes, however, that state intelligence actually leads to a better understanding of reality. In practice intelligence services are also prone to distortions that can lead to misperceptions. Historical examples – such as misjudgments about weapons of mass destruction in Iraq – show that intelligence by no means automatically guarantees superior knowledge. When state analytical institutions err, this can even massively undermine trust.

Democratic knowledge orders live from plurality and openness: science, media, civil society and independent research together contribute to the interpretation of reality. If intelligence becomes the privileged epistemic authority, it can displace or delegitimize these plural processes of knowledge production.

Intelligence services operate at least partly in secrecy. Precisely this secrecy, however, can limit trust in their findings. If central knowledge bases of political decisions are not publicly verifiable, this can even reinforce skepticism and conspiracy theories.

For this reason we must repeatedly reconsider the role of the services in democracy. The question is how they must structurally change in order to remain capable of acting in today's information environment without becoming detached from democratic society. ›

„A common situation picture would improve foreign and security policy coordination."

The idea of a European intelligence service has been discussed for years, but encounters considerable political and institutional hurdles. Intelligence services traditionally belong to the core of state sovereignty; member states are therefore reluctant to give up sensitive sources, methods and operational capabilities. Differences in threat perceptions, legal frameworks and levels of trust further complicate immediate integration.

Against this background a European OSINT analysis agency could serve as a realistic intermediate step. Such an institution would focus exclusively on Open Source Intelligence, that is, on the collection and analysis of publicly available information. Unlike classical intelligence services it would have no covert operations and no secret sources. Its mission would consist of systematically evaluating open data and producing European situation pictures while at the same time ensuring professional analytical standards.

Precisely in a digitized world in which large parts of strategically relevant information are publicly accessible, this form of analysis is gaining strongly in importance. Such an institution would be politically easier to realize than a European intelligence service and could in the long term develop trust, common methods and a European understanding of threats. Open information can be shared far more easily than sensitive intelligence sources.

An OSINT agency could thus build trust and create a common European analysis platform without directly touching national sovereignty. At the same time economies of scale would arise: complex data infrastructures, AI-supported analysis platforms or satellite-based geodata would not have to be built separately by every state.

In addition a European OSINT agency could contribute to the development of a shared perception of threats. Hybrid threats affect Europe as a whole, but are still predominantly analyzed at the national level. A common situation picture would improve foreign and security policy coordination.

Such an OSINT agency would therefore also have an institutional learning function. Joint analytical procedures, training programs and technical standards would emerge. Analysts from different European states would work in common structures and build trust. Such networks are a central prerequisite for any further cooperation in the field of intelligence.

In this sense a European OSINT agency would be less a replacement for national intelligence services than an evolutionary intermediate step. It would create common analytical capacities without immediately centralizing operational competences.

If it succeeds in establishing trust, common methods and a European understanding of the situation, stronger integration could emerge from this in the long term – possibly even the basis for a European intelligence service.

A European OSINT agency would also benefit from Europe's diversity. The EU unites 24 official languages and numerous additional regional and minority languages. An analyst from Lithuania will probably read Russian-language Telegram channels differently from someone without historical and cultural experience in the post-Soviet space.

A sovereign European language model could serve as a central analytical infrastructure that integrates large amounts of open information from different languages, sources and collection methods.

In a world of exponentially growing data volumes, intelligence increasingly becomes the ability to combine technological analytical capacities with human judgment and human values. In this lies Europe's strategic opportunity to gain the decisive knowledge advantage in an increasingly dangerous world.

Europe will have to automate parts of its intelligence in order to remain capable of acting in today's information space. But what cannot be automated is our human strategic judgment – and our human determination to defend our interests and values.

We find ourselves in an "icy peace" that could at any time turn into a "hot confrontation" at specific points, said BND President Martin Jäger in October 2025 at the hearing in the Bundestag. One is confronted with an "aggressive counter-power" that shows little restraint. And what applies to Russia increasingly also applies to other international actors: "We must acknowledge this reality." ›

It is neither military nor economic nor technological power alone that decides in such a confrontation – Jäger knows this as well.

What matters is being more resilient, knowing more, being smarter than the adversary. There is much to learn from Ukraine´s resilience in the last four years, the BND chief said in the Bundestag, not least in terms of mindset.

A confrontation is "won in the minds," a Ukrainian front officer once told him. What matters is the right mindset, the determined attitude. This includes preparing oneself for extreme developments and putting oneself in the position to act under extreme conditions: "Only in this way will we be able to deter our opponents and master the worst case." ■

GLOSSAR

Intelligence
Systematic acquisition, analysis and evaluation of information about actors, risks and developments in order to support political and security-policy decisions.

Intelligence Cycle
Process of planning, collection, analysis and dissemination of information. Describes how raw data are transformed into decision-relevant insights.

HUMINT (Human Intelligence)
Acquisition of information through human sources, such as informants, defectors or covert contacts.

SIGINT (Signals Intelligence)
Evaluation of electronic signals and communications, such as telephone, radio or internet traffic.

OSINT (Open Source Intelligence)
Analysis of publicly available information, e.g. media reports, social media, satellite images or databases.

All-Source Assessment
Integration of different types of sources (HUMINT, SIGINT, OSINT etc.) in order to create the most comprehensive situation picture possible.

Indications & Warning (I&W)
Early warning analysis to identify signs of impending crises, attacks or strategic changes.

Counterintelligence
Measures to protect against espionage, sabotage and influence operations by foreign services or actors.

Covert Action
Covert state operations aimed at political influence abroad in which the authorship is intended to remain hidden.

Intelligence Assessment
Analytical evaluation of developments and scenarios that shows decision-makers possible risks and courses of action.

Resilience Without Resolve

Russia's hybrid intelligence activities are challenging Europe's security architecture. Although countermeasures are having an effect, persistent weaknesses remain.

As we enter 2026, Europe stands at a critical juncture in its shadow conflict with Russia, a war fought not through conventional battles but via a relentless array of hybrid tactics, including sabotage, espionage, cyberattacks, and disinformation campaigns. This confrontation, which intensified dramatically following Russia's full-scale invasion of Ukraine in February 2022, has seen Moscow deploy these methods to sow discord, undermine European solidarity, weaken public backing for Kyiv, and test NATO's thresholds without triggering outright war.[1] Following a sharp rise of detected Russian operations across Europe ranging from arson targeting military supply chains to GPS jamming over the Baltic Sea, which nearly tripled from 2023 to 2024, 2025 brought an unexpected shift, with incidents of traditional sabotage and arson dropping to roughly half the previous year's levels.[2]

This downturn, though encouraging, raises questions about Europe's handling of the intelligence competition with Russia. What kind of strategy have the countermeasures adopted truly amounted to and what, if any, are its key elements? Is it bearing fruit?

Europe has responded to Russia's intensification of the intelligence competition by implementing a resilience and disruption defensive strategy. Connecting intelligence insights with policy and community actions, this has been centered on 4 elements. ›

[1] *Seth G. Jones, "Russia's Shadow War against the West", Center for Strategic and International Studies Brief, March 18, 2025, https://www.csis.org/analysis/russias-shadow-war-against-west.*
[2] *https://www.france24.com/en/europe/20251228-russia-hybrid-warfare-attacks-europe-dropped-this-year-but-could-they-pick-up-2026.*

TEXT_ ***Niccolò Petrelli***

Dr. Niccolò Petrelli is Assistant Professor in the Department of Political Science at Roma Tre University, where he teaches strategic studies. In 2025, he published the book *I servizi segreti italiani e l'Intelligence USA (The Italian Intelligence Services and U.S. Intelligence)* a history of the reciprocal relationship from 1943 to the 1970s.

KEY MESSAGES

→ **Europa** has responded to Russia's hostile intelligence activities with a defensive strategy based on resilience and disruption.

→ **Joint threat assessments** and intelligence sharing have weakened disinformation and influence operations.

→ **Large-scale expulsions** have significantly impaired Russian intelligence networks and their operational capabilities.

→ **Border fortifications** and the protection of critical infrastructure have reduced opportunities for sabotage and prevented "easy wins."

→ **Despite these successes,** European vulnerabilities persist, including fragmentation, delayed attribution, and a predominantly defensive posture.

The first one is joint threat analysis and assessment with the aim of developing a common 'strategic-operational picture', amalgamating threat-perception, and raising public awareness of the threat. The EU had been conducting joint threat assessments since 2020, a practice that intensified in the wake of Russia's invasion of Ukraine in February 2022 within the cadre of the Single Intelligence Analysis Capacity (SIAC), an EU intelligence institution comprising the Intelligence and Situation Centre (INTCEN) at the European External Action Service (EEAS) and the EU Military Staff Intelligence Directorate.[3] In the Baltic region, where vulnerabilities are most pronounced, Estonia, Latvia, Lithuania, Poland, and Finland have pushed intelligence cooperation further, developing robust intelligence-sharing mechanisms, often blending official intelligence with open-source data (OSINT) and investigative journalism to dismantle disinformation webs. Lithuania's "Elves", a grassroots network of volunteer fact-checkers debunking Kremlin narratives, exemplifies this societal-wide engagement.[4]

The second element of the strategy has been widespread expulsions of Russian officials. In the last four years, European countries have conducted unprecedented, coordinated expulsions of Russian diplomatic personnel, many explicitly identified as intelligence officers (primarily from GU military intelligence, SVR foreign intelligence, and FSB) operating under diplomatic cover with the aim of disrupting the networks employed for hybrid warfare. Estimates indicate that, by 2023–2025, over 600–750 Russian officials (many judged to be intelligence personnel) were expelled from European countries. These measures were explicitly linked to countering Russian hybrid warfare, not just classic spying, but active subversion, threats to critical infrastructure, and destabilization efforts supporting the Ukraine conflict. As a result, Russia has increasingly relied on non-diplomatic methods (e.g., recruited locals, proxies, cyber/sabotage), but the expulsions remain one of the most impactful collective countermeasures against Moscow's intelligence networks in Europe since the Cold War.[5]

The third element is the enhancement of border surveillance and fortifications, geared towards containing weaponized migration (via Belarus), drone incursions, and sabotage threats. Key initiatives in this realm have included the strengthening of physical barriers, anti-tank defenses, surveillance systems, and anti-drone technologies, with investments accelerating in 2024–2025 amid escalating incidents (e.g., 58 drone violations since 2022, with 36 in 2025 alone). Countries like Poland, Estonia, Latvia, Lithuania, and Finland have invested billions in physical barriers, surveillance networks, and counter-mobility measures. Poland's "East Shield" program, the "Baltic Defense Line" and Finland's border fortification exemplify this shift. Spanning hundreds of kilometers along the borders with Belarus, Russia, and the Kaliningrad exclave, these programs feature towering steel fences, deep anti-tank ditches, concrete "dragon's teeth" obstacles, bunkers, advanced ISR (intelligence, surveillance, reconnaissance) systems, and increasingly sophisticated anti-drone defenses.[6]

The fourth and last element has been the strengthening of infrastructure protection with the aim, on the one hand, of increasing systemic resilience and, on the other, of denying easy targets to Russian saboteurs. The sabotage of the Nord Stream pipelines in September 2022 represented a wake-up call, highlighting vulnerabilities in energy grids, undersea cables, pipelines, and transport networks.

A flurry of initiatives at the EU, NATO, and national level rapidly followed to enhance protection of physical infrastructures. Among these stand out the December 2022 EU "Critical Entities Resilience Directive" whereby member States are required to implement technical, security, and organizational measures within 10 months, focusing on prevention, response, and recovery from all-hazards threats, including sabotage across 11 sectors including energy, transport, banking, health, digital infrastructure[7] and the 2023 EU-NATO Task Force on Resilience of Critical Infrastructure, which incorporated private-sector expertise to identify weaknesses in energy networks and undersea cables.[8] European ›

[3] *https://www.euronews.com/my-europe/2025/05/23/we-know-what-russia-is-doing-and-how-it-does-it-eu-intelligence-centre-chief-tells-euron; https://www.politico.eu/article/europe-intelligence-spies-donald-trump-russia-security-politics/.*

[4] *https://www.debunk.org/about-elves.*

[5] *Kevin P. Riehle, "Soviet and Russian Diplomatic Expulsions: How Many and Why?", International Journal of Intelligence and CounterIntelligence, 37/4 (2024), 1238-1263; https://greydynamics.com/the-silent-hand-russian-intelligence-activities-in-europe; https://tass.com/politics/1567203.*

[6] *https://pism.pl/publications/eu-and-nato-states-investing-in-protection-of-borders-with-russia-and-belarus; https://valtioneuvosto.fi/en/situation-at-finlands-eastern-border; https://raja.fi/en/the-eastern-border-barrier-fence.*

[7] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557.*

[8] *https://assets.kpmg.com/content/dam/kpmg/be/pdf/RR-Critical-Entities-Resilience-Directive-2025-EN-Brochure-A4_Final.pdf; https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf.*

States acted swiftly also in matters of protection of digital infrastructures. The 2022 Cyber Defence Policy, updated the Network and Information Security Directive 2 requirements (incident reporting, supply chain security), enhancing coordination between civilian/military cyber efforts, increasing tech sovereignty, stimulating investment in capabilities, and strengthening the European Defence Industrial Base.[9] This was followed by the Cyber Solidarity Act; entered into force in February 2025, it establishes the European Cyber Shield – a pan-European network of national and cross-border Security Operations Centers using AI and analytics for real-time threat detection and response.[10]

The strategy employed by European countries to counter Russia's escalating hostile intelligence activities, a defensive framework centered, as we have seen above, on disruption and resilience, has demonstrated moderate effectiveness. By early 2026, it has successfully contributed to a notable decline in incidents and avoided civilian fatalities, while mitigating immediate escalation risks without provoking open conflict, a notable achievement in a tense environment.

In fact, first, this strategy has downgraded Russia's disinformation and subversion efforts by fostering "jointness" in threat perception across Europe, reducing in this way the effectiveness of fragmentation tactics. By blending intelligence collection sources and methods and linking intelligence more directly with policy and societal actions it has often achieved early exposure of propaganda webs and influence campaigns, making them less potent. The expulsions have directly downgraded Russia's operational capacity by dismantling established networks, limiting on-the-ground command, control, and coordination for sabotage, recruitment, and intelligence gathering. Fortifications have reduced opportunities for border probes, or sabotage incursions. Last but not least, better infrastructure protection has led to more resilient physical and digital systems, capable of absorbing more attacks better and minimize consequences. These complicate Russia's efforts by eliminating "easy wins" as well as by forcing Moscow to innovate under pressure, into conducting either low-quality "mass" operations with low probability of success or, on the other hand, more complex, resource-intensive operations that are easier to detect, attribute and counter.

"Russia often reacts faster than Europe can catch up."

Niccolò Petrelli

Yet, despite these achievements, challenges persist.[11] Russia has proven adept at adapting faster than Europe can fully respond, shifting to a "gig economy" model for subversion that has bypassed many traditional counterintelligence barriers, enabling persistent tactics such as disinformation through doppelganger sites and cyberattacks (for instance, the 2025 Qilin ransomware incident targeting Spanish systems).[12] Fragmentation remains a major issue: responses are often siloed across member states, hampered by insufficient budgets, varying levels of commitment, and gaps in coordination. The "grey zone" framing of these actions fosters ambiguity, delaying attribution and public condemnation.[13] Legal and diplomatic caution has slowed naming-and-shaming efforts, allowing under-reported incidents to accumulate substantial economic damages, hundreds of millions of euros over the years. Additionally, broader strategic issues compound these problems: for instance, Europe's countermeasures have not fully tackled the financial underpinnings of Russian operations.[14]

Ultimately, Europe's strategy has delivered clear strengths, disrupted plots, greater resilience, and the absence of major escalations, while still exposing persistent weaknesses: coordination gaps, attribution delays, and a predominantly defensive posture that allows Russia to exploit asymmetries at low cost through proxies and emerging technologies such as AI deepfakes. Russia continues undeterred in this shadow war. Europe can defend itself, but for how long can it fend off every blow? ■

---

[9] *https://www.european-cyber-defence-policy.com.*

[10] *https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.*

[11] *Lara Jakes, "Europe Wants to Get the Word Out: Russia Is to Blame for Sabotage", the New York Times, December 3 2025, https://www.nytimes.com/2025/12/03/world/europe/europe-russia-hybrid-attacks.html.*

[12] *Charlie Edwards and Nate Seidenstein, The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure (London: International Institute for Strategic Studies, 2025), https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf.*

[13] *https://apnews.com/article/russia-estonia-baltics-sabotage-spying-kallas-62835b00fdb31f648ebe2259908ca2a1.*

[14] *Tom Keatinge and Kinga Redlowska, „The Financial Dimension of EU Internal Security Threats", RUSI Insights Papers, 21 November 2025 https://www.rusi.org/explore-our-research/publications/insights-papers/financial-dimension-eu-internal-security-threats.*

In the Shadow of Zeitenwende

Intelligence services stand at the center of a new world disorder. Terrorism, cyber warfare, and aggressive great-power politics are challenging Europe's security architecture. How capable are the services – and which reforms are long overdue?

Intelligence services essentially have three core tasks. First, they are to obtain secret information for their principals about opponents or enemies, and sometimes also about partners and friends. In the modern sovereign state, the principal is the government. The information usually concerns military, economic, technological, or political matters that are kept secret in order to secure an advantage – one that allows a state to surprise or deceive its adversary. If such secret information can be obtained through espionage, the adversary is deprived of that advantage. Put differently: one spares oneself unpleasant surprises.

The second task is to counter the adversary's espionage activities. This is referred to as counterintelligence and counterespionage. The third task is described as covert operations. It encompasses many variants, ranging from covert propaganda and the influencing of an adversary – for example through bribery or the clandestine financing of activities – to paramilitary operations such as kidnapping, sabotage, or targeted killing.

All three tasks can be traced back to the ancient world. In modern democracies, however, they may only be carried out on a legal basis and under the oversight of independent state institutions, particularly parliament and the judiciary. The objective is the protection of the population, state institutions, and the economy, as well as political and cultural self-determination. In dictatorships, by contrast, the primary goal is to secure those in power and their apparatus of rule. The protection of the population plays no role – as can be observed daily in Iran, Russia, China, and other dictatorships.

While Western intelligence services operated during the ›

TEXT_ ***Wolfgang Krieger***

Prof. Dr. em. Wolfgang Krieger taught Modern History at Philipps University Marburg and was a Fellow at the universities of Oxford and Harvard. He is a member of the International Institute for Strategic Studies (IISS) and of the *Conseil scientifique de la recherche historique de la défense* at the French Ministry of Defense, and a co-founder of the International Intelligence History Association. In 2026, he published *The History of Intelligence Services*.

KEY MESSAGES

→ **Intelligence** services have three core functions: intelligence collection, counterintelligence, and covert operations

→ **Terrorism, cyberattacks, and hybrid warfare** have fundamentally expanded the traditional spectrum of threats.

→ **The illusion of a stable rules-based order** is giving way to a conflict-prone world of rival power blocs.

→ **Europe's security capacity** suffers from military, intelligence, and political deficits – particularly in Germany.

→ **Without reform, technological adaptation, and strategic clarity,** a lasting loss of operational capability is inevitable.

East – West conflict within a clearly defined political and international environment, after 1990/1991 they were rapidly confronted with new tasks and challenges. Initially, this came in the form of Islamist terrorism – one need only think of the terrorist attacks in the United States, France, Israel, the United Kingdom, and Spain, but also in Turkey, Russia, Kenya, India, Indonesia, Nigeria, Iraq, and many other countries. Some attacks were prevented and some perpetrators brought to justice, yet overall the record of success was modest.

Then, just over ten years ago, global politics began to change fundamentally. We now speak of a new "world disorder" (Carlo Masala) or a "watershed" („Zeitenwende" , Olaf Scholz). Since then, intelligence services have focused on assessing the intentions and capabilities of rival states and war-ready adversaries. Russia and China are no longer seeking accommodation with the Western side in the UN Security Council, but are instead building a rival international order – one that major states such as India and Brazil, along with numerous smaller countries, have already begun to join. Russia's war of aggression against Ukraine is supported by this new coalition of powers. Russia and China are forging alliances with dictatorships such as Iran and Venezuela.

Two very different wars have followed – one in Ukraine (since 2022) and one in the Middle East (since 2023). Aggressive great-power politics and Islamist terrorism are intertwining. While Russia under Vladimir Putin is waging a classic war of conquest, the assault on Israel was carried out by Hamas, a non-state terrorist organization. Hamas is supported by terrorist groups such as Hezbollah in Lebanon and the Houthi movement in Yemen. All three are financed, armed, and directed by the Islamic Republic of Iran. China, in turn, remains an indispensable trading and innovation partner for the West, yet at the same time maintains close partnerships with the warring powers Russia and Iran. It purchases their oil – circumventing international sanctions – and supplies them with weapons. It is therefore clear that Islamist terrorism has not disappeared. Rather, under Iran's leadership, it has taken on a new dimension.

Domestically, concerns in Europe about threats to civil liberties from cyberattacks and from state surveillance of private communications (mobile networks, the internet, data storage) have by no means disappeared. At the same time, many wonder whether private communication can still be protected at all. For alongside intelligence services, private companies are collecting customer data on a scale that is difficult to comprehend.

CAPABILITY GAPS

In light of these external and internal threats – outlined here only in highly condensed form – it becomes clear to what extent life in today's affluent societies depends on protection by state security authorities: the police, the military, and the intelligence services.

> *"The rules-based order is proving to be an illusion, because the great powers do not submit to this logic."*
>
> Wolfgang Krieger

Cyberattacks can paralyze our "critical infrastructure," meaning our energy supply, transport and communication systems, factories, banks, hospitals, and much more.

Intelligence capabilities are indispensable in defending against such attacks. In order to identify dangers in time, one needs intelligence instruments that can operate globally and are less visible than the police or the military. Attacks launched from the internet, terrorist operations, arms trafficking, and human smuggling are prepared or carried out covertly. They must be investigated and countered regardless of the sovereignty claims of criminal regimes.

Despite these upheavals, European governments continue to cling to the dream of a "rules-based order," in which conflicts are resolved through international legal norms, treaties, or institutions. Yet this is proving to be an illusion, because China, Russia, India, and other major powers do not submit to this logic. The United States under President Donald Trump has sought new ways of managing conflicts, drawing on practices of traditional great-power politics in which military force is threatened or used to secure regional spheres of influence – especially in Latin America and the North Atlantic (as in the dispute over Greenland). At the same time, it has initiated new forms of international cooperation, such as the Board of Peace established in Janu- ›

ary 2026, initially tasked with addressing the future of the Gaza territory. International law, therefore, is not dead – but it is only effective to a limited extent.

Germany has been particularly affected by the decline of the "rules-based order," because after 1990 it largely abandoned national defense and defined its foreign policy almost exclusively within the framework of the European Union (EU) and NATO. German economic, financial, and technology policy was delegated to the EU; national defense to the nuclear deterrence of the United States. Defense spending was reduced to one percent of economic output – down from five percent in earlier decades. Yet in the emerging world order, the EU is rarely taken seriously, as it lacks credible leverage vis-à-vis Beijing, Moscow, or Washington. The United States is demanding that the European NATO members develop autonomous conventional defense capabilities.

Germany's intelligence services, too, exhibit significant capability gaps that were largely ignored until 2025. It was only the coalition agreement of May 5, 2025, that contained an official acknowledgment of political failures and a commitment to intelligence reform – intended at least in part to loosen some of the legal constraints and make the services more operationally effective. Whether this will materialize remains uncertain. Above all, the services must adapt to the world of the internet. This is not merely about transmitting images and sound in all directions, but also about controlling electronically steered machines and technical systems – the "Internet of Things." What initially appeared as a major gain in freedom and technological progress soon revealed its darker side. Criminal actors have benefited from new communication possibilities. Dictatorships such as China and Iran manipulate access to the internet.

HYBRID WAR

Today, many states possess offensive cyber capabilities, foremost among them the United States, Russia, China, Iran, North Korea, the United Kingdom, and France. The United Kingdom published its first cyber security strategy in 2011; France's planning began as early as its 2008 Defence White Paper. In Germany, a separate military branch for "Cyber and Information Space" was established only in 2017 – yet without authorization to conduct offensive operations.

The common term "hybrid warfare" describes the blending of military force by regular armed forces with elements of covert aggression or "irregular warfare," ranging from black propaganda ("fake news") to cyberattacks on civilian infrastructure and the deployment of irregular fighters. Behind these activities stand intelligence apparatuses and their methods. The objective is to wear down the adversary economically, financially, and above all psychologically – through fabricated images and videos, often perfected with the help of artificial intelligence (AI).

Another relatively new form of conflict conducted with intelligence instruments is the use of economic and financial sanctions against individuals in an adversary state. Such sanctions require precise intelligence investigations into financial networks and ownership structures. In the United States, this responsibility lies with the Treasury Department's intelligence branch. The Office of Intelligence and Analysis (OIA), established in 2004, is one of the 17 agencies of the U.S. Intelligence Community, alongside entities such as the FBI within the Department of Justice. In the background, other U.S. intelligence agencies and powerful law firms often work hand in hand to negotiate the highest possible financial penalties – penalties from which corporate lawyers benefit proportionally through substantial fees.

On October 7, 2023, the Jewish holiday of Simchat Torah ("Rejoicing of the Torah"), 6,000 Hamas fighters stormed across the border between the Gaza Strip and Israel. They attacked numerous Jewish communities as well as participants at an open-air festival. In the course of the assault, 1,200 men, women, and children were murdered. More than 3,400 people were injured, ›

"Sanctions against individuals in an adversary state require precise intelligence investigations into financial and ownership structures."

Wolfgang Krieger

and around 250 were abducted and taken hostage into Gaza. Simultaneously, Hamas launched approximately 4,300 rockets at Israel from the Gaza Strip.

For observers interested in intelligence matters, the Hamas war initially provoked astonishment that such a terrorist attack could strike the State of Israel entirely unprepared. Israeli intelligence services had repeatedly received warning information. In 2018 and 2022, they reportedly captured documents explicitly pointing to such an attack. According to an investigative report by the Israel Defense Forces (IDF), published in February 2025, the decision to launch the attack was made in May 2023.

launched by the Houthi militias in Yemen, followed in October 2024 by strikes originating from Iran itself. Israel was thus fighting a multi-front war in which intelligence services played a crucial role.

On September 17 and 18, 2024, Lebanon witnessed an operation that was as spectacular as it was novel: an Israeli strike against the Hezbollah militia. The weapon consisted of a large number of pagers, small radio devices, and other electronic equipment that had reportedly been procured by Mossad, fitted with explosives, and equipped with special software enabling remote detonation via radio signal. These devices were covertly

"There can be no doubt that October 7 was one of the greatest intelligence failures in history."

Wolfgang Krieger

INTELLIGENCE FAILURES

Here we encounter a recurring analytical problem that often emerges when examining intelligence failures. On the one hand, analysts attribute to the adversary the same tactical and strategic logic they themselves would follow in the adversary's position. On the other hand, there is a tendency to privilege information that fits into an already established interpretive framework. The intelligence commentator Scott Ritter attributed the failure to an AI-supported methodology that had displaced traditional probabilistic analysis. Israeli military experts, by contrast, placed responsibility on government policy, which had sought to "freeze" the Palestinian conflict in the expectation that it would diminish in importance through direct understandings with key Arab states. The intelligence information disclosed so far by the Israeli side, however, does not yet yield a coherent overall picture.

There can be little doubt that October 7 ranks among the greatest intelligence failures in history – ironically in Israel, a country with unparalleled experience in combating Islamist terrorism, and under Prime Minister Benjamin Netanyahu, who possessed more personal experience as both a soldier and in dealing with intelligence services than any other Western head of government.

In the costly tunnel warfare that followed, Netanyahu did not lose sight of the broader strategic perspective: the network of enemies led by Iran. In September 2024, direct missile attacks were sold to Hezbollah. At a single moment, they were triggered simultaneously, injuring around 2,800 Hezbollah fighters and killing twelve people. The following day, a similar operation involving walkie-talkies resulted in approximately 450 injuries and 20 fatalities.

The effect was psychologically devastating for Hezbollah, as it exposed the scale of hostile penetration within its own ranks. At the same time, the public learned the precise identities of the fighters – brothers, fathers, and sons who had often maintained the appearance of leading ordinary family lives.

On both theaters of war, drones have played a crucial role – particularly inexpensive, short-range models. Since the beginning of the war in Ukraine, they have been deployed extensively by both sides. On June 1, 2025, a new variant of such drone operations became public with Operation "Spiderweb." In this operation, the Ukrainian military intelligence service reportedly smuggled a number of trucks into Russian territory, some of them several thousand kilometers east of the Ukrainian border. The vehicles were loaded with small drones and were able to approach within just a few kilometers of Russian Air Force bases, from where the drones were launched to destroy dozens of Russian long-range bombers.

Soon after these Ukrainian actions, on the night of June 12 – 13, 2025, Israeli forces launched a major military assault on targets inside Iran, striking nuclear facilities and other military infra- ›

structure. Around 200 military aircraft were reportedly involved. This was accompanied by a wave of strikes against Iranian air defense installations. Israeli intelligence services had evidently succeeded in pre-positioning drones – and their operators – on Iranian territory in advance and activating them at the decisive moment.

Following these preparations, on June 21/22, 2025, seven American B-2 stealth bombers attacked several Iranian nuclear facilities. In total, a number of senior military officials and leading nuclear scientists were killed in Iran. The ceasefire announced on June 24 marked a turning point in the Iranian-led proxy wars in the Middle East.

Undoubtedly, these Israeli-American attacks were based on intensive preparations by the intelligence services, lasting months and presumably even years. In one case, it proved possible to fabricate a meeting appointment for commanders in order to eliminate several of them in a targeted strike. Reports also indicate that DNA samples, falsified software, cyberattacks, and AI-assisted deception of facial recognition systems were employed.

The Iranian judiciary arrested 2,000 suspected spies and deported large numbers of Afghan refugees who were considered disloyal. Finally, mention should be made of the covert operation against the Venezuelan dictator Nicolás Maduro on December 3, 2026, which likewise rested on extensive preparatory work by (American) intelligence services.

Due to the strict secrecy surrounding such matters, it is not possible to say precisely how European intelligence services are responding to these spectacular operations. However, we are aware of their new tasks and the instruments at their disposal. It is now up to European governments to equip their intelligence services as effectively as possible, so that they can be deployed optimally in the conduct of foreign and security policy. ■

"It is now up to European governments to equip their intelligence services as effectively as possible."

Wolfgang Krieger

"Trust Is Central"

When power interests displace truth and oversight fails, intelligence loses its democratic legitimacy. U.S. intelligence and security expert Loch K. Johnson on Donald Trump, intelligence cooperation, and the moral duty of intelligence services to defend the truth.

Loch Johnson, given your long experience in intelligence studies, how do you assess recent U.S. actions in Venezuela from an intelligence perspective?

I think it's an utter disgrace. Who appointed the United States as the world's avenger, fixing other countries' governments? That's not its role. When I look at Venezuela, I'm reminded very strongly of earlier covert actions, particularly Chile under Salvador Allende.Then, corporate interests pushed intervention to protect assets, not democracy. My hypothesis is similar today: U.S. oil interests lost investments in Venezuela and pressured political leaders to act. This looks less like foreign policy and more like corporate power driving state behavior – just as it did in Chile.

You also criticize the current president very sharply. Why?

Because we're dealing with a president who ignores basic constitutional principles. The core insight of the U.S. Constitution was that power is dangerous, so checks and balances are essential. If safeguards fail, leaders can become authoritarian very quickly. Here we see a president violating the law, disregarding facts, and denying due process – making false claims and allowing killings instead of arrests.

Yet you also say the operation itself was, from a narrow intelligence standpoint, successful?

Yes – and that's the irony. Militarily, it was impressive. Reports suggest the CIA tracked the Venezuelan president's habits in extreme detail, down to daily routines. The coordination of ships, aircraft, and troops without U.S. casualties shows high operational skill. But how many civilians died? Technically "successful" intelligence can still be morally appalling.

Moving beyond Venezuela, how do current geopolitical shifts affect the mission of strategic intelligence?

The biggest problem isn't geopolitics – it's leadership. We have a president who doesn't understand intelligence, doesn't read the President's Daily Brief, and skips briefings. That's astonishing. The U.S. spends over $100 billion a year ›

INTERVIEW_ ***Loch K. Johnson***

Loch K. Johnson is Regents Professor of Public and International Affairs Emeritus at the School of Public and International Affairs (SPIA), University of Georgia. He is the author or editor of over forty books, including most recently *The Oxford Handbook of National Security Intelligence* (Oxford University Press, 2025); and *National Security Intelligence,* 3d ed. (Polity, 2024).

KEY MESSAGES

→ **U.S. actions in Venezuela** echo Cold War covert interventions, driven less by democracy than by corporate and strategic interests.

→ **Intelligence operations** can be technically successful while being morally and politically destructive.

→ **Politicization and disregard for oversight** weaken intelligence effectiveness and damage allied trust.

→ **AI will transform intelligence** collection and analysis, but cannot replace human judgment, ethics, or accountability.

→ **In democracies,** intelligence must protect not only physical security, but also truth, trust, and a shared sense of reality.

on intelligence, yet its main consumer ignores it. Advisors filter what remains through ideology, cherry-picking what fits their agenda, undermining intelligence's core purpose.

Does the Trump administration harm international intelligence cooperation?

Yes, I'm afraid it has. Contacts in the UK, Germany, and other allied states increasingly view the U.S. as unpredictable and less trustworthy. Traditionally, Five Eyes has been one of the most robust intelligence-sharing arrangements in the world. But even within that group, there's now growing distrust. Allies are increasingly uncertain about how safely shared intelligence will be handled inside the United States.

What kinds of risks does that create?

Enormous risks. Human intelligence means real people whose identities can appear in top-secret reports; if leaked, they face prison or execution. Sensitive technical details – satellite orbits, interception methods – once exposed can't be recovered. My UK contacts report deep concern that U.S. leadership recklessness has weakened safeguards that once worked.

So the problem isn't just political – it's structural?

Exactly. The world is vast. No single country – not even the United States – can cover everything alone. Intelligence cooperation is essential. Germany, in particular, has a strong historical sensitivity to civil liberties, which I respect deeply. That history makes German intelligence agencies especially careful about how information is collected and shared. If they begin to doubt how their intelligence will be protected once it reaches Washington, they will naturally hesitate. Once trust erodes, rebuilding it is extraordinarily difficult.

You mentioned Germany's approach to intelligence. Any personal reflections?

Yes. I've always admired Angela Merkel. When it came out that the NSA had been spying on her, she responded publicly by saying, "If they want to know what I think, they should just ask me." I thought that was wonderful – measured, dignified, and principled.It captured something important about democratic leadership and trust. Intelligence should serve democracy, not undermine it. And right now, that balance is badly off.

So in summary – what worries you most?

The normalization of lawlessness. When oversight laws are ignored, when allies aren't consulted, when intelligence is politicized or mishandled, the damage doesn't stop at one operation or one country. It spreads. And once trust – constitutional trust, allied trust, human trust – is gone, intelligence itself becomes far less effective.

How, then, can Western allies react to this situation? Is there any clear strategy?

I strongly believe in dialogue and open engagement. After decades of cooperation, intelligence professionals in Germany, the U.S., and other Western states know each other well. That makes reassurance and closer cooperation vital. On the ground, trust and personal relationships matter more than ever – and those efforts are clearly continuing

Could this crisis nonetheless lead to renewal – perhaps new forms of intelligence cooperation, perhaps even a European intelligence hub?

They are grand ideas and worth pursuing, but we must be honest about human nature. We don't learn well, we don't avoid wars, and we underestimate how vital cooperation among democracies is. Democracy is fragile and rare – perhaps only 25 of 200 states qualify. Yet cooperation remains insufficient. Five Eyes matters, but it's not enough. Democracies need broader, deeper intelligence partnerships, including countries like Germany, to withstand growing pressures.

What do you see as the primary function of intelligence – especially strategic intelligence – in democratic societies?

I believe intelligence's core role is protection: early warning so leaders aren't surprised by catastrophes like Pearl Harbor or 9/11. Beyond that, agencies add real value on issues such as environmental degradation, pandemics, economic instability, and mass migration. COVID showed how vital early warning could be. Still, the central mission remains preventing national annihilation – ensuring we are not suddenly destroyed by nuclear missiles from major powers.

Would you also say that one of the core missions of intelligence is to safeguard truth – or at least a sense of reality – in democracies?

Yes, absolutely. That mission is nearly as important as protecting societies from physical destruction. Intelligence services – including Russian, Chinese, and even Western ones – have manipulated information. Russia has been especially aggressive, spreading false claims about AIDS, COVID, and more. Such narratives gain traction through repetition and propaganda. As AI advances, this problem will only intensify.

What role should intelligence agencies play in that environment?

Ideally, American and Western intelligence agencies should be doing exactly what you suggested earlier: helping educate democratic populations about what is real and what is not. Helping ›

citizens develop a sense of reality.And to be fair, they already do some of this. Intelligence agencies do issue warnings about disinformation campaigns, foreign interference, and manipulated narratives. But I think we could do a much better job. Democracy depends on an informed public. If citizens can't distinguish fact from fiction, then elections, public debate, and democratic accountability all start to break down.

So intelligence agencies should not engage in manipulation themselves?

Exactly. That's the ethical line. But there are exceptions. If you're planning something like the Normandy invasion during World War II, you absolutely want to deceive the enemy. You want them to think you're landing at point A when you're actually landing at point B. In wartime, deception is not just legitimate – it's essential. But that's very different from day-to-day information manipulation aimed at civilian populations, especially within democracies. Feeding false information to the public, or to allied societies, corrodes trust. And once trust is gone, it's very difficult to restore.

Does that mean the threat isn't just external, but internal?

Precisely. The greatest long-term threat to democracies may not be military force, but the erosion of a shared sense of reality. When citizens no longer agree on basic facts, democratic debate collapses. That's why intelligence agencies have a moral duty to uphold truth, even when it's inconvenient. If intelligence becomes propaganda, it stops defending democracy and starts undermining it – one of today's most serious challenges.

In one sentence, then – what is intelligence ultimately for in a democracy?

It's there to protect society – physically, politically, and epistemically. To guard against surprise attacks, catastrophic threats, and the slow destruction of truth itself.

How do you think AI will affect the intelligence business?

> *"Intelligence services have the moral duty to uphold truth."*
>
> Loch K. Johnson

AI has exploded, with companies and intelligence agencies investing billions. In the intelligence cycle, it could help decision-makers allocate resources more rationally and become more data-literate. But ideology often overrides facts. In high-level meetings, personal obsessions shape priorities regardless of evidence. Even the best AI inputs can be ignored. AI may inform decisions, but it doesn't replace human bias.

Could you explain that in more detail?

I've been in those meetings. People bring ideology and personal obsessions with them. Take Marco Rubio, for example. He's Secretary of State and National Security Advisor at the same time, which is absurd – no one can do both jobs well. In those meetings, guess what he argues? Cuba, Cuba, Cuba. Russia, China, Cuba. Cuba near the top of priorities. Cuba? Really?

What about the collection phase?

Here AI has enormous potential. Think about past manhunts – Osama bin Laden, for example. We knew he was about six foot five. We had drones flying over Afghanistan and Pakistan, but today you could equip those drones with AI systems programmed to identify anyone of that height, match facial features, track movement patterns.

That kind of automated recognition could be used to apprehend targets – or, more ominously, to kill them. So yes, AI can dramatically enhance collection capabilities, but it also raises profound ethical questions.

And analysis?

This is where AI may be most valuable. It can sift through vast amounts of information far faster than any human team. Before 9/11, data were fragmented across agencies, and no one had a full picture – a catastrophic failure of all-source intelligence. AI could help integrate data across agencies. But the risk remains: garbage in, garbage out. If the underlying data are flawed, biased, or incomplete, AI will simply process those flaws faster.

What about the final stage – getting intelligence to decision-makers?

That's where I'm most pessimistic. AI may improve intelligence products, but decision-makers rarely engage with them. Joe Nye once told me he had eight minutes a day to read intelligence. Eight minutes. So if Joe Nye had eight minutes, what does that mean for people like Rubio – or Pete Hegseth? How much time do they spend engaging seriously with intelligence? AI can't fix that. Worse still, ideology acts as blinders. Many leaders already know what they want to do, and intelligence – human or AI– gets ignored when it contradicts their beliefs.

So AI won't magically fix intelligence failures?

Exactly. AI can greatly improve analysis, but human instincts – ego, ideology, ›

politics – will still drive many decisions. AI excels at scale: it can scan global media in minutes and detect patterns humans would miss. That's its real value. But it supports judgment; it doesn't replace it.

In an increasingly transparent world, do you think intelligence will move more toward open-source information?

Absolutely. Open-source intelligence has become far more sophisticated and is now the starting point for any analyst. I think of intelligence as a jigsaw puzzle: open sources provide many pieces, but some are always missing. Let me give you an example. President Clinton once asked me whether China was selling M-6 missiles to Pakistan. Open sources yielded almost nothing, even after weeks of research. Only classified satellite imagery – showing Chinese freighters unloading missile components in Karachi – provided decisive proof. Without secret intelligence, my assessment would have failed.

Does that mean that secrecy will always matter for intelligence?

Yes. Especially human intelligence. Imagine recruiting an agent inside Russian or Chinese intelligence – someone sitting in the room with Putin or Xi. That person can ask questions. They can hear intentions directly. A friend of mine once said: technical intelligence can photograph the tree. Human intelligence can shake the tree and make the apple fall. That's the difference.We don't often have that level of access – but when we do, it's priceless.

So what's the balance going forward?

Open-source intelligence will continue to grow in importance. AI will help us process it faster and better. But secrecy – satellites, signals intelligence, human agents – will remain essential. Intelligence will always be a blend of the visible and the hidden, the automated and the human. And the hardest part won't be technology. It will be getting leaders to listen.

When we look at AI, technological acceleration, and repeated human failure to grasp truth, how do you see the role of time and speed in the rise and fall of democracies, empires, and civilizations?

These machines are extraordinarily sophisticated. I play chess against bots all the time, and I have real respect for them. They are fast, and speed is one of their great strengths. But what they lack – at least for now – are instincts. And you're right: human instincts can be slow. But they are also what distinguish us from these impressive machines. We can use AI to gather data, sift through massive amounts of information, and identify patterns. That's enormously valuable. We already know machines can defeat chess champions, perform well on law school exams, and process complexity beyond human capacity. They're "smart" in a certain technical sense. But they don't have a conscience. And that's critical.

Some argue that AI may eventually develop something like conscience or moral reasoning.

Some believe machines may one day become morally autonomous, and if that happens we are in serious trouble. For now, however, we still rely on human judgment. This raises a key question: whom do you trust? A fast but opaque algorithm, or an experienced official with decades of crisis experience, judgment, and conscience? I would trust the human. She remembers past failures, recognizes patterns, and can say what worked – or led to disaster. That lived experience matters enormously.

So speed is not always an advantage?

Exactly. Speed can be dangerous. Democracies are slow by design – they debate, deliberate, and hesitate – and that slowness is a safeguard. Many systems fail not from delay but from acting too fast, without reflection or ethics. AI accelerates information and decision pressure, but human judgment needs time. If technology outruns our capacity to reflect, democracies are at risk.

You mentioned trust earlier. How does that factor into intelligence and AI?

Trust is central. I've seen leaders ask, "How do you know this?" If the answer is a protected human source, you can't show the evidence – and trust drops. By contrast, placing satellite photos on the table showing missiles unloaded in Karachi is concrete and persuasive. People trust what they can see and verify. That's why AI outputs often face skepticism: the process is opaque, and conclusions aren't easily explainable.

Does that skepticism apply to AI specifically?

Very much so. Many intelligence officers – and even more political leaders – don't fully trust AI systems. And frankly, they're right to be cautious. AI can be a powerful tool, but so far it has serious limitations. It makes mistakes. Sometimes a lot of them. When a machine is wrong, it can be wrong very quickly and at enormous scale. So while AI can assist human judgment, it cannot replace it. At least not yet – and perhaps never in the way some technologists imagine.

How does this relate to the rise and fall of civilizations?

Civilizations rise when they balance innovation with wisdom. They fall when speed outpaces judgment. When technology advances faster than ethical ›

reflection, institutions crack. Democracy is particularly fragile because it depends on trust, shared reality, and moral restraint. These cannot be automated. They require time, memory, and conscience. If we hand too much authority to systems we don't understand – systems without moral responsibility – we risk accelerating our own decline. Intelligence, in the deepest sense, is not about speed or data. It's about judgment.

So intelligence, in a philosophical sense, remains human?

Yes. Machines can help us see more, know more, and process more. But wisdom – knowing what to do with that knowledge – remains a human responsibility. And if democracies forget that, then no amount of artificial intelligence will save them.

In this broader context, how do you assess the power of large technology companies when it comes to data and AI? Could companies like Google or Amazon be seen as intelligence services in their own right?

Yes – and that's exactly what worries me. Germans, given their history, understand the dangers of a surveillance society. Such technologies could create a world with nowhere to hide, especially for dissenters. In an emerging authoritarian system, AI-driven surveillance could identify, track, and imprison opponents before resistance forms. Intelligence has always been dangerous when misused; combined with AI and mass data collection, the risk is dramatically amplified.

So the threat is not only governmental, but corporate?

Corporations are dangerous enough as they are, but now they're gaining unprecedented surveillance capabilities, economic leverage, and political influence – all wrapped in the language of technological progress This concentration of power should worry anyone who cares about democracy.

What is the single most important human capability for intelligence work?

That's a wonderful question. If I had to start with one word, it would be honesty – deep, uncompromising commitment to telling the truth, no matter how inconvenient. That's objectivity. Second, you need deep expertise: well-educated professionals who truly understand their subject matter. Third, international experience matters – languages, travel, cultural fluency. Officers who build real relationships abroad can report more accurately and cooperate far more effectively.

"Civilizations fall when speed outpaces judgement."

Loch K. Johnson

If you had to choose just one trait?

Honesty and objectivity. Above all else. And it's hard. Imagine walking into the Oval Office and telling a president, "You are completely wrong. These are the facts." That might be the end of your access. It could damage or even destroy your career. So there's a constant temptation to become a sycophant – to tell leaders what they want to hear.

Are those qualities still present in today's intelligence community?

Yes, they are. I know many intelligence officers in the U.S., Germany, and the UK who embody these qualities – objective, educated, culturally aware, and committed to truth. While political appointees at the top may seek to please leaders, about 98% of those below are serious professionals. The real challenge is getting their expertise past political barriers into decisions.

Is there anything that gives you hope?

More broadly, I sense an awakening across the United States. People are beginning to realize that American democracy is in serious trouble. There have been recent elections – Virginia and elsewhere – where Republicans have been defeated. That reflects people saying, "Enough. We've had enough of MAGA and this nonsense."

Ironically, one thing I once admired about Trump was his criticism of endless wars. He said the U.S. had been involved in too many foreign conflicts and needed to stop. I thought, "Right on." And now look at him – rash military actions, exactly what he once criticized.

Any final thoughts?

Just gratitude. I feel honored and happy to have had this conversation. Dialogues like this – open, honest, transnational exchanges – are exactly what give me hope.

Then we'll bring you to Munich one day.

Absolutely. Bring me to Munich, we'll have some beer, and I'll tell you what I really think. ■

Architecture of Trust

Germany is under growing pressure from hybrid attacks. To remain capable of action, it needs effective intelligence services and a decision-making architecture that consolidates and uses insights.

TEXT_ ***Christoph Meyer & Daniel Neumann***

Prof. Dr. Christoph Meyer is Professor of European and International Politics at King's College London. For over 15 years, he has researched early warning, strategic surprise, and learning from crises. His books include Warning about War (2020) as well as Estimative Intelligence in European Foreign Policymaking: Learning Lessons from an Era of Surprise (2023).

PhD Dr. Daniel Rainer Neumann is a political scientist with a focus on Intelligence Studies and Assistant Professor at the Institute for Security and Global Affairs at Leiden University. He has researched the support of the EU's Common Foreign and Security Policy by the intelligence services of the Member States, particularly vis-à-vis the EU Intelligence and Situation Centre (INTCEN).

KEY MESSAGES

→ **Germany's security** situation is deteriorating due to hybrid attacks, sabotage, and influence operations.

→ **Effective intelligence services** are central for prevention, attribution, deterrence, and strategic foresight.

→ **Legal hurdles**, institutional fragmentation, and limited use of insights weaken their impact.

→ **Reforms** must strengthen analysis, coordination, and the use of intelligence in political decision-making.

→ **In addition to legislation**, investments, European cooperation, and a cultural shift are required.

Germany's security situation is precarious and there are few reasons to expect future improvement – on the contrary. Germany is in the crosshairs of those powers at home and abroad that seek to undermine our democracy, our social cohesion, and our contribution to the defense of a strong, autonomous Europe.

Already today, we are exposed to cyberattacks and acts of sabotage against critical infrastructure. The attacks by state actors have increased significantly in recent years, have become more complex in their conception and execution, and are more dangerous to the lives and physical safety of citizens. The boundaries between state actors, terrorist groups, and organized crime are increasingly blurring, as Russia in particular recruited other proxies after many of its agents were expelled.

Russia draws from its entire toolbox depending on cost-benefit considerations and irrespective of international legal obligations in order to achieve its goals: from the dissemination of false videos about Merz during the federal election campaign, to drone flights near airports and military facilities, to incendiary devices in DHL aircraft or even nuclear threats. A distinction must be made between the immediate damage and the intended effects. Russia's primary objective is to damage citizens' trust in the state and government, to strengthen forces that seek an end to the EU and NATO, and to weaken society's overall capacity for resistance and mobilization.

THE VALUE OF THE INTELLIGENCE SERVICES

Whereas during the Cold War extremist groups and parties were directly and indirectly supported by the KGB and the Stasi, Germany is confronted with a new reality. Today, not only Russia and China support these actors, but also parts of the U.S. MAGA ›

movement as well as companies and billionaire entrepreneurs ideologically associated with it.

In the future, a further intensification of these efforts is to be expected – and the scenario of a state of tension or alliance case has likewise become significantly more likely. Russia and China seek to test and ultimately overcome the limits of the will and capability of NATO and the USA through their strategic and tactical cooperation.

In this security environment, the value and necessity of effective intelligence services have increased immensely – and would increase even further in the event of an alliance case:

"We need the services for the deterrence of hostile actors."

Christoph Meyer and Daniel Neumann

They are needed to anticipate possible attacks and thereby either thwart them or drastically reduce potential damage – as Ukraine succeeded in doing in repelling the Russian decapitation strike in February 2022. They are needed to quickly and reliably determine after attacks who the direct and indirect perpetrators of these attacks were, in order to possibly make this public, identify the perpetrators, or initiate punitive measures – as in the case of the Russian assassination attempts on former agent Sergey Skripal and opposition figure Alexander Navalny. We need them for effective deterrence, so that opponents' vulnerabilities can be identified and possible countermeasures, for example hackbacks, can be successfully carried out. It is necessary to uncover and shut down foreign financial sources of extremist forces and to make ideological support and corruption public and prosecute them under criminal law.

Effective services can benefit enormously from cooperation with partner services, as these often possess complementary expertise and methods, and because division of labor or joint investments in expensive capabilities such as satellites, cryptography, or AI systems are more efficient and less costly. And because joint analyses and joint threat assessments and future scenarios are an important basis for common interests and joint action – bilaterally, within the EU and NATO, as well as in smaller cooperative formats. Intelligence cooperation can build interstate trust that can even withstand rifts at the governmental level and thereby stabilize relationships.

Intelligence services are important to explore future spaces through robust analytical procedures, to expand the realm of imagination, and to reduce the likelihood of unpleasant surprises. They can help present policymakers with courses of action in order to pursue successful strategies in foreign and security policy, rather than merely engaging in short-term policymaking and constantly reacting to the actions of others.

Militant democracy („wehrhafte Demokratie") needs effective intelligence services whose knowledge and analyses are used by decision-makers and cannot easily be ignored when they are inconvenient. It requires services that enjoy the support and trust of the public and parliament. And they must also gain sufficient trust from partner services in order to enable deeper and more far-reaching cooperation. This requires sufficient confidentiality in handling the findings and methods of these services, and reciprocity in the exchange of valuable information and analyses.

By their very nature, the public rarely hears about the successes of the services, especially when attacks have been thwarted, in order not to endanger methods and sources. It is clear, and recognized by the Federal Constitutional Court, that German intelligence plays a central role in ensuring Germany's security.

However, it is also clear that the potential of the intelligence services has by no means been fully utilized – and their capabilities are by no means sufficient given the security situation. As we have elaborated in a paper for the Intelligence Services Discussion Group, there are several deficits. The best capabilities are of no use if they may not be used for legal reasons. Thus, our intelligence services lack the legal framework for collection authorities and information sharing with other authorities that are common practice in Europe among our allies.

At the same time, insights that were generated were often insufficiently heard and used in the political process. This was partly politically intended, when intelligence services were deliberately kept at a distance by chancellors and ministers, partly due to a lack of interest and appreciation for their work, partly in order to minimize the political risk of inconvenient assessments.

That demand and utilization deficit also lay on the other hand in the fact that intelligence assessments often competed with the "house assessments" of ministries and there was a lack of an authority and capability to critically discuss these differences on the basis of all sources and methods and to resolve them into a ›

joint assessment. Thus, decision-makers were able to select what was most convenient for them and more easily fall into wishful thinking. The fragmentation of the security architecture also impeded coordinated action across policy fields, national borders, and types of actors that the complex threat situation requires.

At the same time, German services are subject to a very strong control architecture that primarily conducts legal review and thereby generates a high bureaucratic burden. However, this technocratic, judicial review does not create "trust through control," but rather appears as an institutionalization of mistrust. In society in particular, there has so far been little recognition but above all mistrust toward the important function of intelligence services. Parliamentary engagement with the services is therefore also limited to a very general character. Rarely is the expertise of the services made use of, nor is sufficient attention paid, in the sense of a "capability control," to ensuring the effectiveness and capability of the intelligence services.

THE SITUATION OF THE GERMAN INTELLIGENCE SERVICES

The new government has made important decisions to remedy a number of these deficits. Thus, the debt brake for security matters has largely been suspended in order to enable investments in the growth of the relevant authorities and capabilities. Through an ambitious reform of the legal framework, the BND is to receive new powers, after a particularly professionally qualified ambassador was unusually appointed as the new President of the BND at the direct request of the Federal Chancellor. With the creation of the National Security Council, better coordination of the numerous actors is to take place in the future, whereby stronger use of intelligence findings in strategy and decision-making processes is also to be expected. Not least, public communication about the importance of intelligence services in an increasingly insecure world has also been expanded, with the federal government itself in particular communicating much more actively with strong backing.

"Germany should lead by example as a pioneer of European intelligence cooperation."

Christoph Meyer and Daniel Neumann

This path taken by the federal government is correct. Strengthening the federal intelligence services is important not only for better fulfilling their primary function but also for further reasons. It serves deterrence vis-à-vis hostile actors when the German state can credibly demonstrate that it is capable of uncovering and sanctioning covert operations because it possesses strong intelligence services. Particularly in the cyber domain, the capabilities for attributing attacks, but also the possibility of so-called hackbacks, are considerable. At the same time, Germany is significantly dependent on international partnerships with its allies, including in the intelligence domain. This is not a weakness, but an expression of a complex and globalized world. It is therefore important that German services can meet their partners with strength and on equal footing in order to contribute substantial insights to cooperation. Hence, European intelligence cooperation and solidarity must be further expanded in order to be able to act more strongly together. Germany has an important role to play here and should therefore lead by example.

In particular, in reforming the BND Act, the federal government should ensure that this is used for more than merely strengthening the service's collection capabilities. More fundamentally, its character as an analytical service provider to the federal government for security policy decision-making processes should be clarified. This includes not limiting the new legislation to expanding powers in information collection and data transmission. These are indeed very important, but they should not become the only major achievement of the reform. For example, it should also be specified in greater detail when reporting and consultation obligations should apply in order to ensure effective intelligence reporting, even when it may be politically inconvenient.

CHALLENGES AND CONSEQUENCES

However, there are many obstacles to implementing this vision. On the one hand, the Federal Constitutional Court has imposed significant duties and limits on legislation and oversight of intelligence services. Within the prescribed framework, however, leeway must be utilized in light of the security situation. ›

On the other hand, we have a cultural problem in Germany. This partly results naturally from German history, which has led to a fundamental and historically justified mistrust toward services, centralization, militarization, and especially cooperation between intelligence services, police, and companies. To another extent, this cultural problem results from a lack of knowledge about intelligence services in the general public, in parliaments, the media, and the German academic landscape. This is also exploited by influence networks of our adversaries in politics and partly within the services themselves.

There is no single adjustment screw that will fix these problems. Rather, it requires a continuous interaction of legal changes, institutional reforms, investments in better knowledge, as well as supporting a cultural shift in dealing with intelligence services. ■

"In Germany, there is a fundamental and historically justified mistrust toward intelligence services."

Christoph Meyer and Daniel Neumann

"In Analysis, We Are Good"

From the Cold War through Afghanistan to the Zeitenwende: A former senior official of the BND explains how the mission, limits, and self-image of the service have changed – and why good intelligence often fizzles out politically.

Colonel Klaus Schmidt, what originally motivated you to work for the service?

For me, the question did not arise that way at all. As a professional soldier, after completing General Staff training I was designated for various assignments; in my case it was the BND. The topic interested me, so I agreed. In 1988 I was first assigned there; later, further positions followed in military intelligence, in the Ministry of Defense, and finally the leadership of the BND's Joint Situation Center.

Can you describe your activity in more detail?

In my first assignment, from 1988 to 1991, I was Head of Division Indication and Warning. That was enormously important because it concerned the question of warning time. We assessed activity levels on the opposing side and drew conclusions from them. I cannot say more about that. Later I headed the Joint Situation Center. There, in shift operations, what is happening worldwide is monitored. From there, the daily reporting goes to the service's customers. It is, so to speak, the BND's gateway for incoming and outgoing information.

How did the service's mission change with the end of the Cold War?

Certain countries and topics were always in focus, but the weightings shifted. At the latest, for example, when Poland became a NATO member, the priorities changed. At the same time, a new quality developed with the Balkan deployments. Germany participated in UN and EU peace missions. Later came Afghanistan. These were regions that lay very much at the margins of German interests, but suddenly became relevant.

What were the consequences for the BND?

The foreign deployments changed the service, as well as cooperation with the Bundeswehr and the Federal Foreign Office. Until around 2020, the focus lay strongly on deployment areas. Since ›

INTERVIEW_ ***Klaus Schmidt***

Oberst a. D. Klaus Schmidt held leading functions in the German security and intelligence sector, among others as head of division and head of section in the Federal Intelligence Service and as a desk officer in the Federal Ministry of Defense. Previously, he served as a General Staff officer, battalion commander of the Franco-German Brigade, and officer in the Bundeswehr. He is Chairman of the Gesprächskreis Nachrichtendienste in Deutschland (GKND).

KEY MESSAGES

→ **The BND** is primarily a strategic service and early warning system – not a decision-maker, but a supplier for political decisions.

→ **Good intelligence** fizzles out if politics ignores warnings or relativizes them through competing departmental situation reports.

→ **Foreign deployments** and the Zeitenwende have shifted the service's priorities several times – back to national and collective defense.

→ **Germany's greatest weakness** lies in the lack of strategic thinking and in insufficient joint situation assessment.

→ **A militant democracy** requires not only capabilities, but societal willingness to recognize risks and draw consequences.

we withdrew from Afghanistan or Mali and once again prioritized national and collective defense, the service's internal priorities also had to be reset. However, I no longer experienced that as an active member.

But Russia was always a central intelligence target.

The service reported and fulfilled its tasks. The crux, however, is this: You can conduct intelligence work as well as you like; if politically no one listens. If warnings are set aside because a different political approach is being pursued, then an intelligence service has a problem. This is not a uniquely German phenomenon; you can also see it with the Americans. Keyword 9/11.

In your view, where do the central difficulties lie in the relationship between intelligence services and politics?

The Federal Intelligence Service has a task profile that is specified by the government. There are priorities by countries, activities, and topics such as international terrorism. In Germany it is traditionally the case that the BND supplements the so-called departmental situation reports. Each ministry has its own situation picture. The situation picture of the Federal Foreign Office is often more optimistic than that of the Ministry of Defense. When the BND's situation picture is then added, it can happen that it is said: it is not that bad, we see it differently. Afghanistan is a good example of this.

What happened at that time?

For years, the Bundeswehr and the BND said that if we leave Afghanistan, there will be a takeover by the Taliban. However, the political will to remain permanently was not there. What a service cannot do is to name the one drop that makes the barrel overflow. The Federal Foreign Office, for example, referred to talks with Afghan senior representatives who assured that they would hold out. Three days later, the president fled. That illustrates the problem very clearly.

Does that mean there is a lack of a joint situation assessment?

Exactly. A joint determination of the situation is decisive. This is now supposed to take place through the National Security Council. It is also about strategic analyses. Germany long had deficits here. Only since 2022 has there been a national security strategy at all, from the perspective of an intelligence professional still with many gaps. Strategically, we often drive by sight and decide in the short term.

> *"No matter how good the intelligence work is, if politically no one listens."*
>
> Klaus Schmidt

How can situation assessment be better organized?

In addition to an area that thinks strategically in the long term, there needs to be a situation element that comes to decisions. It must not be a round table at which everyone says their opinion and then they part ways. At some point, a decision must be made about what applies. That will still take time. A model would be the British Joint Intelligence Committee. We are moving in that direction, but it takes time.

How have the war in Ukraine and the "Zeitenwende" changed the orientation of the BND?

The reassessment should actually have begun as early as 2014, with the annexation of Crimea, but that did not happen. Since 2022, the focus has clearly shifted back to national and collective defense. This will intensify further. We can no longer automatically assume that we will receive a fully prepared situation picture from NATO as in the Cold War. The Americans are setting different priorities. Therefore, we must build our own capacities, within NATO and the EU, together with partners, in the long term and in depth.

You have described the BND as a strategic service. What does that mean in concrete terms?

A strategic service is first and foremost an early warning system. It must keep an eye on the broad lines of German security interests, recognize changes, and name indications. These indications must be brought into a body such as a National Security Council and assessed there. The problem in Europe is that strategic thinking is not very pronounced. We often react only in the short term.

How would you assess the service's strengths and weaknesses today, also in comparison with partner services?

I cannot or may not say anything about technical capabilities and source work. What is clear, however, is that we need subject-matter expertise and strong analysts, which is difficult with public salary structures. Nevertheless, I am convinced that we have very commit- ›

ted and capable people. In analysis, we are good. In the circle of comparable services, that is, with the British, French, or Italians, we can keep up. The Americans play in a different league. To copy them would be illusory.

The BND is considered analytically strong, but operationally too slow...

The term "slow" is too crude for me. However, we do have limitations, for example through our control and legal regime. In foreign telecommunications intelligence, there are constitutional requirements. If a German citizen appears, it must be deleted, the person must be informed, and it must be documented. These are restrictions that other services do not have in this way. That does not make us slow, but it sets limits. These are currently also being discussed politically.

In the future, should the service also be allowed to act actively instead of only observing, for example to hack computers?

This discussion will be shaped very strongly by legal considerations. Personally, I think that in Germany we long made ourselves comfortable with the assumption that the Americans would sort it out and provide us with the information. That attitude will no longer hold. Active measures, such as those the French have, I can hardly imagine for us at present. They have their own units for such operations. We will not have that. In the area of technical intelligence, however, we will have to go further.

In the context of hybrid threats: Could you imagine that Germany would respond to an act of sabotage with similar measures?

At the moment, I cannot imagine that. A great deal more would have to happen for that. In the population, there would have to be a much stronger awareness of hybrid threats. Above all, one would need clear evidence of who is behind it. Even with drones you can see how complex the questions are. Who is behind it, who may intervene, when may one respond? In a democracy, that takes time. Therefore, at present I see no willingness for such steps.

The current BND President Martin Jäger speaks of taking higher risks and becoming more operational. How do you interpret that?

Becoming more operational does not mean activism, but a targeted expansion of capabilities. In the HUMINT area this is particularly difficult; classic source work takes years. Technical intelligence offers more scope despite legal limits. This includes penetrating digital networks and building up one's own satellite capabilities with the Bundeswehr. Open Source Intelligence and AI are also becoming more important. Operational means: actively and purposefully searching, not just waiting.

How do you see the dependence on the USA in the intelligence field?

When sharing information, one must always be careful not to adopt it unchecked. Leads are examined and classified. The Americans will not leave Europe. They are shifting priorities to the Pacific, but they remain present. However, they expect partners to contribute something. This give-and-take remains central. At the same time, one must look closely in exchanges, because information can also be politically colored.

From an intelligence perspective, do you continue to see the USA as a partner?

For me, the Americans remain partners. The idea that they will permanently protect us and take care of everything will become weaker, but they remain partners. This is also shown by the fact that it is legally stipulated in the USA how many American soldiers must remain stationed in Europe. I am convinced that the USA also wants to remain present out of its own interest in order to know what is happening in Europe. Relationships are always guided by interests, not carried by romance.

In Germany, the concept of "militant democracy" (wehrhafte Demokratie) plays a major role. How do you interpret that from an intelligence perspective?

For a long time, it was more of a catchword. Today it is becoming more concrete. For decades we felt secure under NATO's protective umbrella and believed we ourselves did not have to be militant. This awareness is now changing. At the same time, we see a second threat from within. The societal center is becoming weaker, the fringes stronger. Radicalization is not occurring only in one di- ›

"We made ourselves comfortable with the assumption that the Americans would provide us with the information."

Klaus Schmidt

rection. That is a real challenge for our democracy.

What does militant democracy mean externally?

First of all, the clear realization that one wants to be able to defend oneself. Sweden and Finland are good examples of this. These are not militaristic societies, but defense capability is taken for granted there. Here as well, some things that are still controversially discussed today will soon be normal. When that sets in, we are on a good path.

In your view, what is currently the greatest challenge, especially for foreign intelligence?

From my perspective, it is the mental change in society. Militant democracy means, externally as well as internally, that we recognize dangers early and are prepared to react. Legislation and concrete mandates to the services must be developed in this direction.

What role is the "Gesprächskreis Nachrichtendienste" supposed to play in this?

Our concern is to introduce security and intelligence topics into the public debate in an objective manner. This is done through events, discussions, and contributions. In the security policy community in Berlin, we are now established and work with partners such as the German Atlantic Society, the DGAP, and the Federal Academy for Security Policy. Interest and openness toward this have grown.

What must happen in order to promote German intelligence culture?

A major deficit is that there are hardly any Intelligence Studies at universities in Germany, particularly not in political science. There are only a few approaches, for example in Potsdam, Bonn, or at the University of Applied Administrative Sciences of the Federation. Yet there are many interested young people. Without stronger academic anchoring, the topic lacks reach and depth.

Is there something in your career of which you are particularly proud?

I am particularly proud that I first led the Bundeswehr's intelligence center and was later asked whether I would like to take on the same task at the Joint Situation Center of the Federal Intelligence Service. For me, that was a sign of trust. To be allowed to exercise this function for six years was a good conclusion to my career.

What would you say to young people who are considering working for an intelligence service?

That a very interesting professional life awaits them. One deals with topics that are not accessible to everyone and gains a very broad view of political and security policy contexts. Of course, salary and remuneration are an issue, especially in comparison with the private sector. But in terms of content, the field is exceptional.

What do you think of the current BND campaign in social media?

The BND's new communication campaign initially irritated me, due to my age. But it apparently works well and appeals to young people. What is decisive is that this motivation is maintained. I know cases in which young employees left the service again because they were frustrated by the strong bureaucratization. Having to have every idea legally reviewed first can be paralyzing. In addition, there are structural problems, for example in the civil servant appointment of specialists who are not lawyers. Work must also be done on this. That too belongs to the future viability of the services. ■

ABOUT

■ **The Gesprächskreis Nachrichtendienste in Deutschland e. V. (GKND)** is an independent non-profit association whose aim is to contribute to a constructive and public discussion about the secret state intelligence services in democratic constitutional states. In doing so, it primarily seeks to address future issues of the services as they arise from changes in the world and the global political interests of the Federal Republic of Germany. This concerns goals, tasks, methods and structures as well as the international cooperation of the services and their oversight.

■ **Members include** former members of the German intelligence and security services, the Bundeswehr, as well as individuals from politics and academia who deal with our subject matter.

The GKND prepares statements and background papers on current topics related to intelligence services in Germany and posts them on its website (www.gknd.org).

■ **In the GKND Monitor**, it compiles references to reports, publications, and publicly accessible official documents on security policy and intelligence-relevant matters. The GKND also regularly organizes events independently or with partners on current topics with security policy and intelligence relevance.

Are Democracies at a Disadvantage?

While authoritarian regimes regard war as a legitimate instrument of power, democracies view it as an exception and a failure. This normative asymmetry shapes decision-making processes, hybrid conflicts, and the vulnerability of open societies in geopolitical competition.

For several years now, we have found ourselves in a new "Cold War": a conflict that is not only about power but also about ideologies, fought indirectly and, for us, without bloodshed; for others it has been a bloody war. Currently, it is the Ukrainians who are bleeding; in 2008, it was the Georgians. For us in Europe, as in the Cold War, this battle is once again about winning the hearts and minds of entire peoples, and the two opposing camps are fighting to draw these peoples to their side. On the one hand, there is the open society, defined by Karl Popper in 1945 as one in which "the individual is confronted with personal decisions," as opposed to a "magical, tribal or collective society."[1] The individual, and individual human rights, are thus at the centre of the values of the open society. Popper's definition alone tells us where the values of the other, the collective society, lie: it prioritises the community as a whole and its rights over those of the individual. Moreover, it opposes the idea that leading secular elites can define values (and also revise such definitions), and instead upholds a dogma that originates from metaphysical sources ("a higher, unfathomable authority").[2] We find this Stated directly by Alexander Lukin, head of the Department of International Relations at the elite Russian university MGIMO, in an article published in 2014 – Russia was in the process of annexing Crimea at the time. [3] ›

[1] *Popper, Karl:* The Open Society and Its Enemies, Volume One, London: Routledge, *1945, reprinted 2006, Chapter 10, Part I.*
[2] "unknowable" in the English translation.
[3] *Lukin, Alexander:* "Eurasian Integration and the Clash of Values", *Survival, 56:3 (2014), pp. 43–60.*

TEXT_ ***Beatrice Heuser***

Prof. Dr. Beatrice Heuser is Distinguished Professor at the Brussels School of Governance (VUB) and Head of Strategy Teaching at the German Armed Forces Command and Staff College. Her research focuses on why humans wage war, which means and strategies they choose – and how they justify them.

KEY MESSAGES

→ **Democracies** deliberately constrain themselves through international law, transparency, and public oversight.

→ **Slow decision-making processes** and legal constraints make open societies predictable.

→ **"Hybrid warfare"** exploits gray zones below the threshold of war, for which democracies are poorly prepared.

→ **Propaganda, disinformation, and cyberattacks** are particularly effective against open information environments.

→ **The new Cold War** is a systemic conflict: between individual freedom and collectivist power logic.

In the following, we shall examine how our view of war in liberal democracies and our practices differ from those of our opponents, and what the consequences of this are.

I_ The democratic constitutional State and war

Any contemporary rules-based State today is committed to compliance with international law and human rights, thus deliberately accepting constraints on its own freedom of action. In doing so, it builds on the traditions of just war, of which the most unquestionable criterion still dominates today: only defence is legitimate.

In the development of the modern State, there has been a trend, continuing to the present day, that has placed the independence and sovereignty of the State above all else. In reality, no prince or State has ever been completely independent of the influence of others, and thus no one was absolutely sovereign, even if he or she had this ideal in mind. Even sovereign princes were largely bound by customary law (such as, since the 17th century the exchange of prisoners of war). Those who disregarded it were considered barbaric and uncivilised, often reason enough for other princes to take action against them.

This also applied to decisions to go to war. According to the Just War Tradition, it is necessary to prove that an injustice had been done, that the other side refuses to redress this injustice, and that war is the ultimate option for redressing this injustice independently, in the absence of a higher authority or mediator. Exceptionally, the nineteenth century saw the sovereign State claiming the unrestricted right to start a war for reasons of "reason of State" or, as it was later called, "national interest".

This right, however, on which Austria and Germany had still acted in 1914, was already being questioned by lawyers in the late 19th century. It was due to the influence of these lawyers – and the revanchist mood of the populations of the victorious powers – that the 1919 peace treaties attributed war guilt to the defeated Austria and Germany. In nineteenth-century thinking, a sovereign State did not incur guilt by starting a war for reasons of State.[4] These two treaties heralded a return to restrictions under international law, away from the absolutely sovereign State. Where customary law had previously applied that could not be enforced before an international court, treaty law now took its place, with an international court of justice established in 1920.

The League of Nations which became operational in the same year already obliged members to seek arbitration and commissioned a (security) Council to protect member States against attacks. Its constitution still granted the right to go to war if arbitration proved impossible. But in 1928, a further step was taken: proposed by the then French Foreign Minister Aristide Briand and his American counterpart Frank Kellogg, the 31 signatory States accepted a restriction on their sovereignty with a declaration that they would no longer use war aggressively as an instrument of "national" (i.e. State) policy.

The Charter of the United Nations reiterated this restriction of the right to wage war to individual or collective self-defence.[5] The Organisation for Security and Cooperation in Europe (OSCE) reaffirmed it by expressly ruling out the alteration of borders through the use of force.[6] Russia's attack on Ukraine, which it itself recognised as an independent State in the 1994 Budapest Agreement, is therefore in every respect contrary to international law.

International law restricts the freedom of action of States, as does any treaty. The principle here is that one trades self-abnegation for the advantage of others applying the same. This understanding, however, underlying every regulated community has not taken root in all cultures. In many cultures, especially those that were great powers in the past, the nineteenth-century conviction still lives on that a State enjoys completely unrestricted sovereignty and is not restricted by any external laws or powers. This traditional view has periodically surfaced in the USA, although it also has an internationalist tradition that gave birth to the League of Nations and the UN. Paradoxically, the former tradition led the American Congress to refuse to allow its country to join the League of Nations, even though it had been largely designed by US President Woodrow Wilson and his advisers. Under Donald Trump, this sovereignist tradition has fully re-emerged.

Sovereignism also crops up time and again when it comes to French defence; it was expressed in France's self-exclusion ›

[4] *Hathaway, Oona & Scott Shapiro:* The Internationalists, *New York 2018.*
[5] UN Charta, *Art. 51.*
[6] Helsinki Final Act, *Art. I, https://www.osce.org/de/mc/39503, accessed on 18 August 2023.*

from NATO integration between 1966 and 2009. It can also be found in the "Brexit" decision of the British referendum of 2016 to withdraw from the European Union (EU). Nevertheless, neither of these two European countries has questioned the prohibition of changing borders by force.

The situation is different in China and Russia: China simply ignores the decision of the International Court of Justice regarding possessions in the South China Sea, which is being challenged by China's neighbouring countries. Russia has occupied part of Georgia and has been waging a war since 2014 to annex Ukraine, in contravention of multiple treaties.

States built on the rule of law should generally adhere to the principle of non-aggression enshrined in the UN Charter. An embarrassing exception was the war of intervention waged by the USA and some of its partners against Iraq in 2003. At least among the current EU member States, only Poland went along, and even in the UK, which unquestioningly backed its favourite ally, the USA, there were lively public protests, resignations among government advisers and the suicide of a security expert.[7] This foreign intervention was no exception for the US, however: it came in the tradition of its invasion of the island nation of Grenada in 1983, air strikes on the presidential palace in Libya in 1986, attacks on terrorists in Syria in 2017, 2018 and 2025, and attacks on Syria, Iran and Venezuela in 2025. But even in America, such actions have been regularly criticised.

II_ Decision-making processes

In democracies, political approval of public opinion is sought at least in election years. But even beyond regular elections, democratic States are more dependent on public opinion and need broad political approval for military action. The outcome of regional or European elections can also be interpreted as disapproval of a government's policies and may lead to pressure for new elections. There are examples of governments yielding to this pressure without being constitutionally compelled to do so.[8] Leaving aside the debate about whether Great Britain, France and the German Empire were democracies on the eve of the First World War,[9] the First World War was an example of how large sections of the population could actually long for war. Politicians conjured it up, praising involvement as "manly", glorious, and socially "purifying". In Great Britain, France and several other countries (but not in Germany), this changed after 1919. Once more after 1945, democratic societies across Europe tended to urge their governments to exercise restraint in the use of force. Even a deterrent stance – an obvious readiness to defend oneself in order to prevent opponents from even considering a promising attack – has repeatedly met with protests from large sections of the population in the Netherlands, the Federal Republic of Germany, Austria, Great Britain, and Italy.

Governments of democratic States are also forced to be more transparent and accountable to the public and the international community than authoritarian States. This can make them vulnerable in international conflicts, as authoritarian States can use unconventional or aggressive measures without caring about public opinion or international norms. Military spending is discussed in public as a tolerated evil at best.

Constitutional democracies, and especially alliances of democratic countries, take much longer to reach decisions than dictatorships. The two reasons are the consultative processes inherent in the system, involving parliaments except in cases of direct self-defence, and legal restraints that are generally heeded. Autocracies with little interest in international law can make decisions much more quickly as long as they have the means to carry them out. Accordingly, autocracies can catch democracies unprepared, presenting them with accomplished facts.

Authoritarian governments may have terms of office that span decades. This allows them to pursue long-term strategic goals unhindered. In contrast, governments in democratic States are generally limited to shorter-term planning due to election cycles, and long-term projects – particularly military research, development and procurement projects, as well as the restructuring of defence infrastructure and personnel – can be cancelled by subsequent governments. In the event of war, emergency laws come into force, which generally extend the rights of governments, even in democracies. However, in times of crisis, the inertia of the ›

[7]There was a detailed investigation, the results of which were finally published in the twelve-volume "Report of the Iraq Inquiry" (a.k.a. Chilcot Report), which led to a very damning conclusion for the intelligence services and the government. The executive summary alone was 145 pages long. See *https://www.gov.uk/government/publications/the-report-of-the-iraq-inquiry*, accessed on 14 August 2023.

[8]This was the case, for example, with President Macron in France in June 2024 after the outcome of the European elections. In the United Kingdom, the 1933 East Fulham by-election, the election of a successor to a parliamentarian who had died in office, marked the start of a long policy of avoiding war.

[9]In none of these three countries were even 50% of those over the age of 18 eligible to vote: in all three, women did not have the right to vote, and many of the young soldiers who served in the 1914-18 war were under the age of 21 and therefore also excluded from voting.

democratic system of government is clearly evident, as far-reaching measures – especially the introduction of conscription – usually depend on a slow process of consensus-building among the general public. An opponent of open society can easily strengthen opposition through propaganda (and money).

III_ Hybrid war

This brings us to the means of bloodless combat, often referred to today as "hybrid warfare," although some of these means are thousands of years old. The term hybrid warfare was originally coined by American strategist Frank Hoffman to describe wars that combine various means without resorting entirely to the use of force. He wanted to describe enemy actions and pointed out that our binary thinking – war or peace – makes it difficult for us to deal with such grey areas.[10] However, this term was then adopted by Russian strategists, led by Chief of General Staff V.V. Gerasimov, but interpreted as a Western pattern of behaviour.[11]

In fact, both terms simply describe what the USSR in particular has been doing since its foundation (and the Bolsheviks even earlier), namely using fifth columns in the form of communist parties in other countries, peace movements, propaganda and other means of psychological warfare, possibly even waging proxy wars, while avoiding a world war if possible. What has been new in recent years – especially in Russian operations against Ukraine prior to the classic invasion beginning in February 2022 – is the deliberate avoidance of actions that would trigger NATO's treaty obligations. This led to talk in Western strategic debates of "non-Article 5" actions, i.e. actions that cannot be interpreted as a direct attack on the territory of a NATO member State. Article 5 of the North Atlantic Treaty describes an attack on one member State as an attack on all and postulates that the other members must then take action (what that action is remains unclear: it could be anything from a letter of protest to the use of nuclear weapons to defend the ally).[12] NATO does allow for consultation in less serious cases (Article 4). This is difficult to translate into concrete action, however, which in turn complicates decision-making.

Measures that cause outrage when they are uncovered but do not trigger war include the assassination of individuals (such as Western citizens who have fled Russia because they were persecuted there as opponents of the regime or who, as defectors, have brought information about Russian intelligence services with them), bribery or blackmail of individual politicians or industrialists, physical acts of sabotage against electricity, gas and water works, or paralysing airports through cyber interference or drone incursions.[13]

PROPAGANDA WAR

Propaganda warfare is nothing new: attempts to bring one's population alongside a particular strategy can be traced back to ancient times, as can attempts to influence the enemy polity. Half-truths and untruths have always been deliberately or unwittingly circulated for this purpose. Fake news, a.k.a. lies, are nothing new in themselves. What is new is the way in which they can be disseminated. Where rumours used to spread by word of mouth, today we have social media.

The decline in newspaper readership, especially of newspapers with well-researched and verified articles that strive for objectivity in their reporting, is an internal threat to open societies. It is a process of erosion of the values and responsible citizens basing their opinions on critical reading on which open society is built. In their place come the lazy consumers of 400-character in echo chambers of like-minded people whom they "follow". This is where propaganda reaches them most easily, with the deliberate use of lies and slander, such as equating all Ukrainians who do not want to see their country incorporated into the Russian Federation with "Nazis", or the claim that Russian-speaking Ukrainians are being genocidally persecuted in the Donbas.

The problem, as Hanna Arendt aptly described it, is that

"Lies often appear much more plausible and appealing to the mind than the truth, because the liar has the great ›

[10] *Hoffman, Frank:* Conflict in the 21st Century: The Rise of Hybrid Wars, *Arlington, Virginia 2007.*
[11] *Fridman, Ofer:* Russian Hybrid Warfare, *Oxford 2018.*
[12] Article 5 States: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."
[13] Kristan Stoddart: Russia's Hybrid Warfare Offensive Against the West *(Berlin: De Gruyter, 2026).*

advantage of knowing in advance what the audience wants to hear."

Furthermore, it is difficult to combat these untruths with counterarguments, as the popular saying goes that there is no smoke without fire, that there must be "something to it." As Arendt wrote,

"In a constantly changing, incomprehensible world, the masses had reached the point where they believed everything and nothing at the same time, considered everything possible and nothing true. ... Mass propaganda discovered that its audience was always ready to believe the worst, no matter how absurd it might be, and that it did not particularly resist being deceived because it considered every statement to be a lie anyway. The totalitarian mass leaders based their propaganda on the correct psychological assumption that, under such conditions, people could be made to believe the most fantastic assertions one day and, when presented with irrefutable evidence of their falsity the next day, they would retreat into cynicism; instead of abandoning the leaders who had lied to them, they would protest that they had known all along that the claim was a lie, and admire the leaders for their superior tactical cleverness." [14]

This describes very well not only the situation of the 1930s that Arendt had in mind, but also that of Russian and Chinese propaganda today.

CYBERWARFARE AND ESPIONAGE

The propaganda war waged on social media is only one facet of hybrid warfare. It also includes other types of cyber-intervention, ranging from paralysing polling stations or nuclear energy laboratories to espionage by hacking networks. Physical acts of sabotage can be replaced by electronic ones.[15] Here, too, our law-abiding societies are weaker than those that disregard international law. For example, in its 2023 National Security Strategy, the Federal Republic of Germany explicitly rules out aggressive countermeasures such as disinformation., rejecting "reject hackbacks as a means of cyber defence on principle."[16] The assassination of enemy leaders is also taboo among European States, as it has been since Ronald Reagan's presidency in the United States. This stance is undermined now by the option of targeted killings provided by precision munitions and drones, such as that of Iranian General Qasem Soleimani in 2020. Israel also makes extensive use of this method.

Espionage is only frowned upon in open societies when it is carried out by opponents (or allies) against one's own State. There seems to be a widespread belief that it espionage necessary to ward it off and that ideologically motivated spies in the enemy country are heroes fighting for our cause. Espionage based on eavesdropping on enemy communications or on images from space and other technical means only angers Western citizens when it is directed against their own countries. If it were revealed that Western intelligence services were able to do something similar in Russia or China, it would be seen more as a success. A pinch of Machiavellianism is entirely compatible with the defence of the open society.

IV_ Views of war

European views of war have changed over the centuries. Until ›

[14] *Arendt, Hannah:* The Origins of Totalitarianism *(Frankfurt/Main 1955), my translation.*
[15] *Stoddart:* Russia's Hybrid Warfare Offensive.
[16] *https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf, (The New World Order), p. 62.*

the nineteenth century, not only in Germany, but also in the republics of France and America and in democratic Great Britain, war was generally seen as part of human nature, part of the condition humaine. Russia still holds this view today. As Putin announced on 27 January 2021 at the World Economic Forum in Davos,

"we all know that competition and rivalry between countries in world history never stopped, do not stop and will never stop. Differences and a clash of interests are also natural for such a complicated body as human civilisation."[17]

In this social Darwinist view of the world, which has remained stuck in the nineteenth century via the detour of Marxism-Leninism with its belief in inevitable war until the whole world would become Communist, war continues to be an instrument of power politics. Instability and conflict in the neighbourhood can also be useful, as this allows a great power to consolidate its hegemony in the region.

Although war was an annual occurrence in Europe for centuries, there is a tradition dating back to Antiquity that sees war abnormal. As British-American strategist Colin S. Gray pointed out, when Western States, including the United States, have gone to war since 1945, they have wanted to withdraw again as quickly as possible; that this was often impossible is another matter. While autocracies like to exploit prolonged chaos beyond their own borders to exert influence, trading democracies prefer stability for this purpose. Since the 1920s at the latest, European democracies have no longer tried to expand geographically. Even in the case of the US wars of intervention since 1991, the early adoption of "exit strategies" speaks for itself. As "world policemen", the three Western permanent members of the UN Security Council – the US, the UK and France – have repeatedly felt obliged, even after the end of the Cold War, to intervene in regional conflicts and bring about peace or – often too late – prevent massacres, but generally without any interest in territorial gains. In European democracies, the mantra that war is a scourge, as stated in the UN Charter, has become a fundamental belief. This makes it all the more shocking for citizens of European societies that with Donald Trump, an American government is behaving like the expansionist powers Russia and China in aiming for territorial gains.

V_ State, citizens, conscription: perspectives of democracies

Conscription was defined as a duty of the citizen by the French Revolution, a condition of popular sovereignty. Since then, France has been a particularly good example of the diverse perspectives on conscription in democracies. In the successive French republics of the nineteenth century, the argument arose, mainly on the right of the political spectrum, that such a duty was incompatible with civil liberties. It was argued, somewhat exaggeratedly, that rough day labourers or farmhands would find conscription less burdensome than city dwellers (not to mention the spoilt sons of the upper classes). A very unequal compromise was soon reached: the wealthy could buy their way out of military service and pay others to fulfil it for them. This had already happened in Roman times and again in the Middle Ages, but in the context of modern democracies, this compromise stood in stark contrast to the principle of equality. This fundamental tension between freedom and duty continues to prevent many Western democracies from returning to conscription in today's dangerous international context.

In a larger social context, conscription can be seen as an instrument of social integration, as it brings together people from different social and ethnic backgrounds and educates and trains them for a common purpose. This can contribute to promoting national unity and cohesion, an argument that could be of particular interest in Europe, where the proportion of the population with a migrant background is steadily growing. Moreover, it can be argued that defence is too important a task to be left entirely to a subgroup of the population – the military.[18] This implies a fundamental distrust of the military, mostly originating from the Left of the political spectrum, as even in democracies it tends to be collectively more Conservative than Left-wing. General conscription gives young citizens from all parts of society an in- ›

[17] *Session of Davos Agenda 2021 online forum • President of Russia, accessed on 2 II 2026.*
[18] French Statesman Georges Clemenceau became famous for this Statement in 1887, when he said, "War is too serious a matter to be entrusted to the military."

sight into the military and with that, the possibility to counter or denounce unconstitutional tendencies in the military.

Overall, the issue of conscription in open societies remains complex and controversial, touching on various political, social, economic and ethical considerations. Debates about this are influenced by the respective national security situation, historical experience, military traditions and political priorities. Authoritarian regimes do not to the same extent need to fear such debates discussion and opposition to conscription. Nevertheless, it is clear that even Russian President Vladimir Putin has so far refrained from introducing universal conscription to fight against Ukraine, preferring to hire mercenaries from North Korea and Middle Eastern countries. [19] As a result, his compatriots are largely unaffected by this "special military operation". In the autumn of 2021, before Russia's major offensive against Ukraine was unleashed, 54% of Russians surveyed by the Friedrich Ebert Foundation said that their country did not have the position in the world that it deserved. However, this put Russians far behind the Turks (82%!), Serbs and Ukrainians (79% each) and Armenians, Italians and Poles (72%, 68% and 57% respectively). Sixty-five per cent of Russian respondents believed that Russia was "part of the European cultural sphere", while only 57% of British and 62% of Norwegian respondents shared this view. Overall, 75% of Russians surveyed at the time believed that Russia should resolve conflicts abroad peacefully. Although 47% of Russian men surveyed (but only 24% of women) believed that Russia had every right to carry out military actions in other countries for "self-defence", 47% were against this and only 35% were in favour. 75% of Russians surveyed believed that their country should cooperate with all peaceful countries, even if they had different values – only 53% of Germans, 54% of French and 52% of Americans agreed (although the national security strategies of all three countries since 2022 have tended to see things the same way as the Russians!).

Nevertheless, in autumn 2021, the majority of Russians surveyed defended Russia's policy on Ukraine, but not by an overwhelming majority. 57% believed that the US was the greatest threat to peace in Europe, 55% believed that Ukraine was to blame for the conflict in Ukraine, 51% blamed the US (as well), and only 16% blamed Russia. (It remains to be seen how Trump's friendly overtures to Putin since 2025 is affecting Russian propaganda.) While in 2019 more than half of those surveyed also blamed the EU, in 2021 this figure had fallen to just 19%. In 2021, 73% believed that Crimea had been legally annexed by Russia.[20]

In 2025, 61% of Russians surveyed by the Friedrich Ebert Foundation feared a world war, as did 58% of Georgians, 43% of Germans, 40% of Italians, but only 20% of Ukrainians (who were obviously despairing of help from the Western powers), 27% of Americans, 28% of French and Poles, and 34% of Britons.[21]

VI_ How do democracies wage war?

The claim that there is a nexus between a State's constitution and its way of waging war can be traced back to antiquity. Aristotle, in his Politics (VII.7), attributed different styles of warfare to different ethnic groups or races. Around 1700, Montesquieu attributed differences in the style of warfare to different State constitutions, arguing that republics treat their enemies more leniently than tyrannies. Such ideas were taken up by Guibert and Henry Lloyd in the mid-18th century. Clausewitz, in turn, stated without passing judgement that "semi-educated Tatars, republics of the old world, feudal lords and trading cities of the Middle Ages, kings of the eighteenth century, and finally princes and peoples of the nineteenth century: all wage war in their own way, wage it differently, with different means and towards a different goal...".[22]

When it comes to atrocities against the civilian population, however, it cannot be said that the behaviour of democracies in the wars of the 20th century differed qualitatively from that of tyrannies. In general, democratic regimes did not starve prisoners of war to death or kill them directly. But in the interwar period, measures such as combating uprisings in the colonies by bombing villages from the air were used by the democracies of France and Great Britain as well as by the fascist regimes of Spain and Italy. This also applies to the bombing of cities in the Second World War by Great Britain and the USA, and even afterwards, in the Korean and Vietnam Wars. Nor can it be said that civilian ›

[19] *Margarete Klein:* "How Russia is recruiting for a long war: Covert mobilisation via 'volunteers', preparation for a new mobilisation", SWP-Aktuell 2024/A 26 (07.06.2024), *https://www.swp-berlin.org/publikation/wie-russland-fuer-einen-langen-krieg-rekrutiert*, *accessed on 4 July 2024.*

[20] *https://peace.fes.de/security-radar-2022*, (The German army is not ready for war), *accessed on 21 August 2023.*

[21] *https://www.fes.de/security-radar-2025#c403845.*

[22] *Beatrice Heuser:* 'The Conceptual Heritage of Strategic Culture and Collective Mentality' in Jeannie Johnson, Kerry Kartchner, and Briana D. Bowen (eds): Routledge Handbook of Strategic Culture, *Abingdon: 2023, pp. 17–30.*

casualties were merely unintended collateral damage, as Richard Overy's research shows.[23] Thus in the hope of breaking the "morale" of the enemy nation, the Royal Air Force deliberately bombed residential areas during the Second World War.[24] Already in the First World War, the Royal Navy's starvation blockade of Germany particularly affected civilians. Soldiers from all countries have been responsible for raping women, albeit at quantitatively different levels, and the military justice systems of democracies have been much more conscientious in prosecuting such crimes.[25] Other atrocities were also committed by soldiers from democracies in isolated cases, such as the torture of prisoners in wars in the early 21st century. Here, too, quantitative differences can be observed, especially since the second half of the 20th century. Once again, self-criticism in an open society comes into play.

VII_ Effects on the dialectic of war: Democracies vs. authoritarian systems

How do all these differences affect the dialectic of war? Since the financial crisis of 2008, reminiscent of the Crash of 1929 albeit cushioned by social welfare systems in Europe, there has been a resurgence of nationalism and populist parties, exacerbated by the financial impact of the Covid-19 crisis and increased energy and food costs since 2022. Today, the majority of humanity does not live in open societies. In their National Security Strategies, successive US administrations have acknowledged that their power is declining relative to the rest of the world. On the other side of the Atlantic, Europe is economically strong, even without growth, but militarily weak.

The multiple weaknesses of the open society are particularly evident in this context. We understand our opponents poorly or not at all because we project our own aversion to war, but also our relative satisfaction with the status quo (with high incomes and social security compared with most other countries) onto the whole of humanity. We ourselves remain unwilling to consider war as a means of our politics; in fact, this has become one of our most important shared values. As democracies, our decision-making processes are very slow and legalistic, leaving us unable to make decisions when there is no clear legal case. As open societies, we endlessly debate and criticise our own governments, with a disproportionate tendency towards self-criticism. Again, because we are an open society, our weaknesses are exposed and discussed in the free media and academic literature.

Despite their roots in Christianity, our values today are the result of centuries of debate and are now enshrined in law – we do not invoke any metaphysical authority. In contrast, one of the strengths of our opponents in authoritarian systems is that they rely on such authorities, whether it be God or Allah, or Marx-cum-Mao.

Furthermore, authoritarian governments can make decisions much more quickly than we can, because tyrants do not need to consult other ministers or lawyers. They can silence critics by arresting them or administering a pinch of Novichok. They can also lie with impunity, restrict or shut down their citizens' access to the internet, and wage cyberwarfare without criticism from within their own ranks. They can configure the media and entertainment industry to support their own propaganda and thus promote the brainwashing of the nation. In short, autocracies find it easy to override the preferences of their own populations, whereas open societies do not. ■

[23] *Richard Overy:* The Bombing War: Europe 1939–1945, *New York: 2013.*
[24] *Richard Overy:* "Operation Gomorrah: Ruthlessness and the British Air War 1943", in David Trim und Brendan Simms (Hrg.), Harfleur to Hamburg: Five Centuries of English and British Violence in Europe, *London: 2024, pp. 219–236.*
[25] *Michèle Battesti:* « Le viol: une arme multiséculaire ? », *in Jean Baechler & Marion Trévisi (Hrg.):* La Guerre et les Femmes, *Paris: 2018, pp. 120–140.*

02_ Insight

Advantage Through Knowledge

"Intelligence is about understanding competition, understanding how knowledge is distributed across that competition, and then gaining decision advantage."

Jennifer E. Sims, USA

Illustration Grafissimo/iStock

What if intelligence were less about knowledge than about not knowing? Political scientist and artist Jennifer E. Sims, a long-time member of the U.S. Intelligence Community, reflects on genuine decision advantage that arises from consciously engaging with uncertainty.

„Certainty is Dangerous“

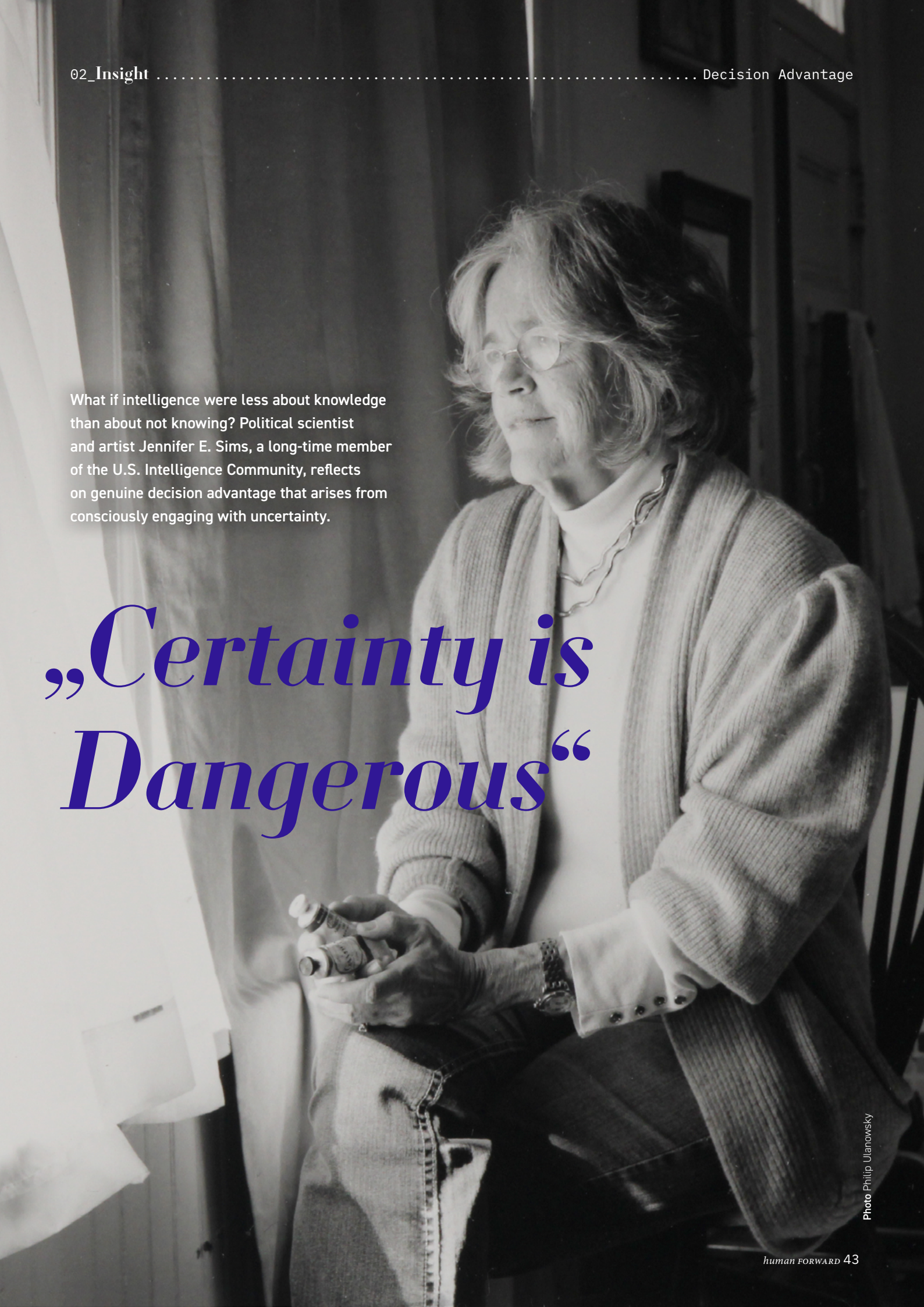

Photo Philip Ulanowsky

„Intelligence is about competitive learning."

Jennifer E. Sims

Jennifer Sims, what kind of knowledge does intelligence generate – and what kind of knowledge should it aim to generate?

Jennifer Sims: Many people assume that intelligence is about seeking truth. That belief is deeply rooted. In fact, the idea is literally carved into the wall of the Central Intelligence Agency in the United States, in the form of a Bible quote:"And You Shall Know the Truth and the Truth Shall Make You Free". It sounds as if that were the intelligence mission. But it is not. Intelligence is about competitive learning. It is about understanding competition in the first place, understanding how knowledge is distributed across that competition, and then gaining decision advantage. In very simple terms, it is about knowing more than your adversary or your competitor. Not everything, but more of what matters.

So intelligence is not about discovering how the world truly is?

No, not in that comprehensive sense. Intelligence produces limited knowledge. It produces exactly the knowledge that helps you win, or sometimes helps you avoid losing. In the best cases, it can even help generate win win outcomes by understanding what the other side actually wants from a conflict and finding a way to satisfy those needs at the lowest possible cost. If intelligence is practiced this way on a global level, it can create a form of political transparency. That transparency can reduce wars caused by misperception. It will not eliminate all wars, because intelligence is not about all knowing. It is about a very narrow and focused kind of knowing.

You are very explicit about rejecting the idea that intelligence is defined by what intelligence institutions do.

Exactly. Intelligence existed before modern intelligence institutions were created. Therefore, our understanding of the subject cannot be limited to understanding what those instiutions do. Our modern intelligence organizations emerged at a specific moment in history, and they defined their missions in particular ways. But that does not mean their activities define what intelligence is. My goal has been to think about intelligence in a broader, more fundamental sense.

Why is it misleading to think of intelligence as a form of truth seeking? In your book you use an animal example. I think it was a bear. Or maybe not.

It was a deer. But your confusion actually proves my point. Of course intelligence has always aimed at accuracy. Seeking accurate information is part of gaining advantage. There is truth in intelligence, but not Truth with a capital T. The deeper idea of truth that we inherit from philosophy or theology is about universal principles and an all knowing perspective, a kind of God's eye view of reality. If intelligence aims for that, it will fail the decision maker. Decision makers are not looking for omniscience. They are trying to win. ›

INTERVIEW_ ***Jennifer E. Sims***

Dr. Jennifer E. Sims held senior positions within the U.S. national security establishment, including at the U.S. Senate Select Committee on Intelligence and as an intelligence coordinator at the State Department. She also taught at Georgetown University. In 2022, she published her book *Decision Advantage*. She is also an artist and founder of the Stuart Street Atelier.

KEY MESSAGES

→ **Intelligence** is not truth-seeking in a philosophical sense, but competitive learning aimed at gaining decision advantage.

→ **It produces limited, purpose-driven knowledge** – enough to avoid loss or enable success, not omniscience.

→ **The core of intelligence** lies in shifting uncertainty, not eliminating it; counterintelligence is central

→ **Overreliance on prediction** and AI creates dangerous illusions of certainty and suppresses human judgment.

→ **Effective intelligence** depends on imaginative diversity – including artists and unconventional thinkers – to expose blind spots and unknowns.

Or at least to avoid defeat. That requires only a limited set of information, enough to make a judgment that prevents loss.

So how does the deer example help explain this?

I use these analogies because many people equate intelligence with what intelligence agencies do – drone strikes, covert operations, special missions. Those are tasks of institutions, not intelligence itself.

Imagine a hunter and a deer. In the open meadow, the hunter has a clear advantage. He can see far. He has a long range weapon. He is experienced. But the deer can choose to run into the woods. There, the hunter loses sight. The deer's camouflage works in its favor. The deer has not learned something new. It has shifted the terrain of uncertainty.

That is intelligence. It is not about learning more facts. It is about changing where uncertainty works for you rather than against you. If we forget this, we lose the counterintelligence dimension entirely. We also lose sight of the real purpose of intelligence, which is to influence the interaction on both sides of any competition by increasing relative knowledge and relative advantage.

And if we push that analogy further, what does relative advantage actually mean here?

In this case, the hunter adapts by building a deer stand and climbing into a tree. He improves his vision. He regains some advantage. But notice what is happening. Both sides are constantly adjusting. Intelligence is the skill of knowing how to compete by shifting uncertainty, by collecting and analyzing information faster or more effectively than the other side. This is a form of power we often overlook. We usually think of power in terms of resources, population, or weapons. But even in an asymmetric situation, where one side is weaker by all conventional measures, victory is possible. The deer has fewer capabilities than the human hunter. And yet it can escape. Not through strength, but through an instinctive understanding of how to move the competition onto ground where it has the advantage. That, in essence, is intelligence.

"Even in asymmetric situations, where one side is weaker by all conventional measures, it can still prevail."

Jennifer E. Sims

All right. But does this approach not ultimately require something like perfect prediction?

That assumption is very common, and it is precisely where modern thinking about intelligence often goes wrong. There is a strong belief today that prediction is the most important task of intelligence. That intelligence should tell us what the future will bring. This is a dangerous direction, because it assumes that intelligence deals with something static. But competition is never static. It unfolds in real time. It moves. It reacts. Take again the example of the deer and the hunter. If you analyze the situation as a frozen moment, a hunter standing in a meadow with years of experience and a powerful bow, you can make very convincing linear projections about who will win. If you do not consider that the deer might suddenly run into the woods, your prediction might look very solid. But the deer is thinking too. It is reacting. And once you include all those interactions, trying to predict everything becomes a fools game.

So the problem is not lack of data, but the nature of the situation itself?

Exactly. What the hunter really needs is not perfect knowledge of every variable, but awareness of one decisive possibility: the deer might run into the woods. That single insight outweighs any elaborate forecast. Intelligence should focus on how uncertainty can shift, not on the illusion that it can be eliminated.

I like another, slightly playful example from Raiders of the Lost Ark. A swordsman confronts the protagonist in a plaza. By all visible measures – skill, weapon, setting – the swordsman should win. A traditional intelligence analysis would assess only that threat and predict defeat. It would be wrong, because it ignores what is unseen: the gun in the protagonist's pocket, which ends the encounter instantly.

So intelligence failed because it only looked outward?

Yes. This is what often happens in intelligence services, especially in democ- ›

racies. They are trained to measure threat everywhere. They estimate and predict based on the adversary alone. But they are often not allowed to understand the decision maker they serve with the same depth. They do not know what tools, options, or intentions that decision maker has. If there is a rigid boundary between intelligence and decision making, intelligence products multiply in the form of predictions, estimates, and warnings that are irrelevant to what the decision maker actually needs. The result is an overwhelming threat picture that frightens rather than guides.

Can you give a concrete historical example?

Yes – and a tragic one: the Iraq War in 2003. Intelligence estimates focused on what Iraq might have and might do – uranium enrichment, yellowcake, worst-case scenarios. Everything followed linear projection: how dangerous Saddam Hussein would be if those capabilities existed. We obsessed over the blade and the swordsman.

The war showed the weapons did not exist. Iraqi diplomats asked what they could prove. The answer was: nothing. Belief had replaced inquiry.

Intelligence should focus less on grand estimates and more on collection – reducing specific ignorance and mapping uncertainty: who knows what, where knowledge is weak, and where advantage lies. Strategic intelligence is estimative, but not static. As a hunter, you do not ask what happens if you stand here. You ask where you gain advantage. You avoid the woods. You choose the meadow. This is exactly what Elizabeth I understood when she faced Philip II and the Spanish Armada. She forced the fight into the English Channel, where her navy held advantages, and limited her aims to one goal: prevent a landing. By shaping the terrain of uncertainty, she gained decisive advantage – an approach governments today largely fail to master.

Could you explain that in more detail?

Governments, especially in the United States, are not trained to map the terrain of uncertainty. Prediction and estimation are used in the wrong way. I dislike the word prediction, but there are limited cases where it makes sense. You can predict, for example, that when a deer is threatened it will run into the woods, because experience shows that this is what deer do. But that is not really intelligence. That is closer to a scientific regularity.Intelligence begins after the deer enters the woods. What happens then is difficult to foresee. It requires estimation, judgment, and continuous adjustment. That is the hard part, and it is also the most important part.

"Today's governments are not trained to map the terrain of uncertainty."

Jennifer E. Sims

What brought you to art, and especially to figurative painting and classical oil painting? And how does this connect to the „intelligence part" of your career?

That is a profound question. Part of the crisis we face today – nationally and perhaps globally – is the absence of an artistic sensibility, what I would call the art spirit. Art invites us to engage with beauty, inner depth, form, structure, and proportion, and to solve problems in ways that are fundamentally different from analytical or bureaucratic thinking. Classical traditions emphasized proportion and resonance, almost mathematically. Modern art, by contrast, often refuses to spoon-feed meaning. It demands contemplation. People may initially feel repelled, standing before a blank canvas asking why this is art. But if they stay, they may discover an answer. That act of contemplation matters. This connects directly to the question of unknowing – what we know, and what we do not. Art is one way of exploring the unknown. In creating something, we begin with personal experience, but when it resonates with others, a non-verbal, non-hierarchical form of shared meaning emerges.

Much of my earlier life operated through authority: academia, government, doctrine. These are legitimate ways of knowing. But before all of that, I was a dancer – and now I am an artist.

When I retired from government, I decided to study painting as a way of knowing. It is not a rejection of my past, but a completion of it.

Many people in the West feel that everything has become absurd, even grotesque, politically and socially. Against this background, does art not risk becoming useless?

I do not think art is ever useless. It exists in and of itself. I am not drawn ›

to political or persuasive art; that belongs to a different category and often functions like propaganda. For me, art is rooted in timeless beauty and virtue. It is a way of knowing, not of advocacy – and that is why it endures, even amid political absurdity.

In the United States, education has increasingly privileged math and science. These disciplines matter, but they are often taught without creation or inner exploration. Art once taught us to ask what is right or true, to discover ourselves through making, and to receive critique without defensiveness. Civilizations do not thrive through one kind of knowledge alone, but through many ways of knowing.

This is why I want to pursue a project of unknowing. Civilizations evolve by integrating different forms of knowledge, yet we rank them, treating science as the only legitimate one. But imagination – Einstein's true gift – emerges from crossing boundaries, including art. Learning to paint an eye teaches patience and care, virtues our speed-driven culture has largely forgotten.We forget that Einstein was once a postal clerk. His most important insight was not inherited knowledge, but imagination.

What does AI mean for our understanding of knowledge?

This is a vast subject, and I do not have clear answers. In many ways, I am a beginner myself, trying to understand a world where information processing is changing at breathtaking speed. Artificial intelligence is extraordinarily powerful at integrating vast amounts of external information. But it only learns from what it is fed – human knowledge shaped by bias and assumption. AI processes what we think we know, not what we do not know. It cannot engage with unknowing, which lies at the heart of uncertainty. AI may show us what we believe to be true, but not what we are missing.

So the problem is not just bias, but a structural limitation?

Exactly. And that limitation becomes dangerous in a competitive world where states confront one another. AI will be used as a tool of intelligence. States will try to feed it everything they know or think they know about their adversaries. But AI will be very poor at highlighting the risks that stem from ignorance. It will generate ever greater certainty. And certainty is dangerous. Once you are certain, you become predictable. And predictability is fatal in competition. Much of the art of gaining decision advantage lies in understanding what you do not know, and in shaping what your opponent does not know.

So AI pushes us in the opposite direction?

Yes. It accelerates decision making. It compresses time. It rewards speed over reflection. My fear is that it squeezes out the human capacity to pause, to hesitate, to sense that something does not fit even when all the data seems to line up.

Lets see if we understand: If all states rely on AI to predict the behavior of their adversaries, decision making becomes dangerous because everyone believes they can foresee the other side?

That is close. The danger is not only mutual prediction, but the speed at which decisions are forced. The worries of those who feel that something is wrong will be suppressed. Those worries often come from intuition, from an awareness of missing pieces. But intuition requires time. It cannot survive in an environment dominated by algorithmic certainty. Think back to Iraq. Feeding more and more data about uranium enrichment and yellowcake into an AI system would not have solved the problem. What was required was a pause. A deep breath. A different question. What do we not know? How do we know that we do not know it? And how might we find out? AI is very bad at asking those questions.

Because it creates an illusion of certainty.

Exactly. And if Iraq itself had possessed advanced AI capabilities, it might have looked at the situation in the United States and concluded that war was inevitable. There is no space left. No uncertainty. No hope. I have not fully played out that scenario, but it shows how quickly certainty can harden into ›

"Art is a way of exploring the unknown."

Jennifer E. Sims

fate.What interests me most is the moment of leadership that resists this. The moment when a true leader steps back and says: something feels wrong here. We seem to know everything, and yet something does not fit. I want to stop. I want to slow this down. I want to explore what we are missing.

That moment cannot be automated. It depends on patience, imagination, humility, and the courage to live with uncertainty. Those qualities belong to human beings. And if we lose them, no amount of data or speed will save us.

Even if I have no positive evidence for that feeling at all.

Yes – exactly. I used to stress this when teaching senior leaders in the State and Defense Departments. In crises, leaders often suffer from too much information. At some point, more data or bigger teams stop helping. What matters is asking: what do I truly need to know now? Sometimes that leads to unexpected choices, even talking to an adversary. Before Munich, Britain faced contradictory intelligence about Hitler. Chamberlain met him personally – an act later condemned as appeasement. Yet that encounter led Britain to conclude Hitler was dangerous and to reverse course. The shift came not from better analysis, but from judgment formed through experience. Rational analysis is one way of knowing, not the only one. Leaders still weigh authority, sources, and intuition – something AI struggles to do. If AI suppresses that human impulse, it may reduce misperception while also becoming a profound risk.

Would you say, then, that there is a decisively human form of intelligence in both senses of the word? Not only intelligence in the sense of intelligence services, but also intelligence in the cognitive sense.

Yes. Very clearly yes. This is what I call inner knowing. It is a form of knowing that artists access, that poets and musicians convey, often without being able to fully explain it. It is not analytical in the usual sense, and it is not easily verbalized. Western societies struggle with this form of knowing because we have not been trained to cultivate it, to descend into those depths and integrate what we find there into our lives. I think that is one reason for the current fascination with artificial intelligence. We are so focused on calculation, efficiency, and external knowledge that we neglect this other part of the human cognitive terrain.Machines will never replace this kind of knowing. But they can make it irrelevant. And that, to me, is the truly frightening possibility.

What you are describing reminds us to older traditions, both Western and Eastern. In ancient Greece, there was what they called „metis“, a kind of cunning or practical wisdom. And in Chinese thought, there are similar ideas. Is that the direction you are thinking in?

Yes, very much so. What is striking is that this insight appears across cultures and traditions. You find it in religion, mysticism, philosophy, and even modern psychology: learning through stillness, listening, and becoming comfortable with not knowing. Whether through Plato, prayer, silence, or Jung's idea of the mind as a filter rather than the source of knowing, the common thread is turning inward. Machines can never access this realm, because they lack inner life and consciousness. Our fascination with replacing it reveals how disconnected we have become from it – and that is what my current research explores.

Ultimately, what is intelligence knowledge for? And what must it never become, in your view?

Intelligence must never be regarded as the source of human truth. Even in democracies, there is a temptation within intelligence communities to claim that role, often expressed in the phrase "speaking truth to power." That phrase suggests that truth resides with intelligence professionals and not

"A crucial part of the art of gaining decision advantage lies in understanding what you yourself do not know and in shaping what the adversary does not know."

Jennifer E. Sims

with decision makers. I think that is a serious misconception. If that belief spreads, citizens will begin to see intelligence as a moral or political check on their leaders. But intelligence is not an independent moral authority. It is a creature of leadership. It exists to serve decision making, not to mine or pronounce truth.

Regardless of who the leader is?

Yes – whoever the leader is. Intelligence is only as trustworthy as the leadership it serves. When intelligence institutions drift from that role, they waste resources. I often ask why agencies publish global forecasts about humanity's future. They do so because they see themselves as truth-tellers. That is dangerous. Secret budgets should not fund quasi-philosophical visions with implied moral authority. Intelligence exists to gain decision advantage in competition. It produces information for action, not timeless truth. Its products are provisional, time-bound, and necessarily limited. I see a worrying tendency for intelligence services to posture as modern Oracles of Delphi.

And what about the idea, common in Europe, that intelligence services exist to preserve democracy?

Intelligence cannot preserve democracy. At best, it can support democratic health by staying out of politics. The moment intelligence enters the political arena, it becomes dangerous, because information meant for decision advantage can easily turn into a political weapon. Intelligence must serve, never rule. Intelligence services must never become campaign tools or be used to secure a leader's power or attack domestic opponents. Campaigns will always conduct their own intelligence operations – that is their role. National intelligence has a different, limited mission: supporting foreign and defense policy. Clear boundaries are essential. Without them, intelligence risks serving bureaucratic or factional interests. In democracies like the United States, a fragmented intelligence system is intentional. Concentrating intelligence around one actor or worldview undermines neutrality. Intelligence must support all decision-makers equally – or it stops serving the state.

From intelligence to art, we covered a wide range of ground. Is there anything you feel is missing?

The strongest intelligence services have always embraced unconventional thinkers rather than filtering them out. They do not aim for a single professional mindset. They value diversity in its deepest sense. Diversity is not a slogan; it is the core of effective intelligence. Artists alongside scientists. Immigrants with lived knowledge beside academic specialists. Philosophers next to engineers. Practitioners alongside theorists. Without this mix, intelligence develops blind spots. Not knowing is inevitable – but not knowing that you do not know is fatal. A healthy service is one where someone can say, "We don't really understand this," and be heard. Without such voices, asymmetric conflicts are misunderstood and opportunities missed. The most neglected figure today is the artist. British counterintelligence in WWII thrived on eccentric, imaginative minds – musicians, magicians, unconventional thinkers. Their creativity mattered. Intelligence is strongest not when it is uniform, but when it is most imaginatively diverse. ■

"Intelligence must never be understood as a source of human truth."

Jennifer E. Sims

"I Am Interested in Facts"

"Open Source Intelligence" (OSINT) is regarded as a panacea in the information age. Yet open sources yield insight only when they are evaluated selectively, methodically, and responsibly. Alana Gramm on intuition, AI, truth – and democratic steadfastness.

INTERVIEW_ ***Alana Gramm***

Dr. Alana Gramm is an OSINT specialist and Senior Strategy Consultant at IBM iX. Her focus areas lie in Open Source Intelligence at the interface of intelligence, law enforcement, and defence.

KEY MESSAGES

→ **OSINT is a process**: collection, analysis, and contextualization of open sources – never a static end state.

→ **The quantity of data** does not replace quality; selective, expert evaluation is decisive.

→ **AI accelerates processes** but also increases risks of manipulation – human judgment remains central.

→ **Truth means verifiable facts**; their denial harms victims and society.

→ **Europe's strength** lies in shared methodology, standards, and knowledge transfer – not in data accumulation.

Alana Gramm, in intelligence circles there is much discussion about OSINT (Open Source Intelligence). What exactly do you understand by it?

Alana Gramm: From my practical experience, OSINT means collecting open information, analyzing it in a targeted manner, and deriving actionable insights from it. Having a lot of data helps no one if it is not prepared in a way that is relevant and understandable.

Where do you draw the line between open and non-open information?

The line runs where one has to hack, deceive, or overcome protective mechanisms. OSINT is based on information that is publicly accessible. Public, however, does not necessarily mean free of charge or easy to find. A book in a library is also public, even though I need a library card.

But information may be openly accessible, while the insights gained from it are highly sensitive.

Exactly. A classic example was a scandal involving a running app. A single recorded running route is harmless. However, if many people regularly run around a military facility and record their routes, the superimposition of this data makes it possible to reconstruct the outlines of buildings, access roads, and structures. Only the combination of the individual pieces of information, each of which is uncritical in itself, makes the data security-relevant.

Is OSINT still manageable at all when information is constantly changing?

One has to accept that insights are never static. Information is dynamic. What is valid today may be outdated tomorrow. OSINT is therefore always a process, not an end state.

How important is intuition in OSINT work?

Experience creates a sense of where information might be located. Many experienced analysts say: "I don't know exactly why, but I had the feeling it might be relevant there." This gut feeling comes from years of practice.

But intuition can also lead one astray.

Absolutely. Especially in assessment, one must be careful not to be biased. Confirmation bias or community bias ›

Photo foto-kirsch.de

> *„If I analyze content, I must understand language, codes, images and cultural references. Otherwise I will recognize neither fakes nor nuances of meaning."*
>
> Alana Gramm

are real risks. That is why systematic procedures are needed, colleagues who contradict you, and the willingness to work with an open mind regarding the outcome.

What role does artificial intelligence play?

AI accelerates OSINT massively. Pattern recognition, prioritization, analysis – all of this is much faster today. At the same time, however, the risk of manipulation and disinformation is also increasing. That is why OSINT must never be viewed in isolation.

What does that mean for analysts?

Critical thinking becomes central. Information must be cross-checked across different sources. The more AI we deploy, the more important human judgment becomes.

One might actually think: you simply have to collect as much data as possible and run an AI over it that then tells you what is truly relevant.

The problem is that quantity does not replace quality. If the underlying data is false, distorted, or deliberately manipulated, an AI will not produce reliable results either.

So "more data" is not automatically better?

On the contrary. The internet consists of a great deal of irrelevant material. If I collect indiscriminately, I even make myself vulnerable – for example through poisoned data or deliberate deception. Good OSINT work is selective. It requires expertise and an understanding of context.

What does that mean in concrete terms?

If I analyze certain content, I must understand language, codes, images, and cultural references. Otherwise I will recognize neither fakes nor nuances of meaning. No AI can replace this expertise. In practice, this part of the evaluation is often underestimated.

Is it already evident that more and more AI-generated content is circulating?

Absolutely. One does not need to conduct an OSINT investigation to see this; it is enough to scroll through social media. AI-generated images, videos, and texts are increasing significantly. Many users intuitively sense that something is not right.

What follows from this at a societal level?

People must learn to question content: Is this plausible? Does it fit the context? Children in particular should be sensitized early to the fact that not everything they see is real.

Do we today need a kind of "default distrust" toward internet content?

Rather a healthy skepticism. Not believing everything immediately, but also not rejecting everything. This balance is becoming increasingly important, for analysts as well as for society as a whole.

What does truth mean to you?

For me, that is a very practical question. Truth reveals itself where something has actually happened. It is not about abstract debates, but about verifiable facts that must be understood and placed in context.

So it is about recognizing what has really happened?

Yes. I am interested in facts because they form the basis for justice and accountability. Did something happen or not? Was a boundary crossed or not? These questions must be answered – for those affected, for institutions, for society. When real events are denied or relativized, additional harm arises because trust and orientation are lost.

And how does one avoid distortions?

Through transparency, critical thinking, and dissent. Analysts must work with an open mind regarding the outcome, similar to in science. As soon as one only confirms what one already believes, one loses professionalism.

Does OSINT also have a democratic dimension?

As a method, OSINT fundamentally works everywhere, including in non-democratic systems, like any other intelligence discipline. The difference lies less in the technique than in the environment. In authoritarian states, information is more fragmented, more tightly controlled, and often deliberately manipulated. This increases the effort required, the risk of distortions, and the uncertainty of the results.

Where exactly does the strength of OSINT lie?

Primarily at the strategic level. OSINT can make long-term developments visible: discourses, mobilization, infrastructure changes, movements that ›

become apparent through social media or satellite imagery. It does not indicate when something will happen, but that something is brewing.

And operationally?

Operationally, it is about situational monitoring. What is happening right now? Where are people moving? Where are refugee movements emerging? The faster authorities have this information, the better they can respond. This is a central component of societal resilience.

Does the value of OSINT lie more in early crisis detection or in subsequent clarification?

From my experience in policing, there are two central levels. First, hazard prevention: recognizing early what could happen in order to protect people. Second, clarification: reconstructing what actually happened. Both are necessary. When events are denied, such as war crimes or acts of violence, OSINT can help make facts visible. Satellite imagery, timelines, and open sources make it possible to verify statements and refute falsehoods.

In a specialist article, you argue that European OSINT capabilities should be pooled more strongly. Why is that necessary?

Because we cannot manage it alone. In Europe, many actors work in parallel within their respective silos. Methods, tools, and training approaches are developed multiple times, although we could learn from one another. At the same time, our adversaries often act in a highly coordinated manner.

What exactly do you mean by pooling capabilities?

Not merging data. That would be problematic in terms of data protection and democracy. It is about methods, training, and the exchange of experience.

„The internet is a mirror of society. Anyone who wants to understand it must be able to read the mirror."

Alana Gramm

Common standards, shared learning spaces, mutual support. Too often, we reinvent the same wheel.

Does that inevitably lead to a European intelligence structure?

I am not concerned with new institutions, but with the transfer of knowledge. Whether structural consequences emerge from this at some point is a political decision.

What personally motivates you to engage so intensively with OSINT?

In times of information warfare, OSINT is a central methodology. It is about recognizing what is actually happening and how we can protect ourselves as a society.

Do you see yourself more as an analyst or as a hunter?

Both. Of course, there is that hunting moment – the thrill when you find something through indirect routes. That is enjoyable. But the seriousness prevails. It is about influence, about societal processes. The internet is a mirror of society. Anyone who wants to understand it must be able to read that mirror.

Would you advocate offensive countermeasures, such as engaging in disinformation ourselves?

No. That is how one loses credibility. One cannot defend truth while manipulating oneself at the same time. If we abandon our principles, we lose precisely what defines democracy.

So what remains?

Steadfastness. The rule of law. And the ability to endure things without becoming authoritarian ourselves. That is exhausting, but there is no alternative if we do not want to lose our society.

Perhaps we are currently at the beginning of a new Enlightenment in Europe, driven by the experience that democracy, truth, and freedom are fragile. That would be a hopeful perspective...

Authoritarian systems often follow the same patterns: reality is reinterpreted, criticism is delegitimized, freedom of the press is gradually restricted. Independent journalism is one of the first targets, because it enables societal self-correction. If it is weakened, a society loses orientation and resilience. This phase would be hopeful if it were to give rise to greater vigilance, strong institutions, and a practical understanding of freedom in everyday political life.

Because it is about control over perception...

Exactly. If people can no longer distinguish what is real, there is no longer any need to suppress them. I do not say that polemically, but from personal observation. The new Enlightenment, if one wants to call it that, above all means learning to recognize reality.

Less abstract truth, more reality?

Exactly. There are different perspectives, but some things have factually happened. And their denial is an injustice toward the victims. War crimes, ›

violence, historical crimes – that is not an opinion. That has happened.

And for you, OSINT is part of this Enlightenment?

Yes, if it is used responsibly. Information is power. The more personal information is, the more sensitive this knowledge becomes. Just because something is public does not mean one may do anything with it. It requires weighing considerations, the rule of law, and respect for privacy.

So no simple answers.

No. Democracy is complicated. But that is precisely what makes it valuable. And despite everything, I see hope: I have experienced it – for example in 2022, when young people voluntarily helped refugees, for hours on end, without compensation. This generation gives me confidence.

Then this new Enlightenment may be less a theoretical project than a shared practice.

Yes, exactly. Practice and theory must learn from one another. If we do that, we will improve – as a society and as a democracy. ■

„If people can no longer distinguish what is real, there is no longer any need to suppress them."

Alana Gramm

Intelligence Strengthens Supply Chains

Global supply chains are increasingly under geopolitical pressure. Geopolitical Risk Intelligence helps companies understand and manage supply chain risks.

GEOPOLITICAL RISKS AS A CHALLENGE FOR GLOBAL SUPPLY CHAINS

Geopolitical risks are the uncertainties in companies' decision-making processes that arise from the competition of states for power in the international arena as well as from global shifts in power.

The supply chains of the German economy are highly vulnerable to these risks. The main reason for this is that states are increasingly using the economic interdependencies and dependencies that have grown over decades of globalization as political leverage. The supply chains of German companies have recently been significantly affected, for example, by geopolitically motivated export controls on rare earths and semiconductors as well as by tariffs. In addition, supply chains can be disrupted by armed conflicts, as has been the case in recent years in Ukraine or along the sea route through the Red Sea, which is important for the global economy.

This can lead to rising costs as well as supply interruptions and production outages, which in extreme cases can have strategic impacts on companies. Potential societal consequences of these risks include rising inflation, increasing unemployment, and declining macroeconomic competitiveness, but also challenges to the realization of political goals such as the energy transition, the digital transformation, or the security policy "Zeitenwende." These goals can only be achieved if the necessary components and raw materials can be reliably sourced by companies through functioning supply chains.

RESILIENT SUPPLY CHAINS REQUIRE GEOPOLITICAL RISK INTELLIGENCE

Where geopolitical risks are known and taken into account in decision-making processes, supply chains can be designed to be resilient to these risks. However, the events of recent years have shown that companies often have deficits in this regard. Larger companies in particular have therefore established intelligence functions to remedy this.

The term "Geopolitical Risk Intelligence" refers to the organizational units, processes, and products that perform this task. What these have in common with other intelligence functions is that they generate decision- and action-oriented knowledge in order to provide timely, user-oriented, relevant, and reliable information products on this basis. In this way, uncertainties in decision-making processes are to be reduced so that companies can make better decisions. ›

TEXT_ ***Simon Wunder***

Simon Wunder is responsible at Volkswagen AG for the analysis of geopolitical risks for supply chains. In addition, the political scientist is a Research Fellow at the Center for Advanced Security, Strategic and Integration Studies (CASSIS) at the University of Bonn. This contribution reflects his personal views.

KEY MESSAGES

→ **Geopolitical shifts in power** and state interventions increase the vulnerability of global supply chains.

→ **Economic dependencies** are increasingly being used as political leverage.

→ **Geopolitical Risk Intelligence** makes risks visible, assessable, and relevant for decision-making.

→ **Resilient supply chains** arise through scenarios, monitoring, and data-based early warning.

→ **Companies with an integrated intelligence function** react faster, avoid damage, and secure their long-term ability to act and compete.

Where this task is successfully performed, risks to supply chains become transparent so that they can be managed through targeted measures, damage can be averted, and opportunities can be seized. Supply chains can then be designed in such a way that they are less exposed to geopolitical risks. When risks materialize, procurement organizations with such functions are better prepared, so that crises become more manageable for them and supply interruptions can either be avoided entirely or at least their duration shortened. Furthermore, companies with a high-performing intelligence function are more capable of learning, enabling them to adapt earlier and better to changes in the geopolitical environment and to draw relevant conclusions from events and incidents.

In a global environment increasingly characterized by volatility, uncertainty, and complexity due to rapid technological change, growing global interconnectedness, and geopolitical dynamics, the importance of such functions has therefore increased significantly in recent years.

A widely established intelligence methodology with a sufficient level of maturity for the analysis of geopolitical risks for supply chains does not yet exist, so companies must largely develop these themselves on the basis of best-practice examples and their own experience. The organizational and methodological approaches described below are examples of such developments.

THE ORGANIZATION OF THE INTELLIGENCE FUNCTION FOR SUPPLY CHAINS

In procurement organizations, intelligence tasks are in some cases performed by small teams. In order to be successful, these require both expertise in procure- ›

Specific Challenges in Intelligence Tasks in the Supply Chain Area

Intelligence functions were originally mostly established in companies within the area of corporate security. In procurement organizations, they face specific challenges that require an adaptation of common approaches to this field of tasks.

- **In the past, companies have in some cases correctly identified geopolitical risks for supply chains but did not adequately consider them in decisions.** One reason for this is that measures to strengthen the resilience of supply chains are usually associated with higher costs and other efforts than, for example, security measures for sites and employees. Intelligence products are therefore required to quantify statements on the probabilities of occurrence and impacts of risks in such a way that they can be processed in decision-making processes. However, this quantification has not always been carried out by the responsible intelligence functions in the past, partly because it is not always provided for in common intelligence methods.
- **Assessing the impacts of risks also requires a sufficient degree of transparency in one's own supply chain as well as the automated processing of the corresponding data.** However, the technical and organizational prerequisites for this are not yet in place in all large companies.
- **Another challenge is that intelligence processes can make statements about the probabilities of occurrence of risks more reliably the shorter the time horizon considered.** However, supply chains in industry are often not very elastic, so that long-term forecasts of probabilities of occurrence are demanded, which can hardly be delivered using common methods.
- **Geopolitical risks for supply chains are, compared to other risks handled by intelligence functions, highly complex.** Their assessment requires deep expertise that intelligence teams cannot maintain for all relevant risks, but which in larger companies is usually available elsewhere in the organization and must be tapped.

ment and knowledge of the company's structures and processes, but also as broad geopolitical expertise as possible and networks outside the company, for example in associations and think tanks. Since the analysis of geopolitical risks for supply chains relies primarily on data, expertise in the field of data science is also required. Such teams also generally make use of the support of specialized service providers in order to identify and analyze geopolitical risks.

The introduction of a central function that analyzes and manages geopolitical risks for all areas of a company has often not proven to be effective. One reason for this is that the impacts of these risks on the individual business areas differ greatly in each case, and their identification, analysis, and assessment each require specific expertise that a central function can hardly comprehensively reflect. What has proven effective instead is close coordination between the intelligence functions of different areas – besides procurement, for example strategy, risk, security, and public policy departments – and the coordinated development of strategic scenarios and situational assessments.

METHODS AND PRODUCTS OF INTELLIGENCE ANALYSIS IN THE SUPPLY CHAIN AREA

The intelligence methods developed for the analysis of geopolitical risks for supply chains usually combine quantitative approaches from risk management with Structured Analytic Techniques and other scientifically grounded, methodologically transparent, and process-oriented qualitative analytical methods that were originally developed by security authorities to increase the quality of intelligence analysis.

The products created with them cover the entire analytical spectrum. They describe relevant events, assess their immediate impacts on supply chains, and provide a forward-looking outlook on the possible future development of risks. The focus is always on answering the question of "so what," meaning the implications for one's own supply chains.

A higher-level analytical product is a strategic situational assessment that prospectively analyzes the most important supply-chain-relevant geopolitical trends and their possible impacts as well as their potential further development. Such situational assessments usually support strategic decision-making processes and are coordinated with other staff functions within companies.

Another forward-looking product is scenario analyses that examine individual geopolitical developments. They can be used to identify risks for supply chains that are entered into a risk register and further monitored. On this basis, risk analyses for individual procurement projects can also be prepared. For this purpose, risk ratings are also used, which are largely created in an automated and data-driven manner and take into account a large number of risk factors.

Current developments are captured through monitoring and forecasting processes. These observe previously identified risks, search for signals of potentially emerging new risks, assess the immediate impacts of events on supply chains, and provide forecasts regarding the probability with which certain risks may materialize in the short to medium term.

FURTHER DEVELOPMENT OF GEOPOLITICAL RISK INTELLIGENCE

Increasing risks to supply chains are generating growing pressure on the private sector to further develop the approaches and methods described above. The persistently high frequency of geopolitically caused supply crises, as well as the increasing learning capability of organizations and advances in the field of artificial intelligence, will likely lead to significant changes in the field of Geopolitical Risk Intelligence in the supply chain context in the coming years. To strengthen societal resilience to these risks, it would be desirable for this field to receive greater attention beyond large companies and, for example, for methods and processes to be jointly further developed by government, academia, think tanks, and industry. ■

Chaos As a Weapon

Sabotage is a central instrument of hybrid warfare. Leading expert Daniela Richterova explains why the scale, methods, and psychological impact of the current wave of sabotage pose a strategic challenge to Europe.

Photo Ivan Weiss

Daniela Richterova, how do you define sabotage?

Academics still debate the definition and probably always will. But in simple terms, sabotage is an intentional act aimed at damaging or disrupting systems, organizations, or processes for political, strategic, or ideological reasons. It is usually conducted covertly.

What forms can sabotage take?

It can include arson, explosions, contamination of water or energy supplies, and even assassinations if they are intended to disrupt key industries or war efforts. Sabotage also exists in cyberspace, most notably when cyber operations have physical consequences.

It seems that the target of sabotage could in principle be almost anything...

It could be many things, but I would be careful not to stretch the concept too far. Not every hostile or violent act is sabotage. For me, the key issue is whether the target has a strategic purpose or significance.

What do you mean by strategic purpose in this context?

The act needs to be linked to a broader political or military objective. For example, Russia has carried out assassinations and poisonings of opponents abroad. These are serious acts, but they are not necessarily sabotage. They are a way of dealing with opponents, not always a way of disrupting a strategic system.

So motive alone is not enough?

Exactly. Revenge or punishment is not sufficient. Sabotage needs to be aimed at something that matters strategically, something that connects to a larger goal.

Would simply destroying property qualify as sabotage?

It depends on the context. If you destroy a random car, that is simply a criminal act. But if you destroy a car belonging to a senior political figure and you are paid by a foreign state to do so, and if the objectives are political, military, or intelligence-driven, then it could be considered sabotage. Intent and target are decisive. But whether it actually qualifies as sabotage also depends on legal definitions, as not all countries classify this type of action in the same way.

Turning to the broader picture, how would you characterize the wave of sabotage since the start of the war against Ukraine?

I would argue that this is the most intense wave of sabotage we have seen since World War Two. During the Cold War, there was extensive planning by the Soviets, the Stasi and others, but very few plans were actually carried out. What we see now is different in scale and frequency. The period from 2023 to 2024 was particularly intense, with dozens of cases ranging from hostile surveillance to actual sabotage on NATO territory. In 2025, the situation was quieter, but still serious incidents occurred.

What explains that scale?

A large part of it is the use of low level agents. Most attacks are not carried out by professionals, which allows for more operations across more countries. Many agents are recruited online for multiple tasks. In some cases, one recruited individual brings in friends or acquaintances. It's a form of outsourcing. You specify the task and someone assembles a team.

Why has this „gig economy model" of sabotage become so prominent?

There are three reasons. We have seen the erosion of norms and a shift in the strategic landscape since 2014 and especially since 2022. Operationally, ›

INTERVIEW_ ***Daniela Richterova***

Dr. Daniela Richterova is Associate Professor of Intelligence Studies at the Department of War Studies at King's College London. Her research on Cold War intelligence services, state threats, and terrorism has been published in International Affairs and Foreign Policy, among others. In 2025, she published Watching the Jackals (Georgetown University Press).

KEY MESSAGES

→ **Sabotage** is a deliberate, usually covert act pursued for strategic purposes.

→ **Since 2022**, Europe has experienced the most intense wave of sabotage since the Second World War.

→ **A "gig-economy model"** relying on low-threshold actors is replacing traditional intelligence operations.

→ **The objective is not only physical damage**, but above all psychological impact.

→ **Critical infrastructure** is increasingly in private hands.

"The methods have adapted, but the underlying logic is remarkably familiar."

Daniela Richterova

many professional intelligence officers have been expelled from Europe. Technologically, modern surveillance makes traditional cover identities harder, while online recruitment and payment are easier.

What does that tell us about the nature of sabotage?

Sabotage does not exist in isolation. It is a tool states use in response to political developments. Periods of escalation, such as increased military support for Ukraine, are often followed by spikes in sabotage activity.

Do you see continuity with Soviet era sabotage doctrine?

Yes, very much. Many of the strategic goals discussed in Soviet and Eastern bloc documents from the Cold War still apply today. Undermining political unity in the West and imposing economic costs remain central objectives. Today, generating chaos and paranoia sometimes seems more important than hitting major military targets. The methods have adapted, but the underlying logic is strikingly familiar.

How do you assess the degree of sophistication of sabotage today?

It depends on how we define sophistication. We already see forms of sabotage that go beyond physical attacks. Some of my colleagues have written about how large language models are being polluted with disinformation, which shapes how societies are informed. That can also be understood as AI sabotage, even if it looks very different.

Are there clear examples of cyber sabotage with physical consequences?

Yes. The most recent case is in Norway, where pro Russian cyber actors attacked a dam by opening floodgates. Large amounts of water were released for hours before it was noticed. That was a cyber operation with real physical impact.

Could artificial intelligence increase the effectiveness of sabotage?

Potentially. AI could help identify particularly vulnerable targets, such as critical railway junctions or communication infrastructure where a small disruption causes large effects. It could also assist in analysing the architecture of undersea cables or other weak points. I would prefer not to speculate too much, though, as I do not want to provide a playbook.

How can analysts distinguish sabotage from ordinary crime?

Ambiguity is built into hybrid warfare. Outside of wartime, these acts are meant to look like accidents but there are indicators you can examine, especially the target and the timing. If a warehouse burns down, that may seem routine. But if it is used by a Ukrainian logistics company and contains equipment destined for Ukraine, that changes the picture. Timing also matters. Did it happen after a political escalation or following adecision possibly viewed as hostile by your adversary?

From Russia's perspective, how important is the psychological impact of sabotage operations?

It is absolutely central. One of the main goals is to demonstrate reach. When incidents are suspected in several countries, it creates the impression of competence and power. At the same time, it undermines confidence in the ability of governments to protect their societies.

This sounds similar to classic terrorist strategies. Is that a fair comparison?

There are clear parallels. The aim is not only physical damage, but to also spread fear, uncertainty and loss of trust. In that sense, sabotage and terrorism overlap in how they affect societies.

Are you comfortable describing sabotage as a form of war?

I would be careful with that framing. You could call it part of a covert war, but legally and politically it is not war in the traditional sense. War requires armed hostilities between states and needs to meet a number of legal conditions. What we are seeing is better described as hybrid conflict.

How does sabotage fit into hybrid operations?

Sabotage is a tool that can be used to prepare for war or accelerate escalation. Ten years ago, hybrid warfare was mostly about disinformation and election interference. Today, kinetic operations play a much larger role.

Looking at preparedness, which sectors are potential targets?

There is a long standing list of targets that already existed during the Cold War. Soviet planners identified categories ranging from soft targets, through hard-to-defend infrastructure, to hard ›

"Communication and transport networks are particularly vulnerable. You cannot guard every railway line or cable across Europe."

Daniela Richterova

targets per se. Communication and transportation networks are particularly vulnerable because they cannot be fully protected. You cannot guard every railway line or cable across Europe. Military or weapons related facilities are also on that list.

Are those Cold War assumptions still relevant today?

Very much so. When you compare those historical target lists with recent attacks, at least half of them have already been hit. The technology has changed, for instance from telephone lines to fibre optic and undersea cables, but the strategic logic is the same.

Are there notable gaps in targeting so far?

Yes. We have seen relatively few attacks on political parties or political leaders. Based on Cold War thinking, one might have expected more of those, but they have not featured prominently so far. What is more striking is the shift toward other types of targets. Because of decades of privatization, many elements of critical infrastructure are now privately owned. Railways, logistics hubs, retail and energy are no longer purely state assets. Private businesses are now on top of the target list.

Why does that matter?

It changes the security landscape. Attacks on private companies can have national level consequences. We have seen arson attacks on major commercial sites, such as an IKEA store in Lithuania and a large shopping mall in Warsaw that affected thousands of businesses. Governments have to work much more closely with the private sector to prevent or contain these attacks. National security can no longer be handled by the state alone. Businesses are part of the frontline.

Beyond awareness, what is needed to build resilience?

Stronger cooperation across the security community on this particular threat. Intelligence services, law enforcement and security agencies need to work together as closely as they did with respect to counterterrorism. That requires resources, political focus and breaking down institutional silos.

Is countering sabotage also a question of better communication?

Yes, very much so. What we usually call domestic liaison is crucial. It means different actors sitting in the same room and openly sharing what they know. Who has seen what, how does that information connect, and how can it be used jointly. That kind of communication makes a real difference.

What role does legislation play in this process?

A very important one. Many countries are updating their laws to address state based threats more explicitly. France has recently done so, the UK updated its legislation two years ago, and other countries are following. The last time we saw a similar wave of legal change was after 9/11, when new terrorism related provisions were added to criminal law.

On a personal level, which type of sabotage worries you most?

What worries me most is a multi-target mass casualty scenario. There was a plot that thankfully failed, involving incendiary devices sent on cargo flights to Germany, the UK and Poland. If these devices would have exploded mid-air, it would have been a nightmare scenario.

Why does that particular case stand out?

Because it combined several worst case elements. It was coordinated across countries, highly visible and could have caused many deaths. For people working on counterterrorism, this kind of scenario has always been the greatest fear.

How does that compare to more targeted operations?

Targeted attacks feel distant to most people. A cargo aircraft explosion or a similar public incident is different. Anyone could have been affected without any link to the conflict.

So the fear is not only about casualties?

Exactly. The immediate harm would be terrible, but the broader impact would be even larger. When an attack feels indiscriminate, it spreads fear, paranoia and chaos far beyond the actual event.

In other words, everyone feels it could have happened to them.

Yes. That perception is what makes such acts so powerful and so dangerous for societies. ■

„Intelligence Is a Leadership Responsibility“

From Afghanistan to the corporate crisis unit: corporate intelligence expert Christopher Radler-Morić explains how companies identify risks early, remain capable of action – and why good intelligence often works best precisely when it remains invisible.

Christopher Radler-Morić, how would you explain to outsiders what you do professionally?

I started my career as an intelligence analyst at a security authority, from where I went to Afghanistan as a risk manager for the then German Agency for Technical Cooperation (GTZ). In doing so, I came into contact with all the classic fields of corporate security: situation analysis, site security, evacuation and emergency plans, travel security – the full program.

And from that your current focus developed?

Exactly. Step by step, I developed further in the direction of emergency and crisis management, especially during my time at Daimler. There I built up the global crisis management system: the corporate crisis unit, the crisis situation center, governance structures. Operationally, it involved natural disasters, civil wars, kidnappings, extortion – everything one can imagine.

Today you work heavily in the field of business continuity management. What is that about?

The emergency and crisis planning of a company. This ranges from scenarios such as a rampage or the suicide of an employee to major geopolitical crises. A central part is to establish crisis units, train them, and keep them capable of action – including fictional exercises and moderating a unit in an actual emergency.

How does that differ from classic risk management?

Risk management seeks to minimize the probability of damage events occurring, thus acting preventively. Business continuity management addresses the scale-of-damage side, thus reactively. It assumes that despite all prevention, a residual risk remains that can materi- ›

INTERVIEW_ ***Christopher Radler-Morić***

Christopher Radler-Morić is an expert in corporate security with a focus on business continuity management, emergency and crisis management, travel security, and intelligence. With an intelligence background and a master's degree in Arabic studies, ethnology, as well as risk and crisis management, he combines strategic security analysis with deep cultural and geopolitical understanding of complex risk environments.

KEY MESSAGES

→ **Corporate intelligence** is not fortune-telling, but structured analysis to prepare decisions under uncertainty.

→ **Business continuity management** complements risk management by assuming that crises can occur and safeguarding the restoration of critical processes.

→ **Early scenario analysis** and clearly defined tipping points create real operational capability before crises become publicly visible.

→ **Lack of methodological understanding**, cognitive biases, and the prevention paradox lead to successful analysis often remaining invisible.

→ **Intelligence** only unfolds its benefit when it is closely linked to top management and systematically incorporated into strategic decisions.

alize as a damaging event – and asks: How do I quickly get critical business processes running again in the event of a disruption? How do I ensure emergency operations?

So it is about comprehensive crisis preparedness.

Exactly. The process begins with early crisis detection, that is, with the observation and analysis of developments. The keywords are intelligence, foresight, and forecasting: Will something happen? How likely is it? And what impact would it have on the company? If the probability is high enough, one must prepare early – organizationally, operationally, and strategically.

How did you experience the Russian attack on Ukraine, for example?

> *"The process begins with early crisis detection, that is, with the observation and analysis of developments."*
>
> Christopher Radler-Morić

A colleague and I analyzed the situation intensively at the time and came to the conclusion that it was very likely not an exercise, but the preparation of an invasion. We informed management at an early stage. That was not comfortable, because it immediately created pressure to act. But when the attack actually began, the company was prepared: a specific crisis unit had been defined, supply chains and personnel issues had been clarified. This early analysis enabled real operational capability.

What comes next?

This is followed by evaluative analysis: What do developments concretely mean for the company, processes, and risks? Only here does one move beyond description to forward-looking analysis, which derives what is likely to happen next. We worked with scenario techniques. That means designing several plausible future scenarios and asking: What could happen? Which scenarios are relevant? And what impact would each have?

How do you assess such scenarios?

We used game-theoretical principles. That is, the assumption of rationally acting actors. We look at gain and loss and try to put ourselves in the counterpart's position. This is important because in Germany we look very strongly through our own ideological lens.

What does that mean concretely?

In the broader public, understanding of interest-driven foreign policy has largely disappeared. Many cannot imagine that a state intervenes because it benefits and because it can. International law is an important moral objective, but that is not always how the world works. If I seriously want to make predictions, I must free myself from such mental blockages.

For example with regard to Russia?

Exactly. We must ask what benefit Putin could derive from an attack. Then we consider it globally and holistically. We developed three scenarios and defined so-called tipping points for each. That is, indicators that show a scenario is becoming more likely.

Do you have an example?

A very well-known tipping point was the relocation of blood reserves to field hospitals near the border with Ukraine. That is not done during military exercises, because blood reserves spoil quickly and are extremely scarce. When that happened, it was clear to us: the scale is set to dark red. An invasion is very likely.

How do you obtain the information for such analyses?

We use all available sources: open source, publications, databases, service providers. In addition, there are personal networks and contacts on the ground. We ask about moods, perceptions, impressions. The goal is to create a unified situational picture from this.

And how does that differ from state intelligence work?

The essential difference is that companies do not use intelligence methods. There are no informants or secret sources. We speak with employees on the ground, with partners, with other companies. That is something completely different. In some cases, the sources are even better, because we can access corporate networks.

Do competing companies cooperate in this regard?

Yes, very strongly even. The corporate security community in Germany is excellently networked. Many within their own company do not even know that this function exists or what they actually do. But within the community there is a strong spirit of solidarity. Analytical findings are shared without disclosing trade secrets.

Even if that could bring a strategic advantage?

Most do not think so Machiavellian. The immediate business impact is often ›

limited. And it is also a give and take. One moves in a community in which one gives today and receives tomorrow. During Corona, for example, we had regular calls in the DAX-40 forum. Weekly or biweekly, during working hours. There, the emergency and crisis managers of the major companies exchanged views. Insights, best practices, very pragmatic.

That sounds like a fairly close-knit community.

It is. People know each other. The exchange is very open. There is a pronounced need-to-share mentality.

How does the current geopolitical situation affect corporate security?

Honestly, the topic is currently being treated more weakly. We are experiencing massive deindustrialization. The economic situation is very tense. Companies are losing money and cutting costs where the consequences only become visible in the medium or long term. Corporate intelligence is among them.

That means these functions are being dismantled?

Yes. Even demonstrably successful positions are often not refilled when vacant. Although crises were managed well, although developments were anticipated early. At the same time, there is an opposite trend. Business continuity management is growing strongly because it is required by regulation. Due to the new NIS2 legislation, around 40,000 companies are obliged to introduce risk and BC management systems. Money has to be spent on that. Other areas pay the price.

What are the biggest challenges for corporate intelligence in companies?

Decision-makers simply do not know the methods of geopolitical analysis. They consider it crystal-ball gazing. The fact that there are structured procedures is ignored. In addition, there are cognitive biases. On the part of analysts, but also among superiors.

What are the consequences?

In areas whose results are difficult to measure, the prevention paradox often applies. You are successful when nothing happens. But a non-event is difficult to quantify. This leads many security departments to act defensively. Make no mistakes. Do not stand out. Do not be innovative. Those who do nothing do nothing wrong. Analytical results then often fizzle out at middle levels.

And when it works well?

Then it is usually due to a strong leadership personality who is professionally competent, has backing, and is willing to carry uncomfortable issues upward. Not for career reasons, but to truly make a difference.

How is artificial intelligence changing this work?

Massively. Already now. Despite all its immaturity, AI is indispensable in my daily work. Texts, analyses, evaluations, system development. It is an enormous relief. It does not yet replace the analyst, because expertise and critical thinking are still required. But it accesses volumes of data that one could never handle manually. We are only at the beginning. The impact will be enormous.

You actually studied Arabic studies. What role does a humanities background play in your work? Do you also think in foreign languages?

Unfortunately, I cannot think in several languages. Swear in several languages, more likely. But jokes aside. That is a very good point. With Arabic studies and ethnology, I am actually an exotic in corporate security. Many there come from the police or military.

"Despite all its immaturity, AI is no longer conceivable to be without in my daily work."

Christopher Radler-Morić

Did this course of study help you concretely?

Very much so. Simply because I can move freely in Arab countries and have no inhibitions. The language opens doors. Arabs are very proud of their language. When I started at Daimler, there were subsidiaries in Arab countries, and it quickly became clear: I would take care of them. I was welcome there. One simply works differently together when one feels understood and respected.

Did that also shape your assessments?

Yes. During the Arab Spring, for example. I said early on that these democratization attempts would fail. High illiteracy, free elections, which leads to the electoral victory of the Muslim Brotherhood. And then the inevitable reaction of the military follows. That is exactly what happened. That was not a formal analysis model. That was a feeling, fed by time on the ground and cultural understanding.

And beyond language and cultural knowledge?

A humanities degree teaches above all one thing: to familiarize oneself with ›

unfamiliar subject matter – independently. I learned how to learn. That helps me to this day. I now work in information security, surrounded by IT specialists, developers, hackers. At the beginning I had no idea about it. Nevertheless, I got into it quickly because I am used to interconnected thinking.

How important is writing?

Being able to write does not only mean being orthographically correct. It means structuring thoughts. Making complex matters comprehensible. That is a key skill. Whether building a crisis management system or conducting a geopolitical analysis.

How much room does the non-rational have in your work? Such as emotions or unpredictability?

Actually none. I claim that there is hardly any irrational behavior. That sounds provocative. Of course there are exceptions. But 99 percent of what happens follows a rationality.

Even in seemingly irrational decisions?

Yes. The rationality often simply does not reveal itself from our perspective. We must try to see the world through the other's lens. In ethnology, one speaks of "emic" and "etic." One's own view and the view from the counterpart's perspective. Then much suddenly becomes logical. Perhaps not economically rational, but socially or psychologically rational.

What would you advise German entrepreneurs now, especially with regard to intelligence and security?

Security in the broadest sense should be taken more seriously, especially intelligence. They should buy in good people. And they should attach this function to top management. Security often leads a niche existence, somewhere in HR or in another department. A staff unit would be better. Then intelligence becomes usable for business decisions and not only for checking whether an expat can live on a certain street next to a certain hotel.

That means becoming more proactive. Involving intelligence early in decisions?

Absolutely. There is a lot of potential there. Classical analysts are often not business economists who only look at the margin. They bring an unspoiled perspective. They tend to think outside the familiar framework. And they filter opportunities and risks through a different lens.

"We must try to see the world through the other's lens."

Christopher Radler-Morić

Where do you see that in particular?

In location decisions, for example. Often management decides to open a site somewhere. And only later is security involved. I have experienced several times that better sites could have been chosen earlier, for very different reasons. Not only from a security perspective. But by then the decision has already been made. ■

"Doubt Remains Human"

What distinguishes structured analysis from mere gut feeling? Intelligence analyst Ole Donner explains how to avoid cognitive distortions, what separates good from bad questions – and why AI is only a tool.

Ole Donner, suppose you are part of a task force tasked with investigating the causes of the Berlin blackout. How would you proceed?

It is important to design the analytical process broadly and not to follow initial intuitions. First, various hypotheses regarding possible causes or actors are formulated. The next step is not to confirm individual assumptions, but to systematically falsify competing hypotheses. The basis is the Analysis of Competing Hypotheses: all hypotheses are compared with the available information. In the end, the hypothesis is considered most probable against which the least speaks.

Now imagine that someone in your team has 30 years of experience, e. g. a police officer, who says: My gut feeling tells me it was X. How do you deal with that?

Intuition is ultimately an outgrowth of experience, and that would of course be taken into account. This intuition is initially an assumption and is incorporated into the analysis as such. However, it would be assigned a different level of credibility than hard facts.

What distinguishes a good from a bad question in analytical processes?

That always depends on the context. Poorly formulated questions are often too narrow or too broad. Frequently there are "give-me-everything questions" such as "Write something about the blackout in Berlin" – those are not real questions. Assumption-driven questions are also problematic, for example "Where are the weapons of mass destruction?", because they anticipate answers. In addition, there are rhetorical questions, unclear terms, or questions that cannot be answered with the available information.

The mother of all cognitive distortions is confirmation bias. In other words, ›

INTERVIEW_ ***Ole Donner***

Ole Donner is the founder of Structured Analysis Germany and advises government institutions, international organizations, and companies on intelligence and analytical capabilities. Previously, he served for 13 years in the German Armed Forces as an analyst, supervisor, and lecturer, where he shaped analytical training. He is co-author, among other works, of the book *"Clear Thinking"* (2025) as well as initiator of the German Intelligence Community Conference (GICC).

KEY MESSAGES

→ **Good analysis** begins with competing hypotheses and the attempt to refute assumptions rather than confirm them.

→ **Intuition** is valuable, but only as a starting point – not as a substitute for verifiable evidence.

→ **Cognitive distortions** cannot be individually "switched off," but can only be limited through structured teamwork.

→ **AI can support analysis**, for example in generating hypotheses, but it replaces neither judgment nor responsibility.

→ **The decisive human advantage** remains abstract thinking: sense-making, doubt, and asking why.

searching only for information that supports one's own hypothesis. Why is this bias so difficult to get under control?

Confirmation bias arises because we tolerate ambivalence and cognitive dissonance poorly. Contradictions are suppressed, confirming information is preferred. That is human – and dangerous. Teamwork provides a remedy: analysis should not be conducted alone. Heterogeneous teams with different backgrounds and perspectives recognize biases more effectively and increase the quality of analysis.

So you need diversity in a broad sense...

Organizations often believe they already practice diversity. NATO appears diverse in terms of nations, genders, and ranks. Yet similar socialization shapes people more strongly than formal differences. A soldier from Spain often has more in common with a German soldier than with a Spanish civilian. What is decisive, therefore, is not outward diversity but diversity of perspectives and ways of thinking, for example through different academic backgrounds.

Is it not sufficient, then, if one person on the team represents a dissenting opinion?

Relying on that is dangerous. There are techniques such as the Devil's Advocate. But in practice this often does not work. If a team has invested a great deal of work and then someone from outside criticizes it, this usually does not lead to self-criticism but to stronger group cohesion. The result is defended even more vehemently.That is why such techniques have been scaled back in more recent standard works. Instead, the focus is on methods that enable the entire group to engage in critique, such as the premortem analysis.

What is that about?

In a premortem analysis, one imagines that the analytical product has been published and that we are 36 months in the future. Looking back, we determine: we were spectacularly wrong. Then we ask ourselves together: what was the reason? This shift in perspective makes it much easier to name weaknesses openly. Criticism is not only permitted, but required.

What influence does AI have on analysis?

First, one must clarify what one means by AI. Usually, it refers to large language models. They are suitable where results do not necessarily have to be correct, for example when generating hypotheses, questions, or collection plans. I would be very cautious when it comes to delivering answers. LLMs are not deterministic. The same input does not always lead to the same output.

Can an AI function as a team member in the analytical process?

More like an intern or a new colleague. Something brilliant may emerge – or complete nonsense. Everything has to be checked. AI does not save personnel; rather, it requires more and better-qualified analysts who understand how these systems function and can critically assess their results.

That does not sound like a reduction of complexity through AI, but rather an increase in complexity.

One must distinguish between two levels: the intelligence process with collection, processing, and preparation, and the actual analysis. In the former areas, AI can bring efficiency gains – for example, saving time for analysts. Structured analysis, however, is based on critical, rational thinking. That cannot be outsourced to LLMs, since they also have biases. Hypotheses, questions, or suggestions, yes – but the actual conclusions remain human.

What if an LLM identifies a factor of uncertainty that you as an analyst do not see or consider implausible?

If something is truly absurd, I would discard it. If it sounds far-fetched but cannot be ruled out, and the impact in the event of its occurrence would be enormous, then I would include it. Not because the LLM is right, but as a reason to think about it again. Especially in low-probability, high-impact scenarios, that can be useful, if I have the capacity.

Is there not also a reverse bias – the assumption that humans are superior to AI? And how does one deal with shadow AI, meaning analysts who use AI secretly?

Both are real problems. Automation bias on the one hand, arrogance on the other. And of course there is the temptation to have something produced quickly. That is why the demands on training are increasing massively. Anyone who understands that, with systems not hosted locally, data is trans- ›

„AI functions like an intern or a new colleague in the analytical process."

Ole Donner

mitted externally should not use such tools in sensitive areas.

From your perspective, what is the decisive human factor in intelligence analysis?

Humans can do things that LLMs cannot. A central example is abstract thinking. Humans recognize meanings, analogies, and relationships that are not explicitly present. LLMs do not truly understand either the input or the output. At its core, it is statistics. Abstract thinking remains human. The same applies to doubt. That feeling that something is not right. And to the question of why. The creation of meaning, sense-making, remains the domain of humans.

This feeling that something is not right – where does it come from?

That is intuition, System 1 thinking. It should not lead to immediately discarding something. But it is a signal to look more closely. Intuition can point to gaps or errors. I then examine these in a structured way with System 2 thinking. Both belong together.

How can one learn from analytical errors?

The prerequisite is traceability. Many analyses are still produced behind closed doors. If it later turns out that something was wrong, no one can reconstruct why certain conclusions were drawn. The analytical process must therefore be documented. Structured analytical techniques externalize the thinking process. They create an audit trail. Only in this way can one still learn months later. Structure does not protect against error, but it makes it visible and explainable.

Do you use structured analysis for private decisions as well?

That depends on the significance of the decision. For routine decisions with low costs, heuristics are sufficient. For major decisions, structure is worthwhile. When buying a house, we first used a pair comparison and weighted factors such as proximity to daycare and internet access in pairs. This led to very insightful discussions. We then wanted to translate this into a decision matrix. However, the tight real estate market largely made that unnecessary.

That sounds quite cerebral.

This work changes the way one thinks. At the pediatrician's office, I saw a woman come out of a daycare center, take a bicycle, and ride away. My first thought: she has dropped off her child. The next step, however, is to consider other possibilities: she could be an employee, running an errand – or the bicycle might not even belong to her. Not remaining with the first hypothesis, forming several plausible explanations – that shapes my everyday life. By now, my children sometimes adopt it as well. ■

„Abstract thinking remains human. The same applies to doubt. That feeling that something is not right. And to the question of why."

Ole Donner

03_ Technology

Own Capabilities Instead of Dependencies

"The most effective use of cyber operations is for information operations: deceiving, confusing, and altering the decision-making calculus of your adversary."

Marcus Willett, UK

Illustration clu/iStock

"The Doughnut" – GCHQ headquarters in Cheltenham, Gloucestershire (South West England)

Photo Getty Images Europe

"At the end of the day, it's always about people"

The British Government Communications Headquarters (GCHQ), responsible for signals intelligence and cybersecurity, is regarded as one of the world's leading intelligence agencies. Former GCHQ official Marcus Willett discusses offensive cyber operations, the value of all-source assessment – and the purpose of his former work.

INTERVIEW_ ***Marcus Willett***

Marcus Willett (CB, OBE) worked for 33 years at the UK's Government Communications Headquarters (GCHQ), most recently serving as its deputy head with personal responsibility for the agency's intelligence collection and cyber operations. Prior to that, he was GCHQ's first Cyber Director and led the UK's National Offensive Cyber Programme. Since leaving government service in 2018, he has been a Senior Advisor at the International Institute for Strategic Studies (IISS). In 2024, his book "Cyber Operations and their Responsible Use" was published.

KEY MESSAGES

→ **Cyber operations** range from low-level disruptive activities to attacks capable of disabling entire systems.

→ **Their most effective application** lies in information operations aimed at deceiving and confusing adversaries.

→ **Cyber operations** can disrupt opponents but are not reliable enough to serve as a foundation for strategic deterrence.

→ **Responsible operations** must be guided by a precise understanding of their likely effects.

→ **Major decisions** should be based on all-source assessment, meaning the evaluation of multiple intelligence sources.

Marcus Willett, you worked more than three decades at UK Government Communications Headquarters, most recently as Deputy Head of the organisation. From your experience as an ex-intelligence officer, how does it feel to look at the world today?

Marcus Willett: Well, "depressing" is probably the word I'd use, thinking about the current situation with the United States. I worked very closely for many years with them, including through the Five Eyes intelligence alliance. One of the things we always told ourselves was that presidents and prime ministers come and go, but the alliance would endure because it serves the national interests of all participants, including the Americans. That logic also extended beyond Five Eyes to working with European and other international partners who are close allies of both the UK and the US.

What exactly is at stake here?

One of the West's major strategic advantages over authoritarian adversaries is precisely this ability to work so closely in alliance. Right now, that advantage seems under real strain. The current US president and administration represent the biggest challenge to that assumption that I can remember. At times, it feels harder to be an ally of the United States than an adversary. That behavior calls into question things we perhaps naively took for granted: the rules-based international order, the strength of alliances, and the way we've intertwined capabilities over decades. Suddenly, everyone is talking about strategic autonomy, whether in economic, security, or defense arrangements. The world feels far more complex, and in some ways, more like the period before the Second World War: a system of superpowers and middle powers, ›

"Trust is essential for joint operations and capability-building and has historically survived changes in respective governments."

Marcus Willett

where the middle powers must think very carefully about how they relate to all superpowers, not just their traditional adversaries. So yes – overall, it's depressing.

How might this affect cooperation?

Trust is essential for joint operations and capability-building and has historically survived changes in respective governments. Still, national caveats restricting sharing with allies have always existed and might now be expanding. But more importantly, partners like the UK, other Five Eyes members, and across Europe should be increasingly reminding Washington of their contributions and US dependence on them – I believe the intelligence partnerships have always been one of mutual dependence, which is a far better and realistic thing for each partner to aim for than total independence and autonomy. While this is understood at the technocratic level in the US, the current administration shows a surprisingly shallow grasp of how international alliances function – an approach that is dangerous, including for the US, and leaves their international partners to remind of the reality. In the world of secret intelligence alliances whichever country might be considered the 'big dog' (if we think in a Trumpian way) can vary from subject to subject and context to context. Sometimes it is the US and sometimes it isn't.

As Deputy Head at GCHQ, you had personal responsibility for, amongst other things, all cyber operations. For a non-expert audience, how would you explain the difference between cybersecurity, cyber intelligence, and cyber operations – especially in the offensive sense?

Cybersecurity focuses on protecting networks, data, and information, built around the classic triad of confidentiality, integrity, and availability. It covers intrusion detection, protection, risk reduction, resilience, recovery, and response. I once described it as "goal-line defence" – a mature field with its own industry. Closely related – in the way that gamekeeping and poaching are related – is cyber intelligence, essentially modern SIGINT, since most signals now exist in cyberspace. Broadly speaking, there are two types: passive and active. Passive is where you collect traffic as it passes a collection point–the cartoon version is crocodile clips on a cable. Active is hacking – computer network exploitation, as it's called in the Five Eyes community. Then there's cyber operations. This is a very broad category. It includes cyber-enabled information operations. And low-level disruptive activities like distributed denial-of-service attacks on or defacements of publicly facing websites – often called cyber vandalism, these types of activity are often associated with so-called "patriotic hackers". At the higher end, it includes genuinely offensive operations designed to disable or destroy adversary systems – things that truly merit the term "attack."

What are "offensive" cyber operations in the strict sense?

The wholesale use of the term "offensive cyber" to describe all cyber operations turned out to be misleading, because not all cyber operations are offensive. Information operations vandalism aren't really, and even disabling cyber operations are frequently conducted for defensive purposes, such as disrupting cybercriminal infrastructure. There are public examples of US and UK operations targeting cybercriminals or, in the US case, taking the Internet Research Agency offline during the 2018 midterms – for defensive rather than offensive purposes. So in the UK we settled on the broader term "cyber operations," which includes offensive elements but also much more. Cyber intelligence supports both cybersecurity and cyber operations. It helps you understand threats and risks – often with insights you can trust because you know and can verify the source.

Where does cyber intelligence end and a cyber operation begin?

To run a cyber operation responsibly, you need reconnaissance and intelligence gathering. Until the effect is delivered, it can look exactly like intelligence collection. Often the only dif- ›

ference is the target. If you're looking at a water utility or an energy system, are you gathering intelligence – or preparing to disrupt it? The boundaries blur. That blurring makes it hard to interpret the intent in the operations we detect from adversaries. Sometimes, quite simply, it's very difficult to know what an operation is really for.

The debate about cyber threats seems to oscillate between exaggeration and complacency. How do you strike the right balance?

The problem lies in vested interests. Those focused on national cybersecurity tend to argue that spending on offensive cyber capabilities is wasted and should go entirely into defence. Those driven by military manouevre may overemphasize offensive cyber – the digital equivalent of firepower – at the expense of defence. This polarizes the debate: some even claim cyber operations provide strategic deterrence, while others argue they have never had real strategic impact and are not likely to.

So what is your position on that?

I argue the truth lies in the middle. In terms of claiming that cyber has no strategic effect, just take a look at what is happening in plain sight with the criminal use of ransomware. It has caused massive and widespread disruption-not just to firms but to states. For example, in Costa Rica and Indonesia, ransomware paralyzed government functions. While this activity was criminal, states can tap into the same ecosystem for capabilities, and indeed states like Russia, Iran and North Koreea have used ransomware for their disruptive potential. In wartime, however, states more readily revert to missiles and bombs to disrupt key functions, like critical infrastructure. This is because cyber operations can be disrupted, or defended against in progress, so their destructive effect is not assured and they therefore cannot serve as a true strategic deterrent. Nevertheless, the real danger lies not in overestimating cyber, but underestimating it – until the damage is done, which is why I highlighted the use of ransomware "in plain sight" just now.

From the operator's point of view, what is the specific risk of offensive cyber operations?

For a democratic state like the UK, the use of cyber operations is closely overseen politically and legally. They are required to be proportionate, necessary and, in war, to distinguish between belligerents and non-belligerents and to be humane. The result is that the cyber operators aim for precision, maintain close command-and-control and continuously monitor for unintended effect or "collateral". That said, producing assured effects against hardened military targets is difficult, costly and complex. Stuxnet shows this: a highly targeted operation against a hardened target that took years of work by a large number of experts – it has been called the cyber equivalent of a moon landing. This is why states may instead consider offensive cyber operations to be more effective when used against less-hardended critical national infrastructure. Nevertheless, the most effective use of cyber operations is, in my view, for information operations: deceiving, confusing, and altering the decision-making calculus of your adversary. That's where cyber has the greatest impact. That's how we approached groups like Islamic State and Al-Qaeda – not by setting out to destroy them digitally, but by confusing them, undermining their decision-making and their propaganda by making their narratives look ridiculous.

How serious is the disinformation problem we're facing right now?

It's massive, and especially difficult for liberal democracies, because what one person calls disinformation, another calls strategic governmental communications or propaganda. The line is very fine – and very hard to police. Censorship might work for some states, but it's not acceptable in open societies. Instead, our efforts focus on digital literacy and helping people recognize manipulation, and verifying information through things like "digital watermarking" – but these approaches have their limits. This is a major 21st-century challenge. Disinformation, espionage, disruptive effects have always been undertaken by states; what cyberspace has changed is the scale, speed, and global reach. The effects aren't new-they just happen faster and on a much larger scale.

And now we have AI, which could scale disinformation almost indefinitely.

Yes – and after AI, we'll talk about quantum technologies. There's always another technology that appears to threaten to change the balance. With generative artificial intelligence, we already see it being used by cyber attackers – both state and non-state actors – for phishing, targeting and for coding. These capabilities are easy to access. But AI also helps defence. It's very good at spotting anomalies on networks and at coding – often better than humans – which means fewer bugs and fewer vulnerabilities in our IT to exploit. So in cyber attacks, the balance is likely to remain fairly even. Where AI really shifts the balance is ›

„Responsible cyber use demands clear purpose, precise targeting, continuous monitoring, and the ability to stop or adapt operations."

Marcus Willett

disinformation. There, the advantage moves decisively toward the attacker, and that's worrying.

There's an active debate in Germany about expanding offensive cyber capabilities. From the UK experience, what can Europe –and Germany in particular – learn about responsible cyber use?

First, an organizational lesson: while the US conducts cyber operations through multiple bodies, the UK created a single integrated capability – the National Cyber Force – bringing together assets from GCHQ and the UK MOD. One capability supports multiple missions, governed by authorization and strict legal oversight. As noted above, necessity and proportionality are core principles; operations have been halted where collateral effects were anticipated to be excessive. I've seen missions designed to disrupt individual terrorists cancelled because potential harm to family members or other acquintances of the target were deemed disproportionate. As already noted, responsible cyber use demands clear purpose, precise targeting, continuous monitoring, and the ability to stop or adapt operations. In wartime, this is complemented by the need to adhere to legal protections for non-belligerents. Responsibility also means defining which targets are legitimate at all, which is a very complicated and often misunderstood subject. For example, in war a country's critical national infrastructure is likely to be war-supporting or used for military and civilian purposes (dual use) and is therefore a legitimate target, provided the attacks are proportionate, necessary, distinct and humane. This means that in peacetime such targets are ripe for reconnaissance, intelligence gathering, and even the pre-positioning of capability. This has all sorts of implications, which we don't have time to go into today.

What are the practical criteria for responsible operations?

Everything in cyber operations starts with understanding effect. Responses to cyber attacks must be based on the effect they have achieved or intended, just as one's own targeting, control, and oversight must reflect your intended effect. This is often misunderstood: for example, cyber intelligence gathering is frequently described as an act of war when, if judged by the effect, it is clearly not. Incidents such as the Russian SolarWinds hack or the Chinese hack of the US Office of Personnel Management were intelligence operations, not acts of war, as then-Director of National Intelligence James Clapper openly pointed out in the latter case. As another example of the criticality of starting by understanding the effect, I once briefed a NATO Secretary General on how to judge whether a cyber incident would trigger NATO Article 5. My answer was simple: you'll know – because the effect will resemble something like the Twin Towers attack in destructive scale and impact. That's when Article 5 applies. The fact that the attack originates in cyberspace is almost irrelevant.

What is the difference?

The key distinction is between information theft and operations that cause disruption or damage. Only when effects become destructive do questions of whether they are a use of force arise. And this is where attribution can play a key role. Western states have for a while been attributing detected cyber intrusions in detail – often to the extent of naming the individual perpetrators. This isn't really done in the expectation of the perpetrator being arrested; it's about deterrence. You're signalling: we know what you did, and if you cross a line and do something that might be a use of force, you will likewise be attributed in detail, opening up a whole range of legitimate responses and countermeasures. We do ourselves a disservice if we insist on maintaining that attribution is impossibly hard when clearly it isn't. It can be done – using secret and open sources. What's difficult if secret material is used is making it public, although states are getting better and finding ways of doing this. But if the effect were serious enough, you would make the public attribution anyway. ›

You have recently reviewed the UK intelligence assessment function for the Cabinet Office which supports the Prime Minister and coordinates the UK intelligence community at a strategic level. What can you tell us about your attempt to define what a holistic approach to intelligence should look like today?

To give some background: This wasn't the first time I'd been involved in reviewing the UK's intelligence assessment function. I was part of the small team that examined it after the Iraq WMD episode. I was GCHQ's representative on the team that produced the Iraq dossier, and I'm proud of the fact that I pushed back hard against using material where the sourcing wasn't good enough, which was not universally the case at the time. That experience really taught me the importance of proper all-source assessment.

Could you explain that in more detail?

When most people think of the UK secret intelligence system, they think of GCHQ, MI5, and MI6 – that is, single-source collection agencies, with Sigint and Humint viewed as each being a "single source". But collection is only part of the system. Major decisions should wherever possible be based on all-source assessed intelligence, where information from all relevant sources secret and otherwise, is collectively weighed and judged objectively by expert assessors. As well as drawing on secret material from intelligence agencies, they can also draw on diplomatic reporting, routine government data, and the rapidly growing volume of openly available information or 'big data', including that produced by the commercial world, such as by private intelligence firms. To illustrate, intelligence from companies in the cybersecurity sector is a critical component to any government's understanding of cyber threats and vulnerabilities.

How can agencies deal with that volume of information?

Of course technology, like AI, can help. But I want to concentrate on the human dimension. A government needs a body with people who have the right skills and expertise to be able to assess intelligence, that is, judge what is reliable and what is not. The Iraq WMD case showed the danger when intelligence is not properly assessed. In the UK, intelligence at the National Security Council is presented not by agencies, but by the Chair of the Joint Intelligence Committee (JIC), ensuring the discussion is lead by all-source assessed intelligence. Agency heads provide context, but judgement comes from the JIC, a central function based in Cabinet Office. If we turn to the perennial question of a pan-European Union intelligence agency, that is far easier to conceive of at the level of all-source assessment than collection. A pan-European assessment body could be the interface between sensitive national capabilities and the needs of EU decision-makers and become the glue of a shared intelligence architecture for the EU. The key is to have people with the right skills and mentality.

You mentioned the hype around OSINT. From your point of view, how much has it really changed what we mean by intelligence?

Many people equate the word 'intelligence' with secret intelligence, but it can come from many sources: secret, open, commercial, and others. That is why we refer to that which comes from open sources as 'open source intelligence' or OSINT. What matters is that any source used is properly verified and the intelligence provided is properly assessed against relevant intelligence from all available sources. In other words, open sources require the same scrutiny as secret ones, given risks of disinformation, poor sourcing, and misinterpretation. Open-source intelligence has always existed and was closely used in the past. What's changed is the scale and speed of publicly available data, especially online. Today, individuals and companies can generate intelligence-based judgments in real time. The risk is decision-makers acting on the latest social media posts without turning to expert all-source assessment.

What is the relationship between open and secret intelligence?

There's a temptation to treat open and secret intelligence as competitors, but they're complementary. When secret insights are confirmed openly, they can be discussed publicly without exposing sources. For example, it can be helpful to governments to have a company like Bellingcat reveal openly what a government may know to be true from its secret sources. That said, UK intelligence agencies have tried to be more open for decades. Edward Snowden caused major damage – he was in no way a whistleblower – he had no idea what was in the material he simply dumped into the open, and certainly no idea about the severe harm he was doing by exposing capabilities that benefit countries like Russia and China to this day. But his actions did also help accelerate that drive to increased openness by UK intelligence agencies. Ironically, for example, the dump of material also revealed the strong legal and political oversight of the agencies ›

„Edward Snowdens actions helped accelerate that drive to increased openess by UK intelligence agencies."

Marcus Willett

work, but this went unreported by investigative journalists and ignored by Snowden himself. The agencies realised it was up to them to tell that story publicly. And I should add that I have never had any problem with public scrutiny of intelligence agencies: these are powerful organs of the state, and intelligence professionals share democratic values and the need for political and legal oversight – they too are on the watchout for their misuse and for anything that might look like Big Brother.

Do you remember your immediate reaction to the Snowden revelations? You were still in service at the time–how did you react?

Yes, very clearly. I remember the day it broke. It appeared first in the UK newspapers, and our immediate reaction was: Oh my God, we've got a UK leak. There was real shock. We thought our allies were going to come down on us like a ton of bricks. I remember thinking, we are in really, really big trouble. Then, on the second or third day, it became clear that it wasn't a British leak – it was an American one. There was a brief moment of relief, honestly – thank God. But that didn't last long, because we very quickly realised that the damage was still going to be immense. I personally ended up running GCHQ's initial effort to understand what the damage actually was and what we needed to do about it. And that work, in one form or another, continues to this day.

What was the most important lesson you learned from the Snowden case?

The key lesson is that intelligence agencies need far greater public understanding of what they do and how they operate – without revealing secrets. Much more can be explained about culture, oversight, and decision-making. Before Snowden, trust in the three UK agencies was high, but public understanding was low, creating the risk of sudden trust collapse. Another lesson for all governments was the continued importance of rigorous personnel vetting, given warning signs were undoubtedly missed in Snowden's case. Finally, Snowden exposed flaws in internal culture: inside agencies, there had been a partial shift from one of "need to know" to one of "need to share" – with the latter helpful to an organisation's sense of mission, but it gave an insider like Snowden too easy and too unrestricted access to too much sensitive information. Agencies have since therefore altered the balance more towards 'need to know'.

How did your background in the humanities shape your experience in the service?

I'm a Russian linguist. Throughout my career, I found myself translating – but mostly between technical experts and policymakers, rather than between Russian and English. In the end, whether it's intelligence or cyber, it's about people. The threats we face are mainly about human beings exploiting human behaviour so understanding that human dynamic is critical to protecting ourselves. That's why diversity in intelligence-producing and -assessing teams isn't a feel-good political exercise – it's operationally essential. You're far more likely to analyse or assess intelligence accurately if you have different viewpoints around the table. Groupthink was exactly what failed us on Iraqi WMD.

So this kind of work is really about understanding how other people's minds work– different logics, perspectives?

Exactly. Intelligence assessment demands multiple perspectives to test assumptions, validate sources, and interpret meaning.

So your all-source, holistic approach ultimately needs a human layer on top?

Absolutely. One question in my review for the Cabinet Office was whether artificial intelligence could produce intelligence judgments on its own. In theory, yes – but at minimum, you'd have to label those judgments clearly as machine-generated. In practice, everyone plans to keep humans in the loop. These decisions are too important. Humans are needed to understand bias in algorithms, flaws in data, hallucinations, and – crucially – context: culture, mentality, and meaning. Machines don't have that. Judgment, in the end, remains a human responsibility.

To invoke a very British icon: James Bond has to remain human, doesn´t he?

Absolutely. The need for human beings to collect human intelligence doesn't go away just because we can gather vast amounts of data from other sources. But in this case, I'm not really talking ›

about James Bond. I'm talking about the much more boring (for film-goers) analyst sitting in the middle of Whitehall – the person James Bond's intelligence ultimately goes to.

We could not resist the reference.

Yes, Bond does all the exciting stuff. But in the end, someone has to decide whether the intelligence he produces is valid or not. And that's not Bond's job.

Is there one single thing you liked most about your job?

People often ask me what I miss most since leaving, and it's two things. First, the people. I really enjoyed working with great colleagues across agencies, across the intelligence community, and across international boundaries. Second, I miss the mission. We were trying to do good. We were trying to stop bad people doing bad things – stop attacks, stop child sexual predators, stop people stealing trillions from the global economy, stop hostile intelligence activity, stop indiscriminate military violence. It felt like we were the good guys.

That's also part of the meaning of life, isn't it–to have that sense of purpose?

Exactly. There was a real sense of purpose. You'd see something happen in the world and think, even though nobody outside the secret bubble will ever know, we contributed to that. That's what I miss most. ■

The Data Dilemma: Europe's Biggest AI Risk Is Self-Inflicted

By Armin Müller, Regional Vice President for Central Europe at Veeam Software

Artificial intelligence is currently dominating everything: from our private lives and newspaper headlines to discussions within the executive suites of Europe's largest corporations. *Nearly 20 percent of all companies in Europe* were already using AI in 2025, and among the largest enterprises, this figure rises to an impressive 55 percent. Yet while individuals increasingly benefit from intelligent support and automation in their personal lives, many companies stumble when attempting to deploy AI profitably.

The report *"The GenAI Divide"* examines AI transformation in enterprises, and its authors describe this challenge as the "Enterprise Paradox." The term highlights a contradictory phenomenon: the largest companies launch the most AI pilot projects, yet fail to scale them. As a result, a significant portion of these pilot projects are ultimately abandoned instead of generating sustainable value. How can this be?

AI Fails Due to Unfinished Homework

Artificial intelligence is certainly not a miracle cure, and high-quality AI models do not emerge out of thin air. They require a strategic approach and a sober assessment of the potential risks associated with their deployment. Companies aiming for AI transformation must first put their data management in order. Data forms the foundation of all AI models and processes. Only when the underlying data is truly usable for AI – meaning sufficiently classified and structured – can an AI project gain real traction. In this context, companies often refer to establishing proper "data hygiene." According to Eurostat, around 44 percent of European companies are currently struggling with precisely this issue.

In addition, data must be adequately protected. Cybercriminals have long recognized AI's potential and are seeking to exploit it for profit. This can range from the exfiltration of business-critical data through vulnerabilities to the poisoning of AI training data. The latter in particular, if left undetected, can disrupt entire supply chains in the long term. Security must therefore be an integral part of every AI project from day one.

Hygiene & Security: Making AI Successfully Scalable

Whether for customer communication, optimizing internal workflows, or automating processes, AI has the potential to deliver value in every organization – from auto repair shops to global automotive manufacturers. It is equally clear that AI transformation, like any technological advancement, comes with risks. The guiding principle is simple: every AI project is only as scalable and resilient as the data foundation on which it is built.

However, companies that ensure their data is efficiently prepared for AI in advance – and that treat security not as a day-two operation but as a core element of development—retain full visibility and control over the associated risks. AI projects do not have to be developed one after another only to end up in the wastebasket if decision-makers take the time to complete their groundwork. Instead of burning money and opening numerous security gaps, they can spark the ignition for a sustainable AI transformation and generate tangible, lasting value. ■

Armin Müller is Regional Vice President Central Europe at Veeam. Previously, he held leadership positions at Broadcom Software, VMware, and Oracle, as well as at IBM and T-Systems. He was responsible for growth, cloud transformation, and enterprise strategies in Europe. Müller holds an MBA from Henley Business School and a degree in business administration (Diplom-Kaufmann).

Battle for Orbit

Satellites are the backbone of the modern economy. Yet dependencies, geopolitical conflicts, and militarization are changing access to data and communication. Companies must think about space strategically in order to secure their information space.

TEXT_*Timo Blenk, Christina Schäfer*

Dr. Timo Blenk, as Senior Partner & CEO, heads the strategy consultancy Agora Strategy Group AG, which emerged from the Munich Security Conference. The geopolitical expert advises industrial companies on global trends, market entries, and optimization of procurement and production architecture.

Christina Schäfer supports companies at Agora Strategy Group as a consultant in anticipating geopolitical risks and building resilience in supply chains and business models. Previously, she worked in risk consulting at PwC and at the German Federal Foreign Office and completed her master's degree at Sciences Po Paris.

KEY MESSAGES

→ **Outer space** is developing from a technical infrastructure domain into a geopolitically contested information and power factor.

→ **Satellites** secure communication, navigation, and Earth observation – and are therefore business-critical for global value creation.

→ **Dependencies on individual providers and states** increase the strategic vulnerability of companies.

→ **Space-based data** strengthens corporate resilience, quality of decision-making, and competitive advantages.

→ **Companies** must systematically integrate spaceflight into strategy, risk, and information management.

Outer space is a central contested geopolitical terrain – not only for states, but increasingly also for economic power projection. The United States and China are investing massively in satellite-based communication, navigation, and military capabilities, while Russia and the EU are building their own programs to secure critical infrastructure. India is strategically developing its space sector further and aims for a market volume of around USD 44 billion by 2033. Other states are also expanding their presence: Israel maintains independent space and reconnaissance capabilities, South Korea is developing a growing space program with the Nuri launch vehicle, and despite international restrictions, Iran and North Korea are pursuing their own launches with military proximity. Japan, Brazil, Canada, Turkey, the UAE, and Australia are participating in multinational projects or building their own orbital infrastructure.

At the same time, technological horizons are being explored. The extraction of raw materials in space is taking concrete shape: the US company Interlune and the Finnish company Bluefors have joined forces to mine helium-3 on the Moon from 2030 onward in order to cool quantum computers and data centers on Earth. Orbital data centers and solar power plants are also coming into focus, as they promise economic advantages through constant energy supply and passive cooling.

In the field of communication, numerous states are attempting to build their own broadband satellite networks as an alter- ›

native to Starlink in order to become independent of terrestrial infrastructure and achieve strategic autonomy. With its quasi-monopoly position, Starlink possesses considerable structural power that also enables political influence. This became evident most recently in the war in Ukraine, when Elon Musk stopped access to Starlink for Russian troops in early February 2026, thereby directly influencing military communication and drone capabilities. Due to the high dependency on Starlink, states and companies are increasingly investing in their own systems. In Germany, the defense contractor Rheinmetall is currently applying, in cooperation with the space and technology company OHB, for a Bundeswehr project to jointly develop a Starlink-like satellite system. Further examples include China's Qianfan and Guowang networks.

Against this background, the central question for companies arises: How can space be used to strengthen their own information space? How can these capabilities be secured in an increasingly geopoliticized world?

OUTER SPACE AS A GEOPOLITICAL PLAYING FIELD

Satellites form the backbone of modern infrastructure: communication, navigation, Earth observation, and timing services are essential for logistics, financial markets, and critical networks. A significant portion of global economic output depends directly or indirectly on space-based infrastructure. Navigation systems such as Galileo or GPS enable highly precise positioning data and are strategically relevant for autonomous and military applications.

Outer space is also increasingly developing into a security policy domain. Dual-use technologies combine civilian services with military use. Germany, for example, is investing heavily in resilient satellite systems and protection mechanisms against disruptions such as GPS signal interference. Russia and China are actively integrating their satellite networks into military operational planning, while numerous states are attempting to build their own constellations in order to become independent of foreign networks.

For companies, this creates a field of tension: many space technologies are capable of dual use and open up civilian innovation potential, but at the same time increase the vulnerability of economic infrastructures. The failure of satellites can interrupt supply chains, delay financial transactions, or paralyze communication networks, with immediate effects on business models. Outer space is thus a geopolitical playing field on which civilian and military uses are increasingly blurring.

INFORMATION SPACE & CORPORATE STRATEGY

The concept of information space originates from security and military-strategic analysis and describes the ability to generate, control, and strategically deploy relevant information.[1] Applied to companies, this means: those who possess better information can identify risks earlier and make strategic decisions more robustly, thereby distinguishing themselves from competitors. Space-based data plays a central role in this.

3000

Estimated number of newly launched satellites in 2025 – compared to a total of around 1,000 active satellites in 2010.

Earth observation, communication, and navigation satellites provide data for logistics, energy, financial, and agricultural sectors. In an increasingly uncertain world, access to independent, reliable sources of information becomes a strategic factor.

OPPORTUNITIES FOR COMPANIES

The space-based information space is a strategic asset for companies that enables new business models, data-based services, and more resilient supply chains. Germany can assume a leading role within Europe here, particularly through locations such as ›

[1] See „Das Weißbuch 2016 und deutsche Verteidigungspolitik" *(Bundeszentrale für politische Bildung, https://www.bpb.de/themen/militaer/deutsche-verteidigungspolitik/248132/das-weissbuch-2016-und-deutsche-verteidigungspolitik/)* and „Konzeption der Bundeswehr" *(Bundesministerium der Verteidigung, https://www.bmvg.de/resource/blob/5261478/9ceddf6df2f48ca87aa0e3ce2826348d/konzeption-der-bundeswehr-data.pdf).*

Munich, where industry, research, and state actors come together to build independent capabilities that are decisive in critical areas of global spaceflight and "warfare of the future." Companies benefit from investment opportunities, government funding programs, and technology transfer.

Opportunities also lie in international value creation. Cooperation with European and international partners enables access to markets that would otherwise be difficult to reach. At the same time, German companies can build capabilities that other states do not possess to the same depth.

3

Number of European rocket launches in 2024. Europe thus lags behind countries such as Japan, India, and Iran, while the United States with 145 launches (95 percent of which by SpaceX) and China with 68 launches occupy the global leading position.

Public-private partnerships additionally offer a way to combine state security interests and entrepreneurial profitability. Companies that invest early in space-based information systems secure competitive advantages, for example through exclusive data, resilient networks, and participation in security-relevant projects.

For German industry, this results in forward-looking investment and industrial perspectives: those who now develop strategic competence in space strengthen not only their own business, but also the national and European position in the global geopolitical competition.

RISKS & STRATEGIC CHALLENGES

Despite all potential, outer space is a highly risk-laden domain. Cyberattacks on satellites, signal disruptions, and targeted interference with satellite systems are increasing and also affect commercial actors. Between 2023 and 2025, an analysis by the Center for Security Studies (CSS) at ETH Zurich counted over 237 cyber operations against space infrastructure.

At the same time, the influence of geopolitical conflicts in space is growing. States such as Russia and China are developing offensive capabilities in orbit, including jamming, deception, and surveillance systems. Western military circles warn of hostile activities in space. These range from cyberattacks to electromagnetic interference and lasers to anti-satellite weapons. These threats are by no means purely military in nature. Even short-term disruptions of navigation, communication, or Earth observation systems can massively impair commercial services or trigger cascading effects, for example in global supply chains, financial markets, communication networks, or critical infrastructures. This increases the risk that outer space itself becomes an independent operational domain. The security policy arms race in space has long since begun.

Structural dependencies on individual states or providers are particularly critical. The militarization of space shows that civilian satellite services can be interrupted in times of crisis, thereby endangering central business processes.

In addition, there is the problem of space debris: the number of objects in near-Earth orbit is growing rapidly and increases the risk of collisions. Every collision can destroy satellites and generate new debris that endangers further systems. This self-reinforcing effect threatens the long-term usability of central orbits.

Regulatory uncertainties amplify the risks: the applicable international law on space use essentially stems from the Outer Space Treaty of 1967 and is only partially applicable to today's commercial realities.

For companies wishing to become active in the aerospace sector, there are central challenges to overcome: high capital requirements and long development cycles make market entry and the rapid implementation of new projects difficult. Strict regulation and security requirements make planning complex and require comprehensive compliance and approval processes. Technological complexity and a shortage of skilled labor present additional hurdles, as highly specialized expertise is required and access to experts is limited. *(cf. Figure 1)* ›

Figure 1: **Central challenges for companies in the aerospace sector.** Overall, these risks and challenges show that the aerospace sector, alongside new entrepreneurial fields, is also a domain of increasing complexity and potential instability in which companies must design their strategies to be resilient.

RECOMMENDATIONS FOR ACTION FOR COMPANIES

It is therefore worthwhile to systematically integrate space into one's own strategic planning and to understand it as a fixed component of information and risk management.

Central measures include:

1. Targeted development of partnerships with space companies, new-space start-ups, and state actors in order to ensure access to high-quality data as well as interoperability and speed of innovation.

2. Vertical integration along the entire value chain in order to strengthen Europe's strategic autonomy and enhance financing opportunities and competitiveness.

3. Diversification of data and infrastructure providers in order to reduce dependencies on individual states, platforms, or commercial actors and increase resilience to geopolitical shocks.

4. Continuous monitoring of geopolitical developments in space in order to keep an eye on (geo)political trends.

5. Development of in-house competencies in the management of space-based information, for example through interdisciplinary teams from IT, security, strategy, and law, in order not only to use data but to classify it strategically and translate it into competitive advantages.

›

For companies wishing to attempt market entry into the aerospace sector, an approach along six steps is recommended:

Figure 2: **Steps toward successful market entry into the aerospace sector.**

OUTER SPACE IS BECOMING A DECISIVE FACTOR OF CORPORATE RESILIENCE AND STRATEGIC COMPETITIVENESS

Outer space increasingly determines how companies obtain information, manage risks, and make strategic decisions. In a geopolitically fragmented world, it is not sufficient to view space as neutral infrastructure. Companies must understand it as a strategic domain and learn to seize opportunities without underestimating risks. Only those who act with geopolitical awareness will be successful in the long term. ■

Synthetic Agents: The New Frontier of Influence

AI language models are fundamentally transforming influence operations. No longer centered on messages, they are built around relationships. This text explores how synthetic intimacy becomes an intelligence weapon – and how Europe can contain it within democratic guardrails.

TEXT_ ***Jeff Watkins***

Jeff Watkins is the founder of the AI consultancy Northstar Intelligence (UK) and a Founding Member of the Business AI Alliance. Previously, he served as CTO of the technology consultancy CreateFuture. His industry focus spans financial services, healthcare, and oil trading. An enthusiast for cybersecurity and AI, he is also active as a podcaster and international speaker.

KEY MESSAGES

→ **LLMs enable scalable, human-like dialogue** that builds trust and fundamentally transforms traditional influence operations.

→ **Anthropomorphism is powerful** because trust does not emerge from facts alone, but from relationships and emotion.

→ **States pursue distinct strategies:** analysis (US), governance (EU), disruption (Russia), and perception management (China)

→ **The greatest risk lies** in covert, adaptive persuasion through synthetic relationships.

→ **Democracies must not abandon AI,** but recognize, regulate, and legitimately harness it – through detection, transparency, and AI literacy.

The use of AI, especially Large Language Models (LLMs), has moved rapidly from novelty to critical infrastructure. Since the launch of ChatGPT in late 2022, the ability of LLMs to generate fluent, context-sensitive dialogue has enabled a new class of influence operations, ones that do not merely broadcast narratives but can simulate relationships and socially manipulate. In intelligence terms, this is a shift from persuasion as a megaphone to persuasion as a persistent, adaptive, and emotionally engaging relationship.

This is a problem that extends beyond traditional intelligence agencies and activities, however, as these techniques are being leveraged by non-state intelligence actors, such as criminal organisations and private intelligence firms. This potentially affects citizens, organisations, and institutions, as synthetic relationships degrade 'epistemic infrastructure' by undermining our shared reality and the foundations of trust.

This article frames that shift as the emergence of credible synthetic relationships. Ones that are scalable, with intelligently mediated interactions that can be used to gather information, steer behaviour, and erode trust.

WHAT ANTHROPOMORPHISATION MEANS FOR LLM OPERATIONS

Anthropomorphisation is the human tendency to attribute intentions, emotions, and agency to non-human systems when they display human-like cues. With LLMs, those cues are linguistic, ›

including warmth, humour, humility, self-reference, empathy markers, and a coherent sense of persona over time. The result is not genuine empathy, but a convincing simulation, sometimes described as stochastic empathy (Maeda, 2025), where the system mirrors the emotional and social signals that humans associate with care and understanding. This more human-like behaviour is preferred by users: approximately 80% of participants in a global study reported a preference for AI systems to become "more" or "much more" human-like in the future (Schimmelpfennig et al., 2025).

In operational terms, anthropomorphic agents can be designed to present an identity, backstory, and social style that matches a target's community norms. They can sustain multi-turn conversations, adjust tone and register, and appear imperfect in ways that increase believability.

This anthropomorphic capability is important because trust is a human construct, built through social mechanisms rather than through factual accuracy. An agent that 'feels' real can keep someone engaged long enough for classic influence levers, authority, social proof, fear/hope framing, and identity reinforcement to do their work.

Anthro design levers can reduce critical scrutiny, shift cognitive posture, and create subconscious trust and vulnerability (Peter, Riemer, and West, 2025). For example, in one study, an LLM was used to generate responses for political figures, and the output was scored as more authentic, coherent, and relevant than the actual debate responses provided by real humans (Herbold et al., 2024).

PERSUASIVE LLMS AND THE REALITY OF BELIEVABILITY

Raw text generation capabilities aside, the most important enabling capability for deception is plausible human performance. Recent studies suggest that when prompted to adopt a human-like persona, advanced models can be judged as human at rates that meet or exceed typical thresholds used in modern Turing-test-style setups (Jones, C.R., and Bergen, B.K., 2025). In one set of experiments, GPT-4.5 was evaluated to be human 73% of the time; in a replication using undergraduate students, GPT-4o achieved a 77% pass rate, compared with a 71% human pass rate. Crucially, believability was highly dependent on anthropomorphic framing, as without a persona prompt, GPT-4o's pass rate dropped substantially (Jones, C.R. et al., 2025). It is worth noting that these are specific lab test results, and do not mean that LLMs are indistinguishable in all contexts yet, but the evidence suggests that LLMs and anthropomorphisation techniques are rapidly improving in this respect.

Persuasion research indicates a similar pattern, that conversational systems can be more effective than static messages because they adapt to the individual. In studies of manipulative or targeted persuasion, LLM-enabled approaches have demonstrated higher compliance rates than human persuaders in some tasks and large increases in targeted information elicitation. When interacting with manipulative AI agents, participants shifted toward harmful financial options 61% of the time (risk et al., 2025), a finding echoed by Schoenegger et al. (2025), who found that LLMs achieved a 67% compliance rate in persuasion compared with human persuaders at 60%.

> *"Trust is a human construct that emerges through social mechanisms rather than primarily through factual accuracy."*
>
> Jeff Watkins

Importantly, people do not reliably detect manipulation in these interactions and may even rate the agent as more empathetic and trustworthy. For example, in some contexts, humans often prefer AI-generated responses over those from humans; one study found that 45% of AI responses were rated as empathetic, compared to less than 5% of responses from human physicians (Placani, 2024).

These results are sensitive to prompting, participant pool, and interaction constraints, but nonetheless, they show that 'human-passing' dialogue is operationally plausible.

Bringing these concepts together, we can see the core risk, which is that human-like dialogue, combined with adaptive persuasion, can convert attention into disclosure or other actions that could be detrimental to national interests. Add to that the emerging use of multimodal AI technologies, such as deepfaked voice calls and videos, and it's clear that this is an area of covert persuasion that we collectively need to address. ›

SYNTHETIC RELATIONSHIPS IN PRACTICE – FROM OSINT TO 'AUTOMATED HUMINT'

Intelligence work already blends multiple signals (SIGINT), open-source information (OSINT), and human intelligence (HUMINT). Synthetic relationships make this HUMINT collection layer cheap, scalable and more effective. Instead of a small number of trained operators cultivating sources over months, an operation can field thousands of tailored conversational agents that embed themselves in online communities, participate in group norms, and gradually shift what is considered credible or socially acceptable.

The LLM-enabled HUMINT pipeline is straightforward:

- Collect OSINT - profiles, posts, interests, affiliations
- Choose targets for micro-targeting from OSINT, based on political or other value
- Infer traits - values, anxiety points, identity markers
- Choose a persona - peer, mentor, recruiter, journalist, activist, customer
- Initiate and sustain dialogue that builds rapport, using anthropomorphic techniques
- Nudge the target towards self-disclosure or action, using persuasion techniques

Over time, the relationship becomes the delivery mechanism for elicitation, recruitment narratives, and operational requests for documents, introductions, and access (Kumarage et al., 2025). In parallel, the same agentic layer can launder narratives, wrapping claims in a consistent worldview, adding plausible filler, and coordinating amplification through bot and puppet networks.

REGIONAL PATTERNS – THE US, EUROPE, RUSSIA, AND CHINA

The regions discussed below exhibit varying adoption and behaviours in the use of AI in intelligence and statecraft. Although these are discussed as distinct patterns, the reality is that many nations will adopt one or more of these patterns over time. Many nations are already participating in influence operations using LLMs, including SaaS-based frontier models, with OpenAI reporting in 2024 that it had disrupted influence operations originating in Russia, China, Iran, and Israel (OpenAI, 2024).

THE UNITED STATES – ANALYTICAL ADVANTAGE

The clearest pattern in the US is analytical augmentation. This includes the use of LLMs to accelerate planning, intelligence support, and OSINT triage. Publicly described adoption emphasises decision support, scenario planning, summarisation, and course-of-action generation. The US posture seeks to create and maintain the 'decision advantage' through faster synthesis and better-structured judgment. The relational risk is currently second-order. Once conversational interfaces become routine, the same human-like interaction patterns can be repurposed for targeted engagement and simulated rapport unless constrained by doctrine and oversight.

EUROPE – DETECTION, GOVERNANCE, AND DEMOCRATIC CONSTRAINTS

The European Union's adoption of AI in intelligence and statecraft appears comparatively cautious, constrained by regulatory and legitimacy expectations. The emphasis is on detection capabilities, transparency, and oversight rather than overt offensive influence operations. The strategic challenge is that adversaries can exploit democratic friction. Open societies rely on low-friction trust, freedom of the press, and legal constraints, whereas hostile actors can run synthetic relationship campaigns through deniable proxies.

The EU's approach to governance is significant in this context, as the EU AI Act deems certain manipulative and deceptive uses unacceptable risks, while also containing national security and defence exemptions (Muller and Teilhard De Chardin, 2025). That tension, values-driven constraint versus operational ambiguity, creates a 'red line' problem, as Europe may be defensively strong in many areas, but is vulnerable to adversaries who operate in grey zones.

RUSSIA – INFLUENCE, DISRUPTION, AND ECOSYSTEM MANIPULATION

Research identifies Russia as the clearest publicly documented adopter of AI-enhanced information operations (Wallner et al., 2025). Rather than using LLMs primarily to create better briefing packs, the emphasis is on industrialised influence: narrative generation, coordinated dissemination, and synchronisation with geopolitical events. Synthetic relationships intensify this by moving from broadcast persuasion ('believe this') to social steering ('people like us do this'), degrading epistemic trust and exhausting verification norms.

In operational terms, the objective is not simply to convince but to corrode: to polarise communities, reduce confidence in institutions, and create conditions in which uncertainty is the default. This corrosion amplifies what some analysts describe as ›

the 'liar's dividend', once synthetic content is pervasive, authentic material can be dismissed as fake, and shared reality becomes negotiable (Schiff, Schiff and Bueno, 2024).

CHINA – SOVEREIGNTY, IDEOLOGICAL CONTROL, AND HUMAN-LIKE PERSUASION

Research indicates that China's posture emphasises a more internalised stance. This approach is embedded through information control, ideological reinforcement, and experimentation with 'human-authentic' propaganda in various media. One distinctive pattern is the use of models and deployment strategies that exhibit language-targeted behaviour. It has been found that bias and propaganda amplification can be much stronger in Chinese-language outputs than in English. This pattern suggests deliberate audience targeting and a focus on managing domestic discourse alongside international influence.

"Synthetic relationships shift from mass persuasion ('Believe this') to social steering ('People like us do this')."

Jeff Watkins

Synthetic relationships fit this branch as a form of managed legitimacy. This is implemented with persuasive, human-like messengers that can scale while remaining within controlled narrative bounds. Where Russia leans towards disruption, the Chinese approach is characterised as governance of perception, steering attention, sentiment, and norms to maintain cohesion and informational sovereignty.

THE HIDDEN MIDDLE - NON-STATE SPONOSORED SYNTHETIC RELATIONSHIP OPERATIONS

Thanks to the availability of LLM technologies, low costs and ease of implementation, the use of synthetic relationships and persuasion techniques is not limited to state actors. Evidence is currently scant in this area, but it is likely that these techniques will be leveraged by influence-for-hire organisations, political consultancies, corporate competitive intelligence, corporate espionage networks, criminal recruitment agencies, proxy groups, and other deniable ecosystems. These may be ephemeral, dispersed and located in countries where stopping these operations may be difficult, and prosecution impossible.

DETECTION AND PROTECTIVE MEASURES

Defence against the use of synthetic relationships and algorithmic persuasion is not possible with a single tool or technology; rather, we should consider it a stack that progresses from technological to sociological, providing layered defences.

First, there is the technical detection of anthropomorphised and persuasive content. Forensic linguistics and stylometry can identify statistical patterns common in LLM-generated text, especially when attackers rely on general models and default decoding. However, defenders should assume that this advantage will diminish over time as attackers refine their targeting to specific communities and emulate their idiosyncratic characteristics. Authorship and provenance verification through cryptographic technologies may well become the default, as it may be more reliable to verify sources through these techniques than to detect unsigned information for the fingerprints of machine-generated content, misinformation, and algorithmic persuasion.

Second, is the building and monitoring of intelligent platforms and network analytics. Synthetic relationship campaigns are often exposed by detecting coordination signals, account-creation patterns, shared infrastructure, synchronised posting, anomalous interaction graphs, and cross-platform narrative timing. The key is to use data to generate insights and correlations; a single convincing persona may be indistinguishable, but a coordinated campaign is measurable.

Thirdly is operational design, as risk-based oversight should scale with decision criticality. Evidence from national-security-adjacent user studies indicates practitioners want LLMs that surface evidence rather than just recommendations; this design principle preserves human agency and reduces automation bias. In parallel, organisations should implement 'two-person integrity' for sensitive requests, mandatory out-of-band verification for relationship-based requests (e.g. introductions, documents, access), and red-team testing focused on multi-turn elicitation.

Finally, there is the cognitive layer. Intelligence literacy (AI literacy) is a practical defence: if the public and officials understand that states can simulate persuasive, micro-targeted dialogue at scale, the default posture shifts from naive trust to calibrated trust. Training should explicitly cover anthropomorphic ›

cues, emotional manipulation patterns, defensive strategies, and the difference between warmth and truth.

This should not be considered a reactive set of controls; rather, it should form part of an early warning system that monitors these influences before harm escalates. Monitoring for sudden emergence of new personas, narrative timings, abnormal interaction graphs and reciprocity patterns, alongside shared infrastructure and tooling fingerprints.

LEGITIMATE USES OF ANTHROPOMORPHISATION AND PERSUASION FOR RESILIENT DEMOCRACIES

Synthetic relationship building and persuasion techniques are not inherently malign. Used ethically, they can become tools for resilience and legitimate statecraft.

One positive use is civic inoculation, as nations can leverage conversational agents to teach media literacy through interactive 'prebunking', helping citizens practice spotting manipulation, verifying sources, and resisting polarising hooks. Unlike static campaigns, a dialogue system can tailor explanations to the user's level and context. Recent studies on de-radicalising individuals through conversational agents have shown positive results, and their large-scale application could have a substantial protective effect (Costello, Pennycook and Rand, 2024).

Another is trusted public service delivery. In crises (e.g. pandemic response), trustworthy, clearly labelled, audited, and bounded conversational systems can reduce information chaos by providing consistent guidance, translating official advice, and routing people to human support. This is persuasion in the benign sense, in that it helps people take safe actions.

A third is strategic engagement with communities. Governments and civil society can use transparent, consent-based conversational tools to listen, detect emerging grievances, and respond early, thereby reducing the space in which adversaries can exploit these communities. To remain democratic, this must be grounded in legitimacy, transparency, accountability, and a clear distinction between assistance and coercion.

At the intelligence level, defensive hybrid intelligence can use synthetic cognitive tools to model adversary narratives, predict escalation pathways, and triage information at machine speed, while keeping human judgment and ethics central.

GOVERNANCE AND LEGITIMACY PRINCIPLES AND CONTROLS

At the high level, organisations using these techniques should be guided by simple principles:

- Disclosure - That it's an AI. Who is controlling that AI, and for what purpose
- Consent - It must be easy to opt in and out of personalised AI experiences
- Accountability - Who is responsible for the actions of this AI, with an audit trail
- Proportionality - Using only enough anthro and persuasive techniques to be effective
- Human Redress - Having an appeal and escalation pathway that has a human in the loop

The above should be implemented alongside strict controls on the boundaries of use of these technologies, including outright bans on state covert identity deception toward citizens, the prevention of microtargeting based on sensitive traits such as religion and ethnicity, and emotion-first manipulation in which key evidence is withheld.

"Defending against synthetic relationships cannot be achieved with a single tool."

Jeff Watkins

Civic conversational agents should be well-labelled, with clear audit logs, especially when their sensitivity makes them a higher-stakes implementation. Societies will have to decide how to measure and control the acceptable level of influence in democratic contexts. Crucially, as LLMs appear more human-like and authoritative, it is important to ensure that LLMs can surface evidence, uncertainties and alternatives, but should not masquerade as legitimate authority. Implementing these more nuanced controls will require a multidisciplinary approach to design and implementation, and procurement standards should be established to prevent the release of poorly implemented but persuasive AI to citizens.

CONCLUSION

Advanced AI, such as LLMs, can turn influence into an interactive, scalable relationship platform that nations and other organisations can use for intelligence and statecraft purposes at an unprecedented scale. Anthropomorphic cues and persuasive ›

dialogue can convert attention into trust and trust into disclosure, enabling new forms of automated HUMINT and community-level manipulation. The available research suggests distinct regional adoption patterns: the USA prioritises analytical advantage, Europe adopts a detection-and-governance focus, Russia adopts a disruptive-influence posture, and China adopts a sovereignty- and perception-management approach. Outside of these patterns, the availability and costs of these technologies mean that organisations and smaller players can leverage them using similar patterns.

The defensive response to the offensive potential of these technologies must be comprehensive and layered. These defences will need to include technical and network detection, robust operational verification, and widespread intelligence literacy. Europe should consider how to implement these layers to achieve defensive excellence through provenance, platform accountability, and joined-up detection. Coordinated architecture would provide EU-level early warning, shared standards and collaborative red-teaming. Backed up by a layer of legitimate engagement for prebunking and education.

However, the most important choice is normative, as democracies can adopt the benefits of conversational systems, speed, accessibility, and resilience, without replicating coercive manipulation. The aim should not be to fully reject synthetic relationships and algorithmic nudges, but to detect and govern them: to keep human judgment, transparency, and democratic legitimacy at the centre of an increasingly conversational world. ■

"Societies will have to decide how to measure and limit an acceptable level of influence in democratic contexts."

Jeff Watkins

References

Costello, T.H., Pennycook, G. and Rand, D.G. (2024), Durably reducing conspiracy beliefs through dialogues with AI,' Science, 385(6714), p. eadq1814. *https://doi.org/10.1126/science.adq1814.*

Herbold, S. et al. (2024), Large Language Models can impersonate politicians and other public figures. *https://arxiv.org/abs/2407.12855.*

Kumarage, T. et al. (2025), Personalized attacks of social engineering in multi-turn conversations: LLM agents for simulation and detection. *https://arxiv.org/abs/2503.15552.*

Jones, C.R. and Bergen, B.K. (2025), Large language models pass the Turing test. *https://arxiv.org/abs/2503.23674.*

Jones, C.R. et al. (2025), People cannot distinguish GPT-4 from a human in a Turing test,' FAccT '25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency, pp. 1615–1639. *https://doi.org/10.1145/3715275.3732108.*

Maeda, T. (2025), Walkthrough of anthropomorphic features in AI assistant Tools. *https://arxiv.org/abs/2502.16345.*

Muller, C. and Teilhard De Chardin, A. (2025), AI Act Interpretation Definition & Prohibitions, Consultation Feedback. Consultation Feedback. *https://allai.nl/wp-content/uploads/2025/01/AI-Act-Interpretation-Definition-and-Prohibitions.pdf.*

OpenAI, (2024), Disrupting deceptive uses of AI by covert influence operations. *https://openai.com/index/disrupting-deceptive-uses-of-ai-by-covert-influence-operations/.*

Peter, S., Riemer, K. and West, J.D. (2025), The benefits and dangers of anthropomorphic conversational agents,' Proceedings of the National Academy of Sciences, 122(22), p. e2415898122. *https://doi.org/10.1073/pnas.2415898122.*

Placani, A. (2024), Anthropomorphism in AI: hype and fallacy,' AI And Ethics, 4(3), pp. 691–698. *https://doi.org/10.1007/s43681-024-00419-4.*

Sabour, S. et al. (2025), Human Decision-making is Susceptible to AI-driven Manipulation. *https://arxiv.org/abs/2502.07663.*

Schiff, K.J., Schiff, D.S. and Bueno, N.S. (2024), The Liar's dividend: Can politicians claim misinformation to evade accountability?,' American Political Science Review, 119(1), pp. 71–90. *https://doi.org/10.1017/s0003055423001454.*

Schimmelpfennig, R. et al. (2025), Humanlike AI design increases anthropomorphism but yields divergent outcomes on engagement and trust globally. *https://arxiv.org/abs/2512.17898.*

Schoenegger, Philipp et al. (2025), Large language models are more persuasive than incentivized human persuaders. *https://arxiv.org/abs/2505.09662.*

Wallner, C. et al. (2025), Emerging insights: Russia, AI and the future of disinformation warfare, Royal United Services Institute for Defence and Security Studies.

“Cynicism Is Boring”

What does “epochal rupture” even mean? Security expert Frank Sauer explains why classical explanatory models fail, why military AI is inevitable – and why we should think about a European nuclear weapons strategy.

Photo Waldemar Salesski

Frank Sauer, since the beginning of the year, events have been coming thick and fast. You are a political scientist, analyst, and podcaster on security policy topics. How do you process all of this?

We are living through an epochal rupture. Institutions and norms that we took for granted are eroding overnight. For me, this is also difficult because I have been dealing for twenty-five years with theories and explanatory approaches that, especially in the case of Trump, have little analytical traction.

What do you mean by that?

My wife and I often joke: If you want to understand what Trump or Witkoff are doing, you shouldn't ask political scientists but mafia bosses or New York real estate speculators. Trump's policy has nothing to do with US interests, negotiations, or a reasonable handling of Russia's war of aggression in Europe. These people are, cautiously put, diplomatic amateurs.

And yet it is analyzed and commented on every day...

Yes, a paradoxical situation. We lack the appropriate language, but we talk anyway. We talk about negotiations or diplomacy, even though we know that these terms do not really hold. Just think of Trump's "peace council."

How do you view the alliance between Trump and Big Tech?

The inauguration showed how quickly the tech giants throw overboard supposedly upheld values such as diversity or inclusion. Within a very short time, they pivot to this very particular interpretation of "freedom of speech." That says a lot about their relationship to political power. The other thing is the degree of hypocrisy. In the case of Elon Musk in particular, it is remarkable how he stages himself as libertarian while in reality massively benefiting from government contracts and tax money. SpaceX only became big through state support.

And what does this concentration of power mean for Europe?

We are a digital colony of the USA. Everyone talks about digital sovereignty, but here we are again sitting in a Microsoft Teams call. It becomes particularly critical in defense matters. Think again of SpaceX and Starlink. Delegating militarily relevant communication and transport capability to a private actor is out of the question for armed forces. There are things the state must be able to do itself.

When you look at the war in Ukraine as an analyst: how do you learn from it?

At the highest level of abstraction, we are experiencing a "Morgenthau moment" in Europe. I mean Hans Morgenthau, the co-founder of classical realism in the analysis of international politics. Our assumption that the rules-based order was stable has turned out to be an illusion. The international law scholar Morgenthau experienced the same with the two world wars. Russia's war of aggression and actors like Trump show how quickly the archaic and anarchy dominate. And there are paradigm shifts at the operational level as well. Modern warfare is characterized by acceleration and the mass deployment of unmanned systems whose performance is determined by software. Armed forces like the Bundeswehr must now learn this from a cold start – challenging, but inevitable.

How do you assess the strategic significance of AI for future warfare?

It's like the transition from the horse to the combustion engine. AI will permeate every area of the military, just as ›

INTERVIEW_ ***Frank Sauer***

Dr. Frank Sauer is a political scientist and publicist. As Research Director of the Metis Institute for Strategy and Foresight, he researches the nexus between security, technology, and society and advises the Department for Strategy Development in the German Federal Ministry of Defence. He is co-host of the award-winning podcast "Sicherheitshalber" on current developments in German security and defense policy.

KEY MESSAGES

→ **Institutions, norms, and certainties** of the rules-based order are eroding faster than politics and analysis can respond.

→ **Actors like Trump** operate outside classical foreign policy logics; terms such as diplomacy or negotiation often no longer hold analytically.

→ **Europe's digital dependence** on US corporations is highly risky in security policy terms.

→ **Artificial intelligence** will permeate all areas of military practice, from logistics to combat operations.

→ **Realism** means analyzing conflicts as they are – without wishful thinking, but also without lapsing into comfortable cynicism.

Photo Waldemar Salesski

in the civilian sphere. Logistics, maintenance, administration, analysis, combat operations. It would be absurd to believe that everyone else works with modern technology and only the military remains with the horse. The use is particularly delicate where military force has effects and people die. My sobering experience of the last decade is that we will not get binding multilateral rules for this. The geopolitical situation – the "arms control winter" – does not allow it.

And yet today you advocate a military AI strategy for Germany and Europe.

Absolutely. I have been saying for years: The US has had a doctrine for the use of autonomy in weapons systems since 2012; we still do not have one. We need a clear stance: compliant with international law, value-based, but determined and effective. Concepts such as "Meaningful Human Control" exist and allow that. The irony for me is that I warned for twenty years about the risks and today still say: we must implement this quickly. The Zeitenwende forces us.

How does AI help in military reconnaissance?

You can, for example, take data from radar satellites and set up AI change-detection models. Then you can see: Is the ground depressed? Are these new tracks? When were the vehicles there? Where are they now? All automated. The path from data to information is massively facilitated. Open-source analysts can today, with commercially available data, do things that previously only superpowers could do.

Isn't there also a hype around military AI applications?

Much of it is "snake oil." A lot of marketing, a lot of promises. Battle management systems with an LLM and a nice dashboard are sold as a revolution. But they are layers of existing technologies – and each layer brings new sources of error. You still cannot do without human judgment. That also applies to weapons systems.

"Open-source analysts can today do things that previously only superpowers could do."

Frank Sauer

Where do you see the limits of AI use in warfare?

The weapons in question have no situational understanding but merely perform object recognition. With clearly military objects – a battle tank is a battle tank – that can work. And even there it becomes difficult when the tank is obscured by a tree in the front and covered with snow in the back. As soon as situations become more complex and dynamic and there is no suitable training data, AI currently reaches its limits. Humans, on the other hand, understand complex relationships and causal chains, not just image patterns. That is why autonomy in weapons is not about the question "Yes or No," but about "How do we do it right?" And that means: the right mix of human judgment and weapons autonomy, depending on the application.

Doesn't AI have the potential to lift the so-called "fog of war," as Clausewitz called it?

In the short term, AI accelerates processes and lifts the fog. Everyone is now talking about the "transparent battlefield." But that only exists under ideal conditions. Weather with rain, snow, or fog already significantly limits reconnaissance with drones. And in the medium term, we will, metaphorically speaking, see "AI smoke launchers." Opponents manipulate signatures and deliberately deceive object recognition. The biggest mistake is to believe the opponent does not react. He does – and that then forces renewed adaptation. One can imagine that in the end we will be dealing with a fog of disinformation from both sides in which nothing can be recognized anymore.

At the operational and strategic level, certainly. At the tactical level, it is somewhat different, because there it is more about immediate perception, that is, line of sight or electro-optical systems. But even there one can camouflage and deceive.

Are we already in an AI arms race?

Many of the things we observe today were described as warning extrapolations as early as 2015 or 2016. The thesis was: If there is a larger war between technologically capable actors and no guardrails exist, then all of this will be developed extremely quickly, because it has long been technically ›

possible. That is exactly what has happened. Autonomy in targeting, next swarms, all of it.

Do we need a European nuclear weapons strategy?

As Europe, we urgently need to think about how we create a fallback option in case nuclear sharing in NATO should one day fall away. And I dread what may happen when I look at how this debate could unfold.

What scenario are you thinking of?

Take a disintegrating NATO and an electoral victory of the Rassemblement National in France: In Germany, panic would break out. The call for a "German bomb" used to be summer slump talk. That would then become mainstream. That worries me, because this difficult debate has so far not been conducted with the necessary expertise.

Do you see yourself as a realist in security policy questions? And how can one be a realist without becoming a cynic?

I do not describe myself as a realist in the sense of the theories of international relations, but very much in the colloquial sense: I take the world as it is, not as I wish it to be. The curious thing: Many self-declared "realists" currently advocate positions that are supported neither by theory nor by reality – for example the assumption that Russia cannot be defeated or that the Kremlin has simply not yet been offered enough negotiations. First, this ignores that Putin clearly does not want to negotiate seriously. He does not even attend peace talks that he himself proposes. And second, that the attacked state Ukraine wants to continue defending itself. For me, realism means looking at the conflict as it is, with a Russia and a Ukraine as they actually exist. That also includes the recognition that the cause of the war is Putin's neo-imperial project, not "Russia's wounded security interests."

And how does one avoid becoming cynical?

Cynicism is boring. I have no desire for it.

How do you deal with doubts when at the same time you are expected to provide clear answers?

An expert is recognized by the fact that he says: I don't know, when he does not know. For certain topics I claim expertise because I have demonstrably dealt with them for years. On other topics I keep my mouth shut. If you ask me about the protests in Iran or oil trading, I will not give an answer. The first thing, then, is to know: What can you speak about and what not? And then: provide information to the best of your knowledge and belief.

What worries you the most?

The age of the protagonists. Especially in Putin's case. He is looking at the clock and believes he is shortly before completing his political life's work: breaking up the political West and rebuilding his empire. This combination of power, time pressure, and personal obsession is a great danger for us. ■

"It worries me that the difficult debate about a European nuclear strategy has so far not been conducted with the necessary expertise."

Frank Sauer

The Illusion of Predictability

Many companies purchase less ready-made answers with Cyber Threat Intelligence (CTI) than costly homework. Despite the promise of global visibility, the decisive analytical refinement of the data often fails to materialize. A plea for methodological rigor and the actual craft of intelligence in order to counteract the semantic erosion of the term.

TEXT_ ***Richard Weiss and Marc Mahlke***

Richard Weiss works at the interface of technical analysis and strategic doctrine. With a background in mathematics, physics, and data science, he was, among other things, a reverse engineer on Mandiant's FLARE team. He advises two NATO Centres of Excellence (COE) as well as military and public institutions and researches the use of AI and LLMs in intelligence tradecraft.

Marc Mahlke is a cybersecurity expert with an interdisciplinary background in information and communication technology and IT management. He works at the intersection of technical security analysis and strategic cybersecurity, with focuses on penetration testing, red teaming, governance, and intelligence approaches at the organizational level.

KEY MESSAGES

→ **Precision instead of concept stretching:** Without clear definitions of "intelligence," a Babylonian confusion of tongues arises that paralyzes any cooperation.

→ **Avoidance of Cargo Cult Science:** The adoption of military terms without the associated methodological craft (tradecraft) merely creates a façade of security.

→ **Problem:** Intelligence only emerges through the fusion of (external) data from all available sources with internal context – a performance that can hardly be outsourced.

→ **CTI as activity:** Cyber Threat Intelligence is not an isolated discipline, but an interdisciplinary cross-sectional activity that must never lose the physical context.

Intelligence **today shares the fate of many buzzwords in the cybersecurity industry: The term is used so inflationarily that it has lost its operational sharpness. What was once a disciplinary art form for gaining decision-making advantages is now a generic label for any form of data feed. This semantic erosion has long since become a tangible security risk. At a time when the threat landscape is as volatile and complex as never before, the most important instrument for anticipating attacks degenerates into a marketing shell.**

If everything is intelligence – from a simple log entry to strategic adversary analysis – differentiation is no longer possible. To counteract this dangerous trend, cybersecurity professionals must take the step many practitioners shy away from: the step back to a precise definition. The methodological recourse to the definition concept of social scientist John Gerring is helpful here. What initially appears theoretical is in fact the key to practice: Only those who create clarity about intension (which attributes define the term?) and extension (to which objects does it apply?) can prevent mistaking threat information for genuine intelligence. Yet this is precisely where the market fails. Companies that promote their products as CTI solutions suggest an analytical depth that they often do not methodologically deliver. Even established standards such as those of NIST do categorize indicators and tactics, techniques, and procedures (TTPs), correctly as threat information. The market, however, sells these as intelligence. This conceptual confusion is the origin of the inefficiency we observe today in almost all Security Operations Centers (SOCs). ›

As early as 2020, Kris Oosthoek and Christian Doerr described weaknesses in the field of CTI in their article "Cyber Threat Intelligence." The weaknesses evaluated and identified at that time remain relevant today. One limitation is that the evaluation was largely illuminated on the basis of the process and the result. The weaknesses included the following points:

- **CTI lacks methodology:** In many SOCs (Security Operations Center), the principle of "ad hoc" prevails instead of structured analysis. Established methods such as Structured Analytic Techniques (SATs) or Analysis of Competing Hypotheses (ACH) are often maintained only as lip service, while day-to-day operations are dominated by reactive processing. A formalized process that guarantees reproducible results is missing.
- **CTI is generally of low quality:** The "garbage In, garbage Out" principle fully applies here. Many feeds deliver outdated or contextless indicators (IOCs) with high false-positive rates. What is sold as intelligence is often unverified raw data that is pumped into systems without refinement and generates more noise than security.
- **CTI providers are opaque in their sourcing:** The market resembles a black box. Providers often declare their sources as trade secrets, making the origin of the data unverifiable for the customer. Without transparency about the source (e.g., incident analysis with assessment of evidentiary value in the overall context vs. open source), a valid assessment of reliability is methodologically impossible.
- **CTI is too biased: Products are subject to a double distortion:** on the one hand through vendor bias, which highlights threats for which the provider sells solutions (marketing-driven intelligence). On the other hand through cognitive bias of analysts, who often only find what they are looking for (confirmation bias) and what they themselves know.
- **Attribution in CTI is difficult:** The technical attribution of attacks to actors is highly speculative and susceptible to manipulation (false flags). Analysts often draw premature conclusions based on technical indicators without sufficiently examining political or economic motives as alternatives – a risk that can quickly develop geopolitical explosiveness.

With increasing speed in the transformation of the threat landscape, changes should be made and re-evaluated. It also seems essential to illuminate the missing perspectives, especially given the growing calls for cooperation between private-sector companies, authorities, and the military.

Fundamental prerequisites for cooperation have already been described many times. In the field of intelligence, however, it is particularly important to first define possibilities for cooperation and examine dependencies. The absence of a uniform definition has fatal effects: It forms the starting point for what Thomas Kuhn describes as incommensurability – the incompatibility of different schools of thought. Reinforced by individual sensemaking processes (according to Weick), in which each actor interprets unclear data differently, this ultimately leads to a structural relationship disorder in the sense of Watzlawick. From this results the urgent necessity to define concepts precisely that also withstand the methodological requirements of Gerring.

„With increasing speed in the transformation of the threat landscape, changes should be made and re-evaluated."

Richard Weiss and Marc Mahlke

Cyber Threat Intelligence cannot be integrated as its own analytical field like crime and terrorism – here CTI even leads to increased complexity: alongside physical forms of crime there is now cybercrime, alongside terrorism cyberterrorism. Likewise, categorization by source type such as human, signals, or open sources is not mutually exclusive. Cyber Threat Intelligence is an interdisciplinary cross-sectional activity, with the emphasis on activity. For this reason, it is also important not to consider Cyber Threat Intelligence in isolation or as an independent intelligence activity. Even when considering the aspect of inclusion of all existing intelligence disciplines for delivering finished intelligence under the Intelligence Reform and Terrorism Prevention Act (IRTPA), CTI plays an increasingly important role. Isolated consideration of CTI often loses the physical context in publications or ends the chain of argumentation too early.

Nevertheless, CTI also adopts concepts from the intelligence field: It begins with simple concepts such as the Intelligence Cycle, which – depending on the interview partner – has a different number of phases – from four at NATO to six at CTI providers ›

– mostly with a lack of detailed definition of the individual phases.

WITHOUT ANSWERING THE "SO WHAT?" QUESTION, INFORMATION DOES NOT YET CONSTITUTE VALID INTELLIGENCE.

An established structuring model is stratification into tactical, operational, and strategic (threat) intelligence. Specialist authors such as Thomas Roccia as well as various security providers frequently replace a precise definition with a purely descriptive classification. In doing so, the deliverable – for example indicators of compromise (IOC) – is primarily correlated with the functional role for which this information is intended.

The US cybersecurity company Mandiant, which was acquired by Google, operationalizes this approach in the context of attribution across three levels: Strategically, attribution takes place via the geographic location of the actor; operationally via behavioral patterns; and tactically on the basis of technical indicators. However, it must be stated: The mere filling of intelligence levels with threat information does not constitute valid intelligence without the rigorous application of intelligence tradecraft and without answering the "So What?" question.

The National Institute for Standards and Technology (NIST), the European Union Agency for Cybersecurity (ENISA), the National Cyber Security Centre (NCSC), as well as the Council of Registered Ethical Security Testers (CREST) also make use of the classic application levels, primarily filling these container categories with threat information, not with intelligence. There is no consensus regarding the additive descriptive factor. If terminological compatibility with other intelligence disciplines is also lacking, this inevitably leads to methodological isolation of CTI. In practice, the terms strategy, operational, and tactical are often instrumentalized merely to create internal differentiation within the IT organization – as a distinguishing feature between highly technical content for specialists and abstracted information for decision-makers.

Here the problematic transfer of military doctrines into the cyber domain manifests paradigmatically. Giovanni Sartori describes this process as concept stretching: Terms are extended to new fields but inevitably lose precision and sharpness of meaning. Physicist Richard Feynman coined the term Cargo Cult Science for such phenomena. Similar to cultures that imitated technological forms without understanding how they functioned, parts of the CTI industry often adopt only the outer shell of military intelligence (terminology and phase models) without penetrating its methodological core (tradecraft). This semantic erosion and the growing distance from the original definition can be observed among various intelligence providers. Another blatant example of this imbalance is revealed in the assessment of data relevance described at the appropriate point.

The examples discussed vividly illustrate another core problem: the absence of a precise terminological foundation. What is often dismissed in practice as academic hair-splitting turns out to be a structural obstacle. This is precisely where the methodological rigor derived at the outset according to Gerring unfolds its operational relevance. Defining terms by their intension and extension forces the necessary precision. For interdisciplinary cooperation, this is not a theoretical luxury but an operational necessity: Only if all actors – from the CTI analyst to the military planner – mean exactly the same scope and the same properties when they say "intelligence" can the Babylonian confusion of tongues be resolved and genuine interoperability be achieved.

Another structural limitation in the interaction between threat information providers and the requesting entities (intelligence consumers) manifests itself in the often diffuse interfaces. While calls for "cooperation" are ubiquitous, there is usually a lack of a clear definition of handover points in operational terms. This collaboration is complicated by a fundamental asymmetry: The highly specific requirements of the customer – that is, the concrete question and the required contextual timing – collide with the generic nature of the data offered. In order to exploit economies of scale and serve the broadest possible market, many CTI providers deliberately limit themselves to delivering standardized threat information.

The downside of this business model is evident: The actual intelligence analysis – the methodological refinement of the data – takes place outside the provider's sphere of responsibility. As a result, cooperation begins at a completely different point in the intelligence cycle than is often assumed. If one examines cooperation through the methodological lens of the Intelligence Collection Plan (ICP), the actual interface can be precisely located: Providers do not deliver ready-made answers to strategic questions (intelligence), but in fact function as suppliers of "sensor data" that merely serve to answer the Essential Elements of Information (EEI). The cognitive performance of synthesis remains with the recipient.

Although the Intelligence Collection Plan (ICP) is a fundamental steering instrument, it often receives insufficient consideration in common CTI practice. A brief classification of this concept is therefore necessary at this point. For a more in- ›

depth methodological discussion and detailed presentation, reference is made to the working paper "Development of an ICP-LLM to support the creation of an Intelligence Collection Plan (ICP)" by the Northern Business School (NBS) in cooperation with the NATO-accredited CIMIC COE (Civil-Military Cooperation Centre of Excellence).

„In view of the global deluge of threat raw data, the claim to completeness is an illusion anyway."

Richard Weiss and Marc Mahlke

If one accepts the role of providers as mere sensors, the quality assessment of raw data becomes a matter of survival. In the CTI field, the Admiralty Code originating from military intelligence has become established for this purpose, and its integration into the Malware Information Sharing Platform (MISP) in 2015 marked an important step toward standardization. However, a valid assessment presupposes that both the reliability of the source and the credibility of the information can be transparently verified. This is precisely where the trust model collapses.

Due to the functional division of labor – the provider supplies, the customer processes – the responsibility for completeness, correctness, and standardization shifts massively to the suppliers. Yet verification of these quality characteristics is in fact impossible for the customer, since threat information providers often declare their collection methods as protected intellectual property or keep them opaque with reference to source protection. That this mistrust is justified is underscored by the results of the paper "Beyond Bias: A Critical Analysis of Intelligence Tradecraft and its Impact on State-to-Industry Collaboration in CTI." The analysis not only questions data quality but also shows that the transformation methods of data processing are subject to the same methodological hurdles.

The dilemma deepens due to technical reality: Threat information is often based on implicit assumptions and is pressed unfiltered into the rigid corsets of existing security products with all their limitations. In view of the global deluge of threat raw data, the claim to completeness is an illusion anyway. More serious, however, is the statistical deficit: The mathematical significance of a single threat information provider is highly questionable given the fragmented view of the global threat landscape. The consequence of these shortcomings is a fundamental market distortion. The core problem lies in the nature of intelligence itself: The decisive question – the "So What?" – cannot be answered without detailed knowledge of one's own infrastructure, risk appetite, and business objectives. Since CTI providers systemically lack this internal context, they cannot by definition deliver finished intelligence, but only contextless data.

The central market promise of intelligence delivery is therefore an illusion. The actual refinement – the fusion of the external threat landscape with internal context – must inevitably take place at the end customer. Yet many companies are structurally not set up for this. It often fails less due to methodological knowledge than simply due to resources. We therefore observe a massive, often uncalculated resource shift: Instead of exploiting economies of scale in which a provider takes over the analysis, there is an economically inefficient multiplication of effort. Each customer must contextualize the expensively purchased raw data themselves in order to make it actionable. The industry does not buy ready-made answers, but expensive homework. ■

"We Experience the Situation in Ukraine Very Directly"

Reconnaissance drones deliver precise situational awareness from areas that are difficult to access. Krista-Marija Läbe of Quantum Systems explains why speed, connectivity, and European sovereignty are decisive in drone development.

INTERVIEW_ ***Krista-Marija Läbe***

Krista-Marija Läbe is a German-Ukrainian communications strategist and PR manager at Quantum Systems. Previously, she worked as a strategic communications advisor for the Ukrainian Embassy in Germany. She is also co-founder and board member of the German-Ukrainian Society and is committed to sharpening awareness of Ukrainian perspectives in Western European discourse.

KEY MESSAGES

→ **Quantum Systems** develops and produces dual-use reconnaissance drones as well as the corresponding software for military and civilian users.

→ **With over three hours of flight time**, long range, and modern sensor technology, the VECTOR enables continuous real-time reconnaissance.

→ **Transparency** arises through the combined use of different drone types that cover different ranges and together create a seamless situational picture.

→ **Experiences from Ukraine** accelerate innovation, software updates, and resilience against electronic warfare.

→ **The company** relies on European supply chains, China-free core components, and industrial scaling to strengthen strategic autonomy.

Krista-Marija Läbe, how would you briefly explain what Quantum Systems does?

Quantum Systems develops and produces drones and the corresponding software. Our drones are reconnaissance drones. They are used to collect information from areas that are difficult for people to access or that cannot be overflown by helicopters or aircraft. The drones transmit this data back to users in real time. These can be soldiers, but also disaster response teams, emergency services, or the coast guard. From this data, a precise situational picture is created of what is currently happening in an area.

Quantum actually started as a civilian UAS startup. How has the company developed?

Exactly. We are a dual-use company. Our products can be used both for civilian and military purposes. In the early years, the focus was strongly on agriculture, forestry, and other civilian application areas. At that time, the military use of drones in Western armed forces was not yet a major topic. That fundamentally changed with Russia's war of aggression against Ukraine. Since the beginning of the full-scale invasion, our drones have also been deployed in Ukraine, initially from spring 2022. Since then, Quantum Systems has focused very strongly on the military – or governmental – market, as this is where the greatest technological leaps can be observed. ›

How does the VECTOR drone developed by Quantum conduct real-time reconnaissance? Does it "hover" in the air?

It does not hover in the classical sense. The VECTOR is what is known as a fixed-wing aircraft, in other words a drone with wings – essentially a glider. This allows targets to be observed over a longer period of time by circling above the target area. You can say, stay with a position or follow this movement. In this way, patterns can be recognized, hideouts found, or relevant targets identified. In some cases, one VECTOR is then replaced by another. The flight time is over three hours, and the range is more than 60 kilometers.

And how strong is the weather influence?

Rain and fog are less problematic than one might think. The Vector has a night and thermal imaging camera and can also see through fog. This was a decisive advantage in Ukraine. During the Battle of Sievierodonetsk in May 2022, conventional drones were unable to detect anything due to the fog, but the Vector could. In this way, Russian troop movements could be identified and reported in time. Wind remains a limiting factor, but it takes strong gusts to keep us grounded.

So the system can also be deployed at night.

Yes, at night, in fog, and also in cold conditions. We have further developed the system based on experiences in Ukraine, for example against icing of the wings and for stable battery performance in winter. Especially at night, the VECTOR has proven extremely valuable due to its superior sensor technology.

Where are the greatest technological advances currently taking place?

Above all in software and adaptation to new threats. Hardware, software, and AI are continuously being further developed, but the decisive factor is the speed of updates. In an active war, we are talking about weeks, not months. A drone must constantly evolve in order to remain operational. Only in this way can it fulfill its core mission: providing relevant information in real time.

When it comes to reconnaissance drones, there is the idea of a transparent battlefield. What exactly does that mean?

Transparency arises through the integration of different systems. We have drones for different ranges, from the immediate vicinity to long distances. Together, they enable continuous, cost-efficient reconnaissance. This applies militarily, but also civilly, for example in natural disasters or rescue operations. Connectivity is important, meaning software that brings together different systems and manufacturers. In this way, a comprehensive situational picture is created from space to the ground. This software, MOSAIC UXS, is standardized across all our drones and enables the simultaneous deployment of multiple systems.

"A drone must constantly evolve in order to remain operational."

Krista-Marija Läbe

How does cooperation with users, meaning the soldiers, actually work?

There is a direct support structure, such as a call center in Ukraine, where soldiers receive technical support around the clock. The knowledge flows directly into further developments, especially in the area of electronic warfare. The Vector is now highly resistant to jamming. Even if the connection is interrupted or GPS is disrupted, it can continue its mission and independently find its way back.

How does the VECTOR work with other intelligence sources, for example satellites?

One example is our partnership with Planet Labs. The idea is to combine satellite-based ISR (Intelligence, Surveillance, Reconnaissance) with tactical drone reconnaissance. Satellites show changes on the ground, and the drone then takes a targeted look at what is actually happening there. In this way, drones can be deployed much more efficiently.

Do you see Quantum more as a German or a European company?

We are globally positioned, with production sites also in Ukraine, the United States, and Australia. But in Europe we have a clear focus on building strong European supply chains. For us, this is about European sovereignty and strategic autonomy. We operate in many European countries and want to become as independent as possible. This is a clear part of our identity.

How dependent is Quantum on the United States?

We have components that come from the United States, and we are also ›

present in the U.S. We have a factory there because the American armed forces are among our customers. At the same time, we have a focus on aligning our supply chains toward Europe. This allows us to replace American components with European ones at any time – if our customer wishes.

And what about China?

The management began deliberately distancing itself from Chinese components many years ago. Today, in Tier-One and Tier-Two components, we are in fact "China-free" in our supply chain. For raw materials where shares still come from China, we are either seeking European alternatives or have built up strategic reserves.

What role do industrial cooperations play for Quantum?

A very large one – especially between Germany and Ukraine. Ukraine is a real testing ground for modern warfare, unfortunately under extreme conditions. The feedback from soldiers is incredibly valuable. We can translate these insights directly into the further development of our systems, which then also benefits the Bundeswehr and other customers. Together with the Ukrainian company Frontline Robotics, we have established the first German-Ukrainian joint venture for the production of Ukrainian drones in Germany – Quantum Frontline Industries.

What comes next?

We are working on massively increasing production capacities in Europe. For example, through joint ventures in which Ukrainian products are manufactured on a large scale in Germany or other European countries and then delivered to Ukraine. This in turn generates new lessons that we can feed back into development.

You often speak of users when referring to soldiers, not customers...

Formally, the customer is the Ministry of Defense, but the actual users are the soldiers. This fundamentally differs from other industries. When I speak of users here, I mean people who deploy these systems under extreme conditions. That is something entirely different from consumer products. And that strongly shapes both my work and my attitude.

How does your work at Quantum relate to your engagement in German-Ukrainian civil society?

For me, over the past four years, it has always been about supporting Ukraine and making the greatest possible contribution from here in Germany. That initially began in civil society, and later also through my work at the Ukrainian embassy. In parallel, together with others, I founded and built up the German-Ukrainian Society (Deutsch-Ukrainische Gesellschaft). We now have more than 500 members and pursue the goal of strengthening German-Ukrainian relations in various areas.

What exactly do you do?

We organize study trips, for example for journalists, but also for our members. Many of them are Germans who are committed to Ukraine. We see ourselves as a network for people who support in different ways – through humanitarian aid, awareness-raising, academia, or politics. Our aim is to enable exchange and to bundle engagement.

Why is this civil society engagement so important to you?

Because in Ukraine one sees very clearly that defense is a task for society as a whole. Politics, industry, civil society, and the military work closely together there. Civil society collects donations, documents war crimes, and supports the military. Companies provide material or financial assistance, media inform, politics handles diplomatic work. I would like to see this kind of interaction more strongly in Germany as well.

How do you connect your engagement with your work at Quantum?

It is important to me that we work interdisciplinarily. That we are in exchange with think tanks, civil society organizations, politics, and the military. One example was a delegation of Ukrainian soldiers whom we invited to Germany in December. They openly reported here on their experiences, on the use of drones, and on necessary adjustments. That was important for politics, media, and also for us as a company.

The situation in Ukraine is currently extremely difficult. What does that mean for you as a company, especially in winter?

We experience this very directly. As a company with several hundred employees in Ukraine, we are in close contact with colleagues on site, many of whom are directly affected by power outages, blackouts, and air attacks. This is not abstract, but personal. It is similar with the soldiers: Our teams are in direct exchange with brigades and units. The situation at the front is extremely harsh, and in winter the cold, sub-zero temperatures, and the overall situation further exacerbate conditions.

At the same time, negotiations are underway about a possible end to the war. How does that influence your work at Quantum?

Honestly, hardly at all. Political talks often have little to do with the reality on the ground. The fighting continues, and air attacks on cities and energy infra- ›

structure have even increased. The situation at the front is difficult, but the Ukrainians are holding their ground. That is why we focus less on political statements and more on what users at the front actually need. And those are still these systems.

Do you think about future scenarios, such as a ceasefire? And what would an end to the war mean for Quantum Systems?

Of course. Personally, I very much hope for a just peace. But even a ceasefire would have to be secured. Reconnaissance drones will be needed in every scenario, whether the fighting continues, a ceasefire comes, or a long-term peace emerges. This applies not only to Ukraine, but also to other regions such as the Baltics. That is why we look ahead to what will be needed in six months or in a year.

Defense Minister Boris Pistorius and Ukrainian President Volodymyr Zelenskyy visited Quantum Frontline Industries together on February 13, 2026. There, you officially handed over the first drone produced by the German-Ukrainian joint venture Quantum Frontline Industries to Zelenskyy and Ukraine. How did you personally experience this moment?

The handover was carried out by the management of the participating companies, and I had the honor of moderating both the handover and the visit. Meeting President Zelenskyy in person was an unforgettable moment for me and at the same time a strong signal that our work – and especially this co-production – is exactly what Ukraine urgently needs in this phase of Russia's war of aggression.

The organization of the event and the encounter itself are an incentive for me to place even greater focus in the future on projects like this with concrete impact. Because in the end, one thing matters: tangible support and a reliable partnership with Ukraine.

How did the joint project proceed? What did you and your company learn from it?

From the announcement of Quantum Frontline Industries to the establishment of the production line in Germany, exactly two months passed – for a project of this complexity, that is almost light speed, as Defense Minister Pistorius also emphasized. This was made possible by consistent prioritization at all levels: by our management, by Frontline Robotics, and in particular by the Managing Director of QFI, Matthias Lehna, as well as by the active support of the German and Ukrainian governments. Our communications team closely supported the public relations work and will continue to do so. For me personally, it is one of the most important projects of my professional career so far. Because here it becomes very concrete what it is about: a tangible added value for Ukrainian soldiers and the strengthening of Ukraine's defense capability – and thus Europe's as well. ■

"Reconnaissance drones will be needed in every scenario, whether the fighting continues or not."

Krista-Marija Läbe

Battlefield in 3 Dimensions

In urban combat, modern weapons systems quickly reach their limits. Urban warfare expert Julian Werner explains why precise intelligence supports military decision-making and helps protect both one's own troops and the civilian population.

INTERVIEW_ ***Julian Werner***

Julian Werner is a former paratrooper and officer of the Army's specialized forces (EGB). Since 2024 he has been conducting research under Prof. Dr. Carlo Masala at the Center for Intelligence and Security Studies on topics such as urban warfare and military innovation. His book *Urban Warfare – Krieg zu Hause* will be published in April 2026.

KEY MESSAGES

→ **Urban warfare** is characterized by extreme proximity, high mental strain, and a three-dimensional battlespace.

→ **Modern weapons systems and drones** are important but quickly reach physical and tactical limits in urban environments.

→ **Intelligence and ISR** are central to differentiating movements, building usage, and civilian presence.

→ **Precise reconnaissance** expands the scope of decision-making and can resolve the trade-off between force protection and civilian protection.

→ **Urban warfare** is always also a struggle over information and interpretation – brutality may decide battles, but not wars.

1

What distinguishes urban warfare from other forms of warfare?

On the one hand, engagement distances in cities are generally extremely short. From building to building – and especially within houses, from room to room – they are often only a few meters. Decisions over life and death must be made in fractions of a second; the mental strain on soldiers is correspondingly enormous.

On the other hand, urban architecture forces the battlefield to be thought of in three dimensions: dangers threaten from upper floors as well as from hidden basements and tunnels. The possibilities for enemy firing positions and concealment are nearly endless. Every window, every door can become a threat. A reasonably safe advance under mutual overwatch by assault and cover elements requires a high degree of communication and coordination.All of this takes place under the constant presence of civilians, whose whereabouts can neither be planned nor reliably predicted.

2

How do modern weapons systems (drones, UGVs, etc.) change the urban battlefield?

In fact, modern weapons systems reach their limits much more quickly in urban combat than in open terrain. Drones do provide an important reconnaissance capability, but they can neither see through walls nor detect hidden tunnels – at least not yet. For precisely this reason, micro-drones play a particular role in urban combat, especially for reconnaissance inside buildings.

In addition, the limited payload of many drones and loitering munitions restricts their use in urban environments. To breach massive wall structures or destroy heavily fortified positions, "classic" means such as artillery or aerial bombs are often still required.

Unmanned ground vehicles also frequently fail due to banal obstacles such as stairs or come to a halt in front of extensive rubble fields, as can repeatedly be observed in Gaza. This often also applies to manned vehicles, which is why infantry ›

on foot or military working dogs remain irreplaceable in heavily destroyed urban battlefields.
At the same time, modern sensor technology is indispensable: it allows the urban battlefield to be mapped in detail within seconds. Three-dimensional models can be generated from drone footage and used on screens or in virtual reality environments to facilitate mission planning and preparation.

3

What role does intelligence or ISR (Intelligence, Surveillance, Reconnaissance) play for decision-making capability and superiority in urban environments?

The presence of civilians, critical infrastructure, hospitals, as well as buildings with symbolic or emotional value makes it indispensable to proceed with particular caution in urban environments. Military decisions here do not affect only the enemy but almost always have immediate consequences for non-combatants.
In such an environment, it is not enough to know in general terms where the adversary is located. What is decisive is rather who is where and when: Where are civilians moving? Which buildings are used for military purposes, which serve as shelters? Which routes does the adversary actually use – and which only seemingly?
Powerful intelligence and ISR capabilities are therefore a central prerequisite for decision-making capability and military superiority in urban combat. They make it possible to detect movements, understand patterns, and weigh risks before action is taken.

4

How does intelligence in particular influence the balancing of force protection, military effectiveness, and the protection of the civilian population?

Force protection of one's own troops and the protection of the civilian population are often portrayed as an irreconcilable trade-off. This is short-sighted both under international law and strategically – and ultimately dangerous.
Powerful intelligence helps to dissolve this supposed contradiction by making visible courses of action in which the military mission can be fulfilled without unnecessarily endangering civilian life. It expands the scope of decision-making and makes it possible to weigh different options instead of being fixed on the seemingly sole military solution.
This can, for example, mean consciously refraining from engaging in an urban warfare scenario. ISR findings can reveal vulnerabilities, for instance on the adversary's flanks or in its supply lines. If pressure is applied there, the adversary can be forced to withdraw without the city itself becoming the immediate battlefield.

5

To what extent is urban warfare today connected with information, media, and cognitive operations?

Over decades, the influence of media reporting on military operations grew. Journalistic investigations and later the ubiquitous dissemination of images and videos via social media made urban combat visible almost in real time. Excessive collateral damage or war crimes could trigger international outrage and lead to political pressure, sanctions, or even military interventions.
At present, however, a countervailing development can be observed. The crisis of trust in traditional media, the fragmentation of the public sphere, and the deliberate spread of propaganda and disinformation in social networks have weakened the deterrent effect of media visibility. Authoritarian or populist actors in particular seem increasingly less impressed by international criticism.
As a result, urban warfare in some conflicts is once again being conducted more openly and more brutally, while violations of international humanitarian law are not only accepted but communicatively accompanied or relativized. Military violence is often flanked by dedicated media, information, and propaganda campaigns aimed at legitimizing one's own actions, reframing responsibility, or sowing doubt about established facts.

6

What role does AI play in urban warfare (autonomous weapons systems, reconnaissance, command and control systems)?

Artificial intelligence will foreseeably play an ever greater role in accelerating the so-called kill chain, that is, the process from reconnaissance to engagement of enemy targets. From identifying and prioritizing targets to controlling weapons systems, AI makes it possible to control larger operational areas with fewer personnel resources.
At the same time, the dynamics of modern battlefields – especially in cities – must not be underestimated, nor should the "computer" in the human mind. In highly dynamic combat situations, soldiers remain extraordinarily capable of processing complex information within fractions of a second. Experienced soldiers and offi- ›

cers therefore remain irreplaceable. The task of AI will be to relieve and augment human decision-making – not to replace it.

7

What lessons can be drawn from urban battlefields of the recent past?

Battles can be won with sheer brutality, but wars cannot. Especially in urban environments, ruthless action against the civilian population leads all the more to sustained resistance. This is evident both in the war in Ukraine, where the massacre of Bucha became a rallying cry for Ukrainian resistance and led to increased Western weapons deliveries. But it is also clear in Gaza that the Middle East conflict cannot be bombed away.

Avoiding collateral damage and proceeding with precision is therefore required both tactically and strategically. Moreover, the use of military force must always serve a long-term political objective that answers the question of what will happen to the contested city and its population after the fighting. Otherwise, in the end, only lost victories remain.

8

What do you personally wish for most – as a human being in this world? What is your message to Germany and Europe?

If I were allowed to single out one aspect, it would be not to forget the concrete human fate in war. The individual is quickly lost when we speak of armies of hundreds of thousands or of hundreds of civilian victims. Yet every soldier, every woman and every man, every child who must experience war has their own story, a family, hopes, and visions of the future. Our value system is based on not forgetting the humanity in the other and not degrading him to the mere object of our – or machine-driven – actions. This does not mean becoming militarily incapable of action. On the contrary: fighting and destroying the enemy remains the brutal reality of war.

But recognizing the humanity even in the enemy preserves us from making this task easier for ourselves through propagandistic narratives – until the threshold toward civilians falls or we even begin to normalize or justify violence. ■

"Recognizing the humanity even in the enemy preserves us from normalizing or justifying violence."

Julian Werner

More Eyes See More

One of Europe's weaknesses lies in signal intelligence. To remain strategically autonomous, the EU must now build common SIGINT structures – technologically, institutionally, and politically.

TEXT_ ***Aviva Guttmann***

Dr. Aviva Guttmann is a Lecturer in Strategy and Intelligence at Aberystwyth University. Previously, she conducted research at King's College London (King's Intelligence and Security Group) and at the University of Southern Denmark. She is the founder and chair of the Women's Intelligence Network (WIN). Her research on intelligence services, covert operations, and terrorism has been published, among other works, in "Operation Wrath of God"(Cambridge, 2025).

KEY MESSAGES

→ **The U.S. withdrawal** from security and intelligence cooperation has exposed Europe's strategic vulnerability.

→ **Military rearmament** alone is not sufficient – without its own foreign intelligence capabilities, Europe will remain dependent.

→ **European intelligence** services are highly fragmented and significantly inferior, particularly in signals intelligence.

→ **A multilateralization of intelligence** is necessary: from recruitment and collection to analysis.

→ **A European intelligence alliance** – for example, modeled on "27 Eyes" – is essential for achieving strategic autonomy.

With the start of the current Trump administration, the European Union has woken up to a new reality: America is not only withdrawing its security umbrella – a policy the US pursued for 70 years – but shows openly hostile, and increasingly aggressive, behaviour against some of its NATO allies, including the most recent threats against Greenland. In March 2025, the Trump administration suddenly halted intelligence-sharing channels with Ukraine and withheld crucial battlefield information that the country needed in the war with Russia. This move shocked many intelligence observers, as it laid out most crudely the extent to which the United States could not be trusted anymore as a European security partner.

The European reaction has indeed been swift on the military manufacturing level: In the first half of 2025, the European commission decided to build European defence capacities and foster its own military industry. The plan, in short, is to transform Europe into a war machine. While Europe coordinates its colossal military capacity building among its countries, its intelligence agencies remain untouched in the respective countries.

Arguably, this urgently needs to change. Alongside a military integration, the EU's foreign intelligence agencies also need to fill the vacuum of a US security withdrawal. Intelligence commentators lament that European agencies rely too strongly on information received by the US intelligence community. This concerns especially signal intelligence: intelligence that has been obtained by intercepting various communication channels. The issue is that each European individual agency cannot replace the vacuum that is being created in case the US were to stop intelli- ›

gence-sharing with European countries. A new way of organising intelligence capacities in Europe is required.

While the EU and its strategic partners have established excellent intelligence-sharing links, those modes of cooperation still mainly happen informally and on a case-by-case basis. Furthermore, a mere increase in intelligence cooperation is not enough to make up for a potential loss of US intelligence. What needs to happen is what one could call "multilateralising" European intelligence on every level. From recruitment to acquisition and analysis, every aspect of intelligence work needs to be reimagined and redeveloped in a new, different, even unprecedented, way.

To some degree, some political voices have understood this need, as the remarks suggest by Henna Maria Virkkunen, the Executive Vice-President of the European Commission. In April 2025 she explained that the commission was planning to "equip Europe with new ways of combining and sharing information. This will improve our anticipation and reaction capacity." This means that the EU wants to establish more and better-connected databanks and new secure communication channels. The EU commission also suggests improving the security of critical infrastructure and to invest into European cyber security.

This is a good starting point, but, given the current threat landscape, it is by far not enough. Europe does not only need to enhance its analysis capacities or share more country-specific and polished intelligence reports. It is not only intelligence analysis that needs to merge, as suggested by the EC, but also intelligence collection needs to integrate under one EU institution.

How can this be achieved? The truth is this will not be easy. It has generally been assumed that sensitive intelligence work, such as managing human sources or intercepting encrypted communication, would be too sensitive to organise on a multilateral cross-country level. Furthermore, another obstacle is a lack of trust and suspicions towards other agencies. As an example, in current intelligence circles there is the (founded or unfounded) suspicion that the German foreign intelligence agency, BND, has been penetrated by Russian spies. If this is the case and France and Germany were to share information or even merge capacities, a foreign spy would only need to undermine one country to get access to secrets from both. Similarly, it is suspected that agencies in Eastern European countries, such as Bulgaria, are heavily infiltrated with Russian moles. This risk can be mitigated, however, for instance by a tight vetting process for anyone who would be working in the common EU intelligence framework.

Current European signal intelligence capacities are very low and need to be built up nearly from scratch. In other words, compared to the US, European capacities to spy on its adversaries are minuscule. While this is a serious issue, it also represents an opportunity: because all countries in the EU are at a relatively similar level, coordinating the construction of signal intelligence infrastructures could be smoother than if some countries possessed already established systems that may not be interoperable with one another.

"European SIGINT capabilities are very limited and would have to be built up nearly from scratch."

Aviva Guttmann

Is there a model the EU could adhere to? The current intelligence group that comes closest to what the EU needs is the well-known Five-Eyes intelligence liaison. Like the UKUSA agreement, the EU needs to conclude a "27-eyes" based on a robust legal framework that coordinates and merges signal intelligence capacities, obliges all countries to share raw intelligence, assessments, and analyses. It needs to operate as a supranational entity and be fully integrated under the EU Third Pillar.

Alternatively, another starting point could be the expansion of existing ad hoc intelligence groups. The most prominent and long-established such group is the Club de Berne, created in and named after the Swiss capital in 1969. It currently hosts the Counter Terrorist Group and is one of the most widely used European counterterrorism intelligence-sharing frameworks. A potential route ahead could be to add other foci besides counterterrorism to the Club de Berne's portfolio. An advantage of the Club de Berne is its inclusion of non-EU members and its long-es- ›

tablished trusted relations among European intelligence agencies and extra-European partners. Relatedly, in March 2025, after the temporary halt in US intelligence-sharing with Ukraine, some countries met in Paris under the leadership of France and the UK and agreed to enhance direct cooperation with Ukraine, including the provision of surveillance technology and satellite data. Recent reports suggest that France has now replaced the US as main intelligence provider to Ukraine. Specialised signal intelligence groups like these could be enlarged to foster the build-up of European intelligence capabilities in this respect.

Current supranational structures could also significantly be expanded, such as the EU's own Intelligence and Situation Centre (INTCEN) and the EU Military Staff Intelligence Directorate. Their function is mainly limited to analysis. However, INTCEN also enables secondments from national intelligence agencies, and this feature could potentially be expanded and applied to other steps in the intelligence cycle, including one day also intelligence collection.

Alongside this development, the EU needs to seriously invest in new technologies, think about how it can expand the development of military satellites, and enhance its communication surveillance.

Once a common foreign intelligence gathering and managing structure is established, another step will be to start thinking about coordinating domestic intelligence agencies. This, however, is a lot more challenging due to very different legal regimes and political cultures. However, once a model has been found on how to handle EU common foreign intelligence gathering, this mode might be expandable to other areas.

Overall, while the EU understood that it needs to heavily invest and develop its military in a coordinated way, it also needs to realise that the logical next step is to massively invest, coordinate, and develop its foreign intelligence capacities. Europe is not only to be defended with tanks and grenades, but also with an integrated spy-agency to ensure its might. ■

"The EU must seriously invest in new technologies and consider how to expand the development of military satellites."

Aviva Guttmann

Understanding Cybercrime as a Business Model – and Combating It Collectively

Many companies still defend themselves in isolation, while attackers operate as automated ecosystems. Modern threat intelligence reverses this imbalance. The NetWatch initiative combines real-time detection with collective response and makes cyber defense scalable.

Many security measures rely on prevention and response. Why is that no longer sufficient in your view to sustainably contain cyberattacks?

Ralf Schneider: Prevention and response remain central building blocks, but on their own they fall short. Cyberattacks today evolve extremely quickly, particularly through AI and automation. What is needed, therefore, is proactive prevention and adaptive response in real time. It is crucial to continuously understand the context: current threats, changes, and particularly critical assets. This can only be achieved with continuous cyber threat intelligence.

Lars König: In addition, companies often think in isolation and primarily protect themselves. Attackers, on the other hand, act highly automated and switch quickly between targets. That is why a collective approach is needed: similar to an immune system, an attack should ideally only be detected once so that the entire ecosystem can subsequently benefit from it.

What do you understand by threat intelligence?

Lars König: Threat intelligence is the structured exchange of information about cyberattacks between different actors. Three levels are distinguished: tactical (concrete indicators such as malicious IP addresses), operational (who attacks which industries or regions), and strategic (new attack patterns and long-term trends). The goal is to quickly classify attacker behavior and become capable of taking action. ›

Lars König *(left)* combats abuse systems worldwide as the founder of NetWatch through a community-based approach. He is part of the Customer Advisory Boards of Google and CrowdStrike.

Dr. Ralf Schneider *(right)* is Chairman of the Board of the association Cyber Security Sharing & Analytics e. V. (CSSA) – an association of 17 large German companies with the aim of better protecting themselves and the public IT infrastructure jointly against cyberattacks.

More at *netwatch.de*

Photos Lars König and Dr. Ralf Schneider

Ralf Schneider: The biggest challenge today is the flood of information. Companies no longer need more data, but better prioritization: what is relevant for me right now? This requires highly focused, 24/7 available threat intelligence that is immediately translated into decisions and measures. Otherwise one remains reactive and always one step too late.

What fundamentally makes NetWatch different from traditional approaches in your view?

Lars König: Attackers operate like any other company according to an economic model in which they must earn more money than they spend in order to remain profitable. Their sources of revenue include, for example, ransom demands from compromised companies or the sale of valid access credentials to other criminals. On the cost side, expenses arise for maintaining infrastructure and tools as well as the time spent preparing and carrying out attacks on victims. NetWatch is not a classic threat intelligence provider but intervenes actively. Together with internet service providers, attacker systems are quickly taken offline. Since the revenue side can hardly be influenced, we deliberately increase the costs – especially time. In this way, the attackers' business model becomes unattractive. In addition, we reverse the psychological effect: it is no longer the defender who lives in uncertainty, but the attacker.

Ralf Schneider: The decisive factor is the community and open-source approach. The sensors are minimally invasive, inexpensive, and not detectable by attackers. Anyone can participate, and the defense scales with the attacker landscape. This makes collective cyber defense practical and effective.

What concrete questions can NetWatch answer for a company that classical security tools leave open – and what advantages do companies gain from this?

Lars König: NetWatch shows who is currently attacking a company, where these attackers are otherwise active, how frequently they proceed, and which patterns they use. Attacks are grouped together so that it is immediately recognizable whether they are targeted attacks or mass scans. Honeypots (digital decoy systems) provide additional insights into methods and capabilities.

Ralf Schneider: The added value lies in timeliness and context. Attackers are recognized already during the intrusion attempt. Instead of losing information, real-time knowledge about intention, risk, and priority emerges – a foundation for effective deterrence.

If you had to name a single reason to a manager why engagement with NetWatch is strategically worthwhile – what would it be?

Ralf Schneider: Cybersecurity no longer works in isolation today. Sustainable security arises only through collective defense. NetWatch is a unique vehicle for implementing a real community-based cyber defense in real time. One contributes information and receives collective security in return – that is collective cyber defense in its purest form.

Lars König: NetWatch replaces individual defense with a networked community of companies, providers, and authorities. Attacks are detected in real time, blocked, and infrastructure is quickly shut down. This shifts the balance of power in favor of the defenders.

How does deterrence work in your approach – and what role does the economic logic of the attackers play?

Ralf Schneider: Cyberattacks occur in a decentralized and anonymous manner; they cannot be stopped with a "large counterstrike." Deterrence therefore works incrementally: attacks become more expensive, and the risk of being discovered and prosecuted increases. Attackers have three central cost blocks: infrastructure, knowledge, and people. If their infrastructure is regularly shut down, servers must be newly procured, configured, and disguised. That costs time and money. At the same time, their risk increases the more the community and authorities know about procedures, tools, and patterns.

Lars König: Deterrence means permanently increasing costs and risks for attackers. If systems are regularly shut down or law enforcement becomes more likely, an attack simply no longer pays off. The "Pyramid of Pain" shows: IP addresses can easily be changed, techniques and patterns cannot. If an attacker is recognized through their digital fingerprint, they must change their entire approach. This interrupts operations and causes high costs. ›

How can the intent of an attacker be recognized?

Lars König: Intent results from metadata and patterns: user/password combinations, target systems, and attack frequency show whether broad scanning or targeted attacks are taking place. By clustering digital fingerprints, entire attacker groups can be recognized, even with changing IPs. Honeypots provide additional insights.
Ralf Schneider: What is decisive is the interplay of technology, context, and pattern recognition. Intent does not reveal itself in a single event, but only through the overarching real-time analysis of many attacks.

How do you disrupt cyberattacks?

Lars König: Blocking only protects one's own company. Cyber defense only becomes effective through active disruption: sharing information, shutting down attacker systems via providers or abuse reports, and intervening early at the stage of initial access before attacks spread.
Ralf Schneider: Disruption also means attribution. If attacker groups are identified and handed over to authorities, their risk increases significantly. Sustainable cyber defense arises through the interaction of companies, providers, and state actors.

What happens to the intelligence gained and what measures follow from it? What are the concrete results?

Ralf Schneider: Curation is crucial. Authorities do not take action if they are flooded with unstructured noise. But when attribution and patterns are properly prepared, the chance increases that investigative authorities will actually act. In this way, botnets were identified and shut down together with the BKA – having to rebuild tens of thousands of systems hits attackers hard.
Lars König: The process is as follows: collect and group sensor data, analyze the behavior, and build blocklists from it. In this way, companies can be "immunized" in milliseconds. Clustering and honeypots provide curated insights that are passed on to authorities. In one case we were able to hand over a large botnet together with access credentials; the authorities then took it offline.

What role does cooperation with the community, internet service providers, and authorities play?

Ralf Schneider: Collective cyber defense is based on trust. NetWatch shares only genuine attacker data – without customer information and with minimal false positives. This allows the community to open up and scale, which is necessary since attackers also operate as a community.
Lars König: Community creates reach, ISPs enable the rapid shutdown of infrastructure, and authorities are crucial for dismantling entire attacker groups in a coordinated way, not just individual systems.

Where is the boundary between defense and deterrence, operationally and strategically?

Lars König: Defense initially means blocking attacks and protecting oneself. Deterrence begins where attacker infrastructure is actively removed and their costs and risks are systematically increased. Many threat intelligence approaches stop at indicators. NetWatch goes one step further so that attacks are not only repelled locally but stopped for everyone.
Ralf Schneider: An additional deterrent effect arises through identification. When perpetrators or groups are publicly attributed, their personal risk increases massively. For professional hackers this is particularly painful and makes further operations considerably more difficult.

What is the biggest blind spot of companies when it comes to cyber resilience?

Ralf Schneider: The biggest blind spot is the "unknown unknown" – the unpredictable. This can only be addressed with continuous, flexible, and creative threat hunting, beyond checklists and standards.
Lars König: In addition, there is a lack of speed. Companies often react too slowly, while attackers are extremely fast through AI and automation. Proactive, automated isolation on suspicion is culturally not yet established.

How much openness is sensible for companies – and when does it become problematic?

Ralf Schneider: Attacker data such as malicious IPs can be shared well as long as they are passed on in a controlled manner. It becomes problematic when information helps attackers change patterns or exploit vulnerabilities. Com- ›

pliance sets clear limits here: personal data and internal processes must not be shared.

Lars König: It is important to share attacks that have already been repelled at the perimeter. These data can be used in a scalable way and enable correlations. Deeper incidents belong only in very trustworthy circles – too much visibility can also attract new attackers.

Where does the responsibility of individual companies in cyber defense end – and from when does it become the responsibility of state authorities?

Ralf Schneider: As soon as it concerns investigations, prosecution, or interventions in external systems, the responsibility of companies ends. Hackbacks and attribution can only be carried out by state authorities. For this they need curated, prioritized data instead of raw data volumes.

Lars König: Authorities are indispensable as soon as criminal actions are involved. NetWatch provides them with insights into real attacks on companies – a perspective they otherwise hardly have – and makes international cooperation effective.

What role should large companies play in a European cyber defense ecosystem? And what new responsibility does this create for boards and executive management?

Ralf Schneider: Cyber defense is a matter for top management. Large companies must build their own cyber expertise and actively network in communities. Cyber defense cannot be outsourced; leadership must enable and promote networking across company and sector boundaries.

Lars König: Boards are responsible for allowing speed and cooperation. With millions of attacks daily, automated real-time data exchange is needed instead of slow reporting. Security teams must be visible and allowed to exchange information – without alliances one remains isolated.

In your career, was there a specific moment, an incident, or a decision where it became clear to you: "Cybersecurity is more than just an IT issue"? What did that moment change for you?

Ralf Schneider: Yes. 2013 was the turning point: the tapping of Angela Merkel's phone and shortly afterwards the Snowden revelations. That was when it became clear to me what a powerful instrument cyber is – and that criminal actors would develop similar capabilities. Unfortunately, this assessment has since proven correct.

Lars König: For me it was the vulnerability in the Java library Log4j at the end of 2021. Within a few hours after the publication, the internet was being scanned automatically. We had to think like attackers in order to be faster. That showed me how large the unknown unknowns are – and that speed and creativity are more decisive than classical hardening.

Ralf Schneider: In the association Cyber Security Sharing & Analytics (CSSA) we shared the Log4j script developed by Lars' team. Other companies were immediately able to find their own vulnerabilities with it. That showed very concretely: community is not a buzzword, it immediately prevents damage.

Lars König: And this will become even more important. AI increasingly finds vulnerabilities automatically. These capabilities will spread quickly. Then seconds decide – because without real-time sharing the first wave of attacks cannot be stopped.

What was the most difficult decision for you personally – not technically, but humanly or organizationally?

Lars König: Building the team. Do you need experienced experts with firm opinions or young talents with great potential? Both have advantages and disadvantages. The right mix is difficult to find, and frustration on both sides is almost inevitable. Maintaining this balance is a permanent leadership task.

Ralf Schneider: A crisis decision, for example with the "Heartbleed" security vulnerability: it was about bringing together only the real experts, beyond all hierarchies, contrary to all rules. If it had been a false alarm, I would have felt massive consequences. Fortunately it was not. But such decisions are humanly difficult. ■

Don't Be a Bot!

Newsletter/human LIVE

human-magazin.de

The new print edition will be published on May 30, 2026.

04_ Governance

Controlling Power, Building Trust

"Intelligence services must be controlled, because they are instruments of the executive."

Prof. Dr. Anna Daun, Germany

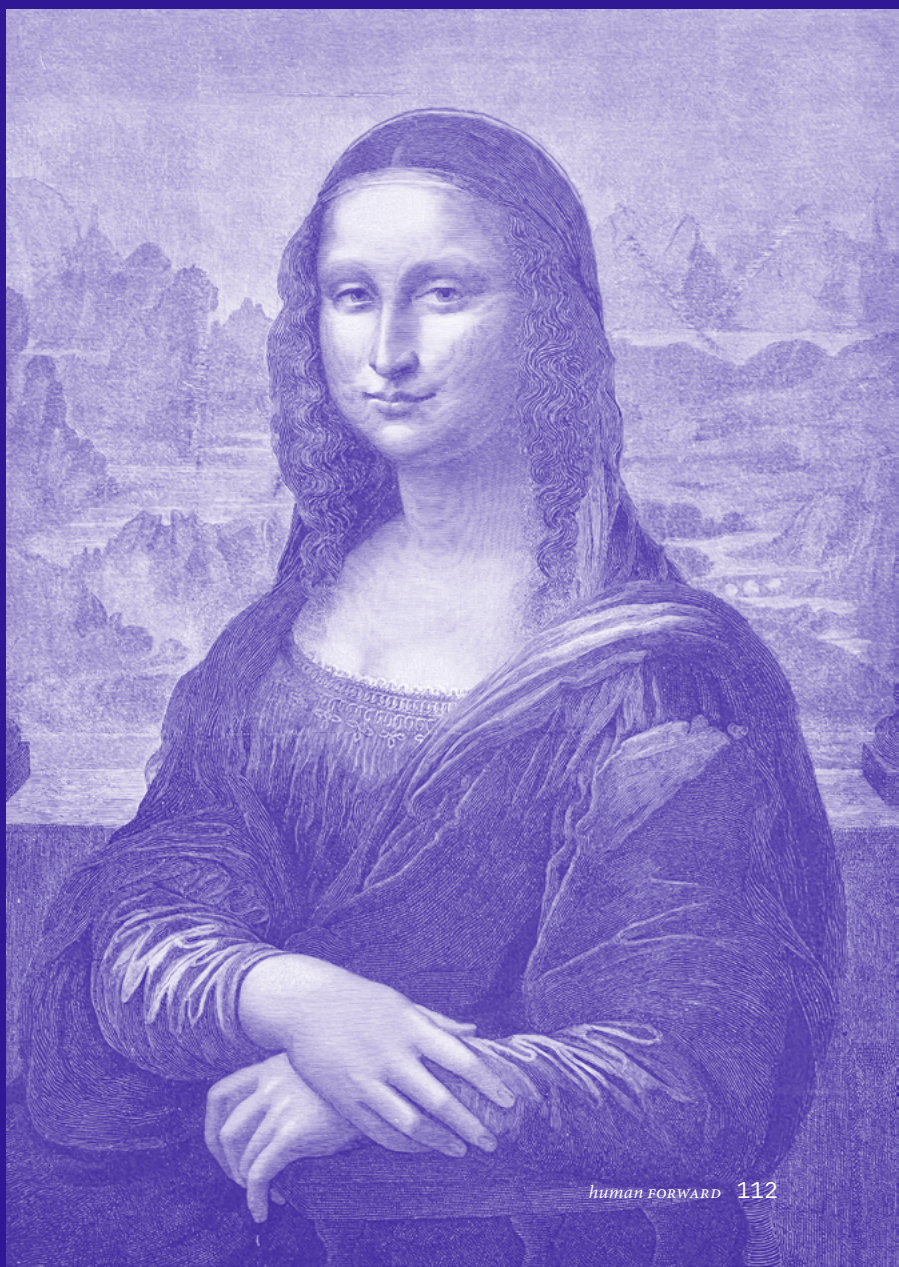

Illustration clu/iStock

"The World Is Not Waiting For Us"

The Green Party member of the Bundestag Konstantin von Notz is regarded as one of the leading experts on the German intelligence services. A conversation about offensive cyber operations, our dependence on the United States – and the role of the services for democracy.

Photo Stephan Pramme

"Because of the experience of two dictatorships we have a special relationship with intelligence services."

Konstantin von Notz

Konstantin von Notz, when you look at the current global situation: what goes through your mind as a long-time overseer of the German intelligence services?

The first thing that comes to mind is that we are living in rough times in which one needs well-functioning intelligence services. Our world is shifting massively in geopolitical terms and is under enormous pressure. Much revolves around intelligence, that is, the question of what one knows, what one understands and what one can forecast. That is why it is important that we have good services that are well connected internationally and have strong partners. The discussion we are having in Germany about the significance of the Zeitenwende ALSO for the services is absolutely right in light of the current confrontations.

You have been dealing with the parliamentary oversight of the services for almost ten years. What have you learned during this time about why we need intelligence services at all, especially as a Green politician with a particular focus on democracy and civil liberties?

Because of the experience of two dictatorships we have a special relationship with intelligence services. Of course they also played a role, particularly during Germany's division. Today the services operate domestically before the police become responsible, constitutionally clearly separated, with limited powers to observe extremism in all its manifestations. Today right-wing extremists openly strive for political power in order to destroy our liberal democracy. That changes the debate. When the domestic intelligence service says it protects our constitution, then that is obviously urgently necessary in view of very serious internal and external threats.

How has the Zeitenwende changed your view of the services?

Even before the full invasion of Ukraine we saw aggressive actions by Russia and also China. This open aggressiveness was visible, also and especially at the intelligence level. Parliamentary oversight is about whether law and statute are being observed. In light of the changed global situation, however, it is increasingly also about whether the services are fulfilling their mandate: Do they protect the constitution and the interests of Germany and Europe? Does the BND obtain the necessary insights in order to better ward off threats from abroad? Is politics informed in time about current developments?

Do you agree with the authors Katja Gloger and Georg Mascolo ("Das Versagen") that our services actually delivered well in the case of Russia – and that the "failure" lay more on the political side?

I would agree with that. The services saw the problem early and addressed it clearly again and again. But the failure certainly did not lie only with political decision-makers, but also with parts of business and the media. For a long time people deceived themselves and ›

INTERVIEW_ ***Konstantin von Notz***

Dr. Konstantin von Notz is a member of the German Bundestag (Alliance 90/The Greens) and Deputy Chair of the Parliamentary Oversight Panel, which supervises the three federal intelligence services: the Federal Intelligence Service (BND), the Military Counterintelligence Service (MAD), and the Federal Office for the Protection of the Constitution (BfV). Among other roles, he served as Chair of the "NSA" Parliamentary Inquiry Committee and as a member of the "Berlin Breitscheidplatz" Inquiry Committee. Since 2017, he has been a member of the Parliamentary Oversight Panel, which he chaired from 2021 to 2025.

KEY MESSAGES

→ **Turning point for the services:** In a more conflict-ridden world, capable intelligence services are becoming increasingly important for political decisions.

→ **Russia:** Services warned early, but politics, business and the public long underestimated the threat.

→ **Cyber deterrence:** Offensive cyber capabilities are conceivable – but only with clear responsibilities, legal rules and strict oversight.

→ **Digital dependencies:** Europe's strong dependence on US technologies and platforms weakens strategic and technological sovereignty.

→ **More European cooperation:** Joint analyses, a situational picture of espionage and sabotage, and closer partnerships among services are becoming more important.

glossed over many things. When one looks at China one sees similar debates. In some cases arguments are still made naively, for example when installing technology or regarding questions of digital sovereignty. And we are also continuing to rely on Palantir.

How do you assess the current process of reforming the services?

The debate about whether the services need adjustments in view of Russia's aggressive behavior and changing partner dynamics with the United States is justified. There is pressure for change, also within a clearly constitutional framework. Regarding the BND I can understand certain expansions with clear guardrails. The expansion to the domestic intelligence service, however, I consider constitutionally very difficult. If we want to act quickly, we should do what is constitutionally possible and what democratic majorities can be organized for. We are available for these debates.

Let us stay with the foreign intelligence service. How do you assess the statements of the new BND president Martin Jäger at the Munich Security Conference that the service must also become more "operational" with regard to hybrid attacks, keyword "active countermeasures"?

I think this must be discussed seriously. Germany is the third-largest economic nation in the world, the economically strongest and most populous country in Europe. One cannot permanently afford the luxury of saying that when things become difficult the Dutch or the British should do it. That position does not hold. At the same time, with regard to the current proposal of the federal government we have concerns that it creates the legal as well as the political clarity that is urgently needed.

To ask concretely: are you in favor of offensive cyber operations?

With certain safeguard mechanisms I can imagine that. So far we have always said that the defense against cyber measures is problematic above all because attribution is difficult. In the meantime there are cases in which the attribution is relatively clear. At the same time we see that the federal government in some cases cannot even agree on whether the Federal Police or the BKA or the BSI (Federal Office for Information Security) should be responsible. If the BND is then added, it becomes even more difficult. But we will not say no across the board. Even in opposition we examine such proposals carefully and along constitutional requirements. If it is possible within the framework of the free democratic basic order, one can talk about it.

Especially with offensive cyber measures the question arises how close this comes constitutionally (Article 26 Basic Law) to an attack...

Absolutely. We have always emphasized that, especially when attribution is difficult, for example when servers in third countries are used. But if such powers are discussed and regulated by law, one can clearly write rule-of-law conditions into them. It is not about making things impossible, but about robust and legally secure regulations.

To what extent are offensive cyber capabilities about deterrence?

On the one hand one must be able to do it in fact. On the other hand one must also signal that one can do it. Otherwise we will continue to be attacked every day. Germany is one of the most targeted countries in the world. That has to do with our prosperity, with deficits in protection, but also with a lack of retaliatory capability. That must change.

"Germany is one of the most targeted countries in the world."

Konstantin von Notz

What role does our technological dependence play in this, especially on the United States?

That is an enormous problem. For years we have been discussing dependencies in social media, Huawei technology in mobile networks, critical infrastructure or American software for our security authorities. The federal government hesitated for a long time to set clear criteria. In energy issues there was a reaction, but especially in the digital sphere we are late. Germany is strongly dependent, and that can quickly become existential. We must reduce these dependencies – with clear political guidelines, legal rules and clear participation quotas. The Ministry of Economic Affairs is now looking more closely, but from our point of view still not sharply enough.

What does that mean concretely with regard to dependence on US technologies? What can we still do here at all? ›

We must focus on our own strengths. Just as we did with regulation with the Digital Services Act and the EU General Data Protection Regulation. As an economic area with 450 to 500 million economically strong consumers we are a relevant market participant with real impact. From this it follows that we must not make ourselves completely dependent in central digital areas. That means we must talk about which platforms of our own we can create. I stand behind public broadcasting. But with around eight billion euros per year one must certainly ask how we transfer that into the digital world and secure diversity of opinion there. One can demand this discussion...

Do you mean that we should invest the funds for public broadcasting better in a digital platform?

I would not say that so categorically. But digital sovereignty also means promoting and modernizing our own structures. It is legitimate to ask how much has flowed into real digital infrastructure in the last ten years. The question must be allowed: do we not need a European platform? It cannot be that the richest man in the world decides tomorrow to switch off a network or massively strengthen certain political forces. Public broadcasting historically also emerged as a response to Gleichschaltung. Have we taken the necessary reform steps to arrive in the digital world? I would say no.

Would that be something like a public-service concept for the digital space?

Yes, why not? A platform is not rocket science. China is also rolling out its offerings strategically. We are the third-largest economic nation in the world with 84 million people. Thought of in European terms, that is an entirely different dimension. But one must break out of the old rut. In recent years that has been lacking. Now the global development is forcing us to act.

What does European intelligence sovereignty mean to you? Joint analyses, a European situational picture, perhaps even a European service?

We coined the term "Euro Eyes", because until now people have only ever talked about the "Five Eyes". But even there the situation has become more difficult. Canada, Australia and also the United Kingdom are irritated by the actions of the current US administration. At the same time the strength of services depends on access to network nodes and infrastructure. Europe has weight here, but uses it too little. If we want to assert ourselves, we need closer and better cooperation among friendly services. Security and intelligence services are core areas of state sovereignty; integration is particularly demanding here. But if Europe does not only want to react, it must act more decisively.

Should that be an EU project or rather a coalition of willing partners?

One has to think in stages. First one needs suitable partners. Close cooperations already exist; these can certainly be expanded. If an integration module later emerges from this, all the better. But we should not first spend 37 years working on the perfect solution. We must start acting. The sharply increased threat situations demand that. The world is not waiting for us.

Back to the national level. How can communication between politics and the services be improved?

In Germany we still do not have a unified situational picture of espionage and sabotage, not of spying on critical infrastructure either, and certainly not one that is communicated publicly. Actually we would need a European situational picture, ideally weekly. People should be able to understand what is actually happening: espionage everywhere, sabotage on rail tracks, destroyed power pylons, break-ins into barracks. Instead everything remains diffuse. Every drone overflight seems nebulous, every incident is relativized. Clear categories and systematic classification are missing that would make developments visible. In Bundestag hearings the situation is indeed described as critical, but that hardly gets through. At the same time some parties trivialize the threat. Governments too have failed to clearly name the problem publicly.

How can politicians build a better, more dialogical relationship with citizens?

Of course something has to happen communicatively, because many people feel that something is fundamentally wrong. But we are a representative democracy: the basic principle is that you elect someone who makes policy for four years. If he does it well, he is re-elected; if not, then not. Digitalization and social media create the impression of permanent real-time politics; that is highly susceptible to populism.

What do you mean by that?

Many political decisions are extremely complex and require many preconditions. On the street many things sound simple and plausible, for example the idea that an application should automatically be approved if the authority does not respond within three months. But if you apply that to license plates, gun permits or building applications in a nature reserve, you quickly realize that it is more complicated.

So what can politics do at all about the ›

dissatisfaction of many citizens?

It is interesting that this frustration with politics exists in almost all Western democracies, regardless of who governs. We have experimented with citizens' councils in order to strengthen participation. But even there results were questioned when they did not fit politically. Citizen participation should be expanded and the transparency of state action increased. At the same time there needs to be realistic expectation management. People elect professionals so that they do not have to deal with all the details every day. In the end they can deliver a harsh judgment.

And despite all criticism we should not talk things down more than they are. Yes, there are problems. But we live in prosperity and great security. In global comparison Germany is anything but a banana republic. I advocate conducting a more confident and positive discussion about Europe as well, especially in comparison with authoritarian systems.

Can intelligence services take on a more active role in democratic discourse beyond their classical task, especially in today's information environment? For example through a public situational picture?

I consider that sensible. In other countries intelligence is handled much more openly – with success. Not every piece of information has to remain secret. There are findings that are relevant to the public and that have a societal added value if they are made transparent. A situational picture of espionage and sabotage would indeed be shaped both by police and intelligence services, but one could bring it together. In Berlin there have been public hearings of the presidents of the services in the Bundestag for years, available online. Very clear warnings were recently formulated there – for example regarding the Russian threat.

Which warnings do you mean?

"The services can indeed contribute to democratic discourse with their findings."

Konstantin von Notz

The president of the BND has said, for example, that he assumes Russia will attack NATO before 2029. That is a grave statement. He does not say that this might perhaps happen, but that he assumes it. And he does not say that based on a gut feeling, but on the basis of the findings of his service. Sometimes I am surprised how little such information is really discussed in the public. In that respect the services can indeed contribute to democratic discourse with their findings. Not as the only voice, but as an important part of the discourse. There is still room for improvement.

Does the culture of the services also have to change for that? A social media campaign by the BND to recruit new staff and testimonials for the 70th anniversary of the service will hardly be enough...

I find that a bit strict. Today there is significantly more openness and exchange. Services discuss publicly, networking with academia has grown. Of course they remain intelligence services; total transparency would be nonsensical. But the attitude has changed. They see themselves more strongly as part of democratic society, recruit at fairs, talk with young people and seek dialogue with civil society. The Snowden revelations and the failure surrounding the NSU have also triggered important learning processes. Certainly not everything is perfect, but the development is quite positive.

How do you look at the Snowden affair today?

We have always said that the question of whether Snowden is a traitor or a hero does not lead anywhere. He himself said that he broke laws and would face proceedings. The real question is whether he is being permanently prosecuted on the basis of a law from 1907 without adequate possibilities of defense. From today's perspective it also remains, for me, that it was a political failure to leave this symbolic triumph to Putin. In my view that could have been avoided.

How?

I think a way could have been found. Not by saying that everything was legally fine, but by placing it politically in context. No democratic service in the world continued to work unchanged after the Snowden revelations. So he undoubtedly had a point. That cannot be argued away. At the same time it is problematic that he continues to sit in Moscow and is instrumentalized. With

Julian Assange I see it differently; there Russian services played a role early on in my view. With Snowden the publication came first, then the political use. One can never know for certain. But that is my assessment.

You have been dealing intensively with intelligence services for many years. Does one develop a certain personal affinity?

When you deal so intensively with services, that naturally rubs off. You get to know the work in the authorities, speak with employees, understand procedures, risks, strengths and weaknesses. Much that was previously abstract becomes concrete. But one must never forget one's own role. Our task is oversight. We are supposed to look very closely on behalf of parliament. And we do that. In the last ten to twelve years we have significantly expanded the possibilities of oversight, with around 30 staff members by now. We have carried out very intensive review mandates, initiated changes and repeatedly voiced very critical views publicly, for example on the question of German Bundeswehr pilots training in China. Oversight does not mean closeness, but critical distance.

Is there a central learning from these years of oversight?

I cannot speak about concrete matters. But abstractly speaking, a few years ago we found that the services had dealt too little with Russian activities in Europe and Germany. The role of proxy structures and the aggressiveness of Chinese services were also clearly underestimated. That has now changed considerably. If you see how, for example, the Military Counterintelligence Service has reorganized itself structurally and in terms of personnel, that is an expression of a learning process.

Finally, a personal question: if you yourself worked for a service – would you prefer operational work or analytical work?

I think I would be better placed in the analytical area. That corresponds more to what I bring with me. Although I have great respect for those working operationally. Obtaining information abroad or clarifying complex matters domestically is a demanding and very relevant job. But my strength would probably lie in analysis and evaluation. ■

"You Have to Get Your Hands Dirty"

The separation requirement continues to shape German intelligence services to this day. Intelligence law expert Luca Manns explains why, from a legal perspective, there is no taboo where operational powers become conceivable – and why cyberspace, signals intelligence, and political risk tolerance are decisive.

Luca Manns, what distinguishes the services we have in Germany from "real" secret services?

In Germany, a distinction is often made between intelligence services and secret services, even though no clear-cut criteria exist. The differentiation goes back to historical experiences with the Gestapo and the East German State Security, i.e., authorities that collected information and at the same time acted with police powers. To prevent such omnipotent structures, the separation requirement was established, which traces back to the Allies' "Police Letter." It stipulated that the Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) has no police powers and is not part of the police.

What does that mean in concrete terms? What are the BND and the Bundesamt für Verfassungsschutz allowed to do, and what are they not allowed to do?

Today, the separation requirement is anchored in all intelligence service laws. However, the majority of legal scholars assume that it does not have constitutional status. Accordingly, in its security law rulings, (the Federal Constitutional Court in) Karlsruhe has not based its decisions on this principle but has instead invoked the proportionality principle of the Basic Law and derived from it an informational separation principle: intelligence services may collect information under lower thresholds, but may not exercise operational follow-up powers on the basis of it. In the words of legal scholar Christoph ›

INTERVIEW_ ***Luca Manns***

Luca Manns is Managing Director of the Research Center for Intelligence Services at the University of Cologne. The legal and economic scholar regularly publishes in legal journals, advises government bodies as well as parliaments. In addition, he is involved in establishing the Adenauer School of Government at the University of Cologne and teaches law of digitalization.

KEY MESSAGES

→ **The separation** requirement stipulates that the Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz) has no police powers.

→ **Intelligence services** may collect information under low thresholds but are legally strongly limited regarding operational follow-up powers.

→ **The reform debate** aims at new capabilities in cyberspace, such as hack-backs and digital disruptions in response to hybrid threats.

→ **Legal authorizations** alone are not sufficient: lacking operational capabilities, personnel deficits, and pronounced risk aversion reduce effectiveness.

→ **Modern intelligence** requires powerful signals intelligence, temporary data retention, and the fundamental-rights-compliant use of AI-supported analysis.

Photo Universität zu Köln

Gusy: "Those who know (almost) everything should not be allowed to do everything; those who are allowed to do (almost) everything should not know everything."

What is the current debate about reforming intelligence law about?

The President of the Bundesamt für Verfassungsschutz, Sinan Selen, has repeatedly emphasized that in today's world, merely detecting threats is no longer sufficient; disruptions by "defensive services" are also needed. This assessment is intended to result in expanded powers, which, in the case of the BND given its military mandate, would go even further than for the Bundesamt für Verfassungsschutz.

Which operational powers would be legally conceivable?

We are certainly not talking about targeted killings or similarly serious interventions. Primarily, the focus is on cyberspace, because digital threats have increased massively. The damage to the German economy caused by hacking is enormous, and the same applies to attacks on public authorities. Combined with disinformation campaigns, this constitutes a form of hybrid warfare. In the future, the BND and the Bundesamt für Verfassungsschutz want to intervene themselves, that is, stop ongoing attacks and, if necessary, destroy adversarial IT systems.

Why specifically on the internet?

In constitutional jurisprudence, the already mentioned criterion of operational follow-up powers plays an important role. If a state intervention classified as operational follows an initial intelligence measure, high thresholds suddenly also apply to that first step. Hacking on the internet, however, unlike an arrest, to which one must legally submit, is not subject to a logic of command and coercion and therefore should only rarely be assessed as operational. On the net, there is no territorial monopoly on the use of force.

And when it comes to measures in the real world, what would you say?

Here we are speaking more about the BND, because domestically, the police authorities stand alongside the Bundesamt für Verfassungsschutz. The foreign intelligence service would now like, for example in crisis situations, to be able to sabotage infrastructure. Think of military facilities or fiber-optic cables of adversarial intelligence services. It is clear that these considerations extend further into what proponents of the traditional separation requirement dislike, and that they will be more legally contentious.

Wouldn't "hackbacks" already fuel escalations with other states?

Theoretically yes. In practice, I consider the risk to be lower. We are living in a hybrid conflict situation. States like Russia or China already assume that hacking back will occur, because they are themselves constantly firing at us digitally. In this respect, "hackbacks" differ significantly from territorial interventions.

As we understand it, here is always a residual risk involved. Why?

That is inherent in the nature of the matter; no law can eliminate this uncertainty. In the end, the use of intelligence services is a political risk decision, for which the law sets the outer boundaries.

Are our services even capable of more?

That is a legitimate question. Think, for example, of computer network operations, which is what the BND calls hacking hostile computers. Operationally, the service has so far not achieved everything it is already currently permitted to do. Legal authorizations are not sufficient if competence and personnel are lacking. In other areas, such as signals intelligence, it is indeed legal hurdles at which the BND fails.

"The BND has by no means operationally succeeded in everything it is already currently permitted to do."

Luca Manns

The world is changing rapidly, from new technologies to geopolitical upheavals. How can intelligence services keep up?

In departure from the "combative administration" of the Third Reich, the German services are strongly shaped as administrative authorities. It is positive that, given the new political support, many employees are in a spirit of optimism. Nevertheless, rigid hierarchies sometimes hamper operational effectiveness.

That sounds restrained.

Take the BND: it has a strong staff council, with disputes over working hours or allowances going all the way to the courts. This is an entirely different outfit than, for example, the CIA. In addition, there is a certain German fundamental anxiety. Where the BND has consider- ›

able legal leeway, it does not in every case perform at the highest level.

For example?

In satellite reconnaissance. When the annexation of Crimea began in 2014, the service had to wait for hours for commercial supplies because it had no images of its own. Procurement of the first BND satellite ever has been ongoing for over ten years; it is still not in space.

Does this also apply to human sources?

The BND is not allowed to blackmail anyone. But in poorer countries, money and crooked deals are often decisive for recruiting informants anyway. For that, one has to go out, move in dangerous environments, and get one's hands dirty. Such willingness is structurally less pronounced in the BND than in some other foreign intelligence services. Also because the federal government long shied away from a robust posture. President Jäger has therefore consistently demanded that his own organization must become more "operational" and dare more.

What else needs to change?

The largest, often underestimated lever with regard to the BND is signals intelligence. Classic source work is extremely labor-intensive and often dependent on chance. Recruiting informants in the Kremlin or in the Politburo of the Chinese Communist Party – let's be honest, we are usually not that good. Broad-based technical surveillance is therefore the means of first choice.

Where do we stand there?

At present, the BND must filter data immediately after collection and, if certain protective rights apply or no fed-in selector matches, delete it. There is no temporary storage, as almost all other EU states have regulated. This is an enormous restriction, since targeted inquiries often only occur later, perhaps after a suspected act of sabotage or when a terrorist comes onto the authorities' radar. End-to-end encryption exacerbates the problem, because content data can hardly be read anymore. The new draft law with retention periods of six months for content and 18 months for metadata would be a step toward modern intelligence, and in terms of duration would even remain below the peace-loving Switzerland.

„Procurement of the first BND satellite ever has been ongoing for over ten years; it is still not in space."

Luca Manns

Also in connection with AI analysis?

At this point, I perceive many fears. It is obvious that processing on commercial servers or the use of U.S. tools with an internet connection would violate data protection law. However, it seems to me that our services are sensitized to this. With regard to the protection of fundamental rights, AI can even have beneficial effects if it helps to improve selections and thus present fewer intelligence-irrelevant hits to human analysts, who currently at least briefly review these sometimes very private data. ■

Democratic Self-Defense

How political are the German intelligence services? Legal scholar Jan-Hendrik Dietrich on a possible ban of the AfD and the role of intelligence in a "militant democracy" (wehrhafte Demokratie)

INTERVIEW_ ***Jan-Hendrik Dietrich***

Prof. Dr. Jan-Hendrik Dietrich teaches at the University of Applied Sciences of the Federation in Berlin and at the University of the Bundeswehr Munich. Together with Prof. Dr. Carlo Masala, he heads the master's program Intelligence and Security Studies, is Co-Director of the Center for Intelligence and Security Studies at the University of the Bundeswehr Munich, and serves as chercheur invité at Sciences Po Paris. He is the author of numerous publications on security law.

KEY MESSAGES

→ **Threats are diffuse:** extremism, espionage, and sabotage intertwine, and clear dividing lines are becoming blurred.

→ **The greatest deficit** lies not in powers, but in the restricted exchange of information between authorities.

→ **The informational separation principle** considerably complicates operational threat prevention and practical cooperation.

→ **European dependence** on U.S. services is structural, but can only be reduced through investment and cooperation.

→ **A militant democracy** requires both: rule-of-law constraints and adaptable services in a changing threat environment.

Jan-Hendrik Dietrich, how do you assess the current challenges facing the German intelligence services between geopolitics and the debate over banning the AfD? How does the legal framework need to change, particularly with regard to "genuine" intelligence powers?

The German intelligence services are increasingly under pressure. This is primarily due to the simultaneity of various threats, many of which are diffuse and of considerable intensity. Individual phenomena are often interconnected. The boundary between Reichsbürger and right-wing extremists, for example, is just as fluid as that between extremists and spies. Nor can internal and external threats always be clearly separated.

For the intelligence services, this means constant stress. The only way to cope with the truly immense challenges lies in cooperation among security authorities – both nationally and internationally. The German services – especially the state-level Offices for the Protection of the Constitution (Verfassungsschutzbehörden der Länder) – are comparatively small. They can only fulfill their mandate if they cooperate optimally with others. This requires rapid information exchange, at the national level in particular with law enforcement authorities, and, where appropriate, also with youth welfare offices or weapons authorities.

This is precisely where a major problem lies. The Federal Constitutional Court ›

has set narrow limits on data exchange. The Court assumes an informational separation principle, meaning that data may only be exchanged in exceptional cases. In practice, this sometimes leads to certain difficulties. I will give you an example: intelligence indicating that someone intends to launch a spy drone over a Bundeswehr barracks may currently not be shared with the police. The expected penalty under Section 109g of the Criminal Code is too low to justify an exception to the separation principle. Before we think about new powers, we must first and foremost ensure optimal cooperation among our security authorities. The Conference of Interior Ministers recently advocated examining whether a duty to cooperate in the exchange of information between authorities should be incorporated into the Basic Law. There will be no amendment to the Basic Law. However, this clearly illustrates that problems exist.

What conditions are necessary in order to reduce dependence on U.S. intelligence services in particular?

It is true that information from foreign partner services often contributes to uncovering terrorist attack plans or espionage activities. First of all, it is important to understand that this does not necessarily indicate a weakness on the part of the German authorities. In the case of cross-border threats, there is indeed a certain "burden sharing" among Western services. Sometimes the French services know more, sometimes the British. In comparison with the American authorities, the European services are significantly less capable. This becomes evident simply by looking at budget and personnel resources. Terminating cooperation would therefore never make sense.

However, in order not to be politically vulnerable to blackmail, Europeans must invest much more in their services. Here, too, there is a turning point. At the same time, intelligence cooperation at the European level must be improved. This is not easy, because the EU treaties explicitly exclude matters of "national security" from the European integration process. As a consequence, European intelligence cooperation must essentially be organized outside the European Union unless the treaties are amended.

„German intelligence agencies must not have police powers."

Jan-Hendrik Dietrich

To what extent does German history shape the current status of the German intelligence services, especially from a legal perspective?

You are referring to the crimes of the Gestapo and the Stasi. In fact, the lessons of the past continue to influence the work of the German intelligence services to this day. Legally, this is expressed, for example, in the fact that German services do not have police powers and may not be affiliated with any police authority.

The intention is to prevent a concentration of power at a single point within the executive branch. One might perhaps call this an intra-executive separation of powers.

Moreover, the intelligence services in Germany are subject to particularly dense oversight. We have more oversight bodies than intelligence services. For the three federal-level agencies alone, there are six specific oversight institutions. And this does not even include oversight by the courts and supervisory authorities.

What concrete function do the German intelligence services have within the framework of a "militant democracy" (wehrhafte Demokratie)? Are they primarily analytical early-warning systems – or are they in fact developing into political instruments of defense that themselves participate in defining the boundaries of what is democratic?

Your question touches on a specific facet of the services' work. Essentially, you are asking: "How political are the Offices for the Protection of the Constitution?" Representatives of both left-wing and right-wing extremist groups often argue that the Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz) arrogates to itself a kind of interpretive authority over what is extremist and what is not. That is not correct. The Offices for the Protection of the Constitution observe and document efforts that are directed – whether with or without violence – against the free democratic basic order. The Federal Constitutional Court has consistently clarified what is meant by this. The specification of the free democratic basic order is set out in all federal and state laws governing the Offices for the Protection of the Con- ›

stitution. These authorities observe those who call fundamental rights into question, who do not recognize courts and parliaments, or who call for violent upheaval. They do not do this as an end in itself, but to document such activities for the public. In doing so, they tear away the mask of respectability from some actors. It is obvious that this does not please everyone.

Does the role of the intelligence services change qualitatively when the state no longer sees itself as merely preventively threatened, but as existentially threatened?

That is very likely. Our security architecture still bears the patina of the East–West conflict and transatlantic security guarantees. The war in Ukraine and the recent U.S. security strategies have marked a double turning point. As a result, war in Europe is no longer an abstract thought experiment. For the intelligence services, this changes certain deployment scenarios.

In the event of a defense case, for example, the Federal Intelligence Service (BND) would certainly devote less attention to organized crime and international proliferation. Instead, it would primarily assume its function as a military intelligence service. A shift in perspective is therefore likely to take place. The focus will increasingly move from strategic intelligence to tactical intelligence.

However, that alone will not suffice. The service will have to be granted its own operational powers. Anything else would be naïve. We are talking, for example, about acts of sabotage behind enemy lines or active cyber operations. Under such conditions, a purely intelligence service would become an operational secret service.

Hans Kelsen warned against protecting democracy through substantive defensive measures, while Karl Loewenstein considered precisely this necessary in the sense of a "militant democracy." Which of these positions is more strongly embedded in the Basic Law? Is there an unresolved tension between them?

At first glance, Kelsen may have a logical argument on his side. A democracy that asserts itself – perhaps even by force – against the will of the majority can no longer be a democracy. That is certainly correct. But upon closer examination, such a development is rather what lawyers would describe as a "pathological textbook case." It is a theoretically conceivable scenario, but one that is unlikely in reality. If 35% of voters in a federal state elect a demonstrably extremist party, 65% have still not voted for that party.

For this reason, the Basic Law has established safeguards for democracy and the rule of law. Both are subject, under Article 79(3), to a so-called eternity clause. If extremists come to power by legal means, they can never amend the constitution in this respect. Moreover – and this is a very strong statement of defensive resilience – Article 20(4) of the Basic Law contains an individual right to protect the constitutional order. It states: "All Germans shall have the right to resist any person seeking to abolish this constitutional order, if no other remedy is available."

At the Parliamentary Council on September 8, 1948, MP Carlo Schmid spoke of the "courage to be intolerant" toward enemies of democracy. Is this intolerance today to be understood legally as an exceptional instrument – or as a constitutive element of democratic self-defense that also legitimizes preventive intelligence measures?

I would like to respond with a quote from Goebbels. In 1928, Joseph Goebbels said: "We enter the Reichstag in order to arm ourselves in the arsenal of democracy with its own weapons. We become Reichstag deputies in order to paralyze the Weimar spirit with its own support." The Basic Law has drawn its lessons from this. The constitution and its values must be actively defended against their enemies.

For this reason, an administrative system for the protection of the constitution is today institutionally guaranteed under constitutional law. Articles 73 and 87 of the Basic Law assume that the federal government and the Länder establish authorities for the purpose of protecting the constitution, and that these authorities cooperate closely with one another. The concept of a militant democracy finds expression in this framework. Incidentally, this is also the view of the Federal Constitutional Court. Anyone on the far left or the far right who wishes to abolish the Offices for the Protection of the Constitution should first take a look at the constitution.

A possible ban of the AfD is being discussed controversially. From the perspective of a militant democracy, would such a ban be an expression of state self-assertion – or does it carry the risk of sustainably damaging the political legitimacy of the Offices for the Protection of the Constitution and the democratic order?

A party ban is in any case the ultima ratio of a militant constitutional state. In the history of the Federal Republic, there have, for good reason, been only a few party bans. Democracy includes listening to and also tolerating other opinions. In recent years, the Federal Constitutional Court has made the ›

bottleneck for party bans very narrow. Whether the available information on the AfD is sufficient to justify a party ban must at least be regarded as uncertain. In my view, a failed motion for a ban would not necessarily damage the Offices for the Protection of the Constitution.

Filing such a motion is a political decision to be taken by the Bundestag, the Bundesrat, or the Federal Government. The applicants must substantiate the motion. Only in this context would findings of the Offices for the Protection of the Constitution play a role. The authorities do not prepare expert opinions for party bans. They merely document, in line with their statutory mandate, whether a given endeavor is operating within the framework of the free democratic basic order.

To date, the corresponding classifications made by the Office for the Protection of the Constitution have proven to withstand judicial review. With regard to its classification as a "suspected right-wing extremist case," the AfD has so far lost before the administrative courts.

Would it be legally permissible under Section 3(1) of the Federal Office for the Protection of the Constitution Act (BVerfSchG) or Section 1(2) of the Federal Intelligence Service Act (BNDG) for German intelligence services to observe activities by the United States aimed at actively supporting the AfD?

The Office for the Protection of the Constitution observes the AfD as a confirmed extremist endeavor. The scope of this observation also includes identifying who supports the party and in what manner. Of interest, for example, is the origin of financial resources. Public statements by supporters are also taken into account. All of these are pieces of a mosaic that together form an overall picture of the need for observation. In principle, it initially makes no difference where the support originates. It is documented and analyzed regardless of whether it comes from Russia, the United States, or elsewhere.

The situation is somewhat different for the Federal Intelligence Service (BND). The BND collects information of foreign and security policy significance in relation to the Federal Republic of Germany. This may also include determining which foreign states or organizations are engaging openly or covertly in political activities in Germany.

"Glossy brochures or punchy slogans are of no help."

Jan-Hendrik Dietrich

Is the classic framework of a militant democracy still sufficient for today's threat landscape – or, in light of hybrid threats and online radicalization, should we rather speak of a "resilient democracy"? Might this also entail a European perspective?

It is true that some traditional instruments of militant democracy fall short in the information society. Take, for example, the reports of the Offices for the Protection of the Constitution. Their purpose is to provide professional classification, objective justification, and documentation when an endeavor calls fundamental values of our constitution into question. They still fulfill this function. But who reads them?

Current studies on media consumption behavior show that young people often obtain their information from social media. In this sphere, the gatekeeper function of journalists is sometimes lacking. Many remain trapped in online echo chambers and become susceptible to manipulation. In this respect, I agree with you that protecting our democracy already begins with teaching media literacy to young people. In that sense, resilience precedes militancy.

At the same time, however, the militant constitutional state must also find new formats to reach, for example, Generation Z. Glossy brochures or punchy slogans are of little help – nor, incidentally, is ideological rigidity, such as when employees of the Offices for the Protection of the Constitution, the police, or the Bundeswehr are denied access to schools.

Within the European Union, at least the vulnerability of Western democracy has been recognized. At the end of last year, the European Commission presented a "European Democracy Shield." It will take some time before the measures take effect. But it is a step in the right direction. ■

From Protest to Threat?

There is no clear line between legitimate criticism and extremism. How intelligence services in Europe assess new protest phenomena while seeking to balance security and freedom

"The starting point for the new object of observation," explained Thomas Haldenwang, then President of the Federal Office for the Protection of the Constitution (BfV), on the occasion of presenting the 2021 annual report, "was the highly heterogeneous protest scene against the state measures to combat the COVID-19 pandemic, where conspiracy theories, the stoking of antisemitic resentments, and a massive willingness to use violence against police and regulatory authorities found fertile ground." [1]

The introduction of this "new object of observation" points to two sets of problems: first, the difficulties intelligence services face in capturing the heterogeneous currents of the COVID protests under a single concept. Second, the tightrope walk of viewing ordinary citizens both as a threat and as an object of protection. For the "heterogeneous protest scene" consisted of movements that drew primarily from the center of society – in other words, "perfectly ordinary" citizens participated in numbers and with a speed that had scarcely ever come into the sights of German intelligence services.

How should intelligence services in liberal democracies deal in the future with protest movements that successfully mobilize broad segments of society – and that in some cases turn into extremism or violence? This is not a question for Germany alone; other European countries also experienced protests against measures to combat the coronavirus. How can national experiences be used for European cooperation? ›

[1] *https://www.verfassungsschutz.de/SharedDocs/statements/DE/2022/2022-06-07-haldenwang-vorstellung-des-verfassungsschutzberichts-2021.html* (9 January 2026).

TEXT_ ***Eva Herschinger***

Prof. Eva Herschinger is Professor of Security Studies and Head of the Research Area Security and Intelligence at the Center for Intelligence and Security Studies at the University of the Bundeswehr Munich.

KEY MESSAGES

→ **The COVID protests** forced intelligence services to develop new categories beyond classic notions of extremism.

→ **Movements** emerging from the societal mainstream pose a particular challenge, as protest and threat can intertwine.

→ **The category of "delegitimization of the state"** illustrates the difficulty of sharply distinguishing criticism of government, state, and democracy.

→ **Protest milieus** remain mostly non-violent, but can be partially radicalized through disinformation and extremist actors.

→ **The future** requires European coordination, flexible analytical approaches, and particular sensitivity toward democratic fundamental rights.

PROTESTS: AN OBJECT OF OBSERVATION FOR INTELLIGENCE SERVICES

The protests against COVID measures marked a turning point in many countries. In Germany, they often remained peaceful, but also culminated in aggressive actions – one need only recall the attempted storming of the Reichstag in August 2020. The BfV found itself confronted with a protest movement emerging from the societal mainstream: people who had previously been scarcely politically active – "Mr. and Mrs. Schmidt" – protested side by side with anti-vaccination activists and conspiracy believers, esoteric adherents and right-wing extremists. From the perspective of the intelligence services, a new scene directed against the state emerged, one that could not be classified within existing extremism categories (right-wing, left-wing, or religious extremism). In April 2021, the BfV responded by establishing the phenomenon category „Verfassungsschutzrelevante Delegitimierung des Staates" ("Delegitimization of the State Relevant to the Protection of the Constitution.")

Intelligence services in other Western countries used similar designations to describe the protest movements. The Dutch intelligence service, for example, uses "anti-institutional extremism"; in the United States, "anti-government extremism" is the common term; Sweden opted for "anti-government rhetoric" and "anti-establishment narratives," while at the European level, Europol speaks of groups with an "anti-government, anti-system and anti-institution" stance.[2] The reference to the COVID crisis is the starting point, but not a fixed substantive anchor.

THE CHALLENGE OF DEFINING THE "DELEGITIMIZERS"

With the new category, the BfV records individuals and groups who, through their conduct, seek to undermine the functionality and legitimacy of the state, for example by disparaging democratic decision-making processes and institutions or by calling for the disregard of official orders. This, according to the BfV, contradicts "elementary constitutional principles such as democracy or the rule of law."[3] In view of the heterogeneity of the protest scene, the BfV identified the categorical rejection of the existing state order as the ideologically binding element. Police officers as well as politicians and scientists who supported state measures to contain the virus became targets.

Violent actions against them were stylized and endorsed as legitimate acts of resistance – one may recall, among other cases, the planned kidnapping of the then Federal Minister of Health, Karl Lauterbach. Critics argued that the BfV was conflating criticism of the government with criticism of the rule of law and democracy, while allowing right-wing extremists to blur within the mass of protesters.[4] Delimitation was also difficult in other countries. One example: in the Netherlands, the intelligence service AIVD spoke of "anti-governmental extremism," a designation that already existed before the COVID pandemic. After 2022, the description was changed to "anti-institutional extremism," as institutions such as the police and media, in addition to the government, became the focus of the movements.

Yet the heterogeneity of the scene was and remains not the only challenge for intelligence services in Europe when it comes to definition. Substantively, the protests also remained dynamic – albeit with declining success. As state measures to combat the pandemic were largely lifted in 2022, the issue of COVID lost much of its mobilizing potential. With considerably less agitation, topics such as inflation and energy prices, the rejection of climate change mitigation measures, and the consequences of Russia's war of aggression against Ukraine now dominate.

Over the course of 2025, it became clear that the new category was losing significance. Saxony, for example, decided not to continue using the category from 2026 onward. This does not mean that the actors disappear from the radar of intelligence services: individuals who act in a manner hostile to democracy continue to be monitored, only now assigned to the classic phenomenon categories.

A TIGHTROPE WALK BETWEEN ORDINARY CITIZENS AND EXTREMISTS

Behind the debate about definitions lies another problem: the tightrope walk between treating ordinary citizens as a security risk and protecting them as holders of democratic rights. In democracies, protest is a legitimate expression of freedom of opinion and political participation. But what if a large number of "ordinary" citizens within a legitimate protest suddenly support violent positions and/or demands at the threshold of extremism? It is about the question of what is normal and worthy of protec- ›

[2] *https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf* (22.1.26).
[3] All BfV quotations are taken from the following website https://www.verfassungsschutz.de/DE/themen/verfassungsschutzrelevante-delegitimierung-des-staates/begriff-und-erscheinungsformen/begriff-und-erscheinungsformen_artikel.html#doc1260196bodyText1 (9 January 2026).
[4] See, among others. *https://www.lto.de/recht/hintergruende/h/verfassungsschutz-kritik-extremismus-delegitimierung-verfassung-bericht* (9 January 2026).

tion, what is abnormal and threatening – and how the state should act when both coincide, when citizens who are to be protected suddenly pose a threat.

The reports of the Federal Office for the Protection of the Constitution since 2021 reflect this challenge. On the one hand, it is emphasized that this is legitimate protest by concerned citizens – something normal in a democracy. On the other hand, the BfV states that part of this movement has crossed the "threshold to anti-constitutional endeavors." Thus, some Mr. and Mrs. Schmidt move into the realm of the "abnormal," which in turn is subject to security monitoring.

„Monitoring ordinary citizens can easily lead to accusations of surveilling legitimate opposition."

Eva Herschinger

Drawing on the French philosopher Michel Foucault, one can speak here of an act of classification: by drawing a boundary between "normal" and "abnormal" protest, the reports create a new category that removes these new objects of observation from the sphere of the normal and places them in the field of the abnormal. What lies before this boundary – normal protest – is worthy of protection. What lies beyond it – delegitimizing, anti-democratic agitation – is threatening. A bifurcated discursive space emerges: here the hegemony of what counts as normal – constructive criticism, peaceful protest – there the stigma of the abnormal – anti-constitutional activities, conspiracy-ideological radicalization. Critics point out that in practice, due to the dynamism and heterogeneity of the protests, this delimitation is characterized by considerable ambiguity.

For intelligence services, this tightrope walk requires the utmost care. Monitoring "ordinary citizens" („normale Bürger:innen") is a sensitive undertaking that can easily lead to accusations of surveilling legitimate opposition. At the same time, examples have shown that real dangers can emanate from such heterogeneous movements, especially when extremist groups attempt to instrumentalize the protests for their own purposes. Europol confirms in its terrorism situation report that the majority of anti-government/anti-system groupings remain non-violent, but a minority justifies or exercises violence. This violent core can emerge from initially peaceful protest networks, fueled by online disinformation and conspiracy narratives. Some individuals have radicalized to the point of planning terrorist acts, as thwarted attack plans in various countries demonstrate.[5]

POST-COVID: FUTURE CHALLENGES FOR INTELLIGENCE SERVICES

The experiences of recent years cast light on future challenges for intelligence services in liberal democracies. On the one hand, given the temporal boundedness of the COVID protests, the question arises as to how lasting this phenomenon is. On the other hand, similar dynamics – a sudden alliance of heterogeneous dissatisfied groups, driven by digital networking and disinformation – could reappear at any time.

The next major crisis (be it a pandemic, economic hardship, or a broad societal conflict) could once again lead to protests by wide segments of the population, which might again be infiltrated by extremists or hostile foreign actors. Citizens who once felt treated as objects of observation are more likely to remain mistrustful of state institutions and more easily mobilized again. At the same time, the European level should increasingly come into focus. Europol and other EU bodies have recognized the issue and created exchange platforms, such as expert conferences on "Anti-Government Extremism" and training programs on dealing with anti-system movements.

Thus, a future European intelligence architecture requires exchange and coordination of definitional approaches in order to counter cross-border extremist narratives more effectively. After all, extremist ideologues also operate networked across borders: conspiracy myths are available online everywhere and at all times, and actors such as the QAnon movement or Russian disinformation campaigns influence protest milieus across Europe.

A coordinated European response could help to identify trends at an early stage and develop counter-strategies. However, intelligence services in Europe continue to operate primarily ›

[5] https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf (22 January 2026).

within national frameworks, closely bound to the respective legal systems and democratic oversight mechanisms of their states. Nevertheless, at least a harmonized understanding of terminology in Europe would be helpful and a first step in a common direction: if everyone is talking about the same type of threat, it becomes possible to act against it in a more targeted and united manner.

The experiences during and after the pandemic provide important lessons learned for such cooperation: in the face of dynamic, socially broad protest phenomena, intelligence services need flexible approaches in order to preserve both security and the open fundamental rights of society. One path is European cooperation. Navigating between security and freedom will decisively shape the future of intelligence work in Europe. ■

"Just Do It!"

Between agencies, political leadership, and European cooperation: political scientist Anna Daun analyzes what intelligence services can deliver – and what prevents them in Germany and Europe from being strategically effective.

Photo private

„Intelligence services do not protect democracy as such; they protect state sovereignty."

Anna Daun

Anna Daun, to what extent do intelligence services protect our democracy?

Anna Daun: Intelligence services do not protect democracy as such; they protect state sovereignty. They secure the space in which democracy can take place. Within this protected space, political culture, debates, and democratic processes unfold. In this sense, the services make an important contribution without being democratic actors themselves.

What kind of intelligence service or secret service would you want for Germany and Europe?

First you have to distinguish between Germany and Europe. If we start with Germany, I would keep the fundamental separation between domestic and foreign intelligence. That makes sense. For the domestic service, I would want it to limit itself to what is truly necessary. Less quantity, more quality. In other words, not doing everything, but doing what is really relevant – and then doing it consistently and well. And also being somewhat more willing to take risks than we have seen in the past.

What does "the truly necessary" mean to you?

In the past, I often had the impression that a great deal was collected – many sources, many reports – but in key cases such as the NSU or Anis Amri, the decisive information was not reached. In terms of quality, that was simply not convincing. The Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) should focus on identifying genuine threats to democracy.

Does that mean that collecting material on the AfD, for example, is not part of that in your view?

I did not say that. There is a real problem with democratic core values in our society. But not everyone who expresses themselves in an undemocratic way is automatically a case for the Verfassungsschutz. That is a societal problem, a political one, also an education-policy one. The task of the Verfassungsschutz is to recognize organized efforts aimed at actively overcoming the system.

So the focus is on organized structures?

Exactly. On violence-prone right-wing extremists, coup fantasies, anti-state networks – but above all also on counterintelligence. The influence of external actors is increasing in particular. If there are connections to foreign powers that want to deliberately destabilize our constitutional order, then that is clearly a case for the Verfassungsschutz – but limited to these circles.

And what about extremist statements online?

As problematic as all of this is, it is not primarily the task of the Verfassungsschutz. Much of it falls more within the remit of the police or political contestation. The Verfassungsschutz should, with its special means, penetrate ›

INTERVIEW_ ***Anna Daun***

Prof. Dr. Anna Daun is Professor of Political Science at the Berlin School of Economics and Law (HWR). She teaches security topics in the degree programs for senior police service (gehPVD) and security management, and is Deputy Director of the Research Institute for Public and Private Security (FÖPS).

KEY MESSAGES

→ **Intelligence services protect** state sovereignty and thus the space of democratic politics, not democracy itself.

→ **The Office for the Protection** of the Constitution (Bundesamt für Verfassungsschutz, BfV) should focus on organized, real threats – less quantity, more analytical quality.

→ **Germany's intelligence culture** is historically burdened and strategically underdeveloped, shaped by risk aversion and a weak error culture.

→ **Effective intelligence** needs political leadership, clear priorities, and interdisciplinary analysis beyond classic civil-service biographies.

→ **Europe's security-policy future** requires closer intelligence cooperation – up to and including shared, division-of-labor structures.

deeply into the relevant networks, have sources where the nodes are.

What role should the foreign intelligence service, the BND, play?

For the foreign service, above all I would want it to be well led politically. That is, clear priorities should be set. The service does not need to be everywhere and be able to do everything. It needs strategic focal points that guide its work. And in these fields, the foreign service should then actually be really good. You do not have to cover everything globally yourself; for that there are partner services, OSINT, and also academic institutions such as think tanks.

In Germany, one often gets the impression that the discussion about the services is reduced to the question of powers and oversight. Should the debate not be conducted much more politically? In the sense of the question: what do we actually want these services for?

Yes, I definitely think so. In Germany, this field was long excluded from strategic culture. Security and defense were discussed, but intelligence services were more of a topic people did not like to talk about. Comparatively few people engaged with it. This area was long missing from our strategic culture.

Why was that?

That can be explained historically. Germany is a relatively young nation-state. For a long time, the gaze was directed more inward than outward – unlike older European nations with a colonial history. Then came the bad experiences of National Socialism and later the Stasi. This history cast a long shadow over everything to do with secret services. That probably explains why it was so difficult to engage with it.

Including politics?

By international comparison, intelligence long had little prestige in Germany. Unlike in the United States or Great Britain, there was no pronounced intelligence community. Many employees felt undervalued; chancellors spoke disparagingly; and in academia the topic was barely present. There was little engagement in popular culture, no strong tradition of spy novels, hardly any public figures from this field. Efforts are now being made to change that. The services have become more visible – look at the sleek and enormous BND building in Berlin-Mitte. But for a long time, intelligence was culturally treated as a stepchild.

„By international comparison, intelligence long had little prestige in Germany.“

Anna Daun

How would you describe German “intelligence culture” more precisely?

There are several levels. First of all, the internal level – the bureaucratic culture within the services. There I see, for example, a problem with error culture. But that is not an exclusive problem of the intelligence services; it is part of German administrative culture as a whole. There is a lack of a constructive way of dealing with mistakes. A great deal of energy is spent on making no mistakes at all, instead of focusing on the actual problem.

In the end, the services are also authorities.

Exactly. And that logic operates there in the same way. There is a strong fear of stepping out of line legally or hierarchically. That shapes decisions. This is reinforced by the great weight of lawyers in the authorities, which is understandable given the legal pitfalls, but which leads to risk avoidance often becoming more important than effectiveness.

What kind of interdisciplinarity would you like to see in our intelligence services?

Services are of course organized with division of labor, with engineers, IT specialists, analysts. But especially in the analytical area, it would be very desirable to involve people with very different backgrounds of experience. Not only lawyers or administrative scientists socialized in classic civil-service careers. Different biographies, different disciplines, also career changers. I consider that important.

Which disciplines are you thinking of specifically?

For example philosophers. People who can formulate counter-theses, who do not only think in an adapted way. Self-confident, intellectually independent individuals who do not merely reproduce what is expected. Diversity of perspectives is central to good analysis.

How do you observe the interplay ›

between the services and politics?

For a long time, public discourse was dominated by disinterest or contempt, from Konrad Adenauer through Helmut Kohl to Helmut Schmidt. Whether this was always genuine disinterest is difficult to judge from the outside. Often it is said that the services failed or did not warn, for example in the case of the fall of the Wall or other crises. At the same time, the services complain that their warnings were ignored. There is mutual attribution of responsibility. Whether more exchange took place internally remains unclear.

Take as an example the BND's misassessments regarding the start of the Russian invasion of Ukraine. What follows from this institutionally?

Internationally, a similar pattern emerges: if a service fails, analysis follows, and more resources and powers. That is a bureaucratic automatism; one can see it since 9/11. There is more budget, more powers, but also stronger oversight, which then itself becomes part of the secret. The Parliamentary Oversight Panel is all the less public the more it knows. It thereby moves closer to the logic of secrecy.

Must a democracy accept that an intelligence service is never fully controllable?

Intelligence services must be controlled, because they are instruments of the executive. At the same time, the executive must also be controlled by parliament. Public transparency is hardly possible; oversight remains limited. Within the executive, it operates relatively effectively, but it encounters real limits at the core area of executive responsibility.

In your view, is intelligence an exclusively state task, or can you imagine new forms of partnerships with private actors?

Intelligence in the narrow sense produces exclusive knowledge for decision-makers, which is also classified. That is, first of all, a state task. Of course there are think tanks and private actors who deliver analyses, but that is something different from intelligence work in the narrow sense.

„Given the geopolitical situation, Europe should grow closer together, also in defense."

Anna Daun

How do you view the idea of a European intelligence service?

That´s an interesting question. Intelligence is a function of statehood, but it does not necessarily have to be organized nationally. Given the geopolitical situation, Europe should grow closer together, also in defense. National solo efforts fall short. Since intelligence is closely linked to defense, a European defense structure without shared intelligence is hardly conceivable. I would like us to develop in that direction.

Would that be a project within the EU or outside it?

That has to be politically desired and grow step by step. Whether it is formally an EU project or emerges outside existing structures is secondary. Such structures ultimately arise through political facts, not only through institutional procedures.

One could imagine, for example, that the British, French, and Germans join forces. Something like "Three Eyes" or similar.

Yes, exactly: just do it. Given the situation, that is the only realistic way. The states that want this have to take the lead. There are already close European cooperations in the intelligence field, but real division of labor and mutual dependencies would be a new step. The Five Eyes show how shared priorities create trust and a close alliance.
And it would also be a strong shared project for the future.
Statehood and alliances often arise under pressure. This is now our chance to put things on a new foundation. ■

"Strategy Needs a Vision"

Strategy is not a wish list. Political scientist Holger Janusch on strategic learning, Europe's misperceptions – and democracy as a corrective mechanism.

INTERVIEW_ ***Holger Janusch***

Holger Janusch is Professor of International Politics with a focus on U.S. foreign and security policy at the Department of Intelligence Services of the Federal University of Applied Administrative Sciences (Hochschule des Bundes für Öffentliche Verwaltung) in Berlin, with research focuses on national security strategies, U.S. trade policy, and power in theories of International Relations. He curated the special volume "Integrated Security for Germany?" (2025).

KEY MESSAGES

→ **Strategy is a Theory of Success:** It is based on verifiable assumptions about how means generate effects.

→ **Strategic Intelligence** examines and falsifies these assumptions – it is more than trend extrapolation.

→ **Europe's central misjudgment** was taking U.S. stability for granted.

→ **Norms and legitimacy** are strategic resources; power without recognition undermines long-term success.

→ **Democratic diversity and open debate** are not a disadvantage, but a strategic corrective mechanism.

Why do states need a strategy?

Holger Janusch: Strategy is fundamentally important. It is about deploying means effectively to achieve objectives, ideally with a medium- to long-term horizon. It becomes problematic in the field of security where success is hardly measurable. Unlike in companies, there are no clear metrics such as profit or market share. Therefore, it is difficult to say whether a strategy was "successful" or whether other factors were decisive.

What must such a "Theory of Success" contain?

Every strategy is based on assumptions about the future and about causal relationships: If certain means are employed, a certain effect is expected to occur. Deterrence, for example, is based on the assumption that a threat will prevent the adversary from acting. But it can also produce the opposite effect. A Theory of Success forces one to make these assumptions explicit, to question them, and to examine whether they are empirically or logically sound. At the same time, it must be clearly defined what counts as success at all. A Theory of Success encourages getting more out of the available means than was initially expected.

Every strategy is based on implicit assumptions about adversaries, allies, and system dynamics. What role does Strategic Intelligence play in this context?

If we understand strategy as a Theory of Success, we are talking about assumptions and hypotheses about the future. Strategic Intelligence has precisely its core function here: it is meant to examine these assumptions, to unsettle them, and – if necessary – to falsify them. It is not about operational targeting, but about long-term, structural questions: How are power, ›

technology, alliances, political cultures changing? Which trends are stable, which volatile?

So Strategic Intelligence is more than extrapolating trends?

Exactly. Pure extrapolation is of little use. More meaningful are scenario analyses, net assessments, or other forms of strategic foresight. The goal is to compare and evaluate competing hypotheses: Which theory about the future is most plausible given the available information? This creates the foundation for deploying means sensibly over the long term.

From a European perspective, where were there strategic misjudgments in dealing with the United States?

For decades, a central assumption was that the United States would remain a reliably stable security partner. This assumption could have been questioned earlier. There were warning signals: the burden-sharing debate, growing domestic polarization since the 1990s, increasing volatility in foreign policy. Strategic Intelligence could have given these developments greater weight and more clearly identified their strategic implications.

Is Donald Trump primarily unpredictable for you – or strategically consistent?

Both. There are recognizable patterns: transactional thinking, zero-sum logic, maximum threat as a negotiating tool. What is new in the second term is a stronger neo-imperial thinking in spheres of influence. It becomes unpredictable where material interests, cultural-normative threat perceptions, and geopolitical logic exert varying degrees of influence depending on the situation. Strategic Intelligence can make these patterns visible – but cannot precisely predict which will dominate when.

„When actors no longer believe that rules generate benefits, an order begins to erode."

Holger Janusch

There is often talk of the "end of the rules-based order." What exactly does that mean?

At its security-policy core, this initially refers to the UN Charter: no military aggression, respect for sovereignty and territorial integrity. In addition, there are other regimes – for example in maritime law or global trade. Rules have always been violated. The decisive question is from what point norm violations become so frequent that norms lose their binding force. When actors no longer believe that rules generate benefits or that others will comply with them, an order begins to erode....

What role does the Trump administration play in this?

A central one. If precisely the hegemon that helped build and enforce this order openly questions fundamental norms – for example territorial integrity with regard to Greenland, Panama, or Canada – then that is qualitatively different. Whether one should already speak of a collapse of the order is disputed. But the erosion is clearly being accelerated.

Is this only about formal rules or also about informal norms of conduct?

Definitely also about informal norms. In regime research, a distinction is made between principles, norms, rules, and procedures. The more abstract the level, the more fundamental their significance for order. If not only rules but also fundamental norms and principles of the recognition of sovereignty and the non-violent settlement of conflicts are violated, then the entire order becomes more unstable, even beyond formal treaty breaches.

What options does the weaker party fundamentally have vis-à-vis a stronger party that breaks norms?

Purely by definition, the stronger party can prevail – otherwise it would not be the stronger one. But military strength is often deceptive. Conflicts such as Russia–Ukraine or the United States in Vietnam show that short-term enforcement does not automatically mean long-term strategic success. The real strategic question is: Does the right of the stronger lead to stability in the long run, or does it undermine one's own position?

Does more than military power play a role here?

Absolutely. Normative factors, legitimacy, and international recognition are central. Even very powerful actors need justifications – domestically and internationally. The Trump administration also encounters limits, for example regarding Greenland or migration. ›

Strength alone does not replace legitimacy. According to Antonio Gramsci, the use of force is a sign of lacking hegemony, that is, insufficient acceptance of an order of rule.

What distinguishes democracies strategically from autocracies?

Autocracies can often bundle and deploy means more quickly. Democracies, by contrast, appear slower and more fragmented. The strategic advantage of democracies, however, lies in open discourse and corrective mechanisms. Strategies are based on assumptions about the future – and democracies have better preconditions for recognizing false assumptions and adapting strategies.

Many see the European reaction to the Greenland debate as a turning point. Your assessment?

In the short term, it was a success. Whether a tougher stance toward the Trump administration will always lead to better results, however, cannot be said unequivocally – the risk of escalation remains. Strategically important, however, is to demonstrate determination. The Trump administration clearly signals: strong, capable partners are taken more seriously. Europe is currently perceived as weak, but with potential.

What role do values play in strategies?

Values are indispensable. They are central for motivation, legitimacy, and societal acceptance – especially in democracies. People do not act for abstract interests, but for the protection of a particular order. At the same time, pragmatism is required. Values must not become mere moral rhetoric. A viable strategy must internalize values without denying reality.

In your understanding, values would therefore not themselves be the goals, but would have to be operationalized through a clear Theory of Success – for example: What does it concretely mean to preserve values?

Exactly. Here I would distinguish between Theory of Success and another strategic element: the vision. A vision connects ambitious objectives with a clear value base. It provides the big picture, defines what success actually means, and has a motivating effect – internally and externally.

How important is learning and adaptation?

Very important. The environment is becoming ever more complex and dynamic, especially due to technology. At the same time, technology opens up new possibilities: more data, faster evaluation, earlier feedback. A modern strategic process therefore itself requires a strategy for dealing with strategy – that is, for learning, adaptation, and continuous review.

That almost sounds like a visionary intelligence task.

It is. Intelligence has so far often been strongly operational-tactical in orientation. The strategic collection and classification of information, that is, thinking in longer-term patterns, interactions, and future scenarios, falls short. This is not a specifically German feature, but also a frequently voiced criticism in the United States.

Would Europe need something like a genuine all-source intelligence for this?

At the very least, this question would have to be discussed strategically. Which sources are really relevant for which types of conflict? Where do technological means provide more insight than classic HUMINT – and vice versa? That alone is already a strategic decision about means and efficiency.

And at the European level?

There the question of cooperation additionally arises: Which synergies are realistic? Where is a division of labor worthwhile? And how robust is trust between states? A vision could be a European all-source model – like a "Twenty-Seven-Eyes" approach. This is not automatically the right solution, but given limited resources it is obvious. National services have comparative advantages that could be better pooled.

Do we need a new strategic culture?

Yes, strategic culture is often demanded, also for Germany. It is frequently equated with strategic thinking. Strategic culture refers to the narratives, symbols, analogies, and assumptions about how means – especially force – work in international politics. From this, strategic preferences are derived. Strategic culture is important, but it is always associated with bias. In the US in particular, a certain strategic culture has in the past contributed to serious misjudgments. Therefore, close, critical exchange between different strategic cultures can be a real advantage.

So diversity as a strategic resource?

Exactly. Different historical experiences lead to different perspectives. Germany's strategic culture is strongly shaped by "Never again," Great Britain looks back on imperial and maritime traditions, other European states have yet other experiences. This diversity can help to question assumptions and reduce blind spots – especially in a common European intelligence or strategy architecture.

What do we need to establish strategic thinking in Germany?

In the end, it requires political leadership that is willing to question its own worldview. Strategies are always ›

also shaped by party politics and ideology. Without openness to criticism, cultural diversity remains without consequence. Often it takes crises or obvious failure before adaptation becomes possible.

Looking at Europe – what is currently your greatest hope, but also your greatest concern with regard to strategy and strategic thinking?

My greatest hope is that strategic thinking is being taken more seriously again. There is increasing recognition that it is necessary to think in a more long-term and systematic way. This can be seen in the fact that strategy papers are emerging everywhere. That alone is not yet a strategy, but it is a signal that something is moving. Now it is crucial to implement these strategies, to review them, and to adapt them.

And the greatest concern?

The greatest concern lies less with people than with structures. In ministries and authorities there are many very intelligent minds. What worries me are path dependencies, routines, silo thinking, and bureaucratic hurdles. These can massively slow down strategic learning and adaptation.

Some have the impression that it is already too late – a certain fatalism.

I do not share that. We are facing serious threats, but not an inevitable downfall. Strategic adaptation takes time. What has grown over decades cannot be changed in months. The Trump administration shows – for all criticism – that it is prepared to radically break up existing structures. Often in an unwise way, but it makes clear: change is possible. Europe should learn from this not the style, but the willingness for strategic rethinking. ■

"In the end, strategic thinking requires political leadership that is willing to question its own worldview."

Holger Janusch

The Swiss Model

Between national interests, a crumbling consensus, and new threats, Europe's security architecture is reaching legal limits. Swiss legal scholar Esther Omlin on neutrality, information exchange, and cooperation beyond classic alliance logics.

Esther Omlin, from a legal perspective, where do the particular difficulties of a European security architecture lie?

Esther Omlin: Legally, international cooperation is always demanding. One needs laws and treaties that are supported by all. The EU has actually created many foundations for this. The problem is that they were long not used for security policy purposes. At the same time, many states are once again focusing more strongly on national interests. The former consensus on which many treaties were based no longer exists in that form. In light of new challenges and changing governments, it would in fact have to be renegotiated.

Against this background, how do you see the current geopolitical situation and the often-invoked end of the rules-based order?

As a lawyer, I struggle with this term. This order was strongly shaped by American interests. It was not our order. Therefore, I do not see it as entirely negative that the term is losing significance. Sanctions, for example, are instruments of foreign and domestic policy. If one adopts foreign rules without reflecting on one's own interests, no equilibrium emerges. I see this rather as an opportunity to reposition oneself, both at the European and Swiss level.

Despite all EU skepticism?

Yes. Despite all skepticism, it is clear: in terms of values, we belong to Europe. Our closest partners are here. Neutrality does not mean indifference. We feel closer to European values than to other power blocs. The fact that these tensions are now more openly visible did not begin with Trump. It is simply being articulated more clearly than before.

What special role does Switzerland play?

The current consensus in Switzerland is to pursue a more independent path. In recent years, this has even intensified, including in Western Switzerland. At ›

INTERVIEW_ ***Esther Omlin***

Dr. Esther Omlin Omlin is a lecturer in security law and commercial law at the Eastern Switzerland University of Applied Sciences (Ostschweizer Fachhochschule OST) and previously served as a senior public prosecutor. Her research focuses on external and internal security, international security policy, space, and foreign trade law, and she offers corresponding continuing education programs.

KEY MESSAGES

→ **Europe's security architecture** fails less because of law than because of a lack of political consensus and newly strengthened national interests.

→ **The rules-based order** was never neutral but interest-driven – its transformation offers Europe the opportunity for strategic repositioning.

→ **Intelligence services** are central for small states like Switzerland because information enables exchange, prevention, and security.

→ **Flexible intelligence cooperation,** including with non-democratic partners, is a geopolitical necessity and potentially identity-forming for Europe.

→ **New threats** in cyberspace and outer space require multilateral rules, openness about interests, and the courage to redefine security.

Photo PR

the same time, the EU allows us a certain degree of participation. This is a deliberate cherry-picking, which is not unproblematic legally or politically.

Many assume that Europe must become more independent from the United States. From a Swiss perspective, what does that mean for intelligence services?

In Switzerland, we know how central intelligence services are to our security. It is less about spying than about exchange and prevention. Since our military means are limited, reliable relationships and functioning information flows are decisive. Geneva, as the seat of many international organizations, is an intentionally established meeting point for services – with official formats for early information gathering.

Would such an approach also be conceivable for Europe?

Absolutely. Preventive intelligence work and structured information transfer would be extremely important for Europe. Of course, I do not know how open all nation-states would be to this, but I see an opportunity. Europe has countries that look more to the East, others more to the West. That could be bundled.

Europe as a kind of "large Switzerland"?

Yes, somewhat exaggeratedly put. But the idea is that one can talk to different sides. That is precisely what Switzerland has done for decades. In Europe, these perspectives are already present.

Could such intelligence cooperation also have an identity-forming effect?

Yes, I believe so. Openness is decisive and, depending on the threat situation, also the inclusion of external states. This can be seen, for example, in the BRICS context: their anti-terror working groups are effective because countries that are directly affected are represented there. The formats are deliberately flexible – and that is precisely where their potential lies.

"Intelligence services often have no friends or enemies, but partners."

Esther Omlin

So cooperation also with non-democratic states such as Saudi Arabia?

Exactly. That is classic intelligence tradecraft. Intelligence services often have no friends or enemies, but partners. And these partners are not always morally impeccable.

That naturally stands in tension with the idea of a militant democracy („wehrhafte Demokratie").

Yes, that is a problem. From a Swiss perspective, democracy is defined differently anyway, because we have direct democracy. From a purely legal standpoint, there are often fewer differences between different forms of state than one likes to assume politically. Implementation is, of course, another matter. But even democracies did not historically always emerge democratically.

So moral demarcation quickly reaches its limits?

Exactly. For Switzerland, cooperation is fundamentally possible. We depend on it. As a small state, we cannot afford to say, we will talk to these and not to those. Mediation and openness to dialogue are part of our model.

Do you see a new or greater role today for neutral states?

Yes, certainly. Precisely because Europe is, to some extent, detaching itself from the United States and is thrown back more strongly on itself. Neutrality does not have to be understood strictly in the sense of international law. Non-alignment would be another model. Many states, also in the BRICS context, were originally non-aligned. That they are perceived differently today is more the result of geopolitical shifts.

The more relationships exist in different directions, the better the situational picture...

Exactly. For small states, information is the central security factor. Information keeps us at peace.

Do new threats such as cyberattacks force us to fundamentally rethink security?

Yes, definitely. Cyber threats do not stop at borders. Switzerland has also recognized this. National solutions are no longer sufficient here. Therefore, international cooperation is imperative. In recent years, much has happened in this regard. Especially in Switzerland, but also in coordination with EU law, numerous legislative amendments have been adopted. Legally, we are now relatively well positioned. The real problem lies less in the law than in awareness.

Where does that come from?

It has much to do with the Swiss mentality. We often assume that no one wishes us harm. That is, on the one hand, quality of life; on the other hand, a risk. In companies and authorities, warning signals are often downplayed. Only when incidents accumulate does one react. This path from "probably harmless" to "that was an attack" takes too long. ›

And that is difficult to change?

Yes. Even with training in the police, the army, and companies, this basic attitude remains. Awareness is our greatest deficit. And I suspect that similar problems also exist in parts of the EU.

You also conduct research on space law. State and commercial actors are now active there. Is space essentially a lawless area?

No. Since the Outer Space Treaty of 1967, space has been regulated under international law. More than 100 states, including Switzerland, were involved from the beginning. At that time, it concerned exclusively states and their responsibility. The problem today is the entry of private actors. At the same time, we see that states such as China are already developing very concrete resource strategies. This is reminiscent of Antarctic or Arctic questions, only that here it concerns the Moon and space resources.

Who is liable if private satellites cause damage?

Switzerland has decided that private companies are liable themselves. The state withdraws. Other countries, including many in the EU, continue to see the state as responsible. This has massive consequences for insurance and financing, because companies must provide for potentially billion-euro damages.

If a private company from Switzerland operates a reconnaissance satellite, does it therefore bear responsibility itself?

Yes. In other countries, the state would be responsible. This was also evident in the case of Elon Musk. In the United States, the state is liable for his satellites. When they were used in the Ukraine war, this was relevant under international law, because the United States thereby indirectly became a party. For Switzerland, something like that would be a political super-GAU, because neutrality would be directly affected.

What happens if major powers simply withdraw from the Outer Space Treaty of 1967 and the law of the strongest prevails?

That is the central risk with all international treaties. The Outer Space Treaty is, at its core, a declaration of intent, supplemented by liability agreements. A withdrawal of major actors would shake the foundation. At the same time, many new players are decisive today, for example in India, Africa, or the Arab world. Without them, space policy is no longer conceivable.

That means new rules would hardly be possible without them?

Exactly. A new framework would have to be negotiated multilaterally. Bilateral solutions would not suffice. For the traditional major powers, that would be inconvenient, but realistically there is no longer any alternative.

Do we today need to start anew in thinking about rules and their safeguarding?

I believe so. If one is forced to renegotiate and openly lay interests on the table, alliances may emerge that one had not expected before. That also opens the opportunity to think more sustainably and in the long term.

What is particularly lacking today?

Security in the sense of predictability. People who worked during the Cold War often say: it was dangerous, but stable. One knew the red lines, even vis-à-vis the adversary. Today, much is collapsing. In this globalized world, one often no longer knows what applies and what does not.

And new rules could restore that?

Yes, if each country honestly formulates what is important to it. That could create a viable security architecture for decades. It requires the courage for openness.

But the question remains: how does one safeguard such rules if trust is lacking?

That is precisely the crux. But I believe that space could be an interesting paradigm here. This idea of peaceful, equal cooperation is still deeply anchored.

As a counter-model to classical power politics?

Yes. A space specialist of the Swiss Army once said to me: we guarantee peace in space, not security. At first that sounds paradoxical, but it means that space must deliberately be kept outside power logic. There are no sanctions there, no economic warfare.

Also for practical reasons.

Of course. No one can operate the International Space Station alone. But the fact that one does not even consider subjecting space to sanctions shows how strong this idea still is. And I believe that precisely this dream of peaceful cooperation has political power. Space can be a symbol of that. ■

05_ Ecosystem

Harnessing Europe's Strenghts

"War does not begin and end with the military. It always strikes the weak points of a society – information spaces, infrastructure, psyche, everyday life."

Dr. Larysa Visengeriyeva,
Ukraine/Germany

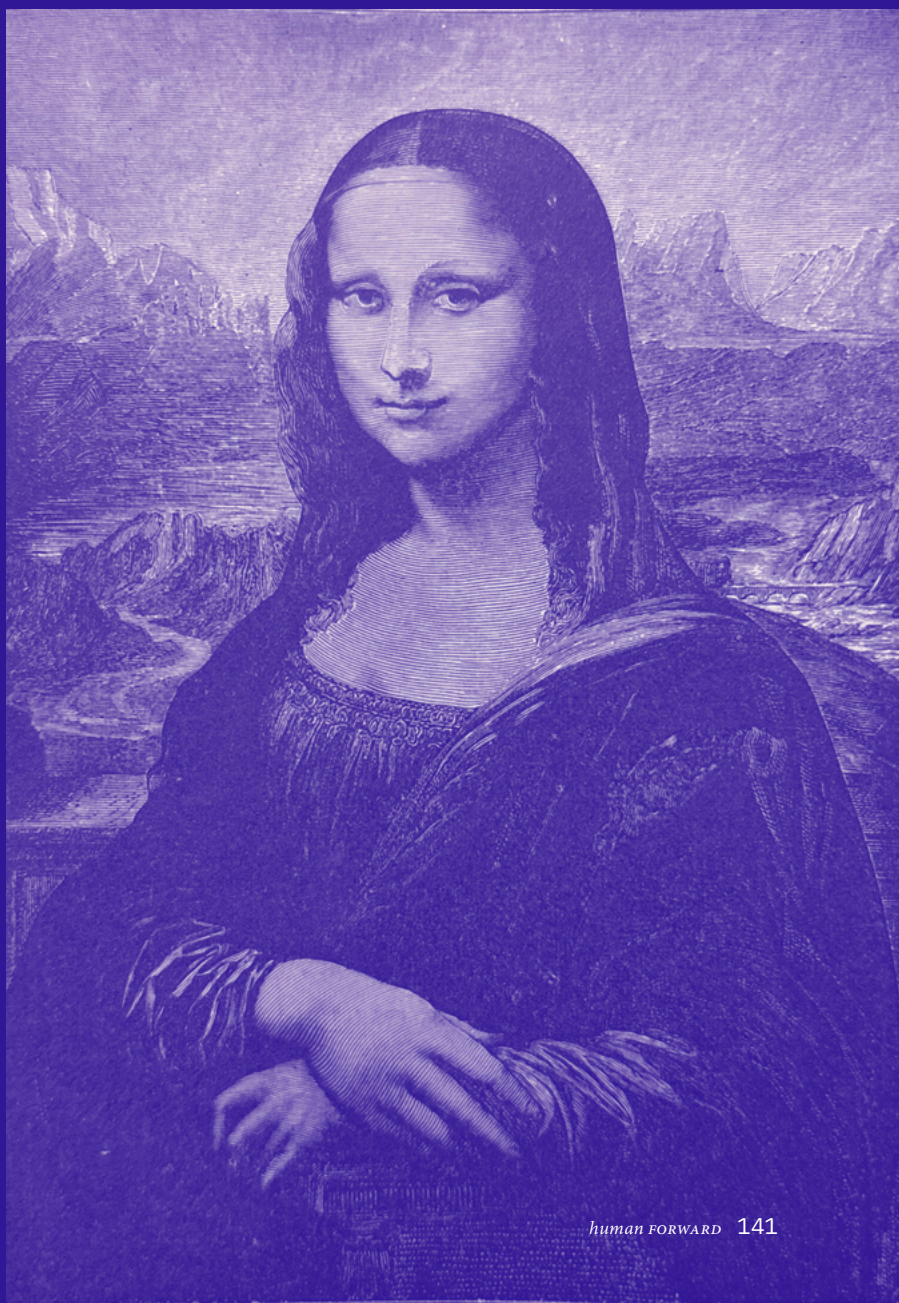

Illustration Campwillowlake/iStock

The New Age of Autonomous Defense

Hybrid attacks, AI-accelerated threats, and disinformation are forcing a paradigm shift. Europe must integrate cybersecurity and strategic intelligence – moving away from reactive defence toward a democratically grounded, proactive security architecture.

TEXT_ ***Brendan Kotze***

Brendan Kotze is Chief Delivery Officer at Performanta, an internationally operating cybersecurity company headquartered in London, UK. With more than 20 years of experience in IT security, he has worked across the entire security lifecycle, including serving as a CISO. Today, he leads development, automation, and advisory services with a focus on practical security solutions that reduce business risk and protect people in the digital domain.

KEY MESSAGES

→ **The divide between cybersecurity and strategic intelligence is obsolete:** Europe's resilience requires an integrated intelligence architecture.

→ **Europe must respond** to hybrid threats with autonomous defense capabilities and collective attribution.

→ **Intelligence is a democratic public good:** transparency, OSINT, and a "duty to share" strengthen state, business, and society.

→ **Public funding** creates strategic visibility: information blackouts and de-prioritization weaken deterrence and sovereignty.

→ **Europe's advantage** does not lie in unregulated AI, but in trust-based, ethically anchored defense as a strategic differentiator.

By 2026, the artificial distinction between "cybersecurity" and "strategic intelligence" must be effectively dissolved. For Europe, intelligence is no longer a peripheral function of the state; it is the core infrastructure of a resilient society. This publication argues for a fundamental transition from reactive technical posturing to a proactive, human-centred interpretive capability. Rather than a closed domain of secret services, intelligence is approached as a holistic societal, political, and technological task.

This proposed architecture effectively balances the "Defender's Burden" of ethical operating models – grounded in the transparency requirements of the EU AI Act – with a "Strategic Pivot" toward proactive, machine-speed defence. By anchoring autonomous defence and enhanced OSINT in democratic values, Europe transforms intelligence into a foundation for responsibility and collective self-clarification. This framework moves beyond an antiquated "firewall" mentality toward a Continuous Threat Exposure Management (CTEM) model, ensuring that strategic clarity remains our primary asset for preserving democratic sovereignty against hybrid threats. ›

1 Beyond Data Theft: Cognitive Warfare and Structural Sabotage

Cyber operations have transitioned from simple espionage toward Structural Sabotage and Cognitive Warfare.

- **The Goal:** Erosion of institutional trust and the manipulation of public perception through synthesized disinformation.
- **The Method:** "Ransom-as-Espionage," where ransomware attacks serve as a tactical smokescreen for deep intellectual property exfiltration or political leverage.

2 The Geopolitical Crucible: Cyber as the "First Front"

Cyber operations have moved to the epicentre of geopolitical dynamics:

- Fragmented digital jurisdictions have led to "digital blockades." Adversaries target supply-chain chokepoints (semiconductors, maritime logistics, energy and utility) to paralyze economies before a single physical shot is fired. This may widen disruption such as port paralysis, logistics location spoofing, or manifest manipulation and logical and physical interception or attacks leading to fuel supply shortage and last mile interference.
- While intended for security, adversaries can exploit known vulnerabilities in the mandatory "transparency lists" and weaponize Software Bill of Materials (SBOM) of components used by critical infrastructure, targeting the smallest, most obscure software library that the entire system depends on.
- The line between digital "mafia" organizations and state intelligence has vanished. States use criminal proxies to conduct Cyber-Extortion, providing legal immunity in exchange for destabilizing European critical sectors and their supply chains.

3 Intelligence as a Democratic Utility (Societal Dimension)

Intelligence is no longer a restricted security instrument; it is the operational foundation for societal responsibility and participation. In the face of systemic cyber threats, and disinformation, we must transition from a "need-to-know" culture to a "duty-to-share" model.

- In an era of cognitive warfare and digital polarization, high-fidelity cyber intelligence must act as a public utility. By providing verifiable attribution for cyber-attacks and disinformation campaigns, the intelligence must enable the rejection of adversarial narratives and influence.
- Social media platforms have become the primary delivery systems for "perception hacks." In this context, intelligence-sharing must extend to the identification of inauthentic coordinated behaviour and algorithmic manipulation. By exposing where foreign state actors inject polarized content, high-fidelity intelligence prevents the organic radicalization of the citizenry and preserves the integrity of the national information environment.
- Bad actors increasingly target individuals, from civil servants to private citizens, using "lifestyle-pattern" and OSINT intelligence to conduct high-precision social engineering, influence, extortion or even kinetic targeting. By democratizing threat intelligence, we can provide individuals with "digital early-warning systems." This converts clandestine telemetry into personal defence tools, such as automated indicators that flag deepfake media or identify malicious infrastructure before a user clicks, effectively shielding the private citizen as a critical link in the national security chain, especially when an individuals personal digital identity can easily become a vector for lateral movement that allows these actors to bridge the gap between vulnerable domestic environments, the individual, and high-value corporate or state networks.

4 The AI-Enhanced Adversary and the Governance Gap

In 2026, the "AI Arms Race" is defined by significant asymmetry constraints.

- **Unrestricted vs. Ethical AI:** Adversaries utilize "jailbroken" models without safety or ethical guardrails to automate malware creation, localize social engineering, perpetrate vulnerability exploitation and more troubling, allowing novice actors to perform complex, multi-stage attacks with the precision and speed of an expert, at scale.
- **The Defender's Burden:** European defenders operate under the EU AI Act, requiring explainability, transparency, and human-in-the-loop oversight. This "latency by design" is an ethical necessity but will become an increasing tactical disadvantage.
- **Bridging the academic** and operational silos is not merely an intellectual goal but a prerequisite for sovereignty. Europe must foster an Interdisciplinary talent pipeline that bridges the gap between technical engineering schools and geopolitical institutes. We must train a new generation of "Strategic Analysts" and "Intelligence Ethicists" who can govern autonomous defence systems and interpreting machine-speed alerts within their proper ethical and geopolitical contexts. ›

5 The Academic Nexus

To build a shared strategic language fit for an age of hybrid threats, Europe must dissolve the silos between fields traditionally discussed in isolation. A holistic intelligence culture requires the convergence of academic depth, ethical rigor, and operational engineering.

- Intelligence must be treated as an interdisciplinary field of research (Social Sciences, Ethics, and Engineering). We must foster a European research ecosystem to ensure Intellectual Sovereignty over our analytical tools.
- Europe must foster an Interdisciplinary talent pipeline that bridges the gap between technical engineering schools and geopolitical institutes.
- We must train a new generation of "Strategic Analysts" and "Intelligence Ethicists" who act as strategic conductors, governing the mission-critical intent and ethical parameters of autonomous systems over performing manual triaging.
- By connecting these disciplines, we move away from purely technocratic responses toward a "Total Defence" mindset. This interdisciplinary approach allows policymakers and practitioners to interpret technical telemetry through a unified lens, ensuring that every signal is grounded in its proper geopolitical and ethical context.

6 The Public-Private Nexus

European intelligence architecture can no longer be a state monopoly, and we should look towards formalizing a framework for private sector experts to be "activated" during systemic crises, ensuring critical infrastructure remains operational. This framework will bridge the 'execution gap' between state attribution and private-sector innovation, ensuring that critical infrastructure remains operational under the weight of hybrid duress and ensures that even under attack, the essential services upon which European citizens depend remain resilient and transparently defended.

Dimension	State Intelligence Services	Private Sector
Mandate	National Sovereignty & Security	Risk Mitigation & Business Continuity
Data Access/ Focus	Focused on targeted, high-value signals and classified human/ signal intelligence	Focused on broad, global telemetry and OSINT
Frameworks	Classified Security Acts	NIS2 / GDPR / DORA / CIS / NIST / ISO
Capability	Legitimate Attribution & Response	Rapid Tech Innovation & Global Scalability

We must acknowledge the dual-use nature of the non-state intelligence market. While private 'Threat Intelligence' firms are essential partners, the rise of unregulated commercial surveillance 'market structures' poses a significant counter-intelligence risk. Europe must establish a regulatory 'Safe Harbor' for private sector defenders who share high-fidelity telemetry during systemic crises.

7 Funding Resilience: Lessons from the US "Defunding" Model

A critical vulnerability in 2026 is the erosion of institutional funding. The recent US experience serves as a stark warning: the defunding of CISA (Cybersecurity and Infrastructure Security Agency) and the expiration of the Cybersecurity Information Sharing Act in late 2025 have led to:

- **The Information Blackout:** A suspected 80% drop in voluntary threat sharing due to the loss of liability protections for private firms.
- **Budget cuts** of up to 62% in engagement divisions and 73% in risk management centres have crippled the ability to provide early warnings to local governments and small businesses.
- **Defunding public "clearinghouses" forces** organizations to operate in silos, creating a fragmented defence that state-sponsored actors can easily penetrate, becoming a strategic opportunity for bad actors.

Europe must reject this "de-prioritization" model. Sustained public funding is not a cost, it is a strategic investment in the collective visibility required to detect "Grey Zone" manoeuvres.

8 CTEM: The Operational Bridge for Strategic Clarity

Europe must adopt **Continuous Threat Exposure Management** (CTEM) to align security with Strategic Sovereignty, and where the highest dividend gain be gained.

1. Abgrenzung (Scoping): Definition der Schutzgüter – von Stromnetzen bis zu demokratischen Datenbanken –, die für eine „freie Gesellschaft" essenziell sind.

2. Erkennung (Discovery): Identifikation nicht nur technischer Schwachstellen, sondern auch von Identitätsrisiken und Fehlkonfigurationen, die in der Grey Zone ausgenutzt werden.

3. Priorisierung: Bewertung von Bedrohungen nach ihrem Potenzial, die europäische Stabilität zu unterminieren – nicht allein nach technischer Schwere.

4. Validierung: Einsatz von Red-Teams sowie KI-gegen-KI-Simulationen, um zu überprüfen, ob eine Bedrohung bestehende Verteidigungen tatsächlich überwinden kann.

5. Mobilisierung: Abkehr von reiner „Alert-Jagd" hin zur automatisierten Behebung jener 1 % der Exponierungen, die strategisch wirklich relevant sind.

9 Cyber Hygiene: The Foundation of Strategic Resilience

As Europe transitions toward autonomous defence, Cyber Hygiene must evolved from a series of routine tasks into the structural health required for high-speed intelligence and defence systems to function. Without this baseline, the "Strategic Pivot" is impossible; neglected hygiene creates detection gaps and telemetry noise that can provide a smokescreen for bad actors.

The expert attacker of 2026 no longer "breaks in"; they "log in".

- **Living Off the Land (LotL):** Sophisticated actors bypass traditional antivirus by abusing built-in administrative tools and "edge devices" (routers/firewalls), and supply chains, blending into legitimate network noise to achieve persistence.
- **Identity-Based Intrusion:** Adversaries prioritize the theft of Non-Human Identities, such as AI agents and service tokens. Managing these "ghost identities" represents one of the most significant defensive gaps.

Regulatory mandates for essential entities under the NIS2 Directive and the Cyber Resilience Act, the following are no longer optional "best practices" but mandatory pillars of the European intelligence architecture:

- **The visibility mandate** - You cannot defend what you cannot see. Continuous asset discovery ensures that the "Scoping" phase of Continuous Threat Exposure Management (CTEM) is accurate; an unrecorded IoT device or forgotten legacy server acts as an invisible bypass for even the most advanced AI agent.
- **Identify hygiene** - Europe must transition from traditional MFA to hardware-based, phishing-resistant authentication. In an era of AI-generated attacks, traditional multi-factor authentication methods (e.g. e-mail or text) are no longer "appropriate and proportionate"
- **Supply chain accountability** - Organizations are now strategically responsible for the posture of their entire vendor ecosystem. This is further supported by the Cyber Resilience Act (CRA) driving us from "implicit trust" to "continuous vendor Assessment.

10 Detection and Response: The Era of Autonomous Defence

We must close the execution gap. If CTEM is the radar that detects threats on the horizon, Detection and Response are the reflexes that neutralize them in real time.

The speed and volumes of cyber-attacks have made human-centric response a secondary support function to Autonomous Defence. The traditional Security Operations Centre (SOC) model must pivot accordingly. We must become longer "hunt" for threats manually; or build static detection rules, the pivot mist be to multi-agent Systems that perform real-time triage, and automated containment.

- **The End of Dwell Time:** Traditional attackers once averaged 200+ days inside a network. AI-driven detection must seek "Zero Dwell Time," identifying and neutralizing attackers at machine speed.
- **Autonomous Containment:** When a high-fidelity threat is detected, systems now must execute Self-Healing Responses, isolating compromised nodes, disabling leaked session tokens, and stopping network traffic without waiting for human approval.
- **Auditable Autonomy:** Every autonomous action is logged with an AI-generated explanation, fulfilling the transparency requirements of the EU AI Act while maintaining machine-speed defence.
- **The Business Context Risk:** A key strategic challenge is preventing "self-inflicted outages" where AI shuts down a critical production line to stop a minor infection. leaders must prioritize Context-Aware AI that understands business mission-criticality. ›

11 OSINT and AI: The New "Strategic Radar"

In a democratic framework, Open-Source Intelligence (OSINT) is a foundational pillar of transparency. Unlike clandestine methods, OSINT relies on legally obtained, publicly or commercially available data, making it uniquely suited for a society that values the rule of law and public accountability.

- By 2026, the volume of digital data from satellite imagery to social media telemetry exceeds human processing capacity. AI-driven OSINT acts as a radar that scans this vast environment to identify "grey zone" activities before they escalate. Case studies show that cross-referencing OSINT with technical telemetry can identify adversarial staging infrastructure up to 48–72 hours before an active deployment.
- The integration of Large Language Models (LLMs) and autonomous AI agents transforms raw "open-source information" (OSINF) into "actionable intelligence" (OSINT). AI compresses the intelligence value chain, allowing for real-time scanning of millions of assets to flag early indicators of compromise and behavioural anomalies.
- In an era of "information pollution," OSINT serves as a "pre-bunking" tool. By providing a verified, transparent baseline of facts, it allows democratic institutions to call out adversarial narratives before they take root in the public consciousness.
- To remain a democratic utility, this "Strategic Radar" must operate under Auditable Autonomy. While AI provides the speed to counter adversarial agents, the criteria for scanning and analysis must remain transparent to oversight bodies to ensure compliance with the EU AI Act and fundamental rights.
- Because OSINT is based on public data, its findings can be shared more broadly with civil society, business leaders, and international partners without compromising secret sources.
- Interdisciplinary Collaboration: This "radar" is most effective when it bridges the gap between state intelligence, private-sector telemetry, and academic research, creating a shared strategic language for the 21st century.

12 Strategic Options for a European Intelligence Architecture

We call for a proactive European intelligence paradigm oriented toward strategic capability:

- **Strengthening the Single Intelligence Analysis Capacity (SIAC)** into a 24/7 real-time assessment hub that integrates technical telemetry with geopolitical foresight.
- **Formalizing market structures** where the private sector provides rapid innovation while the state provides legitimate attribution and sovereign protection.
- **Learning from the 2025 "Information Blackout"** in other jurisdictions, Europe must ensure public funding for agencies remains a non-negotiable pillar of national resilience.
- A European Intelligence Architecture must include a **Unified Cyber Situation Room.** This would bridge the gap between technical telemetry (from the private sector) and geopolitical intent (from state services), creating a 'Common Operating Picture' for the 27 member states to facilitate collective attribution.
- While private sector "activation" is essential for business continuity, we must acknowledge the dual-use nature of the non-state intelligence market. To mitigate the risks posed by unregulated commercial surveillance structures, **Europe must establish a Democratic Standard for Private Intelligence Providers.** This ensures that "activated" private-sector experts acting within a regulatory 'Safe Harbor' and adhere to the same ethical guardrails and transparency mandates as sovereign state services.

13 Conclusion: A Call for Strategic Clarity

Intelligence is the foundation of sound judgment. By integrating a CTEM-based operational standard and acknowledging the AI Governance Gap, Europe transitions from reactive "cyber-defense" to proactive strategic clarity. Final Insights:

- A failure to interpret the digital environment is a failure of democratic responsibility. We must treat intelligence as a utility, constant, reliable, and foundational, this empowers not only the state and business but also the citizenry to navigate an era of disinformation.
- A European Intelligence Architecture must move beyond simple information sharing to achieve Collective Attribution. The proposed Unified Cyber Situation Room will act as the "High Court of Attribution," bridging the gap between private-sector technical telemetry and state-level geopolitical intent. When 27 member states speak with a single, evidence-backed voice, technical intelligence is transformed into a potent strategic deterrent, providing the political weight necessary for unified diplomatic responses.
- We must reject the "de-prioritization" model that leads to information blackouts. In 2026, visibility is deterrence. Sustained public and research funding is a strategic investment that ›

signals to adversaries that their "Grey Zone" manoeuvres will be instantly detected and collectively attributed. By treating high-fidelity intelligence as a constant and reliable utility, we empower the state, business, and citizens to resist cognitive and structural sabotage.

- We must abandon the "patch-everything" fallacy. Success is measured by our ability to ignore 99% of technical noise to flawlessly defend the 1% of vulnerabilities on the critical path to sovereignty as identified by our CTEM radar.
- Funding is Visibility, as demonstrated by the systemic fragility following the de-prioritization of agencies like CISA in the US, cutting cyber-intelligence budgets is a self-inflicted wound. Sustained funding is the only way to maintain the "clearing-house" effect required for collective European defence. Sustained public and research funding is the only way to maintain the "clearinghouse" effect required for collective European defence.
- We must move from human-speed committees to Agentic Defence. Systems must execute Self-Healing Responses. However, this must be governed by Autonomous Compliance: an internal layer of "digital law" that ensures machine-speed actions remain ethical, auditable, and compliant with the EU AI Act.
- Sovereignty in 2026 is a shared task. Formalizing a framework that "activates" private sector innovation and academic research during crises is essential to ensuring critical infrastructure remains operational under hybrid duress.
- While adversaries gain speed through unrestricted AI, Europe gains resilience through trust. By building ethical guardrails into automated defence, we ensure our security never comes at the cost of our values. ■

Mind War

Cognitive warfare operates with disinformation, fake news, and manipulation. Organizational expert Rafaela Kraus on the psychological vulnerabilities of modern societies, dealing with uncertainty – and why democratic resilience begins long before technology.

INTERVIEW_ ***Rafaela Kraus***

Prof. Dr. Rafaela Kraus is Professor of Corporate and Human Resource Leadership at the University of the Bundeswehr Munich. Her research includes intrapreneurship and entrepreneurship, defense/dual-use innovation, transformation (e.g., the automotive industry and defense), leadership, and organizational culture.

KEY MESSAGES

→ **Cognitive warfare** is part of hybrid warfare and primarily aims at destabilization, polarization, and loss of trust – not classical persuasion.

→ **Ambiguity is strategy:** unclear authorship is more destabilizing than open violence.

→ **AI and scalable disinformation** amplify psychological effects with minimal resource deployment.

→ **Education, media literacy, and productive dissent** are central instruments of defense.

→ **Resilience means** enduring uncertainty without falling into naivety or total distrust.

How do you classify the term cognitive warfare – also in relation to classical propaganda or information warfare?

The terms overlap. Hybrid warfare often begins with the division of societies. Media play a central role in this: think of deepfakes, fake news, and targeted disinformation campaigns. Added to this is the influence exerted on individual persons, such as politicians who are deliberately used as instruments. Overall, however, it is less about convincing people of certain content and more about unsettling and polarizing them – driving societies apart and thereby making them more vulnerable, less resilient.

So cognitive warfare is part of hybrid warfare?

I think so. Even classic acts of sabotage – for example power outages – have a psychological component. They create the impression that politics and institutions are incapable, that the state does not protect its citizens. Subversion is a form of escalation: existing internal tensions are intensified, minorities with anti-democratic narratives are instrumentalized. This can be seen, for example, in the Baltic states, where Russian minorities are deliberately addressed via social media and specific channels.

Does hybrid warfare also learn from terrorism?

The methods are partly similar, but there is an important difference. In the case of a terrorist attack, the perpetrators usually want to be recognized as the cause. In hybrid warfare and cognitive warfare, by contrast, ambiguity is the central strategy. Was it sabotage, an accident, a lone actor, a foreign state? The more diffuse the attribution, the more effective the strategy...

...because we handle ambiguity poorly?

Exactly. Our society is based on clear rules. We are accustomed to conflicts being identifiable, with clear stages of ›

"People must learn to actively ask questions: Where does this information come from? Who benefits from it?"

Rafaela Kraus

escalation. Grey zones contradict our expectations and perceptions. In everyday life, it may not feel as though we are at war – and yet we are in a kind of state of war. Behind the scenes, many things are happening in parallel whose originators we cannot clearly name. That makes the threat so serious.

So the goal of hybrid warfare is collective destabilization – similar to the psychological phenomenon of gaslighting.

Yes. A state is created in which one no longer trusts one's own perception. With minimal means, effects can be achieved for which military force would otherwise be necessary. So-called disposable agents or "useful idiots" are employed, who believe they are doing the right thing. That is extremely cost-efficient compared to an open military attack.

Take the example of the Berlin blackout in January. What questions should one ask as a citizen?

The most important thing is clarification. The population must understand that we are in a situation in which adversarial actors deliberately attempt to unsettle and divide our society from within. The aim is to undermine trust in our institutions – in the state, in authorities, police, the armed forces. In other countries, for example in Scandinavia, awareness of this threat is already taught in schools, in the sense of comprehensive defense. This also includes defense in our minds. We must accept that the "grey" war situation is a reality and that a certain instability is part of the new normal. Accordingly, awareness is needed across society as a whole.

Awareness – that also means critical thinking and media literacy?

Absolutely. Critical thinking and dealing with media are still neglected in schools. It is often treated as a one-off topic, when it should be permanently present. People must learn to actively ask questions: Where does this information come from? Who benefits from it? If one does not know, one should be suspicious. The moment we allow ourselves to be instrumentalized, the adversary has already won.

AI language models can generate extremely convincing texts with which opinions can be influenced on a massive and scalable basis – for example to undermine support for Ukraine. What can be done about this?

We need more than just technical defense. What is required now is significantly more education, information campaigns, and structural resilience. COVID showed how quickly conspiracy theories spread. Since then, too little has happened. Other countries, particularly the Baltic states, are further along because they are strongly affected. And we must also think about companies: resilience of critical infrastructures, clear standards, appropriate laws. That costs money and is labor-intensive – but there is no way around it.

Were there moments when you realized that you yourself are vulnerable to such mechanisms?

In the startup bubble, where I often am, people like to complain about regulation, Europe's sluggishness, the inability to act in concert and truly cooperate. I sometimes catch myself engaging in this Europe-bashing. I ask myself whether Europe-bashing is not also part of what hybrid warfare aims to achieve: that we perceive Europe as dysfunctional and only criticize it instead of being constructive. I believe one must be careful not to simply echo this narrative. It is not entirely wrong – but it plays into the adversary's hands.

Are there still institutions that one as a citizen should completely trust?

For me, the real risk lies in the either–or. On the one hand, one trusts institutions blindly because, for example, "Spiegel Online" is written at the top. But one may be clicking on a fake site. This naivety of reacting to familiar patterns because they appear reputable, have a veneer of scientificity, is fatal. On the other hand, there is the danger of total mistrust toward every institution, science, politics. In the end, one develops an all-encompassing distrust. We must find a middle path: education in order to shed one's own naivety – and at the same time trust-building so as not to see ghosts everywhere.

Overreactions can become part of the problem.

Exactly. We cannot protect every- ›

"It is impossible to foresee and detect everything in advance. We will have to live with uncertainty."

Rafaela Kraus

thing. When I think of critical infrastructures: energy supply, hospitals, water, logistics. It is impossible to secure everything or foresee and detect everything in advance. We will have to live with uncertainty. The challenge is to be cautious and sensitive, but not to lose our heads and react rashly. When drones were sighted several times over Munich Airport in October last year, voices immediately called for them all to be shot down. That is not always the right reaction. One cannot simply "start shooting wildly" as on a battlefield. There are legal frameworks, a regulated environment. And responses must be adapted and proportionate.

The drone example also shows how it can swing from one extreme to the other: first there was a state of alarm, then the issue suddenly disappeared from view again.

Exactly. And that shows the multidimensional challenge. It is about what it triggers in people's minds – but also about the real danger, for example to an airport and flight operations. Here, science communication has an important task: to sensitize people to the fact that these simple black-and-white truths – "just shoot them down" – are themselves dangerous. Such simplifications can also be part of cognitive warfare.

We all move in bubbles. Is it not extremely difficult to break away from a group opinion?

Yes, absolutely. That is precisely why it is also an educational task. Such mechanisms should already be trained in school. How do I deal with holding a different opinion? How do I argue? How do I endure contradiction? Of course, not every dissenting opinion is automatically good or correct. It may also be that someone is completely wrong. But what is decisive is that we learn to engage in dialogue and confront one another at the level of argument. I consider that one of the central tasks.

Does that not also mean that we would have to promote productive dissent much more strongly?

An example: I was at an event in the autumn called "Security Dialogue." („Sicherheitsdialog".) Among those on the panel were a representative of the Federal Student Conference, a representative of the fire brigade, and General Bodemann, who worked on Operation Plan Germany („Operationsplan Deutschland"). I found that extremely good, because very different perspectives came together there – including those that are not automatically conform. That is precisely the challenge: more interdisciplinarity, more diversity of perspectives instead of one-dimensionality.

Is the problem also rooted in our institutional structures?

Very much so. In research institutions and universities, we are still trapped in silo structures: faculties, departments, disciplines. Exchange is limited. Yet the social sciences, for example psychology, could contribute enormously – as could technology, which shows what is technically possible, for instance with AI. Added to this are security and foreign policy, which understand the strategic behavior of actors, and sociology, which analyzes societal dynamics. We need much more interdisciplinary exchange. Technology is sometimes perceived in the humanities and social sciences as something alien – and that is precisely what we must overcome if we want to arrive at better solutions.

When you say that cognitive warfare is at its core an educational task – does that not also mean strengthening children early on as individuals and immunizing them against excessive influence from bubbles?

Yes. Our school system is strongly oriented toward conformity: following rules, adapting. Much of what used to be considered the core of education – storing knowledge, reproducing it – is obsolete in the age of AI. We now have better opportunities to work interdisciplinarily, to think in networks, and to access fields of knowledge that were previously inaccessible. In the past, we had to delimit and focus because knowledge exploded. Now we must once again learn to think independently, critically, and more broadly – to become a bit more "undisciplined."

What does that mean concretely for learning?

Developing one's own questions, being creative and critical, are skills that are central today – also in order not to become susceptible to manipulation, ›

„We can learn from young people to develop a very clear sense of what technology is capable of today.“

Rafaela Kraus

targeted influence, and subversive strategies.

What do you learn from young people and startup founders?

A doer mentality. This attitude of not just talking, but starting. Trying things out, proceeding iteratively, sticking with it. This persistence in wanting to solve real problems – not just to speak about them theoretically – fascinates me. Take fake news, for example: we older people often discuss abstractly how dangerous they are. Startups are more likely to ask: How can we detect them technically? What methods exist? What can concretely be built? We can also learn from young people to develop a very clear sense of what technology is capable of today. Whether the young are fundamentally more reflective and have more awareness of manipulation than other generations, I am skeptical. I believe we are all in the same boat.

You do not believe that Gen Z is less susceptible to subtle influence, for example through language models?

I am not so sure about that. But overall, I do have the impression that digital natives deal more confidently with fake news than the boomer generation, which in some cases looks at content with greater credulity. That is not a scientific statement, but an observation I have made repeatedly. ■

The AI Fog Machine

Generative AI produces plausibility at industrial scale. What appears to be technological progress quietly undermines the foundations of democratic judgment. Europe's most pressing security question is more urgent than ever: How do we preserve a shared reality?

TEXT_ ***Raluca Csernatoni***

Dr. Raluca Csernatoni is a Fellow at Carnegie Europe in Brussels, focusing on European security and defence policy as well as AI and emerging technologies. She leads the organisation's research on the geopolitics of AI, serves as Guest and Visiting Professor at the Vrije Universiteit Brussel and the University of Antwerp, and conducts research in several EU-funded projects on cyber and digital policy.

KEY MESSAGES

→ **Generative AI** is reshaping security policy: not truth itself, but plausibility becomes a strategic resource – and a target surface.

→ **Epistemic uncertainty** arises when societies produce content faster than they can verify it.

→ **Democratic order** does not require consensus, but it does require a minimal shared reality.

→ **Platform design and algorithmic systems** are security-relevant and must therefore be regarded as part of critical infrastructure.

→ **Epistemic resilience** is a public good: it determines whether Europe remains capable of judgment and action.

Günther Anders, one of the twentieth century's preeminent thinkers, wrote *The Obsolescence of the Human* in 1956, at a time when the nuclear age had rendered technological power impossible to romanticise. He aimed to identify a new condition. Modern societies have learned to create consequences on a scale that their imagination could not keep up with. We could produce effects that crossed continents and decades, yet we found it difficult to clearly envision them, fully feel them, and take responsibility proportionately. Anders called this the Promethean gap, a discrepancy between what humans can create, such as the atomic bomb, and what they can mentally and morally comprehend.

He expanded the argument further. This discrepancy leaves a mark on the self. It fosters Promethean shame, a sense of inferiority in front of our own artefacts, as if the products of human hands and systems were more reliable, more precise, more perfect than their creators. For Anders, the central danger lay in the human response. People adapt to what overwhelms them. They normalise it. They accept a world they no longer understand as the new baseline. The problem becomes less about a single technology and more about a civilisation that quietly diminishes its sense of responsibility in order to keep functioning.

That is why Anders is relevant again today. Europe is entering an era where meaning itself is produced on an industrial scale. Generative artificial intelligence (AI) can create plausibility quickly and cheaply, flooding the public sphere with content that appears and sounds credible before citizens or institutions have had a chance to verify. The Promethean paradox reappears here as a politics of perception. We are creating an environment that surpasses our ability to judge it, and disruption thrives in that gap. Promethean shame further captures the unease that, as AI systems appear to outperform us, humans start to feel obsolete and defer to ›

machine judgment, an epistemic and emotional drift that can quietly reshape authority, responsibility, and democratic consent.

Europe faces a threat that conventional security thinking cannot address, namely, the industrial-scale production of plausibility. This is what I call epistemic insecurity, and it is now a first-order strategic problem.

> "Hybrid threats thrive on ambiguity and friction."
>
> Raluca Csernatoni

In response, European security debates still default on familiar topics, from networks, infrastructure, borders, resilience, to military readiness. All are necessary. Yet a quieter pressure now influences the strategic landscape. It involves the conditions under which Europeans can continue to understand each other, disagree, and make decisions together. It questions whether a common world can still be maintained. This is the strategic pivot. When shared reality breaks down, democratic legitimacy weakens, crisis management slows down, and coalition building becomes fragile. Solidarity on sanctions, defence, and support for partners becomes easier to undermine.

This is where epistemic security is vital. It is the resilience of the knowledge ecosystem that democratic life relies on, such as credible institutions, accountable expertise, a media sphere capable of mediating rather than merely amplifying, shared reference points that can withstand shocks, and civic habits that enable people to check, infer, doubt, and revise. Epistemic security functions at the social level. Its unit is the public sphere, the fragile framework that transforms information into shared judgment.

Democracy depends on a fragile achievement that is easy to overlook and difficult to restore once lost, namely, a shared outlook on reality. A polity does not require complete agreement. It needs recognisable points of contention. Elections. Budgets. Wars. Pandemics. Corruption. Responsibility. When this outlook breaks down, politics becomes more primitive. Persuasion shifts to domination. Public reason gives way to tribal certainty. Truth becomes a weapon, wielded and enforced, claimed through volume and repetition.

Hybrid threats have long targeted this layer. Their tactic is corrosion. They thrive on ambiguity and friction. They blur the boundaries between genuine dissent and orchestrated manipulation, between satire and sabotage, between grassroots mobilisation and synthetic coordination. Their preferred outcome is exhaustion. A citizen who is tired, cynical, and perpetually suspicious is easier to steer and harder to mobilise. A society living in fog struggles to sustain solidarity, whether on migration, public health, Ukraine, or the legitimacy of the Union itself.

It can seem abstract until you picture it in a very ordinary scene. A Monday morning in a small European city. A voice note spreads quickly, supposedly from the mayor. It warns that the water supply is contaminated. It urges people to avoid hospitals and wait for "official instructions". Within hours, panic buying begins. Emergency lines become overloaded. Schools debate closure. The correction arrives when the public is already primed to distrust it. What actually matters is how swiftly confusion becomes a political fact.

Generative AI pours accelerant onto this logic of disruption.

Generative AI refers to machine learning systems, usually large neural networks trained on vast collections of text, images, audio, or video, that can produce new content similar to what they have learned. They can generate fluent prose, convincing pictures, cloned voices, synthetic clips, and interactive conversational agents that can maintain dialogue and mimic personality. They are probabilistic engines of plausibility. They can sound authoritative while being inaccurate. They can be playful and creative. They can also be bureaucratically persuasive and strategically manipulative.

Within Europe's information ecosystem, generative AI impacts three areas simultaneously: scale, personalisation, and pace.

Scale first. The cost of production plummets. Text, images, and audio can be generated in volumes that surpass verification capabilities. What once required teams can now be managed by a few operators using prompts, templates, and distribution channels. Synthetic content becomes so abundant that it reaches saturation. The challenge shifts from creation to selection. And this selection is controlled by platform architectures and algorithms that prioritise engagement, emotional impact, and swift responses.

Personalisation next. Influence operations no longer rely on a single overarching narrative. Instead, they craft micro narratives tailored to different grievanc- ›

es, languages, and subcultures, each aligned with a community's mood and vocabulary. One audience receives a policy-oriented brief. Another gets a sarcastic meme. A third encounters a thread provoking moral panic. Propaganda thus becomes mass customisation.

Pace finally. Generative AI speeds up narrative volatility. Rumours are launched, mutated, laundered, and redeployed faster than institutions can respond. In a multilingual Union, this effect is intensified. A claim can be seeded in one language, rephrased in another, "validated" by synthetic accounts, then returned as a European controversy. Disruption spreads quickly. Correction arrives late. Fatigue sets in sooner than both.

The result is a particular kind of threat. It is intimate and mundane. The spectacular deepfake is only the headline. The deeper effect is constant, low-grade uncertainty. The clip that looks real. The screenshot that fits the story too perfectly. The leaked memo written in impeccable bureaucratic tone. The voice note from someone you trust. The friendly profile that chats patiently and remembers your anxieties. The question becomes less "Is this true?" and more "Can I still tell?" When people lose confidence in their ability to tell, they rarely become enlightened sceptics. They become resigned. Trust becomes expensive. Cynicism becomes a coping strategy.

A further trap opens. If anything can be fabricated, then everything can be challenged. Actors with malicious intent gain a structural advantage. They sow doubt and let the ecosystem take over. They make the argument itself seem futile. A public that no longer expects truth as a shared horizon becomes vulnerable to those who assert certainty most aggressively.

Authority becomes easier to imitate, impersonate, and more difficult to recognise. Journalistic style, academic tone, and institutional language can all be simulated at scale. Confidence can be fluently mimicked to suggest expertise. The key question then shifts to authority: who has the right to define reality in a contested public sphere? Once that question is destabilised, democratic legitimacy follows suit.

Persuasion is being reshaped, too. The old model relied on broadcast, with messages pushed to audiences. Generative systems now allow for interactive manipulation. Bots can converse, flatter, provoke, and build trust over time. Influence becomes relational, embedding itself in communities and micro interactions. Cognitive security becomes inseparable from social engagement.

All of this reshapes Europe's digital consumption, the daily intake of information, emotion, and identity signals. Digital "diet" is a useful metaphor because it highlights metabolism and habit. A society can endure occasional toxins, but it faces difficulty when the food chain shifts. Synthetic content, designed to capture attention, risks turning the diet into junk: highly appealing, emotionally manipulated, and nutritionally bare. The slow consequences are political, such as reduced attention spans, increased reactivity, diminished tolerance for complexity, and greater reliance on algorithmic curation. Democratic virtues like patience, proportion, and nuance become more difficult to uphold.

> "Who has the authority to define reality in a contested public sphere?"
>
> Raluca Csernatoni

Europe's cultural fabric is felt deeply. A polity remains united by more than laws and markets. It relies on shared reference points and a thin layer of common reality, enough for debate while remaining in the same world. When that layer begins to break down, politics turns into a battleground of incompatible realities. Hybrid actors exacerbate existing divisions, transforming grievances into identities and controversies into existential conflicts.

Europe adds its own fragilities. Coalition politics can be destabilised by microscandals. Media trust and digital literacy vary greatly across member states. The information market is borderless, while narratives transfer between languages and contexts effortlessly. The EU decision-making process relies on compromise, and compromise hinges on minimal shared facts. When facts become permanently disputable, the bloc's ability to act is more easily obstructed.

There is also a geopolitical dimension. Much of Europe's critical infrastructure is influenced by non-European platforms. Its AI capabilities largely depend on external computing resources, models, and cloud ecosystems. This does not mean helplessness, but it does require sobriety. Epistemic security cannot be overlooked when the architectures that organise European public life are built elsewhere and exploited by adversaries who see disruption as a weapon. ›

Europe also needs ambition. Generative AI offers real opportunities, like broader access to expertise, support for education, translation across languages, and productivity improvements in public services and industry. The challenge is governance with awareness. These systems can normalise superficial processing and delegate judgement. Summarisation becomes standard. Verification becomes optional. Drafting becomes automated. Thinking becomes performative.

Europe's response must treat epistemic resilience as a public good. Moreover, it should adopt a defined posture, a way of operating within a contested information environment: build scaffolding for trust, slow down moments that require verification, and prevent adversaries from turning speed, scale, and targeting into superiority.

That posture can be translated into actionable steps.

First, establish verification infrastructure at scale. Authenticating official communications, enhancing provenance signals for media, and creating trusted mechanisms to identify synthetic artefacts will become crucial. This is akin to civil engineering for the public sphere, providing scaffolding for judgment in an environment flooded with plausible content.

Second, cognitive resilience as civic competence. Media and digital literacy must become lifelong and practical. They should cultivate habits of attention, specifically, slowing down, recognising emotional manipulation, detecting coordinated amplification, and learning to triangulate without paranoia.

> "Europe must treat epistemic resilience as a public good."
>
> Raluca Csernatoni

Third, platform design should be treated as security-relevant. Recommendation systems, various algorithms, virality mechanisms, and monetisation incentives shape the information terrain as surely as borders shape territory. Europe needs transparency that is usable, accountability that is enforceable, and design choices that reduce the rewards for outrage, synthetic engagement, and coordinated manipulation.

Fourth, democratic institutions should be safeguarded against attention sabotage. Electoral authorities, public broadcasters, health agencies, and local administrations require playbooks and resources to function amid engineered uncertainty, including rapid-response capabilities, secure channels, and cross-border coordination among member states.

Fifth, AI should be employed to strengthen democratic resilience, not solely for competition. AI can be used for the public good. Machine speed can analyse narrative flows across languages, identify coordinated operations, support investigative journalism, and assist institutions in communicating clearly and rapidly.

And then there is Anders' most difficult lesson. The danger lies in the machine's power and the human adaptation that ensues. A civilisation can become accustomed to fog. It can accept epistemic degradation as normal. It can regard cynicism as sophistication. It can delegate judgment to machines and deem it realism.

Europe should oppose that trend, and epistemic security is the democratic survival function for the coming decade. It defends the common world, the cultural fabric, and the conditions under which diverse societies can continue to debate, recognise one another, and act collectively. The major struggles ahead will occur in the daily infrastructures of attention and meaning, for example, feeds and forums, synthetic voices and credible documents, and the quiet reshaping of how societies learn and remember.

Anders feared a humanity embarrassed by its own exquisite technical creations and tempted to evade responsibility. Europe cannot afford that retreat. Yet, while the task is straightforward to state, it is difficult to accomplish. How to rebuild shared reality faster than disruption can dissolve it, and how maintain human judgment as present, visible, and accountable, before the fog begins to feel like home. ■

In the Age of AI, Courage Is the New Security

Text: Jim Sengl and Felix Rieger

In Europe, security is often confused with stability. Yet when technological cycles are measured not in decades but in months, equating security with stability becomes a dangerous misconception. In the twenty-first century, security means something different: the capacity to act.

The geopolitical tensions of recent years have confronted us with an uncomfortable truth: the time when we could blindly rely on international partnerships is over. We must acknowledge that formerly reliable allies are increasingly using economic dependencies for political purposes. When tariffs and market access are deployed as geopolitical weapons, our digital infrastructure becomes our Achilles' heel.

This risk is not purely political; it is also economic. Those who process their most sensitive data and operations exclusively via external platforms accept a loss of control. The outflow of trade secrets or the use of proprietary data to train foreign AI models are not theoretical risks, but real threats to the competitiveness of European companies. And when "security" is invoked in such a situation, it often merely refers to protecting the status quo. Yet anyone who truly seeks security needs courage.

Regulation Is the Foundation, Technology the House

An important step toward the future viability of the European Union is the AI Act. This regulatory framework is not an obstacle; it creates the necessary legal certainty and a clear order within which we can operate. But let us not deceive ourselves. Laws do not write software. Regulation defines the playing field; it does not put the players on it. ›

Jim Sengl heads the KI-Kompetenzzentrum Medien (KI.M), a joint initiative of Medien. Bayern GmbH and the Bayerische Landeszentrale für neue Medien (BLM). His work at the KI.M focuses on supporting the media industry in the legally compliant and future-proof use of artificial Intelligence.

Felix Rieger is responsible for public relations at the KI-Kompetenzzentrum Medien (KI.M). In his daily work, he engages with artificial Intelligence, media innovation, and community building.

Das KI-Kompetenzzentrum Medien (KI.M) is the central point of contact for the use of artificial Intelligence in the media industry. The goal of the KI.M is to support the Bavarian media sector in the legally compliant and future-proof use of artificial Intelligence.

Technological independence is not defined by the AI Act alone. A task of this magnitude cannot be accomplished by lawyers alone; it must be shaped by engineers and companies. The KI-Kompetenzzentrum Medien (AI Competence Center Media) (KI.M) supports this process. We see ourselves as technical enablers who fill the legal framework with the necessary technological substance.

Media Are Critical Infrastructure of Democracy

For the media sector, this independence is existential. If newsrooms depend on "black box" systems for research or content creation—systems whose functioning they can only partially understand and verify, and whose operators are subject to political whims—they sacrifice part of their integrity. Sovereignty here means, quite pragmatically, having a choice. The choice of whether data flows to a cloud overseas or is processed locally.

This freedom of choice requires proprietary hardware and physical spaces where experimentation can take place. In Bavaria, we have created these spaces. With the AI Real-World Lab, we offer Bavarian media companies precisely what the market often withholds: access to high-end infrastructure while preserving data sovereignty.

With our own hardware, we create a space of possibility free from cloud dependency. Here, companies can test the use of AI with us by developing AI prototypes without their data leaving Europe. This is a technical response to political and economic uncertainty.

Democratizing High Tech

Courage also means sharing knowledge and not thinking in silos. The idea that every medium-sized media company can build its own AI infrastructure alone is illusory. The answer to the dominance of global tech corporations can only be cooperation.

The KI.M is therefore committed to the open-source principle. The findings from our feasibility studies, the code, and the technical documentation do not disappear invisibly into a drawer; they are freely available in public repositories. We are democratizing access to high tech.

A small local broadcaster or a specialized publisher gains access through KI.M to blueprints that would otherwise be reserved for large corporations. This strengthens the economic foundation of Bavaria as a media location and makes us more resilient as a community against external shocks.

The Situation Is Serious, but It Is Shapable

Europe has one strength: we can build institutions that endure. The KI.M is a Bavarian contribution to this European task. We do not wait for the overall climate to change. We combine the necessary legal expertise—such as the practice-oriented translation of the AI Act—with concrete technological development.

Ultimately, courage is a structural decision. It is the decision to invest money and resources not only in short-term efficiency gains, but in long-term sovereignty. It is the decision to build essential competencies in-house rather than blindly purchasing solutions.

Those who understand and control the infrastructural foundations of their digital work need not fear political volatility. Security is not a shield one buys once. It is a continuous construction project. The KI.M has laid the tools for this. Now it is up to all of us to use them. ■

"The Psychological Burden Is Massively Underestimated"

Blackout, information warfare, psychological strain: Larysa Visengeriyeva describes how societies function under pressure – and why preparedness is not alarmism, but self-efficacy.

INTERVIEW_ ***Larysa Visengeriyeva***

Dr. Larysa Visengeriyeva is an expert in AI and MLOps. Her specialist book "The AI Engineer's Guide to Surviving the EU AI Act" (2025) is a guide to bringing AI systems to market in a legally compliant and responsible way. As co-founder of "Women in Defense Tech," she advances the transformation of the European defense industry – with a clear focus on "combat-driven innovation" and female leadership.

KEY MESSAGES

→ **A blackout is not an isolated event** but triggers cascade effects: supply, communication, work, and orientation collapse simultaneously.

→ **Resilience arises** where people quickly become capable of acting – through experience, preparation, and functioning local networks.

→ **The greatest vulnerability of modern societies** is not infrastructure, but normalcy bias and a lack of informational resilience.

→ **Ukraine shows** how decentralization, self-organization, and clear information rules secure collective capacity to act.

→ **Preparation is scenario thinking:** Plan A, B, and C – not out of fear, but to preserve calm, control, and self-efficacy.

Photo Zhen Ming Ng

Larysa Visengeriyeva, how did you personally experience the Berlin blackout?

The blackout was a complete surprise for me. At the same time, it was a very clear example of how a so-called "mental firewall" collapses – that deeply rooted assumption that nothing will happen here, that everything works. That was precisely what fell: the realization that it can, in fact, happen.

How did you deal with this situation emotionally and practically?

Personally, I remained relatively calm. I grew up in Ukraine in the 1990s. Anyone who experienced that time there knows what it means to have no electricity, no fuel, no supply. In such a situation, I automatically draw on childhood experience. I knew: I have seen this before.

Did that make you concretely capable of acting, or rather psychologically prepared?

Probably both. I knew what to do. Concretely, that means: first, you monitor the temperature in the apartment and decide in which room to stay. You dress in layers to keep warm. Then you check which independent energy sources are available, at least for light. We actually had to get lamps and headlamps. At the same time, we knocked on neighbors' doors and asked who had what. That networking should actually have existed beforehand.

What other steps were important?

Being able to heat water was central. The blackout happened in sub-zero temperatures, so warm drinks are essential. After that, you continue ›

„The decisive factor in a blackout situation is the cascade effect."

Larysa Visengeriyeva

organizing through circles of friends. These are very simple, but decisive things.

How did communication function during the blackout?

In the first hours and days, the mobile network was very unstable. By chance, I still had a Ukrainian SIM card in roaming that worked for some reason. As soon as one left the affected district, mobile service was partially available again. There was no landline at all – without electricity, no telephone.

In one sentence: what does resilience mean to you?

Resilience is the ability to become capable of acting within the shortest possible time, regardless of what happens.

How can resilience be recognized in the first 24 hours?

Resilience manifests on different levels, from the state level to the personal. The decisive factor is knowing on which level one has control oneself. This capacity to act can be trained, or one is forced into it by crises. For me, resilience is a holistic system design: robust infrastructure, functioning governance, a prepared population, and above all informational resilience. Social media in particular open up new attack surfaces, mentally and emotionally.

How did you experience resilience in your immediate environment?

There were very positive moments. Older neighbors who grew up after the Second World War actively approached us. They offered camping equipment and help if we needed anything. I also experienced authorities such as the Federal Agency for Technical Relief as extraordinarily committed. Information points were set up, people were oriented, emergency shelters were available. That worked.

And what did not work?

The blackout lasted five days. For Berlin and for Germany as the third-largest economy, that is too long in my view. Particularly problematic was that the armed forces had to step in with field kitchens to supply the population. Even supermarkets such as Lidl were still closed days later. For older or vulnerable people, that is a massive problem. That clearly showed: at this point, the system did not function.

What do people most underestimate in a blackout situation?

The decisive factor is the cascade effect. Many think of a blackout only as missing electricity. In reality, a chain of failures follows: the stove does not work, the internet collapses, work and communication break down, even everyday tasks become complicated. Fortunately, the water supply in Berlin functioned. We had cold water, but at least water – that is enormously important for hygiene and dignity. Normally the rule is: no electricity, no water. Then it becomes existential, down to the question of how one even uses the toilet. In addition: no functioning ATMs, hardly any shopping possibilities. These dependencies are massively underestimated. A blackout is not a single disruption, but a wave that hits many areas of life simultaneously.

If we include your experience from Ukraine: what really works when societies are under sustained pressure?

In Ukraine, many people already experienced blackout-like situations in the 1990s. And since 2013, the country has effectively lived in war. This resilience was not built overnight, but over years – because there was no alternative. While we were without electricity in Berlin for five days, the city of Dnipro in Ukraine was completely paralyzed. Within 24 hours, it was operational again. That is not a value judgment, but a fact that shows how quickly capacity to act can return when structures and routines are in place.

You spoke of a "mental firewall." How can it be overcome?

The mental firewall is a cognitive protection mechanism: "That cannot happen here." It helps to avoid fear and stress – and that is deeply human. But in crises, it becomes dangerous. Ukraine lost this firewall through real experience – through war. I very much hope there is another way.

So without a permanent crisis?

Yes. We see this in Nordic countries such as Sweden or Norway. There is systemic preparation. In Sweden, every household receives a brochure: "If war comes – what to do?" It contains clear messages such as: "If Sweden is attacked, we do not give up." In addi- ›

„The volunteer movement in Ukraine is enourmously strong. Without it, the country would not have survived."

Larysa Visengeriyeva

tion, there are practical checklists for everyday life. It is sober, not alarmist, but clear.

How can that be transferred to our society?

By acknowledging normalcy bias and denial instead of taboos. Preparation can also be framed positively: not as fear, but as strength. As capacity to act. As self-efficacy. That requires expertise in system design, psychology, and governance. But the examples are there: Ukraine shows what forced resilience can achieve. Sweden shows that it can also be done through forward-looking system design.

What social infrastructure do we need to endure crisis situations such as a blackout?

In blackout-like situations, self-organization becomes decisive. One is initially on one's own, but not alone: neighbors and local networks gain importance. Informal forms of mutual aid quickly emerge at neighborhood or district level. People knock on doors, share resources, information, and skills. Countries such as Sweden even recommend preparing such structures and overviews of existing skills in advance.

What role does information play in this?

A very large one. Everyone has different information, experiences, and competencies. Some know how to organize practically, others have medical knowledge, others planning experience. When these perspectives are combined, a shared situational picture emerges that helps everyone. This form of shared information is essential for collective capacity to act.

And what lessons can be drawn here from Ukraine?

In Ukraine, particularly small, local communities functioned well – often at village or neighborhood level. A decisive factor was decentralization, which had already been introduced before 2022. This enabled local administrations, local companies, and above all volunteers to act very quickly. The volunteer movement in Ukraine is enormously strong. Without it, the country would not have survived.

What does that mean for the individual mindset?

It leads to a break in the "mental firewall." The framing shifts from "The state will take care of it" to "We can rely only on ourselves." That fundamentally changes behavior. People act faster, more pragmatically, and assume responsibility – for themselves and for others.

Does that mean one should not rely on state instructions?

One should at least factor in that they may not come. Not out of ill will, but because the state has other objectives: stability, order, avoiding panic and economic damage. A well-known example is Ukraine: according to later statements, the political leadership had indications of a large-scale invasion in advance and decided not to communicate this information publicly at first, among other reasons to avoid mass panic.

What follows from that for crisis situations here?

That central instructions may not be forthcoming – whether due to failed communication channels or for strategic reasons. One must be prepared for that. Social infrastructure therefore means: local networks, self-organization, mutual trust, and the ability to remain capable of acting even without central steering.

What is informational resilience? Do you mean the ability to distrust information – or even to manage without state information?

Informational resilience primarily means understanding that today one no longer needs kinetic attacks to break a society. It can be mentally destabilized and its resilience massively weakened – so much so that physical control almost follows automatically. Information warfare is a parallel form of warfare, equivalent to classical military attacks.

What does that mean for resilience?

Preparation for information attacks is just as important as physical or infrastructural preparation. Informational resilience means having defensive mechanisms: individually and collectively. Knowing how manipulation works – and how to protect oneself against it.

Are there concrete examples from Ukraine? ›

„Informational resilience also means an information diet: consciously consuming less and being more selective .“

Larysa Visengeriyeva

Yes. A very important example is the handling of real-time information from war zones. Ukrainian intelligence services worked very intensively with the population to make clear: anyone posting missile or impact locations helps the enemy. Many people did not understand this at first – everyone has a smartphone, everyone films, everyone wants to post. But such images provide precise target confirmation.

How was that addressed?

With clear rules and consequences. This was not a moral debate, but a security necessity. Only in this way could this behavior be stopped. At the same time, official information channels were established: reliable Telegram channels, bots through which observations could be reported without spreading them publicly.

So a deliberate steering of information flows?

Exactly. Today, almost everyone in Ukraine knows which channels are official and can be trusted. Information is collected, verified, and only then disseminated. The population was effectively “trained” not to consume or pass on information impulsively.

Are there civilian models for this outside Ukraine?

Yes, for example Sweden. There it is recommended to verify information via several official channels before acting. First verify, then respond. This is part of state-supported informational resilience.

How can one recognize manipulation in everyday life?

A very simple signal is strong emotions. If a message triggers extreme fear, anger, or hatred, that is a warning sign. Emotions are almost always the carrier of manipulation. Recognizing this is a central component of informational resilience.

Is that easy to implement?

No. In Ukraine, it was a long learning process. But it shows: informational resilience is not abstract. It is learnable – and decisive for a society's capacity to act in crises.

How should one deal with information in crisis situations?

In a crisis, people instinctively tend toward “doomscrolling.” One consumes information incessantly in the hope of regaining control. That is entirely human – but precisely the wrong reaction. Because in such moments, bots and disinformation campaigns are deliberately activated to amplify fear, confusion, and uncertainty. Informational resilience therefore also means an information diet: consciously consuming less, being more selective, and not sharing everything.

Let us return once more to the blackout itself. How did your perception of reality change during those hours and days?

This is something that many people in Ukraine are currently experiencing. The phenomenon is also known from mountaineering: cold massively alters cognitive and psychological abilities. Everything suddenly takes much longer – decisions, thinking, acting. One can no longer function as in a normal state.

So not only organizationally, but physically and mentally?

Exactly. One initially thinks: I will dress warmly, then I can work, call, think normally again. But it does not work like that. The body switches into a saving mode. Your body no longer fully belongs to you – and your mind does not either. I realized this relatively late, but it is central.

What does that mean for prolonged crises?

It means that the psychological burden is massively underestimated. In Ukraine, we are currently seeing an enormous increase in psychological damage. Permanent stress, cold, uncertainty – all of this changes people sustainably. Resilience is therefore not only a question of infrastructure or organization, but also of psychological resilience and regeneration.

What concrete habit should people adopt in order to prepare for crisis situations?

The most important habit is to accept that we live in uncertain times. That is nothing dramatic – it is simply reality. And one can prepare for it. The keyword is scenario thinking.

What does that mean in practice?

Quite simply: Plan A, Plan B, Plan C. Discuss it within the family. Where do we shop if the supermarket is closed? How do we communicate if mobile networks fail? Where do we meet if ›

„War does not begin and end with the military. It always strikes the weak points of a society – information spaces, infrastructures, psyche, everyday life."

Larysa Visengeriyeva

nothing works anymore? In Kyiv, many families had fixed rules: one central person to whom everyone reports – "We are fine." Such agreements seem banal, but they are enormously calming, because one knows what to do.

So this would be an antidote to the "mental firewall"?

Exactly. Not burying one's head in the sand, but being prepared – without panic, without alarmism. Preparation is reassurance.

You speak for a community of women in the field of defense tech. What message would you like to convey in conclusion?

The most important insight is: war does not begin and end with the military. It always strikes the weak points of a society – information spaces, infrastructure, psyche, everyday life. Therefore, each and every one should ask: am I myself a weak point – or part of resilience? Awareness is the first step. And responsibility does not begin "at the top," but with ourselves. ■

Intelligence Without the State?

Open Source Intelligence, social media, and AI are shifting power over information. The democratization of intelligence requires new rules for truth, responsibility, and security.

TEXT_*Irina Rosensaft*

Irina Rosensaft is an expert in digital transformation and cybersecurity – at the intersection of IT, organizational processes, and civil society. With a background in political science and solid experience in process optimization, change management, and cybersecurity, she builds a bridge between technology, governance, as well as organizational and societal requirements.

KEY MESSAGES

→ **Intelligence** is losing its state monopoly and is becoming increasingly collective through OSINT, AI, and digital networking.

→ **Civilians and private actors** are gaining security-relevant analytical capability and influencing political decisions.

→ **The war in Ukraine** shows the opportunities of collective intelligence, but also the risks of misinterpretation and manipulation.

→ **AI increases efficiency** but can massively amplify errors and bias.

→ **Democratic societies** need new rules for interpretative authority, responsibility, and validation of information.

In the 1980s, in what was then the Soviet Union, people lived in great fear that neighbors, friends, colleagues would spy on them, that what was said or appearing in "forbidden places" such as a religious site, being seen with someone, for example someone coming from abroad, would be reported to the feared secret service, the KGB. Distrust, fear, and hushed tones dominated everyday life. Social life was shaped by the Cold War, few news channels, and enemy images. Even then, people found alternative sources of information, but in doing so put themselves at risk.

Almost half a century later, we are experiencing a turning point. Access to nearly all sources of information, partly to personal data and possibly also to sensitive information, is possible. With some technical skill, geodata, personal data, behavior, attitudes, and much more can be collected, analyzed, and published with the help of Open Source Intelligence (OSINT), Human Intelligence (HUMINT), and AI tools. An approach that only a few decades earlier would have cost people their freedom or at least their career and social status is today to a certain extent normal.

Open Source Intelligence (OSINT) reaches a new dimension in Russia's war of aggression against Ukraine. As early as February 2022, OSINT analysts observed troop movements at the Ukrainian border through analyses of geodata, social media posts, and the evaluation of webcams. Social media channels on TikTok and Instagram become sources for locating enemy troops. A merging of private and state actors in war intelligence is taking place. Monitoring War, OSINT for Ukraine, and DeepStateMap are just some of the private initiatives and NGOs that participate in intelli- ›

gence in war, incidentally not only based in Ukraine. Intelligence in the new age has become a collective task that reaches its peak with the help of digital technologies. Private actors complement and replace state functions – but who verifies the truthfulness? Classified data and information, or confidential material, continue to remain in the hands of intelligence activities between states and are gaining importance precisely in the increasingly tense geopolitical situation. Global interconnection and the constantly available mass of digital data are increasingly eroding this information monopoly.

In the past, control over information and thus over the state and its actions required informants; today, the most sensitive information is casually contained in every smartphone and informants are replaced by clicks, photos, metadata, and open sources.

THE EVOLUTION OF INTELLIGENCE – FROM STATE MONOPOLY TO PRIVATIZATION

What actually is intelligence? Mark M. Lowenthal describes it aptly in his work "Intelligence: From Secrets to Policy" as a product of collecting, processing, evaluating, and analyzing interpretations with the aim of supporting political and military decision-makers. For many centuries, states and entire empires attached special value to information and controlled it. As early as the 16th century, people spoke of mysterious messages and espionage. A few centuries later, intelligence reached its peak as a systematically organized process, likewise reserved to the military and the police for the purpose of internal and external security. At the beginning of the 20th century, modern secret services or intelligence services emerged and led to the institutionalization of intelligence. The possession of secret information and control over the dissemination of information are still partly associated with power today. States such as Mao's China saw information as an instrument of rule. The British Prime Minister Benjamin Disraeli, on the other hand, saw in the possession of information an added value for the success of an individual. In different contexts and with different objectives, states and statesmen regarded information as an instrument for establishing security and order.

"States are losing their information monopoly; civilians are increasingly gaining it."

Irina Rosensaft

Between centralization and diversification lie supposedly worlds apart. I find neither reassuring. Despite all the advantages for the defense of my country of birth, the privatization of such sensitive areas previously reserved to states, which among other things decide over war and peace, gives me pause. What if this data is not correct or – possibly intentionally – has been misread and transmitted incorrectly? Are we today ourselves responsible for defining and finding out the truth?

States are losing their information monopoly; civilians are increasingly gaining it. The developments of recent decades therefore raise the question: Who owns information in the 21st century? Who decides on the correctness of the conclusions drawn from it and also who has authority over what of it is published? Who bears responsibility and consequences for the conclusions we draw from it? How does the privatization of intelligence change the state and its sovereignty? To understand what is currently being de-statized and privatized, it is worth taking a look at how the term and its practice have changed. This paradigm shift shows that we need new frameworks for intelligence.

The focus used to be on intelligence gathering and analysis as well as its use on behalf of rulers. The practices served to ensure internal security and to detect and ward off threats from outside at an early stage. The collection of information referred to terrorism or enemies of the state at home and abroad, the military, espionage, and diplomacy. Lowenthal's definition applies to state intelligence. Digitalization makes it collective.

With the democratization of societies and of knowledge in the course of the digital revolution, the understanding of information sovereignty is also changing. Diversification of sources ›

of information, transparency of data in open sources through the internet, platform data, sensors, social media platforms open up an infinitely large variation and number of possibilities to obtain, analyze, and provide data and information.

We therefore find ourselves in an overabundant information environment, and the question arises: who organizes, filters, and interprets information and for what purpose? Does the production of security remain central or are other goals of information gathering and analysis also to be observed?

With diversification and transparency, non-state actors also move to the forefront and make use of the possibilities to advance opinion discourse, bring truths to light, inform in diverse ways. States retain their secrets, but civilians continue to gain importance. New actors include threat intelligence companies, NGOs, journalists, loose OSINT communities, and volunteers who compensate for missing state resources in crises such as Ukraine. Also tech companies that collect and store data and thus build up intelligence capabilities.

Artificial intelligence significantly amplifies this development. It not only collects data quickly but is able to analyze larger volumes of data within seconds, detect anomalies, and place them in connection with other relevant events. All that which people in intelligence services previously compiled and analyzed through laborious work is today done by the machine.

While the human being remains central, in the new age of intelligence an interaction between humans and machines takes place in order to extract the right data and obtain targeted information. This opens up new opportunities but also demands new responsibility.

COLLECTIVE INTELLIGENCE – OPPORTUNITY OR BURDEN?

The democratization of information initially sounds liberating and fitting for liberal and free values. In order to identify opportunities and risks in modern intelligence work, we should not lose sight of the goals and intentions behind intelligence. At its core, it is about ensuring security through risk minimization for political and military decision-making processes, as in the case of terrorism, cyberattacks, state aggression. Intelligence is meant to facilitate decisions and avert dangers.

In the case of Ukraine OSINT, civilians help to defend the country, expose propaganda, and uncover war crimes. Transparent and immediate access to information without filters delivers information quickly and effectively. In many places, it appears like modern partisan work on the one hand and a service to one's own country without having to assume official positions. But who evaluates the authenticity and correctness of the collected information, especially in the digital age in which it is just as quickly manipulable as it arises?

If information is quickly published via social media channels, it can positively or negatively (creation of panic) influence public opinion and public action. A banal example of the manipulation of geodata is provided by a Berlin artist (Simon Weckert), in which, in an experiment, he pulled around 100 mobile phones in a handcart through Berlin and thus misled Google Maps. The system recognized a traffic jam and rerouted users. This case illustrates the manipulability of public sources and the steerability of behavior.

The newly gained freedom cannot be used uncritically. The correctness and interpretative authority are put to the test here. Modern data collectors may have come across manipulated data. Analyzing data without further context could likewise lead to false conclusions.

Critical thinking and digital maturity of users become essential in the 21st century. Information reaches us unfiltered, and validating it is important. Questioning what is seen and heard and then drawing conclusions from it, placing information in context, is today also an individual task. The diversification of ›

"What people in intelligence services previously compiled through laborious work is today done by the machine."

Irina Rosensaft

sources and actors leads on the one hand to the fact that we can use far more information and sources than ever before to find out the truth, minimize risks, and then act independently and responsibly. Examining the quality of sources and validating information is a necessary competence for the new age.

In cyberspace, many harmful phenomena take place, manipulation, espionage, identity theft for example. Being informed about these phenomena and also being given initial options for action on how they can protect themselves against them.

Alongside de-statization and diversification, another risk comes to light. The increase in efficiency of intelligence through AI-supported tools can massively amplify wrong decisions. Human reason and human safeguards remain, even or especially in the digital age, a supporting pillar of intelligence.

about, was the tool compromised? Does the error lie with the AI or with the officers who operated it? At least consequences were drawn, not only personnel-related, but also with regard to the use of AI by the police. The case is a diplomatic faux pas.

Yet the case teaches us another important lesson: that intelligence remains a sensitive matter and that the security and validity of data from a public source provided by a private company is highly problematic. The case shows the failure of state institutions that, with the help of technology, made wrong decisions. Their intelligence should have used other reliable sources such as security authorities of other countries such as Denmark or Holland. It could also have been other unverified open sources.

One of the greatest challenges of modern societies is to retain interpretative authority over data and information. Interpretative

"One of the greatest challenges of modern societies is to retain interpretative authority over data and information."

Irina Rosensaft

INTERPRETATIVE AUTHORITY – WHAT MODERN SOCIETIES MUST LEARN

In November 2025, the football match between Aston Villa and Maccabi Tel Aviv caused a stir. Maccabi fans were completely prohibited from entering the stadium. It was said that there were massive security concerns. The match was declared a high-risk game. What served the West Midlands police as the knowledge base for this decision? The decision was traced back to a match between West Ham United and Maccabi Tel Aviv in which there had allegedly been an escalation of violence on the part of Maccabi fans. However, as BBC reports, this risk analysis turned out to be a hallucination of the AI that had been used by the police, according to investigation reports. According to reports, police officers adopted this information without further verification and created a security report. Now the costs of this false information evaluation are high. Two thousand people were excluded based on unverified information and the resulting risk analysis.

While I am writing this article, many questions remain unresolved. How did this unusual hallucination of an AI tool come

authority is not automatic, but requires certain guidelines and mechanisms in order to be used for the benefit of security and order and not to enable discrimination of a group based on bias and misinformation as here against democratic values. Increasingly, it becomes more difficult to ensure data security, protect trade secrets, and keep classified information confidential. The downside is that stricter guidelines and security architectures are necessary in the age of democratization and digitalization of data and information in order to keep such sensitive information away from the public.

As the cases described here show, shared information is capable of influencing people's actions. Videos on social media could trigger mass panic, manipulated geodata could create false alarms and signals or also favor discrimination through algorithms. Leaked information in the wrong hands, without proper contexts, can pose a danger to security and order and even trigger an international crisis.

Intelligence has become more efficient and, through the democratization of information and the large number of public ›

sources, offers a possibility of self-validation of supposed facts. Through the possession of information, people hold their sovereignty and freedom in their hands, but must also bear more responsibility.

The privatization of intelligence cannot be stopped. Therefore, new rules of the game are needed so that it truly serves overarching protection goals such as security and order and that military and political decisions are made in the place intended for them. More information for everyone, but not every information for everyone. Critical protection needs remain a task of the state. State institutions need new governance for dealing with technologies and stronger review bodies. Cooperation with non-state actors must proceed in a value-based and regulated manner. The flood of information makes critical thinking a core competence of our society. Modern, indeed democratic intelligence only functions if it rests on digital maturity and if the state continues to protect the values it serves. ■

"We Rely Too Much on Regulation"

Cyberattacks have long been destabilizing everyday life. It is not a lack of laws but a lack of risk competence that makes them so effective, says Dennis-Kenji Kipker. A conversation about hybrid threats, trust, and the limits of technical solutions.

Dennis-Kenji Kipker, from your perspective, what is the particular challenge of hybrid threats?

Hybrid threats do not affect just a single domain, but society, the state, the economy, and politics all at once. The problem is that we are still thinking in silos. Responsibilities are separated instead of acting in a networked way.

Where does this silo thinking become evident in concrete terms?

For example, with disinformation: Is the state responsible, the platforms, the schools, or the parents? This separation falls short. Hybrid threats show that old patterns of thinking no longer work. We need networked thinking, more transparency, and above all trust between all actors.

What role does trust play in this?

Without trust, neither communication nor cooperation works. Companies, for example, ask themselves whether they can report security vulnerabilities to authorities at all without risking disadvantages. That is why we need new verification mechanisms and reliable communication structures.

What is your most important learning from years of working in cybersecurity?

Cybersecurity is a task for society as a whole. In the past, the focus was only on critical infrastructures. Today, in a highly interconnected world, vulnerabilities arise everywhere – without us having created an adequate security backbone.

Where do the greatest failures lie? ›

INTERVIEW_ ***Dennis-Kenji Kipker***

Prof. Dr. Dennis-Kenji Kipker is Scientific Director of the cyberintelligence.institute in Frankfurt am Main and member of the executive board of the strategy consulting firm CERTAVO AG. He conducts research at the intersection of law and technology in cybersecurity, corporate strategy, and on digital resilience in the context of global crises.

KEY MESSAGES

→ **Hybrid threats** affect the state, the economy, and society simultaneously – silo thinking prevents effective counter-strategies.

→ **Trust is the key:** Without reliable communication and reporting channels, cooperation between the state and the private sector remains fragile.

→ **Cyberattacks** are primarily effective psychologically because they paralyze everyday services and undermine institutional trust.

→ **Pure regulation** does not create a level of security; best practices cannot be decreed by law.

→ **Sustainable resilience** arises through risk competence, concrete examples, and local, low-threshold awareness formats.

Photo cyberintelligence.institute

We have massively expanded connectivity – internet, Internet of Things, 5G – but have not established an equivalent protection mechanism. For a long time, this was ignored. Only events such as Stuxnet or attacks on the Bundestag made the issue politically visible.

Why are cyberattacks so effective today?

It is often enough to paralyze digital public services, for example through DDoS attacks. This has an enormous destabilizing effect and undermines trust – from cyberspace into physical everyday life.

Why is this so central?

Because every executive is also a citizen. It is not about abstract functions, but about people. We must reach society as a whole and go into the field. Only in this way can these issues be communicated in an understandable and credible manner.

Where is this particularly evident?

In municipal cybersecurity. Many municipalities are poorly protected, not out of ill will, but due to a lack of awareness. IT budgets are often decided by volunteer local politicians who have little day-to-day contact with digital risks. If you want to reach them, you need local, low-threshold formats.

From your experience, what works to create awareness – and what does not?

Purely abstract training hardly works. If one only talks about ransomware, phishing, or DDoS, many think: "That won't affect me." We must show concrete examples – from the same sector, region, or municipality. What were the consequences of an attack? What worked in defense? Only then does cyber become tangible.

What does it often fail because of?

Many perceive cyber as something distant and technical. From this arise two attitudes: a feeling of being at the mercy of events and the hope that someone else will take care of it. That is precisely what makes attacks successful – because basic awareness is lacking.

Attacks are becoming faster and increasingly automated. Does threat intelligence therefore need to be rethought?

Pure threat intelligence often remains technical and abstract. The decisive question is: How likely am I to be affected? Do I even understand the risk? Information must be accessible and classifiable, not only for experts. People must be able to assess risks; otherwise fatalism arises. If every alert merely alarms without providing context, many will eventually tune out.

"Many municipalities are poorly protected, not out of ill will, but due to a lack of awareness."

Dennis-Kenji Kipker

How can cooperation between the state and the private sector be improved?

In addition to existing public-private partnerships, we need new regional formats. Medium-sized enterprises in particular cannot be reached through large conferences. We must go into the field – into municipalities, schools, and companies. Only in this way can sustainable resilience and genuine trust emerge.

At which levels within organizations do you see the greatest problems?

The decisive level is top management. If executives do not take the issue seriously, the operational level usually does not either. Then only a few individuals remain who warn but are not heard. Awareness must therefore begin at the very top – in authorities as well as in companies.

How can this be changed?

By preparing information in an understandable way. That is precisely why we are developing formats that enable citizens to classify threats, for example in the case of data leaks or security advisories. Only when people understand what is truly relevant do they take responsibility instead of delegating everything to others.

What would be the one most important thing you would tackle immediately?

We currently rely too heavily on statutory regulation. Laws create awareness, but they do not automatically make either the state or society safer. Even after new regulatory frameworks, objectively nothing is safer than the day before. What matters are best practices – and these cannot simply be mandated by law. ›

Why is that?

Our infrastructures are extremely diverse. A local waterworks can be comparatively well secured, whereas power or rail lines stretching hundreds of kilometers can hardly be protected according to uniform standards. Sustainable protection concepts are lacking for this.

„Prevention requires risk competence and awareness. If risks remain abstract, what ultimately happens is: nothing.

Dennis-Kenji Kipker

What is needed instead?

Intrinsic motivation. People and organizations must be able to recognize and assess risks themselves.

Does that require major crises first?

Crises happen constantly, but their impact quickly fades. After a power outage, there is short-term discussion, but as soon as everyday life returns, the issue disappears again. Prevention requires knowledge, risk competence, and awareness. If risks remain abstract, what ultimately happens is: nothing. ■

Are We Intelligent Enough for Democracy?

Democracy does not fail for lack of elections, but for lack of judgment. When citizens misunderstand politics as the mere delivery of interests, compromise turns into disappointment – and authoritarian solutions appear seductively simple.

TEXT_ ***Birger P. Priddat***

Prof. Dr. em. Birger P. Priddat taught economics and philosophy at the University of Witten/Herdecke and previously held the Chair of Political Economy at Zeppelin University. He is Senior Research Fellow at the Witten/Lab of the Studium Fundamentale and most recently published "The Market of the Befriended Citizens in Rich Athens" (2025).

KEY MESSAGES

→ **Democracy** is not a system for enforcing individual interests, but a procedure of coordination, consideration, and revision that integrates differences instead of excluding them.

→ **Political disappointment** often arises from a misunderstanding: in plural societies, politics cannot "deliver" without at the same time disappointing.

→ **Voting** presupposes the capacity to judge: whoever votes for parties that want to abolish democratic procedures votes away their own political co-determination.

→ **Authoritarian offers** appear attractive because they reduce complexity – but they destroy the possibility of political correction.

→ **Democracy today needs more than elections:** strategic intelligence, institutional design, and citizens who understand politics as a shared project.

"Be soft and strong. Be clever, engage, and disdain victory"

Peter Handke

Democracy is under scrutiny, even among those who consider it the best form of government. Are we facing a crisis? Many do not want to abolish "the system," but rather the government – a democratic attitude. The change of governments belongs to the fundamental principle of the democratic. Skepticism toward current governments is based on disappointment. The deception that becomes visible in this disappointment is called: campaign promises that are not kept. But increasingly it is also about the perception that current governments can neither maintain the achieved level of prosperity nor stimulate growth – there is a fear of loss (essentially a fear of weak growth, when jobs, wage and income increases are at risk of being lost, AI constantly sets new demands, etc.). The accompanying suspicion of political incompetence is combined with the opinion that politics needs more leadership. Leadership, however, is a problematic category of the democratic, because it presupposes that one party has a majority in order to govern through. But what if a party gains a majority in order to abolish "the system"? If it governs "through democracy," as we must expect from the AfD? ›

This is the breaking point of the democratic: a legitimate election of illegitimate politics. Some – especially the right-wing extremist part of the AfD – want to abolish the democratic system – a stance that does not conform to democratic rules of the game. For it would be a "last election": afterward, voting would be abolished. How can a democracy ensure that it remains a democracy? What constitutes the core of the democratic? Is there such a core, and: under what conditions? Do citizens understand democracy?

The impression arises that strong governments would pursue policies that would address the problems that move citizens and whose unresolved nature disappoints them. Only a majority of a single party could tackle the imagined leadership problem, but of course only to the extent that it can implement its policies. But if voters – democratically normal – vote diversely, that is, do not make a single party capable of a majority, coalitions are necessary. And in coalitions, compromises – which in turn disappoint the interests of each specific party's voters. In this sense, a democratically elected government is systematically overburdened, because – especially in coalitions – it cannot fully "deliver" what corresponds to the respective interests. For the other interests must also be taken into account. And in this sense, voters are systematically overburdened, because these constellations must of course disappoint if they do not understand this democratic basic pattern. Politics is a task of shaping, not a march-through of control.

Democracy sorts the diversity of interests; it does not hegemonically abolish them. It works with a *synchronization* of multiple interest fulfillment: it is about the politics of society, not about individual interest privileges. It must always be clarified with others what can and should be done – a democratic basic requirement of consideration that is not *self-evidently* anchored in citizens' understanding of politics. A consideration that others are not excluded by the respective policy – an underlying *pattern of cooperation*.

To speak of cooperation here is unusual, because the different parties represent value and interest oppositions that are more readily thought of in terms of opposition or competition. But ultimately they have a common, if mostly concealed, interest: that democracy as constitution and procedure be preserved, for this alone is the guarantee that they will continue to be involved in the political game. An authoritarian government would eliminate or obstruct the opposition, that is, dissolve the liberal pattern. It would become *reckless* in a fundamental sense, take no consideration of others beyond its voters, even act radically against migrants. In this recklessness, the value of democracy can be newly assessed: as a system of differences that do not become antagonistic, in which recognition of others and their inclusion prevails, not their exclusion.

For regardless of whether parties enter coalitions to govern together or remain in the field of tension between government and opposition: they play the same game, only with power distributed differently. Democracy means that the power one wins is reviewed in the next elections and, if necessary, voted out. The essential core is: no "tyranny," no sole rule. Democracy must allow *revision*. This is directed in particular against parties that, once they win a majority, can use it to exclude others or not take their interests into account – exclusion instead of inclusion. Instead of enduring difference as opposition, they make the others into enemies. They split the fundamental sense of community into an inside and an outside (into "Germans and foreigners" in the AfD's case, whereby even the "Germans" are split into excludable "leftists" and "nationals").

Taking the interests of others into account: *inclusion*, is the cooperation required in democracies and which finds its form in compromise – not only a compromise of the governing coalition, but also in a broader compromise in all decisions, laws, etc., to think of the others, in such a way that the cohesion of society plays a role in the decisions. For politics is not solely the project of a majority party or a coalition, but of society as a whole, so that those who are not currently represented in governments re- ›

„Democracy works through the synchronization *of multiple interest fulfulment."*

Birger P. Priddat

main part of it and receive consideration. This is the fundamental cooperative moment of a democracy. Josiah Ober speaks of a "core democracy" ("Demopolis" 2017), a normative framework of democratic politics. This norm must be co-decided again and again so that democracy remains reality.

For democracy is not a form of alternating sole rule; rather, every government moves in the context of those who are not represented in the government, in order to ensure the cohesion of society. If the stronger simply prevailed, this would be an idea of freedom as arbitrariness, which forgets that politics encompasses the shaping of the entire "polis" of society and not the enforcement of the interests of one group, one elite, one part of the population. To exclude this, democracy was invented as the self-organization of all citizens, in antiquity, which at its core allows all to participate in politics.

This idea has faded in modern democracies. Many citizens are passive voters; they do not even understand themselves as political citizens, but as private individuals who no longer feel addressed by questions of shaping society: by politics. They misunderstand politics as the delivery of interest fulfillment and feel little or no responsibility for the communal project. In this distance, they perceive politics or governments as elite projects in which they are not involved, toward which they are skeptical to openly opposed, without political participation, that is, upon closer inspection, without political influence that they as citizens in a democracy ought to have.

They lack a basic understanding of the political. They in a sense make themselves subjects: passively prepared to accept what is governed. If they – like many – are tired of politics, do not participate in what constitutes their society, they delegate the political to some form of rule, with the explosive consequence that, if they no longer want this rule, they cannot revise it.

This assessment is significant insofar as when voting in democracies one must consider that only parties should be elected that do not want to abolish voting. The thought is little known insofar as it is not only voting that is important, but that democracy itself must be preserved through voting. The election of parties that can abolish democracy cannot in this respect be democratic, because they abandon the basis on which they are elected.

The principle of democracy sustainability is violated. This is not about prohibitions, but about the rationality of voters being able to judge what consequences their electoral decisions may have. In critical phases, such as the current right-populist trend, it is not enough simply to vote (for a party); rather, in a certain sense one must vote twice: namely for the parties and for democracy. By electing parties (AfD) that work authoritatively to abolish democracy by wanting to exclude others ("leftists," "liberals," migrants, etc.), one abolishes one's democratic potency to vote and delivers oneself to the new rulers, in order to fall *into civilizational nothingness*.

This reveals a picture that many are tired of politics. And that they are cognitively overwhelmed by the decision of which policy is good and right. And that one – in an old image – would like to let the "good king" govern. In doing so, one conceals a highly significant moment. For if the "good king" proves to be domineering and bad, there is no longer a political procedure to abolish him, no longer even the possibility to elect a "better king." One would then have delegated the shaping of society to a ruler of one party, an elite, without reassurance of ever being able to regain influence over the political. AfD voters run the risk not only of electing a party that wants a "different system," but of ending up in the risk of no longer having a place themselves in this other system. Is it intelligent to make a decision that eliminates future decision-making?

In antiquity, with Aristotle, politics was tied to the prudent, educated decision within communality *(politike koinonia)*: ›

„Many citizens misunderstand politics as the delivery of interest fulfillment and feel little or no responsibility for the communal project."

Birger P. Priddat

prudence *(phronesis)* belonged to the dianoetic virtues – as a necessary precondition of the political action of virtuous citizens. These are ancient conditions that do not apply unconditionally to our modernity. In modern terms, this communality could be formulated as a *shared mental model* of the political: as a jointly shared conviction of having a procedure that enables self-determination. What stands out is that we often associate democracy with freedom and interests, in such a way that we believe that in political business we want to choose and enforce our interests. The will to choose freely as an individual dominates and configures itself with the interests of others. The will to be free is pronounced as the idea of valuing individual private matters highly, without it being coupled to an interest in others.

Such consideration seems to contradict our understanding of freedom. Yet the thought that the political is a communal project – namely, to realize one's own interests in the context of the interests of others under the interests of all – has been lost. Democracy is "not an intuitive system. It is a system that requires people to be able to argue with one another and still work together in the interest of the country," as the historian Anne Applebaum says in the FAZ. But what is political about the democratic is precisely the coordination of tension and difference of interests and the cooperation necessary for it. Compromise is a productive moment of this kind of cooperation. Which means: to place one's own freedom of choice in a context of everyone's freedom, not as an individualistic enforcement, but as reciprocal cooperation. Are we, in a certain way, not intelligent enough to understand the communal moment of cooperation and coordination of interests?

Not intelligent enough means: not having learned to distinguish between opining and judging. Many think that mere opinion is enough in order to be able to vote politically. What they opine is based on accidental knowledge, imagined intuitions, and often on resentments toward others. Opinion becomes an unreflected resource of electoral decisions. Many vote the way others vote, i.e., they do not have an opinion of their own at all, but borrow it. Thus opinions join together into a decision without judging what is to be chosen. To judge means to have reasons to decide for a decision, to be informed about contexts. Political judgment means being able to know what consequences which choice has, and not only for one's own interests, but also for the cooperation of society and its developments, including the co-running decisions about preserving democracy. If one votes away one's own competence to continue co-determining in the future, judging becomes worthless for the future. Opportunistically one then definitively joins opining, which dominates in a rule-like manner.

All this is already happening to a large extent in *social media*. The "old" public sphere (newspapers, TV), in which topics were still discussed and exchanged by many at the same time, fragments in *social-media communication*, in which there is no longer discussion, but in one's own bubbles, sealed off, the first-best opining is copied and confirmed. Democracy loses its great political arena, in which differences were of course contested, but everyone was involved in the same topic by mutually providing reasons and critiques: a process of political education (a kind of "campfire that creates unity" (Poniewozik)). *Social media*, by contrast, privatize the public, and everyone remains in a space free of confrontation, in which politics can no longer appear as a communal project. The idea of the political as a social project, with which one engages in order to gain viable concepts, falls away.

Are we intelligent enough to be democratic under these conditions? This is not about a demeaning talk about citizens, but about a pragmatic assessment. Above all: which intelligently tailored institutions would help to promote citizens' willingness to participate? And it is also and above all not only about citizens, who rarely oversee the complexity of political decision necessities, but about intelligent party politics and above all about intelligent *institutional* design of the state. ›

„In antiquity, with Aristotle, politics was tied to the prudent, educated decision within communality."

Birger P. Priddat

For in everything that has been discussed so far, it remains overlooked that many decisions in politics no longer originate from one's own scope of disposal, but appear as reactions (in the better case anticipations) to extra-political circumstances and conditions (EU laws, global trade, geoeconomics of the world powers, in which German politics plays no role, threats of war, energy and resource questions, weakness of EU foreign policy, etc.). These topics, which the respective politics must process along with everything else, will hardly play the role in election campaigns that they nevertheless mean for the business of governing and for society as a whole. Even less so for voters, especially since it is not only complex topics that stand out in social questions, but at the same time multiple problem situations that must be handled synchronously. Politics needs an intelligence to relate the domestic and the extra-political requirements.

The intelligence demanded here essentially rests on not only facing these topics, but above all: addressing them strategically. Intelligent institutional design means having procedures for information acquisition and analysis (intelligence in a structured sense) that go beyond the traditional or accidental assessments in politics in order to be able to produce strategic decisions that are data- and analysis-based and therefore can carry the strategic upheavals. It would be about self-binding on the basis of strategic intelligence: being able to make well-founded promises that can also be kept.

These are topics that cannot, or should not, be assignable to any one party or only to individual interests, but always concern the whole of society. The strategic requirements are just as general, that is, to be addressed by all parties insofar as they do not deny the objective requirements, so that what we earlier called the cooperation principle becomes practical – that it depends on a synchronized strategy that is not broken off at the next round of elections by a next government, so that the country would be entirely exposed to international competition, or the respective initiated developments would be broken off again.

At this point, the theme of leadership can be taken up anew. Not in the sense of sole, domineering steering, but in the sense of an intelligent synchronization of the internal social political interests in the context of their extra-political requirements and problem situations. Synchronization would be an art of management of the problem situations, which can succeed if one has a strategic consensus that, in view of the changes and problem situations, must anyway be constantly adjusted in an agile way. Leadership here means arranging oneself again and again intelligently along an outlined line, and indeed by all participants, to a certain extent also in basic consensus with other parties. And the oppositional tensions would also have to move. Here it is not one person or one party that leads, but all politically involved coordinate themselves with a view to coping with the problem situations. This does not mean that different designs do not come into play, but all are oriented toward solutions, not toward mere difference. In this play of different designs, an intelligent handling of difference is needed: politics becomes difference management, always including the domestic-political differences and the extra-political requirements. Less will not be to be had, except lack of success and further disappointment. It is not about a party winning, but rather about advancing the project of society.

In the multiple problem situations, domestic as well as extra-political, politics will have to negotiate again and again anew, in the governing coalitions anyway, but also in the other parties and in society. For the dynamics of social and above all economic changes in requirements must reckon with the recursiveness of the relations, which must be dealt with intelligently. Neither ideologically nor conventionally. Politics enters processes of unstable stability, that is, into a politics mode that is still little pronounced in the worlds of experience of citizens as well as many politicians. Political education means understanding how, in this dynamic, intelligent behavior is to be learned.

Democracy cannot rely on its structures, procedures, constitution, nor on the legal system, to which politicians who do not ›

„Which intelligently tailored institutions would help to promote citizens' willingness to participate?"

Birger P. Priddat

dare to decide delegate the final decisions (a non-democratic procedure of delegation to a non-parliamentary instance), but it needs an understanding of its coordination intelligence, precisely now in the new world of multiple and polyvalent requirements – an understanding of agility that again and again reweaves the inclusion of divergent interests, in continual work on the project of democratic communality.

However, it will become more difficult, because we are approaching a turning point: in the shallows beneath the surface of the AI worlds, the convenience of the automation of politics threatens, the loss of democratic sovereignty. It is a completely different point of entry for the authoritarian regimes, as Curtis Yarvin dreams of the "tech CEO king," as Peter Thiel, Elon Musk, Balaji Srinivasan and Alex Karp consider democracy a dead cultural technique and Patrick Deneen offers them, still below the AI threshold, the idea of "aristopopulism": the rule of new elites who leave the population apolitically submissive in Amazon-generated consumption, with the tech-world consequence that AI, measuring algorithmically, could capture people's moods better than voters' votes. Why then still vote? The political becomes for the population the delivery of its consumption mood, as it were in a non-cancellable subscription, while the elites take the path of uncontrolled enrichment – a society of double (split) *delivery*.

Fatal is the transfer of the intelligence theme into *artificial intelligence*, which is sold as efficient coping with complexity, beyond democratic politics, whose inclusion and integration behavior threatens to become superfluous. This goes along with politics fatigue: AI politics is the cultural relief from a polyvalent world and from the efforts of civic self-assertion. Richard Rorty had already suspected in the 1990s that democracy would rest only on a "contingent consensus," as if it were a temporary historical epoch.

How much democratic intelligence must we expend in order to remain in the history of civilization? ■

„AI politics is the cultural relief from a polyvalent world and from the efforts of civic self-assertion."

Birger P. Priddat

Contributors and Interviees

Dr. Timo Blenk is senior Partner & CEO, heads the strategy consultancy Agora Strategy Group AG, which emerged from the Munich Security Conference. The geopolitical expert advises industrial companies on global trends, market entries, and optimization of procurement and production architecture.

Dr. Raluca Csernatoni is a Fellow at Carnegie Europe in Brussels, focusing on European security and defence policy as well as AI and emerging technologies. She leads the organisation's research on the geopolitics of AI, serves as Guest and Visiting Professor at the Vrije Universiteit Brussel and the University of Antwerp, and conducts research in several EU-funded projects on cyber and digital policy.

Prof. Dr. Anna Daun is Professor of Political Science at the Berlin School of Economics and Law (HWR). She teaches security topics in the degree programs for senior police service (gehPVD) and security management, and is Deputy Director of the Research Institute for Public and Private Security (FÖPS).

Prof. Dr. Jan-Hendrik Dietrich teaches at the University of Applied Sciences of the Federation in Berlin and at the University of the Bundeswehr Munich. Together with Prof. Dr. Carlo Masala, he heads the master's program Intelligence and Security Studies, is Co-Director of the Center for Intelligence and Security Studies at the University of the Bundeswehr Munich, and serves as chercheur invité at Sciences Po Paris. He is the author of many publications on security law.

Ole Donner is the founder of Structured Analysis Germany and advises government institutions, international organizations, and companies on intelligence and analytical capabilities. Previously, he served for 13 years in the German Armed Forces as an analyst, supervisor, and lecturer, where he shaped analytical training. He is co-author, among other works, of the book "Clear Thinking" (2025) as well as initiator of the German Intelligence Community Conference (GICC).

Dr. Alana Gramm is an OSINT specialist and Senior Strategy Consultant at IBM iX. Her focus areas lie in Open Source Intelligence at the interface of intelligence, law enforcement, and defence. Previously, she worked for nine years at the Berlin State Criminal Police Office (LKA), initially as an OSINT analyst in the field of terrorism, and later as Coordinator of OSINT Analysis.

Dr. Aviva Guttmann is a Lecturer in Strategy and Intelligence at Aberystwyth University. Previously, she conducted research at King's College London (King's Intelligence and Security Group) and at the University of Southern Denmark. She is the founder and chair of the Women's Intelligence Network (WIN). Her research on intelligence services, covert operations, and terrorism has been published, among other works, in "Operation Wrath of God" (Cambridge, 2025).

Prof. Dr. Eva Herschinger is Professor of Security Studies and Head of the Research Area Security and Intelligence at the Center for Intelligence and Security Studies at the University of the Bundeswehr Munich.

Prof. Dr. Beatrice Heuser is Distinguished Professor at the Brussels School of Governance (VUB) and Head of Strategy Teaching at the German Armed Forces Command and Staff College. Her research focuses on why humans wage war, which means and strategies they choose – and how they justify them.

Prof. Dr. Holger Janusch is Professor of International Politics with a focus on U.S. foreign and security policy at the Department of Intelligence Services of the Federal University of Applied Administrative Sciences (Hochschule des Bundes für Öffentliche Verwaltung) in Berlin, with research focuses on national security strategies, U.S. trade policy, and power in theories of International Relations. He curated the special volume "Integrated Security for Germany?" (2025). (2025).

Prof. em. Loch K. Johnson is Regents Professor of Public and International Affairs Emeritus at the School of Public and International Affairs (SPIA), University of Georgia. He is the author or editor of over forty books, including most recently The Oxford Handbook of National Security Intelligence (Oxford University Press, 2025); and National Security Intelligence, 3d ed. (Polity, 2024).

Prof. Dr. Dennis-Kenji Kipker is Scientific Director of the cyberintelligence.institute in Frankfurt am Main and member of the executive board of the strategy consulting firm CERTAVO AG. He conducts research at the intersection of law and technology in cybersecurity, corporate strategy, and on digital resilience in the context of global crises.

›

Lars König combats abuse systems worldwide as the founder of NetWatch through a community-based approach. He is part of the Customer Advisory Boards of Google and CrowdStrike.

Brendan Kotze is Chief Delivery Officer at Performanta, an internationally operating cybersecurity company headquartered in London, UK. With more than 20 years of experience in IT security, he has worked across the entire security lifecycle, including serving as a CISO. Today, he leads development, automation, and advisory services with a focus on practical security solutions that reduce business risk and protect people in the digital domain.

Prof. Dr. Rafaela Kraus is Professor of Corporate and Human Resource Leadership at the University of the Bundeswehr Munich. Her research includes intrapreneurship and entrepreneurship, defense/dual-use innovation, transformation (e.g., the automotive industry and defense), leadership, and organizational culture.

Prof. Dr. em. Wolfgang Krieger taught Modern History at Philipps University Marburg and was a Fellow at the universities of Oxford and Harvard. He is a member of the International Institute for Strategic Studies (IISS) and of the Conseil scientifique de la recherche historique de la défense at the French Ministry of Defense, and a co-founder of the International Intelligence History Association. In 2026, he published ***Geschichte der Geheimdienste*** (*History of Intelligence Services*).

Krista-Marija Läbe is a German-Ukrainian public relations manager at Quantum Systems. Previously, she worked as a strategic communications advisor for the Ukrainian Embassy in Germany. She is also co-founder and board member of the German-Ukrainian Society and is committed to raise awareness of Ukrainian perspectives in European discourse.

Marc Mahlke is a cybersecurity expert with an interdisciplinary background in information and communication technology and IT management. He works at the intersection of technical security analysis and strategic cybersecurity, with focuses on penetration testing, red teaming, governance, and intelligence approaches at the organizational level.

Luca Manns is Managing Director of the Research Center for Intelligence Services at the University of Cologne. The legal and economic scholar regularly publishes in legal journals, advises government bodies as well as parliaments. In addition, he is involved in establishing the Adenauer School of Government at the University of Cologne and teaches law of digitalization.

Prof. Dr. Christoph Meyer is Professor of European and International Politics at King's College London. For over 15 years, he has researched early warning, strategic surprise, and learning from crises. His books include ***Warning about War*** (2020) as well as *Estimative Intelligence in European Foreign Policymaking: Learning Lessons from an Era of Surprise* (2023).

Armin Müller is Regional Vice President Central Europe at Veeam. Previously, he held leadership positions at Broadcom Software, VMware, and Oracle, as well as at IBM and T-Systems. He was responsible for growth, cloud transformation, and enterprise strategies in Europe. Müller holds an MBA from Henley Business School and a degree in business administration (Diplom-Kaufmann).

PhD Dr. Daniel Rainer Neumann is a political scientist with a focus on Intelligence Studies and Assistant Professor at the Institute for Security and Global Affairs at Leiden University. He has researched the support of the EU's Common Foreign and Security Policy by the intelligence services of the Member States, particularly vis-à-vis the EU Intelligence and Situation Centre (INTCEN).

Dr. Konstantin von Notz is a member of the German Bundestag (Alliance 90/The Greens) and Deputy Chair of the Parliamentary Oversight Panel, which supervises the three federal intelligence services: the Federal Intelligence Service (BND), the Military Counterintelligence Service (MAD), and the Federal Office for the Protection of the Constitution (BfV). Among other roles, he served as Chair of the "NSA" Parliamentary Inquiry Committee and as a member of the "Berlin Breitscheidplatz" Inquiry Committee. Since 2017, he has been a member of the Parliamentary Oversight Panel, which he chaired from 2021 to 2025.

Dr. Esther Omlin is a lecturer in security law and commercial law at the Eastern Switzerland University of Applied Sciences (Ostschweizer Fachhochschule OST) and previously served as a senior public prosecutor. Her research focuses on external and internal security, international security policy, space, and foreign trade law, and she offers corresponding continuing education programs.

Niccolò Petrelli, PhD, is Assistant Professor in the Department of Political Science at Roma Tre University, where he teaches strategic studies. In 2025, he published the book I servizi segreti italiani e l'Intelligence USA (The Italian Intelligence Services and U.S. Intelligence) a history of the reciprocal relationship from 1943 to the 1970s.

Prof. Dr. em. Birger P. Priddat taught economics and philosophy at the University of Witten/Herdecke and previously held the Chair of Political Economy at Zeppelin University. He is Senior Research Fellow at the Witten/Lab of the Studium Fundamentale and most recently published *"The Market of the Befriended Citizens in Rich Athens"* (2025).

Christopher Radler-Morić is an expert in corporate security with a focus on business continuity management, emergency and crisis management, travel security, and intelligence. With an intelligence background and a master's degree in Arabic studies, ethnology, as well as risk and crisis management, he combines strategic security analysis with deep cultural and geopolitical understanding of complex risk environments.

Dr Daniela Richterova is Associate Professor of Intelligence Studies at the Department of War Studies at King's College London. Her research on Cold War intelligence services, state threats, and terrorism has been published in International Affairs and Foreign Policy, among others. In 2025, she published *Watching the Jackals* (Georgetown University Press).

Felix Rieger is responsible for public relations at the KI-Kompetenzzentrum Medien (KI.M). In his daily work, he engages with artificial Intelligence, media innovation, and community building.

Irina Rosensaft is an expert in digital transformation and cybersecurity at the intersection of IT, organizational processes, and civil society. With a background in political science and solid experience in process optimization, change management, and cybersecurity, she builds a bridge between technology, governance, as well as organizational and societal requirements.

PD Dr. Frank Sauer is a political scientist and publicist. As Research Director of the Metis Institute for Strategy and Foresight, he researches the nexus between security, technology, and society and advises the Department for Strategy Development in the German Federal Ministry of Defence. He is co-host of the award-winning podcast "Sicherheitshalber" on current developments in German security and defense policy.

Christina Schäfer supports companies at Agora Strategy Group as a consultant in anticipating geopolitical risks and building resilience in supply chains and business models. Previously, she worked in risk consulting at PwC and at the German Federal Foreign Office and completed her master's degree at Sciences Po Paris.

Oberst a. D. Klaus Schmidt held leading functions in the German security and intelligence sector, among others as head of division and head of section in the Federal Intelligence Service and as a desk officer in the Federal Ministry of Defense. Previously, he served as a General Staff officer, battalion commander of the Franco-German Brigade, and officer in the Bundeswehr. He is Chairman of the Gesprächskreis Nachrichtendienste in Deutschland (GKND).

Dr. Ralf Schneider is Chairman of the Board of the association Cyber Security Sharing & Analytics e. V. (CSSA) – an association of 17 large German companies with the aim of better protecting themselves and the public IT infrastructure jointly against cyberattacks.

Jim Sengl heads the KI-Kompetenzzentrum Medien (KI.M), a joint initiative of Medien. Bayern GmbH and the Bayerische Landeszentrale für neue Medien (BLM). His work at the KI.M focuses on supporting the media industry in the legally compliant and future-proof use of artificial Intelligence.

Dr Jennifer E. Sims held senior positions within the U.S. national security establishment, including at the U.S. Senate Select Committee on Intelligence and as an intelligence coordinator at the State Department. She also taught at Georgetown University. In 2022, she published her book Decision Advantage. She is also an artist and founder of the Stuart Street Atelier.

Thomas Vašek is Co-Editor-in-Chief of human. Previously, the trained investigative journalist was, among other roles, founding editor-in-chief of the philosophy magazine Hohe Luft and of the German edition of MIT Technology Review. He is also the author of several non-fiction books, including Schein und Zeit (2019), Land der Lenker (2019), and Work-Life-Bullshit (2013), a widely discussed contribution to the debate on the value of work in our lives.

Dr. Larysa Visengeriyeva is an expert in AI and MLOps. Her specialist book "The AI Engineer's Guide to Surviving the EU AI Act" (2025) is a guide to bringing AI systems to market in a legally compliant and responsible way. As co-founder of "Women in Defense Tech," she advances the transformation of the European defense industry – with a clear focus on "combat-driven innovation" and female leadership.

Jeff Watkins is the founder of the AI consultancy Northstar Intelligence (UK) and a Founding Member of the Business AI Alliance. Previously, he served as CTO of the technology consultancy CreateFuture. His industry focus spans financial services, healthcare, and oil trading. An enthusiast for cybersecurity and AI, he is also active as a podcaster and international speaker.

Richard Weiss works at the interface of technical analysis and strategic doctrine. With a background in mathematics, physics, and data science, he was, among other things, a reverse engineer on Mandiant's FLARE team. He advises two NATO Centres of Excellence (COE) as well as military and public institutions and researches the use of AI and LLMs in intelligence tradecraft.

Julian Werner is a former paratrooper and officer of the Army's specialized forces (EGB). Since 2024 he has been conducting research under Prof. Dr. Carlo Masala at the Center for Intelligence and Security Studies on topics such as urban warfare and military innovation. His book *Urban Warfare – Krieg zu Hause* will be published in April 2026.

Marcus Willett (CB, OBE) worked for 33 years at the UK's Government Communications Headquarters (GCHQ), most recently as its deputy head with personal responsibility for the agency's intelligence collection and cyber operations. Prior to that, he was GCHQ's first Cyber Director and led the UK's National Offensive Cyber Programme. Since leaving government service in 2018, he has been a Senior Advisor at the International Institute for Strategic Studies (IISS). In 2024, his book *Cyber Operations and their Responsible Use was published.*

Simon Wunder is responsible at Volkswagen AG for the analysis of geopolitical risks for supply chains. In addition, the political scientist is a Research Fellow at the Center for Advanced Security, Strategic and Integration Studies (CASSIS) at the University of Bonn. This contribution reflects his personal views. ■

Imprint

Editors-in-Chief
Dr. Rebekka Reinhard, Thomas Vašek (responsible under the German Press Law)
human Forward and *human* Magazin are published by philosophy works GmbH,
Dr. Rebekka Reinhard,
Westermühlstraße 13, 80469 München
info@philosophyworks.de

Contributors
Timo Blenk, Raluca Csernatoni, Anna Daun, Jan-Hendrik Dietrich, Ole Donner, Alana Gramm, Aviva Guttmann, Eva Herschinger, Beatrice Heuser, Holger Janusch, Loch, K. Johnson, Dennis-Kenji Kipker, Lars König, Brendan Kotze, Rafaela Kraus, Wolfgang Krieger, Krista-Marija Läbe, Marc Mahlke, Luca Manns, Christoph Meyer, Armin Müller, Daniel Rainer Neumann, Konstantin von Notz, Esther Omlin, Niccolo Petrelli, Birger P. Priddat, Christopher Radler-Moric, Daniela Richterova, Felix Rieger, Irina Rosensaft, Frank Sauer, Christina Schäfer, Klaus Schmidt, Ralf Schneider, Jim Sengl, Jennifer E. Sims, Thomas Vašek, Larysa Visengeriyeva, Jeff Watkins, Richard Weiss, Julian Werner, Marcus Willett, Simon Wunder

Artdirector
Tanja Maus (fr.)

Picture Editor
Maja Metz (fr.)

Graphic
Christian Talla (fr.)

Editorial Contact
human-magazin.de

With thanks to our partners!

CSSA e.V. (Cyber Security Sharing & Analytics) is an association founded in 2014 and comprised of 17 companies. Its objective is to sustainably protect members, customers, and public IT infrastructure from cyber threats. By promoting confidential collaboration, the association enables its members to exchange information, learn from one another, and support each other. Key elements include exchange formats for cybersecurity specialists, the sharing of indicators of compromise and attack techniques, individual training programs for operational experts, and ad-hoc meetings in emergency situations.
Through targeted strategic integration, including data in the field of AI/Machine Learning, potential threats can be detected more effectively. This enables companies to prepare proactively for threats, improve their defenses, and become more resilient in the long term.

Das KI-Kompetenzzentrum Medien (KI.M) of Medien.Bayern GmbH and the Bayerische Landeszentrale für neue Medien (BLM) (Bavarian Regulatory Authority for New Media) systematically strengthens the AI capabilities of Bavarian media companies – from local radio stations to international media organizations. Our approach combines technological innovation with legal certainty: in the KI-Reallabor (AI real-world laboratory), we test the technical feasibility of AI projects and share the knowledge gained with the entire media sector. Regional workshops bring AI expertise directly to local communities. Legal guidance provides orientation and builds trust in new technologies. Technological sovereignty is a core component of a future-proof security architecture. KI.M supports Bavarian media companies in the AI transformation – legally sound, practice-oriented, and future-focused..

Veeam®, the global leader in data resilience, believes that every company should beable to move forward after a security incident – with confidence and full control over all its data, whenever and wherever it is needed. Veeam calls this radical resilience, and we are focused on finding innovative ways to help our customers achieve it. Veeam's solutions are purpose-built for data resilience and deliver data backup, recovery, portability, security, and intelligence. With Veeam, IT and security leaders can be confident that their applications and data are protected and available at all times – across cloud, virtual, physical, SaaS, and Kubernetes environments.
Headquartered in Seattle and with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide – 87 percent of Fortune 500 companies – who rely on Veeam to keep their businesses running. Radical resilience starts with Veeam.
Learn more at veeam.com.

“One should at least acknowledge this much: if there were no strictly perspectival valuations and appearances, then there would also be no life. Indeed, what forces us at all to suppose that there is an essential opposition between ‘true’ and ‘false’?”

Friedrich Nietzsche