ISBN: 978-9934-619-45-8

Intelligence and Strategic Communication

PREPARED AND PUBLISHED BY THE

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

ISBN: 978-9934-619-45-8

Author: Niklas Nilsson
Project Manager: Johannes Lindgren
Content Editor: Egil Fredheim
Design: Inga Ropša

Riga, June 2025

NATO STRATCOM COE
11b Kalnciema iela,
Riga, LV1048, Latvia
stratcomcoe.org
@stratcomcoe

Intelligence and Strategic Communication

Contents

Executive summary 5

Introduction 6

Concepts and definitions 8

Method and sources 9

Objectives and perceived utility of intelligence in StratCom 10

- Power and Influence 10
- Deterrence 10
- Attribution 11
- Cohesion 11
- Credibility 12

Secrecy and openness – a shifting balance 14

- A trend towards disclosure 15
- Russia's full-scale invasion of Ukraine, U.S. and UK disclosures 17
- Ukraine's wartime utilisation of intelligence for StratCom 18
- Communication on intelligence threats 19
- Information influence and elections 20
- Strategic assessments of future war 22

Drivers of the utilisation of intelligence for StratCom 23

- New technologies and OSINT 24

Risks of utilising intelligence for StratCom-purposes 27

- Exposure of sources and methods 27
- Adversary adaptation 27
- Unintended consequences 28
- Credibility 28
- Realigning expectations for intelligence 30

Conclusion 31

Recommendations 32

Endnotes 33

Executive summary

The use of intelligence for strategic communication (StratCom) involves the deliberate release of intelligence to shape perceptions, deter adversaries, attribute responsibility, foster cohesion, and reinforce credibility. Recent global developments—especially Russia's full-scale invasion of Ukraine—have accelerated this practice, highlighting the role of intelligence in StratCom.

The utilisation of intelligence in government communication is not new, as demonstrated by pivotal historical disclosures. Over the last decade, communication from European and U.S. security services has become consistently more open regarding threats posed by foreign adversaries.

However, the unprecedented scale of declassified strategic warning intelligence released by the U.S. and UK in the run-up to the 2022 invasion of Ukraine reflects a shifting balance, suggesting that policymakers increasingly perceive the value of using intelligence for StratCom-purposes to outweigh the potential risks attached to doing so.

These benefits include deterring hostile actions by exposing adversary intentions and planning, promoting a unified understanding of threats among allies, and bolstering the credibility of government communication. Moreover, the growing open-source intelligence (OSINT) community has reshaped the information environment by producing timely, credible insights once exclusive to state agencies. The convergence between state-produced intelligence and publicly available information serves to reinforce strategic narratives while mitigating the risks of exposing sensitive information.

Nevertheless, the use of intelligence in StratCom poses serious challenges. The exposure of knowledge and capabilities may present risks to sources and methods, and trigger adaptation and countermeasures among adversaries. Publicly disseminated intelligence that turns out to be inaccurate or exaggerated undercuts credibility. Disclosures can also delimit political and diplomatic options for a government, while the perceived utility of intelligence for StratCom holds inherent risks of politicisation.

The value of intelligence rests on both its secrecy and its perceived accuracy. States must balance operational security against StratCom imperatives, applying a principled approach weighing the objectives and intended effects of each disclosure against short and long-term risks to the integrity of intelligence agencies, ensuring that openness serves national interests without eroding core intelligence functions.

Introduction

The relationship between intelligence and strategic communication is undergoing a shift.[1] While the utilisation of intelligence for strategic communication purposes is by no means a new phenomenon, a range of developments over the last decade have driven a revised view of the broader utility of intelligence. State actors must navigate an information environment charged with an ever-growing amount of competing narratives. There has been a growing awareness of the disruptive power of information influence activities as an instrument readily deployed by hostile state actors and multiplied via proxies, bot-farms and troll factories. The potential outreach of traditional propaganda, information manipulation and other forms of malicious interference have drastically increased. This has increased the need for proactive and timely strategic communication as a necessary capability among governments and states.

At the same time, intelligence has historically quite frequently been utilised for strategic communication purposes. Authorised intelligence leaks to media outlets have been a common practice of communication. But intelligence has also been utilised to motivate fateful political decisions. A seminal example is Adlai Stevenson's disclosure of strategic warning intelligence revealing Soviet preparations to deploy nuclear missiles to Cuba in October 1962, preparing the world for the U.S. blockade. Another is Colin Powell's February 2003 presentation to the UN Security Council of intelligence purportedly providing evidence of Iraq's possession and production of weapons of mass destruction as motivation for the U.S. invasion of Iraq. These examples highlight some of the most important advantages, as well as negative consequences of employing intelligence for strategic communication purposes. The utilisationof and reference to *intelligence* per se awards particular credibility to a political message. In these cases, the vast resources and trusted competence of U.S. intelligence agencies endowed the communicated problem with salience, helping to motivate proposed lines of action to resolve it. Since both instances of communication served to prepare the international community as well as the U.S. public for drastic actions and potentially war, the utilisation of intelligence, presented as a set of facts beyond dispute, served to highlight a severe national security threat and augment acceptance and understanding of subsequent U.S. actions to avert it.

Yet the two examples also highlight the fine balance between success and failure in this respect. Whereas the decisive U.S. reactions to the Cuban missile crisis is in retrospect widely considered a successful intervention, the invasion of Iraq is perceived to be one of the most spectacular failures of U.S. foreign policy since Vietnam. In the first case, the conclusions drawn from intelligence on which the U.S. built its case were correct; in the other, they were wrong. Indeed, the Iraq case highlights the perils of utilisingintelligence for strategic communication, including intelligence failures, politicisation of intelligence, and ultimately undermining both the U.S. image in large parts of the world and the credibility of U.S. intelligence agencies, a damage that was sustained for decades.

This report describes the evolution of intelligence disclosures as an increasingly integrated component of strategic communication.

The example that has received by far the most attention to date was the U.S. and UK decisions to undertake comprehensive releases of strategic warning intelligence in the lead-up to Russia's full-scale invasion of Ukraine in 2022 in order to deter Russia from invading, and to warn allies and consolidate responses in face of the impending threat. The approach taken by the U.S. and UK was unprecedented in terms of the scale and consistency of the disclosures, as well as the nature of the intelligence released. It remains to be seen whether strategic warning intelligence will be utilised similarly in future international conflicts and there are certainly strong arguments and cautions against it. Yet the shift towards increasing openness in the communication of intelligence agencies' threat assessments is by no means confined to events surrounding Ukraine. Western security services have over the past decades become progressively more transparent and outspoken regarding the terrorism threat and more recently the range of hybrid threats and information influence activities traceable to antagonistic state actors including Russia as well as China and Iran.

Several western governments clearly see considerable advantage in leveraging the credibility conferred by intelligence to their communication strategies. The report outlines a set of generalised objectives and perceived benefits of intelligence in StratCom, including the general imperative of increasing power and influence, the deterrence and attribution of adversary action, the substantiation of shared narratives strengthening cohesion among publics, allies and partners, and the reinforcement of credibility for communication strategies. The report also outlines some of the key drivers of using intelligence for StratCom-purposes, including the growing range of perceived threats, the evolution of the information environment driven by new technologies, and the significant growth of the "open-source community". The latter has given rise to competition with the traditional role of intelligence agencies yet has also functioned as a significant enabler for the use of intelligence in StratCom, by producing public and often credible information that supports the disclosure of intelligence assessments without endangering the sources and methods of intelligence agencies themselves. Finally, the report highlights the disadvantages of using intelligence in StratCom, in terms of the potential risks involved. Unless carefully calibrated and applied, the disclosure and communication of intelligence may endanger operational security, expose sources and methods, and ultimately undermine the integrity of intelligence as a crucial component of the national security infrastructure.

Concepts and definitions

This report explores how intelligence has been, could, and should be utilised for strategic communication. It takes a state-centric perspective, assuming that the communicators in question are government officials as well as intelligence services and other state agencies, communicating on behalf of governments and in line with government policy.

Strategic Communications is understood in this report as consistent with the definition in the NATO StratCom COE Terminology working Group publication Understanding Strategic Communications. In this perspective, strategic communications can be conceptualised as taking place at the intersection of power relationships and tensions between on the one hand *persuasion* and *coercion*, on the other *authority* and *legitimacy*. The practice of strategic communications must constantly navigate this context and the tensions therein. This becomes a particularly salient exercise in liberal democratic societies, where the relationships between the four concepts; between those governing and those governed; as well as accountability and transparency, are grounded in ethical stances, values and principles.[2]

In this definition, strategic communication constitutes "a holistic approach to communication based on values and interests that encompasses everything an actor does to achieve objectives in a contested environment"[3] Thus, it refers to StratCom as both a mind-set, as a process and as a set of tools to achieve a certain objective. This is a broad definition reflecting the idea that everything communicates and is thus preferable in this context given the fact that the utilisation of intelligence in StratCom can take many forms and shapes. However, while subscribing to this broad definition, the empirical focus of the report is confined to verbal or written communication based on intelligence disclosures. While communication in other forms, for example concrete physical actions, can certainly be considered as part of a StratCom strategy as well – and successful strategies in this regard should seek close alignment between verbal communication and actions – they nevertheless remain outside the scope of this report.

Intelligence is understood in this report as the product resulting from the directed collection and processing of information regarding the strategic or operational environment and the capabilities and intentions of actions, in order to identify threats and opportunities for exploitation by decision-makers.[4] Thus, it is an information-based product that serves to provide decision makers with insights in order to warn about potential threats and provide opportunities for actions. Thus, through the lens of strategic communications, intelligence constitutes a form of processed information, which can potentially improve and increase the credibility and reliability of states' communication strategies.

Method and sources

The report draws on a literature review of recently published scientific journal articles, reports, studies and news articles on the topic of the evolving practice of intelligence disclosures for the purpose of strategic communication. While the phenomenon is by no means new, the fact that it has gained increased prominence with the events of 2022 has increased the attention paid to the topic by scholars, analysts and journalists. Like much of the intelligence literature writ large, the focus in this study is primarily on English-language sources – which is motivated at least in part by the comparative transparency of Anglo-Saxon intelligence agencies, and the multitude of open sources.

Thus, the report is based on open sources and takes a broad approach to the integration of published materials in the analysis. Among the academic journals consulted are the prominent outlets on intelligence studies *Intelligence and National Security* and *International Journal of Intelligence and Counterintelligence*. In the wider field of security studies and international relations, several articles have appeared on the topic, including in *International Affairs*, *Survival*, and *Prism*. The subject has clearly gained academic attention, and we can expect the debate on benefits, risks and consequences of using intelligence in StratCom to continue.

The empirical sections of the report rely on the extensive and frequently very detailed reporting in English-language media, predominantly but not exclusively in *The New York Times*, *Washington Post*, *Financial Times, Politico* and *Wall Street Journal*. The fact that this degree of continuous and extensive public reporting on sensitive intelligence matters is possible, and the scope of available sources, can itself be considered a testament to the changing practices that this report seeks to describe and analyse. The report is intended to provide an accurate and comprehensive analysis of developments, prospects and risks that are brought forward in recent publications on the use of intelligence in StratCom. However, caveats should be added that the report does not constitute a systematic literature review in the academic sense and is by no means exhaustive. Given time and space constraints, there are certainly several interesting angles that are nevertheless not included in the report. These include, among other things, the role of intelligence in the alignment of StratCom and political/military action and a broadening of the empirical scope. With reference to the latter, the report primarily studies StratCom focusing on Russia as an antagonist, whereas decisions regarding intelligence disclosures relating to other actors, most prominently China, or performed by other states, for example Israel, are certainly interesting avenues of inquiry. In terms of empirical material, follow-on interview studies would arguably provide a fruitful avenue for gaining an improved understanding of decision processes and background thinking relating to the utilisation of intelligence in StratCom.

Objectives and perceived utility of intelligence in StratCom

Decisions to utilise intelligence for StratCom purposes are naturally taken with desired objectives in mind. The motives underpinning these decisions can be multi-layered and complex or address immediate tactical gains. The use of intelligence in StratCom may serve multiple objectives and be directed at several audiences at once. The categories below are thus not intended to function as a definitive categorisation of different StratCom strategies when it comes to intelligence disclosures – rather, they represent different components of a strategy in which several or all these motives may be present. Moreover, all categories represent objectives subject to careful consideration of the balance between persuasion-coercion and authority-legitimacy guiding StratCom efforts, as defined above.

Power and Influence

In the broadest sense, the disclosure of intelligence in strategic communication can reinforce what is commonly referred to as "narrative power", understood as the ability to introduce dominant narratives that influence norms, values and agendas and thus shaping perceptions of what is real and possible.[5] "Intelligence" holds particular status as a form of authoritative knowledge.[6] Thus, intelligence disclosures represent the sharing of knowledge that can aid governments in framing conditions or events in a manner that aligns with their national interests and strategic objectives. In this sense, the use of intelligence in StratCom can be viewed as a profound strategic instrument of power and influence to be employed in international as well as domestic politics. From this general perspective, intelligence disclosures serve as a significant reinforcement of overall StratCom efforts, i.e. to establish a common and dominant frame of reference containing definitions of problems and the means necessary to resolve them. And, moreover, to present these solutions as rational, logical and necessary.

Deterrence

A purported strategic advantage of publicly disclosing intelligence lies in its capacity to deter adversarial actions. By revealing sensitive information about adversaries' plans, military capabilities, or covert operations, states can signal their awareness of hostile intentions and their readiness to respond.[7] However, it should be underlined that intelligence disclosures alone are unlikely to deter a committed adversary from taking aggressive

action. Successful deterrence, especially in the conventional military sense, needs to consist of several mutually coherent modes of signalling backed up with actions, of which intelligence disclosures may constitute one.[8]

This signalling effect is intended to disrupt adversaries' strategic calculations, forcing them to reconsider the viability of their objectives or the effectiveness of their tactics. In addition to deterring from a certain course of action by affecting the adversary's calculus, intelligence disclosures can also impose costs on adversaries by limiting their operational effectiveness, compelling them to adopt countermeasures, divert resources. By making threats transparent, states can create uncertainty and risk for adversaries, reducing the likelihood of escalation or conflict.[9]

However, assessing the effectiveness of intelligence disclosures as a deterrence strategy is exceedingly difficult, since successful cases often constitute non-events and access to adversaries' decision processes is rare. Thus, while successful deterrence will logically induce some kind of behavioural change on the part of the adversary, causality is usually hard to establish. Instead, cases that become publicly known more frequently represent failures of deterrence.

Attribution

As a component of deterrence, and of central importance in the face of compounding hybrid threats and adversarial behaviour designed to be deniable, is the utilisation of intelligence in StratCom to credibly attribute responsibility for hostile actions, such as cyberattacks, information influence campaigns, sabotage, or covert military operations. Public attribution allows states to expose and incriminate adversaries, thereby holding them accountable for violations of international law or norms. Moreover, attribution can be used as political leverage to rally international support and pressure adversaries into compliance or behavioural change.[10] It should be noted that credible attribution is often difficult to accomplish. Hybrid threats, by their very design, are frequently intended to induce ambiguity and leave the target guessing as regards the origin and motive of the threat, and indeed whether it constitutes an adversarial action in the first place.[11] In turn, this can give rise to a dilemma where attribution may be desirable, but where compelling and comprehensive evidence regarding the threat and its origins may be difficult to produce.

Cohesion

The use of intelligence in StratCom can contribute to national and international cohesion by establishing and reinforcing common threat perceptions, fostering trust, and facilitating cooperation. Internationally, the communication of credible intelligence regarding threats, crises or other problems facilitates common efforts to address them.[12] In addition to the proactive sharing of intelligence with allies, usually undertaken within a delimited circle of government or agency representatives, the communication of intelligence in the public domain offers the added value of reaching the broader public in partner

states, thereby contributing to shaping perceptions (and potentially political pressures) on a societal level.[13] Thus, the strategic release of intelligence related to emerging threats can help reinforce unity among allies and partners in addressing shared security challenges. This ability becomes especially pertinent during crises, during which shaping international consensus and garnering support from allies for intended courses of action are essential.

In a domestic setting, using intelligence in StratCom can similarly be instrumental in establishing shared understandings of threats and how to address them, thus enhancing the legitimacy of national security measures and reassuring the public regarding their necessity. It can also constitute an important component in the establishment of authoritative narratives and reinforcing information resilience.[14] This acquires even greater importance in an era of increasingly competing and polarising narratives regarding social challenges, causes and effects in politics, threats, and international developments. Intelligence in StratCom can enable the public, civil society, and the private sector to anticipate and respond more effectively to threats such as information influence campaigns, cyberattacks, or foreign espionage.

Credibility

Intelligence disclosures can be utilised to enhance the credibility of government communication by providing justification for policies and demonstrating commitment to transparency and accountability.[15] Presenting compelling intelligence-based evidence supporting a government's claims can serve to reassure citizens and allies regarding claims made by state institutions and leadership. Intelligence disclosures can be intended to draw attention to aggression and violations of international norms by adversaries, thus helping to mobilise sympathy and maintain the moral high ground.[16]

Moreover, for intelligence agencies, publicly demonstrating the significance and utility of their products can bolster their credibility and enhance their standing within the security architecture, reinforcing their role as indispensable to national security and decision-making processes. Such visibility not only reflects positively on the agencies themselves but can also help justify the allocation of essential resources and funding to them.[17]

Objectives

Power and influence	Deterrence	Attribution	Cohesion	Credibility
↓	↓	↓	↓	↓
Reinforcement of “narrative power”.	Signal awareness of hostile intentions and readiness to respond.	Attribute responsibility for adversarial behaviour.	Establish and reinforce common threat perceptions among national and international audiences.	Demonstrate commitment to transparency and accountability.

In sum, intelligence in StratCom offers significant advantages that extend beyond immediate security considerations. By influencing global narratives, fostering cohesion, deterring adversaries, attributing responsibility, and enhancing credibility, intelligence disclosures serve as a powerful tool for advancing international influence and national security objectives while promoting accountability and resilience.

Secrecy and openness – a shifting balance

The utilisation of intelligence for strategic communication purposes has a long history. Several examples can be identified in the 20th and 21st centuries in which governments or intelligence organisations have released classified or sensitive intelligence for strategic political, diplomatic, or military advantage. Among prominent examples is the Zimmermann Telegram (1917), where UK intelligence intercepted and decrypted a secret message from German Foreign Minister Arthur Zimmermann to Mexico, proposing a military alliance against the U.S. The decision to share this intelligence with the U.S., and the decision by the Wilson administration to publish it in U.S. newspapers, led to public outrage and was a contributing factor to the U.S. decision to enter World War I.[18] Adlai Stevenson's aforementioned 1962 presentation at the UN of aerial reconnaissance photos showing Soviet missile installations in Cuba built international pressure on the USSR and helped President Kennedy negotiate the withdrawal of Soviet missiles.[19] In the 21st century, the by far most significant disclosure was the U.S. decision to reveal intelligence alleging Iraq was developing Weapons of Mass Destruction (WMDs) to justify the 2003 invasion. While later proven inaccurate, the disclosures were instrumental in rallying political and public support for the war.[20]

While these and several other examples indicate that the utilisation of intelligence for communication purposes is an established component in the strategic behaviour of governments and states, the communication strategies employed particularly by the U.S. and UK in the build-up for Russia's full-scale invasion of Ukraine in 2021-2022 have frequently been described as a significant deviation from existing practice. Indeed, the nature of the material communicated, representing strategic warning intelligence that is normally very closely guarded to protect sources, methods and the degree of knowledge regarding an adversary, as well as the volumes and speed with which it was made publicly available, was unprecedented.

While perhaps not representing a fundamental change in how intelligence is utilised for StratCom-purposes and the overall motives for it, the disclosures regarding Russia's invasion of Ukraine reflect an increased realisation of the utility of intelligence for StratCom purposes. Whereas previous occasions where high-level strategic warning intelligence has been utilised for this purpose are rare, the last three decades have seen a clearer inclination towards communicating intelligence in other areas, particularly counterterrorism and counterintelligence. The utilisaton of intelligence for StratCom can be thus said to have undergone a significant evolution, culminating in the actions undertaken in 2021-2022. It is too early to tell whether the disclosure of strategic warning intelligence will become a recurring pattern in future international conflicts, and there are certainly important arguments against viewing the U.S. and UK StratCom relating to Russia's war in Ukraine as indicating a new practice. The cost of revealing what is known of a main adversary's intentions and capabilities could indeed be substantial; however, in this case the judgment appears

to have been that the prospect of deterring Russia from invading and establishing a cohesive understanding of events among western allies, partners and publics outweighed the risks. In future cases of comparable magnitude, for example a prospective Chinese invasion of Taiwan, the calculation may very well be different.

The broader trend towards intelligence disclosures is rooted in experiences from several key events as well as changes in threat perceptions and communication strategies in the last decades. The overall pattern, however, indicates a rebalancing over time concerning competing principles – on the one hand the necessity of *secrecy*, on the other the benefits of *openness* regarding knowledge acquired via intelligence. The perceived utility of intelligence in StratCom, in terms of establishing *powerful and influential* narratives, *deterring* adversaries, building international and domestic *cohesion* in the face of emerging threats, *attributing* hostile actions to adversaries and reinforcing the *credibility* of governments and intelligence agencies constitute categories of motives driving this change. In several respects, these have outweighed the persistent risks associated with intelligence disclosures.

A trend towards disclosure

Karen Lund Petersen describes different attitudes towards sharing and communicating intelligence, in what she terms awareness (communicating to inform), advice (communicating to induce action), and co-production (accommodating input from external players such as the public, civil societies or the private sector). These modes of communication represent different coexisting cultures of risk communication within the intelligence world, yet there is also a historical trajectory towards an increasing motivation for communication and interaction regarding threats and risks.[21] Arguments are increasingly put forward that intelligence communities should adopt a broader and integrative engagement with other parts of society.[22]

This trajectory has taken on different expressions depending on the perceived pertinence of security threats at different points in time. The aftermath of 9/11 and the conclusions of the 9/11-commission paved the way for a paradigmatic shift in the U.S. intelligence community, catering for a transition from stovepiped and secluded compartmentalisation towards increased information sharing within the U.S. intelligence community and with external partners, particularly in the field of counterterrorism.[23] The heightened awareness of the terrorism threat in the early 2000s motivated communication intended to induce awareness, action and co-production primarily regarding threats emanating from non-state actors. However, a correspondingly open approach to threats posed by adversaries in the form of foreign states, particularly regarding the West's main adversaries Russia and China, took longer to materialise. It has shifted in lockstep with the deterioration in relations and threat perceptions stemming from these actors. Regarding Russia, a defining moment came with the annexation of Crimea and the subsequent offensive in Donbas in 2014. Western political responses to these acts of aggression against Ukraine have in retrospect been characterised as slow, reactive, and insufficient.[24] This was the case despite access to intelligence that could have been utilised more effectively to establish and communicate a shared understanding of these events, forming the basis for a significantly swifter and more cohesive collective response.[25] Impediments to the formulation of a coherent western response to Russian actions in Crimea and later Donbas can be attributed to a political unwillingness to act. This may well have been possible to overcome if addressed through the early establishment of an openly communicated narrative of events, supported by strategic intelligence and clearly attributing Russia as the aggressor.

The reactions to several later incidents involving Russian interference and covert operations in western countries indicate a sustained effort to attribute actions to Russia and to publicly present intelligence to support these claims. Russia's interference in the 2016 U.S. elections, which was thoroughly investigated and publicly communicated in its aftermath, constituted a warning supplemented by a thorough description of the methods employed.[26] A similar attempt to manipulate French elections in 2017 was successfully thwarted.[27]

The arguably most elaborate case of intelligence utilised for StratCom in relation to the threat posed by Russia's intelligence agencies was the UK's reaction to the attempted assassination of Sergei Skripal in 2018, which indeed reflects key lessons regarding the strategic utility of intelligence in communication. The Skripal case was groundbreaking in terms of counterintelligence disclosures. British authorities swiftly and publicly identified Russia as responsible for the attack, specifically naming two GRU operatives as the perpetrators of the Novichok nerve agent poisoning and presenting evidence to substantiate these claims.[28]

The UK also successfully coordinated a unified international response, leading to a large-scale expulsion of Russian intelligence personnel across Europe—a collective measure that significantly impacted Russia's diplomatic presence and intelligence capabilities. Furthermore, the British Foreign Office actively tracked and countered Russian information influence by documenting and debunking at least 24 different, non-credible explanations offered by Russia regarding the incident; helping to maintain focus on the actual sequence of events. The central message of the UK's strategic communication was that the attack was not an isolated event but part of a broader pattern of aggressive Russian behaviour, contextualising the poisoning within Russia's wider campaign of intelligence operations and targeted assassinations in Europe. British authorities also shared intelligence with allies to sustain international support, contributing to long-term changes in how Western states address Russian intelligence activities. The incident led to heightened scrutiny of Russian operations and increased awareness of the necessity for coordinated measures to counter this threat.[29]

Russia likely miscalculated the international response to the attempted assassination of Skripal, reflecting a significant failure in its own strategic communication planning. The operation triggered a unified reaction from over 30 countries, resulting in the expulsion of nearly 150 Russian embassy staff—the most extensive measure of its kind since the Cold War.[30] The aftermath of the incident exposed substantial vulnerabilities in Russia's intelligence operations, particularly concerning their digital footprint. Open-source investigations by the NGO Bellingcat successfully reconstructed key aspects of the operation, including personnel, activities, and facilities linked to Russian military intelligence GRU's Unit 29155. For instance, GRU operatives were identified through photographs from previous assignments shared on social media, while digital traces were left by mobile phones carried to and from sensitive locations, forcing the GRU to reassess its operational security and tradecraft.[31]

These and several other examples are indicative not only of the growing threat that Russia poses to Europe, but also of the emergence of a common understanding of the threat and methods to counter it since 2014. The use of intelligence in StratCom has been an integral and significant part of this effort, representing a strategy encompassing all the components of utility listed above. NATO and the EU as organisations, as well as their members, have since systematically employed disclosed intelligence in their strategies to reveal and counter Russian information influence.[32] Russia's communication strategy aims to flood the information space with multiple competing narratives and consistently deflect attention from its own agenda and role in events. This has given rise to an imperative among NATO allies and partners to establish a common and authoritative understanding of

threats attributable to Russia as well as Russian strategy and behaviour, and to support this understanding with credible evidence in the form of intelligence. In effect, the range of hybrid threats comprising Russia's toolbox in interactions with Europe and the U.S., including information operations, cyber threats, political subversion, election interference, attempted coups, sabotage, and military threats, has increasingly become part of the political discourse and public consciousness in western countries.

Russia's full-scale invasion of Ukraine, U.S. and UK disclosures

Russia's preparations for its full-scale invasion of Ukraine provided a significant catalyst for this strategy. While disclosures regarding Russian hybrid threats in Europe had become increasingly commonplace, the U.S. and UK took unprecedented steps when publicly disclosing detailed strategic warning intelligence related to Russia's military build-up in the months leading up to Russia's full-scale invasion of Ukraine on February 24, 2022.

In December 2021, the Biden administration began to publicly share intelligence regarding Russia's preparations for war, supported by the publication of commercial satellite imagery showing a massive Russian military buildup along Ukraine's borders, including the presence of equipment, armoured units, supply chains, and large numbers of troops clearly indicating preparations for a large-scale invasion.[33] Declassified intelligence indicated that the operation could include up to 175,000 troops, organised into 100 battalion tactical groups.[34]

As the invasion drew closer, U.S. intelligence sources accurately predicted that Russia would attack in late February, an assessment communicated by President Biden and National Security Advisor Jake Sullivan, while Secretary of State Anthony Blinken provided a detailed account of Russia's invasion plan at the UN Security Council.[35] The head of UK Defence intelligence James Hockenhull published a map predicting Russia's invasion plan on Twitter the week before it began, arguing "it's important to get the truth out before the lies come".[36]

The revelations were exceptionally detailed, not least in their account of Russia's own StratCom and information planning, including the preparation of false flag operations intended as pretexts for launching the attack.[37] According to the communicated intelligence, Russia prepared staged attacks on Russian-speaking populations as a pretext for war, as well as fake videos of casualties to fabricate Ukrainian "aggression".[38] Moreover, intelligence was disclosed revealing details of Russia's post-invasion plans, including replacing Ukraine's political leadership with a proxy government, detailed measures to pacify the occupied country and population, and a "kill list" including Ukrainian leaders, journalists, and activists targeted for arrest or execution after an invasion.[39]

The employment of intelligence for StratCom in the lead-up to the invasion sought to employ the full range of utilities of such an effort. It intended to establish a dominant understanding of the conflict, with Russia unequivocally defined as the aggressor; deter Russia from implementing its war plans; reinforce cohesion among allies and partners as well as national publics, and to sustain credibility for the message and the intelligence at its core. Among these motives for the StratCom campaign, which has frequently been described as both innovative and largely successful, the objective of deterrence was not attained and Russia invaded nevertheless. The disclosures, however, did establish a dominant narrative regarding what was about to happen. They denied Russia the element of surprise, forcing it to go ahead with its operational

plans without the cover of fabricated pretexts. Although decision-makers in several European allies as well as in Ukraine remained sceptical regarding the impending invasion before it happened, Russia arguably faced a decidedly more unified West, and a better prepared Ukraine, than would otherwise have been the case. After February 24, 2022, the intelligence disclosures had a powerful impact in unifying perceptions among Western governments and publics. This enabled a common and coordinated response among NATO allies including military, political and diplomatic support for Ukraine and a comprehensive sanctions regime imposed against Russia.[40]

Ukraine's wartime utilisation of intelligence for StratCom

Since February 2022, it has become evident that Ukraine has put much thought and effort into its own StratCom strategy, and the utilisation of intelligence therein. Indeed, especially during the first two years, Ukraine's communication about the war's causes and its trajectory became the dominant understanding among western audiences (although the same cannot be said globally). The credibility of Ukraine's wartime StratCom has been underpinned by realities on the battlefield, where the Armed Forces of Ukraine have proven capable of resisting and repelling invading Russian forces. In turn, it has played a crucial role in mobilising and sustaining Western assistance for the war effort.

Ukraine's capabilities when it comes to wartime StratCom comes from significant experience acquired over the eight preceding years of fighting a low-intensity war with Russia.[41] An example of an early success in this regard was the Security Service of Ukraine's (SBU) dissemination of signal intercepts to elucidate the circumstances surrounding the downing of Malaysia Airlines Flight MH17 on July 17, 2014. Shortly after the downing of MH17, the SBU released audio recordings of intercepted phone calls between pro-Russian separatists and Russian military intelligence officers, indicating that the separatists were responsible for shooting down the aircraft. The SBU released the recordings to major international media outlets, ensuring widespread public access to the information.[42] Bellingcat, again, was able to support the case by tracking Russia's transfer to the separatists of the specific BUK anti-air system utilised to down MH17.[43]

Throughout the war with Russia, and most intensely since the beginning of the full-scale invasion, Ukraine has continually and strategically utilised intelligence disclosures to bolster its defence, disrupt Russian operations, and galvanise domestic and international support for the war effort. Whereas international support for Ukraine, particularly from the U.S., has waned over the last year, Ukraine's use of intelligence for StratCom has arguably played a significant part in ensuring more cohesive, sustained and extended Western international engagement than would have been the case without it.

Ukraine's main intelligence agencies SBU and HUR (military intelligence) have been consistently involved in the overall StratCom effort, providing a steady stream of selectively declassified intelligence publicised in a range of media channels.[44] This effort has been qualitative as well as quantitative, creatively packaged and communicated in a tailored manner to different audiences, with skilled utilisation of social media, performativity and in several cases humour. A significant modus has been to showcase Russia's military inaptitude. Ukraine has flooded various public outlets with declassified battlefield footage showing destroyed Russian equipment and incompetent tactical behaviour, as well as successful and innovative Ukrainian operations, for example in its employment of naval drone

attacks against Russian warships.[45] Releases of intercepted Russian battlefield communications have displayed chaos, low morale, and poor coordination within the Russian military.[46] Other disclosures have included reports on Russia's declining ammunition stockpiles, difficulties in replacing lost military equipment, and economic struggles due to sanctions, as well as infighting in the Russian leadership and the Wagner Group insurgency. Disclosures naming Russian units and servicemen responsible for war crimes in areas occupied by Russia have served to attribute responsibility and retain focus on the consequences of Russian success in the war.[47] The defiance of Ukrainian border guards on Snake Island, responding "Russian warship, go fuck yourself" to Russian demands to surrender, became a unifying symbol of resistance, underpinned by the release of an audio recording of the communication.[48]

These intelligence disclosures have helped Ukraine strengthen its defensive capabilities by retaining cohesion domestically, in terms of motivation and resilience among the Ukrainian population and raising morale in Ukraine's military. They have fuelled international cohesion, by demonstrating to Western allies that the war is winnable and that continued military and economic support for Ukraine is a fruitful investment of resources. Moreover, they have aimed to undermine the motivation of the opponent and shape the dominant narrative of the war, in turn countering Russia's corresponding communication efforts.[49]

Whereas the overall objectives of using intelligence for StratCom purposes remain unchanged in wartime, they naturally become more acute. Particularly, as has been the case for Ukraine, when engaged in an existential struggle for survival. Across the board, the imperative of establishing a more convincing narrative regarding the conflict than the opponent, deterring the enemy's will to fight, attributing aggression and breaches of international law, and promoting cohesion within the military, public, and among international partners are all significant features of a war effort.

During Russia's war in Ukraine, the leveraging of intelligence in StratCom efforts by both sides speak to the significant importance of shaping national and international perceptions of the war, and to the advantages of utilising intelligence in StratCom as crucial components of fighting power. However, decisions regarding declassification and disclosure arguably come with higher stakes. If these risk conferring advantages to the enemy by compromising operational security, they could result in significant loss of life and potentially the war itself. Conversely, in recognition of the centrality of StratCom as a component of warfighting, and of declassified intelligence as a considerable resource in this context, decisions not to integrate even sensitive intelligence with overall communication efforts present risks at least as serious.

Communication on intelligence threats

Whereas the disclosures in 2021-2022 represented a modern approach to the utilisation of strategic intelligence, the use of intelligence in StratCom has been a growing practice among security services for a longer period, particularly when it comes to counterintelligence. As noted above, the increased realisation since 2014 of the hybrid threats that Russia employs against Europe has gradually provided for an increasingly open attitude to communication about these threats. This has occurred in combination with steadily increasing Russian intelligence activities in Europe in the years leading up to the full-scale invasion of Ukraine. As noted by Mark Galeotti already in 2021, "The Russian intelligence community is now operating with a wartime mindset. They think they are in an existential struggle for Russia's place in the world".[50] Russia's full-scale invasion of Ukraine nevertheless served as a catalyst also in this field. While this can partly be attributed to increased and progressively

more brazen Russian intelligence activities in Europe after the invasion, it also reflects a perceived need among European governments and security services to provide a more coherent picture of the gravity and complexity of the threat that Russia poses to Europe.

Thus, national security services across Europe have taken an increasingly transparent approach to communicating about Russian (as well as Chinese and Iranian) intelligence activities, with several agencies explicitly warning about the scale and modus of Russian operations.[51] There are numerous examples of public statements from heads of European intelligence services as to their assessments of the threat, with for example MI6 Chief Richard Moore describing the behaviour of Russian intelligence services in Europe as "feral".[52] The activities referred to include increasing amounts of sabotage, targeted assassinations, recruitment, information influence activities, and political subversion conducted by Russian intelligence services in Europe.[53] Public threat assessments from a range of European intelligence agencies today provide explicit and elaborate accounts of the range of threats their countries are facing from Russia.

While Western security services have historically been cautious when discussing Russian intelligence activities, intelligence disclosures by security services, other governmental agencies, or political authorities are today widely available in government publications and other open sources. In cases where crimes have been investigated and prosecuted, there is also material from publicised preliminary investigations, reflecting the increased frequency of espionage cases brought to trial. As a result, information about individuals, methods, and the scope and focus of activities increasingly becomes public knowledge, which raises general societal awareness of the intelligence threat. Moreover, it potentially has a deterrent effect while demonstrating capacity and resolve.[54] Although the communicated intelligence is, of course, adapted for public disclosure, it is now possible for actors outside the "secrecy bubble"—researchers, NGOs, journalists, or the interested public—to gain a much more comprehensive understanding of hostile intelligence activities than was possible just a few years ago.

In other words, European security services have over time engaged in an increasingly elaborate use of intelligence for StratCom aiming to provide a unified understanding of the Russian threat and employ a strategy of attribution, deterrence, cohesion and credibility.

Information influence and elections

The area where this strategy is perhaps most coherent and visible is in connection with preparations for elections. During these, intelligence-based threat assessments have become standard procedure in European countries, as well as the U.S., serving to warn and inform the public by highlighting vulnerabilities related to elections and foreign subversive activities and information influence targeting them.

In recent years, a major effort at disclosing and communicating the threat has been directed at the Russian information influence campaign Doppelgänger, aiming to undermine support for Ukraine, reinforce societal divisions and influence elections in European states and in the U.S. The operation utilises cloned websites mimicking legitimate news outlets such as Der Spiegel, Le Monde, Fox News, and The Washington Post, featuring fabricated news articles promoting pro-Russian narratives. The operation also employs networks of fake social media accounts to disseminate these narratives as well as AI-generated realistic but false content, including deepfake videos. The non-profit organisation EU DisinfoLab identified and named

the Doppelgänger campaign in 2022. During 2024, a concerted effort by security services and other government agencies in several affected states communicated known details about the operation of Doppelgänger, accompanied by the seizure of internet domains and the imposition of sanctions against entities involved in the campaign, including the Social Design Agency (SDA) and Structura.[55]

U.S. intelligence agencies issued several warnings during the 2024 election period, underlining the information influence activities of Russia, and to a lesser extent Iran, to undermine the credibility and legitimacy of the elections in the eyes of U.S. voters.[56] The Director of National Intelligence (DNI) released reports detailing Russia's influence operations, including the use of AI-generated information threats and attempts to induce chaos during Election Day and until the inauguration.[57]

In response to Russian interference in its 2024 presidential election and concurrent EU membership referendum, Moldova employed a multifaceted communication strategy to inform both its citizens and its international partners. President Maia Sandu publicly condemned the interference, describing it as an "unprecedented assault" on democracy, highlighting evidence of significant vote-buying schemes. Alexandru Musteață, Director of Moldova's Security and Intelligence Service, presented a detailed report to parliament outlining Russia's interference during the elections and warned of potential future meddling in the 2025 parliamentary elections. Moldova also invited international observers to monitor the elections and referendums, ensuring transparency and credibility in the face of external interference. The government facilitated access for international media to report on the situation, aiming to raise awareness about the threat.[58]

In December 2024, during Romania's presidential election, the country's intelligence services took unprecedented steps to communicate findings of Russian interference. President Klaus Iohannis authorised the declassification of intelligence, which detailed how Russian operatives conducted a coordinated social media campaign to bolster the far-right candidate Calin Georgescu. The Supreme Council of National Defense (CSAT) released these declassified reports to the public, revealing that Romania had been the target of "aggressive hybrid Russian actions" during the election period. Based on the intelligence findings, the Constitutional Court of Romania then took the significant step of annulling the first round of the presidential election, citing substantial evidence that Russian interference had distorted the electoral outcome.[59]

In the lead-up to Germany's 2025 federal elections, multiple reports and investigations highlighted significant Russian interference aimed at influencing the electoral process. Germany's BfV and Interior Ministry identified the Russian-linked information influence operation Storm-1516, previously identified as active in the 2024 U.S. elections, which disseminated fake videos on social media platforms, aiming to mislead voters and disrupt the electoral process.[60] A study carried out by fact-checking organisations Correctiv and NewsGuard uncovered that over 100 websites, linked to Russian entities, utilised artificial intelligence to produce and disseminate false stories targeting German politicians supportive of NATO and Ukraine. These narratives aimed to sway public opinion and prop nationalist, Russia-friendly parties, notably the Alternative for Germany (AfD).[61]

Strategic assessments of future war

Among the most fateful assessments communicated by European intelligence agencies since the beginning of Russia's full-scale invasion of Ukraine are those underscoring the severity of the deteriorating security situation for Europe and the consequences of an end to the war in Ukraine that is favourable to Russia. Among these, the Latvian Security Service (SAB) warned in its annual report for 2024 that a pause in the war would enable Russia to rebuild its military capabilities, potentially threatening NATO and European states within five years. The report emphasised that a "frozen" conflict might allow Russia to increase its military presence near NATO's northeastern flank, including the Baltic states.[62] Bruno Kahl, President of Germany's Federal Intelligence Service (BND) indicated in November 2024 that Russia could attain the capability to launch an attack on NATO territories by the end of this decade. He underscored that while a large-scale attack against a NATO country was not expected, a more limited operation under the pretext of "protecting" Russian minorities is conceivable, ultimately aiming to test the credibility of NATO's article 5.[63]

In early 2025, The Danish Defence Intelligence Service (DDIS) issued a new significant warning regarding Russia's ability to pose a credible military threat to NATO countries within a few years. The assessment is based on a scenario including the cessation or freezing of hostilities in Ukraine, a perception of NATO as weak and divided, a failure in NATO to undertake a corresponding military build-up, and inability or unwillingness of the U.S. to support European allies in a war with Russia. The report suggests that under these conditions, Russia could be capable of initiating a local war against a neighbouring country within approximately six months. Within two years, Russia might constitute a credible threat to one or more NATO countries, positioning itself for a regional war against several NATO members in the Baltic Sea region. In about five years, Russia could be prepared for a large-scale war on the European continent.[64]

The publicised Latvian, German and Danish intelligence assessments, along with several others, indeed provide an alarming picture of the deteriorating security situation in Europe and the potential consequences of a ceasefire or "peace" in Ukraine that is imposed on Russia's terms. The dire assessments, and the decision to provide an exceptionally clear picture of the threat at hand, indeed provides a common frame of reference for European politics and publics, intended to align perceptions regarding the security threat that NATO and Europe are facing. The aim is to build cohesion, providing legitimacy for the difficult decisions and priorities ahead for Europe in the process of building the collective defence capabilities needed to ensure future security on the continent.

Drivers of the utilisation of intelligence for StratCom

A common denominator for these examples of how intelligence is employed for StratCom-purposes is the objective of establishing a credible official account of a particular threat or security imperative, and to promote awareness and legitimacy for needed courses of action. The shift described above of an increasingly proactive attitude towards the utilisationof intelligence for communication purposes is in turn grounded in the rapid and accelerating evolution of the information environment in which governments and intelligence agencies must navigate.[65]

In an information environment shaped by exponentially increasing volumes of data and a wide diversity of narratives, antagonistic actors like Russia aim to overwhelm audiences with a stream of conflicting information, frustrating efforts to distinguish between facts and fiction. This approach contrasts with the often-reactive attempts by Western actors to win battles of strategic narratives.[66] The vast amount of competing information increases the need for authoritative narratives to capture the audience's attention and convey messages effectively. In this attention economy, the emphasis is not only on the information itself but also on its packaging and delivery to engage the intended audience. Consequently, there is an increasing need for content, narratives and actions that resonate with diverse target groups.[67] In turn, strategic communication, to be successful, aims to influence the overall interaction and discourse of communication among target groups, further reinforcing the dissemination of desired narratives. It is in this context that the power of intelligence as a tool for strategic communication needs to be understood.

The security environment has increasingly come to be conceived in terms of its informational and cognitive dimension, with increased importance attached to the "audience effects" of employing traditional material sources of power, e.g. military and economic means, alongside their consequences in the physical world. As noted above, states in the western hemisphere have over the past decade acquired an increased understanding of their exposure to hybrid threats, the employment by hostile state actors of below-threshold methods with plausible deniability to exploit existing vulnerabilities in democratic societies. Information and communication have thus become perceived as one crucial component of the strategy to counter these threats.[68]

It is also in this context that the political will and perceived necessity to communicate explicitly about threats and attribute antagonistic behaviour to other state actors has gradually emerged. Political will is, of course, a significant driver and a key precondition for the development and utilisation of intelligence in StratCom.

New technologies and OSINT

New technologies have drastically changed the information environment, enabling information, communication, and competing narratives to travel with unprecedented speed. This places a premium not only on the quality of communication, but also its speed and quantity, given the limitations of attention.[69] Thus, the ability to not only establish dominant narratives, but to do so quickly enough to precede and supersede falsified counternarratives, as well as to align verbal communication with actions to close the say-do gap, is a significant task for strategic communicators. Smartphones, social media, and messaging applications have fundamentally transformed how information is disseminated and consumed. State and non-state actors leverage digital platforms to influence narratives and mobilise public opinion. For example, the war between Russia and Ukraine illustrates how information warfare is conducted through a wide range of channels, blurring the boundaries between traditional combatants and civilians.[70]

The ongoing technological leap towards the integration of artificial intelligence (AI) and machine learning offer significant new possibilities in this regard; increasingly developed and employed by western states and their antagonists alike.[71] The opportunities to employ AI for both intelligence collection and analysis, and for StratCom purposes are increasing rapidly. For example, AI can be utilised for tailored strategic messaging, personalising messages for different audiences while natural language processing allows for real-time language translation and sentiment adaptation.[72] AI can be employed to detect deepfakes and information threats as well as for monitoring adversarial narratives, bots, and fake news on social media while optimising counter-messaging strategies.[73] The ethically contested use of psychographic profiling and content amplification allows for effective targeting of specific demographics and enhanced reach of strategic communications.[74] Deep behavioural analysis can be utilised to analyse cognitive biases and behavioural patterns to develop highly effective persuasion strategies.[75] Moreover, machine-generated narratives can adapt in real-time to counter those of adversaries or reinforce desired messages; whereas AI systems can assess emotional states based on speech, text, and facial recognition to tailor communication accordingly.[76]

Opportunities to employ various AI-powered capabilities for StratCom purposes are multiplying and the limitations are determined less by the actual possibilities offered by the technology itself than by the ethical and integrity-related concerns regarding their use that rightfully raise barriers to their employment in democratic societies.[77]

The extensive growth of *open-source data* is another feature of the contemporary information environment with significant implications for the use of intelligence in StratCom. On the one hand, this development has given rise to competition for intelligence agencies, with a range of actors capable of producing "intelligence". On the other hand, the availability of information derived from open sources has also enabled StratCom based on intelligence disclosures.

In terms of *competition*, competitors to intelligence agencies when it comes to the production of authoritative knowledge have emerged due to the availability of information and new technologies. Intelligence agencies have historically derived their authority and strategic value from their ability to access and assess classified or secret information, where intelligence disciplines allowed the uncovering of information that was inaccessible to non-government actors. However, the growth of publicly available data—ranging from satellite imagery and social media posts to corporate records and geolocation data—has expanded the production of intelligence-like analysis and knowledge beyond traditional government agencies. It remains controversial whether what these actors produce can be called "intelligence", which after all constitutes

the combined professional analysis of open and secret sources derived from advanced collection capabilities, e.g. HUMINT and SIGINT. Nevertheless, aside from clandestine collection, non-government open-source analysts today have the means to engage in types of knowledge production that were previously the prerogative of intelligence agencies.[78]

The information and analysis produced by NGOs such as Bellingcat, private intelligence companies such as Palantir, Flashpoint and Recorded Future, as well as journalists and researchers, can be communicated quickly and often faster than intelligence agencies. NGOs and independent investigative groups have utilised open-source data to uncover state-sponsored assassinations, war crimes, and information influence campaigns. Bellingcat's investigation into the 2014 downing of Malaysia Airlines Flight MH17 is a prime example of how publicly available information (including satellite imagery, flight paths, and social media posts) can quickly be pieced together to produce highly credible conclusions. Private intelligence companies specialised in aggregating and analysing open-source data provide services to corporate clients, governments, and media organisations, offering actionable insights into topics such as cybersecurity threats, geopolitical risks, and economic trends. Investigative journalists have increasingly embraced OSINT techniques in their reporting and have been able to break stories on military movements, cyberattacks, and covert operations.

This has created a new ecosystem of knowledge production in the intelligence world—one that challenges the traditional monopoly of government intelligence agencies. Credible intelligence is no longer exclusive to state actors. This development raises important questions regarding the role, function, and relevance of traditional intelligence agencies in an era where their capabilities are increasingly matched—and sometimes surpassed—by external entities.[79]

The growing influence of non-state intelligence producers is due in large part to the speed with which they can disclose their findings. Government intelligence agencies may be constrained by bureaucratic processes and inter-agency coordination requirements, but most importantly apply rigorous methods and analytic standards for quality assurance, which is certainly not necessarily the case for all non-state actors.[80] Operating with classified as opposed to open data, government intelligence agencies must also always carefully weigh the risks of compromising sources and methods into every decision to disclose intelligence.[81] The growing availability of high-quality information produced outside the purview of intelligence agencies can also induce intelligence consumers to turn to external sources for faster access, which may contribute to setting a narrower agenda for intelligence collection since policymakers derive the questions they want their intelligence agencies to answer from publicly available information and the news cycle.[82]

The rise of non-state intelligence producers is thus prompting a broader re-evaluation of what intelligence agencies should prioritise in the 21st century, and what their comparative advantages are. While non-state actors excel at rapidly gathering and analysing open-source data, intelligence agencies have a clear advantage in providing deep and triangulated multi-source analysis. Moreover, as OSINT becomes more accessible, the unique value of classified intelligence collection against hard targets will remain a key advantage for state agencies.

This said, the availability of open-source information has also proven to be a significant *enabler* for intelligence agencies and for the use of intelligence in StratCom. A large share of the information that goes into an intelligence assessment normally consists of open-source data.[83] Partnerships between government intelligence agencies, private actors, the research and educational sector and civil society actors are increasingly becoming recognised as needed for the ability to facilitate intelligence "co-production".[84]

Most importantly, when it comes to intelligence in StratCom, the availability of

open-source analysis can greatly facilitate and support the disclosure of intelligence. Non-state actors operate in the public domain, which allows them to share their findings openly without the limitations imposed by classification systems. The threshold for verifying information already present in other channels is much lower than for disclosing information held exclusively by intelligence services. When intelligence disclosures can be supported by publicly available and credible sources, this significantly reduces the risks to sources and methods. An important case in point is the aforementioned utilisation of commercial satellite imagery produced by Maxar to substantiate U.S. claims of Russia's military build-up on Ukraine's border in late 2021. These images produced credible evidence of the assertion that Russia was preparing an invasion, without having to disclose highly classified images from U.S. military satellites. Moreover, carefully vetted releases of intelligence have served to direct open-source analysts to track troop movements, missile strikes, and information influence campaigns during Russia's war in Ukraine in real time using social media posts, satellite images, and geolocation tools, in a manner that has been very much in synch with the narrative sustained by official intelligence disclosures.[85]

Risks of utilising intelligence for StratCom-purposes

While offering significant advantages, the use of intelligence in StratCom also entails serious risks that can jeopardise national security, diplomatic relations, and operational effectiveness. These risks are multifaceted, encompassing the exposure of sources and methods, adaptation among adversaries, credibility concerns, and unintended strategic consequences. In the longer term, the perceived success of intelligence disclosures as components of StratCom efforts could incentivise political expectations for an increased focus on the production of "communicable" intelligence, hence risking the increased politicisation of intelligence as a practice. Understanding these risks is essential to ensuring that the utilisation of intelligence in StratCom does not undermine its intended effects, or indeed intelligence itself.

Exposure of sources and methods

A primary and well-documented risk of intelligence disclosures is the potential compromise of sensitive sources and methods. Decisions to communicate what is known based on secret intelligence are naturally accompanied with "disclosure dilemmas," where the benefits of disclosure must be balanced against the potential damage to political objectives and operational security.[86] Disclosure can jeopardise ongoing intelligence operations, as well as exploits, field operatives and human sources.[87] The more a state reveals about its knowledge and intelligence assets, the greater the likelihood that adversaries will identify and neutralise those sources or deny access to exploits.[88]

Adversary adaptation

An associated risk is that public disclosure of intelligence can trigger behavioural adaptation among adversaries, compromising future collection efforts. Once intelligence is made public and adversaries become aware of intelligence operations targeting their activities, they can adopt countermeasures and adjust their methods to evade detection, for example by altering their communications or adjusting their counterintelligence strategies, rendering previously effective collection techniques obsolete. Historical incidents, such as the aftermath of the Snowden leaks, demonstrate how adversaries have successfully upgraded their operational security by exploiting publicly available knowledge of intelligence practices. Adaptation results in a more challenging

intelligence environment, as previously effective collection methods may be rendered ineffective. Public intelligence disclosures can also reveal vulnerabilities in collection capabilities by exposing blind spots and encouraging adversaries to exploit them, or to supply deliberately misleading information. This can encourage unpredictability among targets, in turn risking to undermine future intelligence-gathering capabilities, reducing the effectiveness of collection capabilities and impairing the ability to pre-empt threats.[89]

Unintended consequences

Utilising intelligence in StratCom also carries the risk of contributing to unintended strategic consequences, including conflict escalation and diplomatic fallout. By taking public stances supported by disclosed intelligence, governments may inadvertently limit their options and their ability to negotiate or de-escalate conflicts without losing credibility. For example, disclosing strategic warning intelligence to justify military posturing or public ultimatums can increase the costs of compromise or retreat, in turn entailing risks of exacerbating tensions and escalating conflicts.[90] When it comes to foreign interference, decisions to publicly attribute may constrain other policies, expose societal vulnerabilities, and contribute to political polarisation.[91]

Credibility

Decisions to disclose intelligence should always be taken with their long-term impact on future credibility in mind. Intelligence disclosures that are not supported or verified by observable evidence risk giving rise to a "self-negating prophecy" when public warnings based on intelligence fail to materialise, leading to scepticism about future assessments. If intelligence disclosures are perceived as exaggerations or as motivated by political rather than security concerns, this may sow doubt about the integrity and accuracy of such warnings.[92] If, for example, the efforts in 2021 and 2022 to raise awareness regarding Russia's invasion plans had not been followed by an actual invasion, this would likely have undermined the credibility of U.S. and UK intelligence and strategic communication. They would conceivably have been accused of "crying wolf" and fearmongering (although it might, conversely, have represented an example of successful deterrence).[93]

Intelligence disclosures are always selective, which can foster perceptions of bias and manipulation, even more so if disclosures appear to be strategically timed to fit a particular narrative. Such perceptions may hinder collaboration with allies, complicate diplomatic engagements, and reduce the effectiveness of intelligence-sharing agreements.[94] Domestically, disclosures may provoke political backlash and polarisation, particularly if they are perceived as manipulative or fear-inducing.[95] Public mistrust and political criticism can, in turn, weaken the authority of policymakers and intelligence agencies, making future intelligence-related decisions more contentious. Moreover, when disclosed intelligence appears to add little new information aside from what is already publicly available, it can undermine the perceived value of intelligence per se.[96]

Potential inaccuracies in intelligence assessments can become particularly damaging when these are used to justify fateful political decisions. In this regard, the strategy of reinforcing StratCom with strategic warning intelligence in the lead-up to Russia's

invasion of Ukraine can partly be seen as a response to previous intelligence failures.[97] The manner in which assessments from the U.S. intelligence community were politically instrumentalised to justify the 2003 invasion of Iraq caused long-term credibility damage and continue to affect how European counterparts as well as the U.S. public perceive the reliability of U.S. intelligence and the way it is utilised in strategic communication even two decades later.[98] The fact that U.S. and UK intelligence agencies accurately assessed Russia's intentions and presented detailed evidence to substantiate their conclusions has, in this context, served as a form of redemption, helping to restore their credibility.[99]

The credibility risk becomes especially acute in a security environment saturated with contradictory information and defined by unpredictability. European states experience increasingly intense antagonistic behaviour, which is often sufficiently concealed to avoid quick detection and attribution. The heightened threat perception risks incentivising counterproductive communication, in which governments are encouraged to provide timely information and act accordingly, yet proving unable to back this communication with actual evidence. A case in point is the large number of recent damages to undersea cables and pipelines in the Baltic Sea, which were in some cases quickly presented as suspected sabotage by Russian or Russian-affiliated ships, whereas subsequent investigations failed to ascertain malign intent.[100] This underscores an important vulnerability in relation to hybrid threats, which are often ambiguous and deniable by design. By inciting large numbers of incidents that are frequently difficult or impossible to attribute to a hostile actor, adversaries can provoke overreactions from targeted states and governments, which in turn undermine their credibility.

Realigning expectations for intelligence

A final potential long-term implication of intelligence disclosures for StratCom purposes, and the attached growing demand for intelligence products suitable for strategic communication, concerns the role of intelligence agencies and the external expectations placed upon them. A potential tension exists between maintaining the integrity of their core mission—producing intelligence to inform decision-making—and generating materials intended for outward communication aimed at justifying political objectives, which in part contradicts the established function of intelligence agencies in the state decision-making system. Changing expectations from the political level as well as the public regarding what intelligence agencies should produce and why, holds the danger that intelligence may become increasingly politicised. This is particularly the case if perceived successes of disclosure and openness translates into pressure that intelligence per se should be useful for political communication. A crucial challenge lies in maintaining the balance between intelligence as an impartial analytical tool and its use as an instrument for achieving desired effects. This balance can be precarious, with the temptation to blur the lines between analysis and advocacy presenting a significant risk. Intelligence is traditionally produced to provide policymakers with objective assessments, yet can potentially be distorted when selectively disclosed to achieve strategic outcomes. As Huminski points out, the integrity of intelligence disclosures ultimately depends on officials who understand and respect the distinction between assessment, analysis, and advocacy.[101]

Risks

Exposure	Adaptation	Unintended Consequences	Credibility	Expectations
↓	↓	↓	↓	↓
"Disclosure dilemma", risk of revealing sources and methods.	Risk of triggering adversary adaptation, compromising future collection.	Risk of delimiting room for political manoeuvre or triggering unexpected reactions.	Risk of "self-negating prophecy" if warnings fail to materialise.	Risk of damaged integrity and intelligence politicisation.

Conclusion

The evolving role of intelligence in strategic communication underscores its growing importance as a tool for shaping perceptions, deterring adversaries, reinforcing cohesion, and enhancing credibility. As demonstrated by several of the examples elaborated in this report, the strategic release of intelligence has proven effective in countering information threats, rallying public and international support for political action, and legitimising policy decisions. However, it also carries inherent risks that require careful consideration to avoid undermining credibility, compromising sources and methods, or triggering unintended consequences.

In order to ensure the credibility of StratCom based on intelligence, and of intelligence as a practice, careful thought must be given to the balance between strategic objectives and the integrity of intelligence assessments, where boundaries against the misuse or politicisation of intelligence must be carefully maintained. While objectives may vary, disclosures must align with specific strategic outcomes as well as consideration of how various audiences—both domestic and international—will interpret and respond to the information.

The use of intelligence in StratCom is intended to shape perceptions and influence decisions. It carries consequences that can both strengthen and undermine national interests. As Joshua C. Huminski suggests, the central guiding question in any decision to disclose intelligence should revolve around the intended outcomes: "what are policymakers trying to achieve? What are the desired effects or blend of effects?".[102] This question emphasises the importance of effects-oriented disclosures, wherein the release of sensitive information is evaluated not only for its immediate utility but for its long-term impact on national security, diplomacy, and credibility.

Ultimately, StratCom based on intelligence represents a powerful instrument of statecraft that, when used intelligently and responsibly, can bolster national security, deter threats, and promote global stability. In future applications, it is essential to maintain a principled approach that preserves the integrity of intelligence while leveraging its strategic value to navigate an increasingly complex information landscape. Having said that, it is important to underline that decisions to refrain from reinforcing StratCom with declassified intelligence also represents a choice – one that deliberately abstains from a potential advantage in a contested and high-stakes environment. Therefore, governments and states should devise balanced strategies for the utilisation of intelligence in strategic communication, with carefully elaborated perspectives of short- as well as long-term objectives, opportunities and risks.

Recommendations

Decisions to utilise intelligence for StratCom purposes are situation and context dependent. Therefore, recommendations pertaining to the utilisation of intelligence for this purpose must necessarily be formulated in general terms. Each individual decision will require its own consideration of the balance between benefits and risks.

In the short-term consideration of decisions to disclose intelligence for StratCom purposes, responsible officials and authorities need to strike a satisfactory balance between four partly contradictory preconditions:

- The intended and foreseen positive effects of the intelligence disclosure should clearly outweigh the default advantage of maintaining secrecy regarding the knowledge in one's possession.

- The released intelligence should, to the best of the discloser's knowledge, provide an accurate picture of the situation. Whereas intentionally biased or misleading intelligence releases may provide short-term gains and therefore constitute a temptation, the potential damage to the credibility of government communication and intelligence producers is considerable. They should therefore not be considered as an option.

- Intelligence disclosures should contribute unique information, in addition to what is already publicly known. If it does not, the disclosure becomes essentially pointless and may undermine the value of intelligence as a component of StratCom per se.

- Intelligence utilised for StratCom purposes should always be carefully selected and in the process of declassification, cleared of all information that risks endangering sources and methods. Whereas disclosures will in many cases unavoidably reveal some degree of knowledge regarding adversaries' capabilities and intentions, the extent of the disclosure and its potential consequences is an important part of the calculation.

Whereas the safeguarding of operational security has traditionally superseded the potential benefits of communicating intelligence, political attitudes have shifted over the last decades towards a perception that, while the incentives for secrecy remain, the perceived benefits of intelligence as a resource for political communication are so significant that strategies must be devised to allow for increased openness. In decision-making regarding intelligence disclosures, therefore, governments and intelligence producing agencies must carefully balance the *communication* imperatives of openness, effects, accuracy and added value against the *intelligence* imperatives of secrecy and protection.

Yet the development of intelligence communication strategies should also take into account the potential long-term effects of emergent practices regarding the use of intelligence in StratCom:

- A long-term strategy for utilising intelligence in strategic communication should take as its point of departure a careful consideration of its effects in terms of potential impact on the credibility of intelligence producers.

- It is necessary to establish proactive safeguards against politicisation of intelligence. These should include consideration of the expectations placed on intelligence producers in this regard and to what extent this may have long-term effects on the role of intelligence agencies in the national security apparatus.

Endnotes

1 In preparation of this work, the author utilised generative AI and AI-assisted technologies to support the research and writing process, including ChatGPT, Atlas.ti and Unriddle. The author carefully reviewed, edited, and validated the content to ensure its accuracy and integrity and takes full responsibility for the final published work.

2 Neville Bolt, Leonie Haiden, Jente Althuis, and Martha Stolze, ***Understanding Strategic Communications: NATO Strategic Communications Centre of Excellence Terminology Working Group Publication No. 3*** (Riga: NATO Strategic Communications Centre of Excellence, 2023), p. 19-26. [Accessed 26 May 2025].

3 Ibid, p. 15.

4 UK Ministry of Defence, *Joint Doctrine Publication 2-00: Intelligence, Counter-Intelligence and Security Support to Joint Operations* (2023).

5 Linus Hagström and Karl Gustafsson, ***'Narrative Power: How Storytelling Shapes East Asian International Politics'***, *Cambridge Review of International Affairs* 32 no 4 (2019). .

6 Kira Vrist Rønn and Simon Høffding, ***'The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence'***, *Intelligence and National Security* 28 no 5 (2013).

7 Huw Dylan and Thomas J. Maguire, ***'Secret Intelligence and Public Diplomacy in the Ukraine War'*** *Survival* 64 no 4 (2022).

8 Seto Takashi, *Weaponized Disclosure of Intelligence in the Russia-Ukraine War* (Tokyo: National Institute for Defense Studies, 2022).

9 Ofek Riemer, ***'Politics is Not Everything: New Perspectives on the Public Disclosure of Intelligence by States',*** *Contemporary Security Policy* 42 no 4 (2021).

10 Dylan and Maguire, 'Secret Intelligence and Public Diplomacy'.

11 Victoria Smith and James Pamment, *Attributing Information Influence Operations: Identifying Those Responsible for Malicious Behaviour Online* (Riga: NATO Strategic Communications Centre of Excellence, 2022).

12 Joshua C. Huminski, 'Russia, Ukraine, and the Future Use of Strategic Intelligence', *Prism* 10 no 3 (2023).

13 Dylan and Maguire, 'Secret Intelligence and Public Diplomacy'.

14 Ruxandra Buluc, Rubén Arcos, and Cristina Ivan, ***'When Spies Go Public! Lessons Learnt from the Instrumentalization of Intelligence for Strategic Communication in the Run-up to the Russian-Ukrainian War'***, *Intelligence and National Security* 40 no 1 (2025).

15 David V. Gioe and Michael Morell, 'Spy and Tell: The Promise and Peril of Disclosing Intelligence for Strategic Advantage', *Foreign Affairs* 103 no 3 (2024).

16 Dylan and Maguire, 'Secret Intelligence and Public Diplomacy'.

17 Riemer, 'Politics is not everything'.

18 Scott Bomboy, ***'How One Telegram Helped to Lead America Toward War'*** National Constitution Center, 26 Febryary 2024. [Accessed 8 April 2025].

19 James M. Lindsay, ***'TWE Remembers: Adlai Stevenson Dresses down the Soviet Ambassador to the UN (Cuban Missile Crisis, Day Ten)'***, Council on Foreign Relations, 25 October 2012. [Accessed 8 April 2025].

20 Julian Borger, ***'Colin Powell's UN Speech: A Decisive Moment in Undermining US Credibility'***, *The Guardian*, October 18 2021. [Accessed 8 April 2025].

21 Karen Lund Petersen, *'Three Concepts of Intelligence Communication: Awareness, Advice or Co-Production?'*, *Intelligence and National Security* 34 no 3 (2019).

22 Cristina Ivan, Irena Chiru, and Rubén Arcos, *'A Whole of Society Intelligence Approach: Critical Reassessment of the Tools and Means Used to Counter Information Warfare in the Digital Age'*, *Intelligence and National Security* 36 no 4 (2021).

23 Bowman H. Miller, 'The Death of Secrecy: Need to Know ... with Whom to Share', *Studies in Intelligence* 55 no 3 (2011).

24 Rita Floyd and Mark Webber, *'Making Amends: Emotions and the Western Response to Russia's Invasion of Ukraine'*, *International Affairs* 100 no 3 (2024).

25 Nikki Ikani and Christoph O. Meyer, *'The Underlying Causes of Strategic Surprise in EU Foreign Policy: A Post-Mortem Investigation of the Arab Uprisings and the Ukraine–Russia Crisis of 2013/14'*, *European Security* 32 no 2 (2023).

26 Robert S. Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election, Volume I*, (Washington, D.cC.: U.S. Department of Justice, March 2019). [Accessed 26 May 2025].

27 Heather A. Conley and Jean-Baptiste Jeangène Vilmer, *'Successfully Countering Russian Electoral Interference'*, Center for Strategic and International Studies, 21 June 2018. [Accessed 26 May 2025].

28 Kevin Riehle, *'Ignorance, Indifference, or Incompetence: Why Are Russian Covert Actions so Easily Unmasked?'*, *Intelligence and National Security* 39 no 5 (2024).

29 Ibid.

30 Ibid.

31 Luke Harding, *"A Chain of Stupidity": The Skripal Case and the Decline of Russia's Spy Agencies'*, *The Guardian*, 23 June 23 2020. [Accessed 26 May 2025].

32 Buluc, Arcos, and Ivan, 'When spies go public!'.

33 Mark Phythian and David Strachan-Morris, *'Intelligence & the Russo-Ukrainian War: Introduction to the Special Issue'*, *Intelligence and National Security* 39 no 3 (2024).; Paul McLeary, *'Russian Buildup near Ukraine gains Steam, new Satellite Images Show'*, *Politico*, 23 December 2021. [Accessed 26 May 2025].

34 Shane Harris and Paul Sonne, *'Russia Planning Massive Military Offensive Against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns'*, *The Washington Post*, 3 December 2021. [Accessed 26 May 2025].

35 Julian Borger and Dan Sabbagh, *'US Warns of "Distinct Possibility" Russia Will Invade Ukraine Within Days'*, *The Guardian*, 12 February 2022. [Accessed 26 May 2025]; Antony J. Blinken, *'Remarks by Secretary Antony J. Blinken at the UN Security Council on Russia's Threat to Peace and Security'*, United States Mission to the United Nations, 17 February 2022. [Accessed 26 May 2025].

36 Jonathan Beale, *'Ukraine War: Predicting Russia's Next Step in Ukraine'*, *BBC*, 12 August 2022. [Accessed 26 May 2025].

37 David E. Sanger, *'U.S. Says Russia Sent Saboteurs into Ukraine to Create Pretext for Invasion'*, *The New York Times*, 14 January 2022. [Accessed 26 May 2025].

38 Julian Borger and Luke Harding, *'US Claims Russia Planning "False-Flag" Operation to Justify Ukraine Invasion'*, *The Guardian*, 14 January 2022. [Accessed 26 May 2025].

39 UK Government, *'Kremlin Plan to Install Pro-Russian Leadership in Ukraine Exposed: Foreign Secretary Liz Truss Gave a Statement on the Kremlin Plan to Install Pro-Russian Leadership in Ukraine'*, 22 January 2022. [Accessed 26 May 2025]; Gordon Corera, *'US Reveals Claims of Russian "Kill List" if Moscow Occupies Ukraine'*, *BBC*, 21 February 2022. [Accessed 26 May 2025].

40 Buluc, Arcos, and Ivan, 'When spies go public!'.

41 Ivar Ekman and Per-Erik Nilsson, *Ukraine's Information Front – Strategic Communication During Russia's Full-Scale Invasion of Ukraine* (Stockholm: Swedish Defence Research Agency, 2024).

42 Kyiv Post, *'From the Archives: SBU Intercepts Phone Conversations of Separatists Admitting Downing a Civilian Plane'*, 18 July 2014. [Accessed 26 May 2025].

43 Niklas Nilsson, 'De-Hybridization and Conflict Narration: Ukraine's Defence Against Russian Hybrid Warfare' in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm (eds) (London & New York: I.B. Tauris, 2021).

44 Peter Schrijver, *'Beyond Counterintelligence: Understanding the SBU's Social Media Outreach on Telegram During Wartime'*, *Intelligence and National Security* 39 no 3 (2024).

45 Victoria Butenko, Christian Edwards, and Alex Stambaugh, *'Ukraine Says it Has Sunk Another Warship, Disabling a Third of Russia's Black Sea Fleet'*, CNN, 14 February 2024. [Accessed 26 May 2025].

46 The New Voice of Ukraine, *'Ukrainian Military Publishes Intercepted Conversation from Lyman Direction'*, 20 January 2025. [Accessed 26 May 2025].

47 LB.ua, *'Ukrainian Intelligence Posts List of Russians Responsible for Bucha Atrocities'*, 4 April 2022. [Accessed 26 May 2025].

48 Ukrayinska Pravda/Military Times, *'Russian Warship... Go F--- Yourself'*, 28 February 2022. [Accessed 26 May 2025].

49 Ofek Riemer, *'Intelligence and the War in Ukraine: The Limited Power of Public Disclosure'*, The Institute for National Security Studies, 27 March 2022. [Accessed 26 May 2025].

50 Cited in France 24, *'Europe on Alert as Russia Steps up Aggressive Spying'*, 16 April 2021. [Accessed 26 May 2025].

51 The Economist, *'Russian Spies Are Back—And More Dangerous Than Ever'*, 20 February 2024. [Accessed 26 May 2025]; Sam Jones, *'German Spycatchers Raise Game against China and Russia'*, *Financial Times*, 23 April 2024. [Accessed 26 May 2025].

52 The Economist, *'Vladimir Putin's Spies are Plotting Global Chaos'*, 13 October 2024. [Accessed 26 May 2025].

53 Kevin Riehle, *'The Ukraine War and the Shift in Russian Intelligence Priorities'*, *Intelligence and National Security* 39 no 3 (2024).; Andrei Soldatov and Irina Borogan, *'The Rebirth of Russian Spycraft: How the Ukraine War has Changed the Game for the Kremlin's Operatives—And Their Western Rivals'*, *Foreign Affairs*, 27 December 2023. [Accessed 26 May 2025]; Daniela Richterova, Elena Grossfeld, Magda Long, and Patrick Bury, *'Russian Sabotage in the Gig-Economy Era'*, *The RUSI Journal* 169 no 5 (2024).; Julian E. Barnes, *'Russia Steps Up a Covert Sabotage Campaign Aimed at Europe'*, *New York Times*, 26 May 2024. [Accessed 26 May 2025]; Sam Jones, John Paul Rathbone, and Richard Milne, *'Russia Plotting Sabotage Across Europe, Intelligence Agencies Warn'*, *Financial Times*, 6 May 2024 [Accessed 26 May 2025]; Jack Watling, Oleksandr V. Danylyuk, and Nick Reynholds, *The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022–24* (London: RUSI, 2024); Henrik Praks, *Russia's Hybrid Threat Tactics Against the Baltic Sea Region: From Disinformation to Sabotage* (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2024). [Accessed 26 May 2025].

54 Michael Jonsson, *'Espionage by Europeans: Treason and Counterintelligence in Post-Cold War Europe'*, *Intelligence and National Security* 39 no 1 (2024).

55 Jakob Hanke Vela, *'FBI Dossier Reveals Putin's Secret Psychological Warfare in Europe'*, *Politico*,

5 September 2024. [Accessed 26 May 2025]; UK Government, *'UK Sanctions Putin's Interference Actors'*, 28 October 2024. [Accessed 26 may 2025]; Thomas Rid, *'The Lies Russia Tells Itself: The Country's Propagandists Target the West—But Mislead the Kremlin, Too'*, *Foreign Affairs*, 30 September 2024. [Accessed 26 May 2025].

56 Glenn Thrush, *'3 U.S. Intelligence Agencies Warn of Election Interference Efforts by Russia and Iran'*, *The New York Times*, 4 November 2024. [Accessed 26 May 2025].

57 US National Intelligence Council, *'Foreign Threats to US Elections After Voting Ends in 2024'*, 22 October 2024. [Accessed 26 May 2025].

58 Ketrin Jochecová, *'Moldovan Spy Chief: Russia Will Try to Interfere in 2025 Parliamentary Election, Too'*, *Politico*, 13 December 2024. [Accessed 26 May 2025]; European Parliament, *'Parliament Condemns Russia's Interference in Moldova'*, 9 October 2024. [Accessed 26 May 2025]; Filip Bryjka, *'Russian Interference Nearly Overwhelmed Moldovan Presidential Election-Referendum Vote'*, *The Polish Institute of International Affairs*, 20 November 2024. [Accessed 26 May 2025]; Orysia Lutsevych and Valeriu Pasha, *'Is Moldova a New Battleground in Russia's War?'*, *Chatham House*, 26 March 2024. [Accessed 26 May 2025].

59 Deborah Cole, *'Romanian Court Annuls First Round of Presidential Election'*, *The Guardian*, 6 December 2024. [Accessed 26 May 2025]; Valentina Pop, Polina Ivanova, and Dunai Marton, *'How Russia-Backed Influencers Meddled in Romania's Vote'*, *Financial Times*, 9 December 2024. [Accessed 26 May 2025]; Kelvin Chan, *'EU Investigates TikTok over Romanian Presidential Election Safeguards'*, *AP News*, 17 December 2024. [Accessed 26 May 2025]; Sarah Rainsford, *'Romania Hit by Major Election Influence Campaign and Russian Cyber-Attacks'*, *BBC*, 4 December 2024. [Accessed 26 May 2025]; RadioFreeEurope/RadioLiberty, *'Romanian Elections Targeted by "Aggressive Hybrid Russian Action"*, Declassified Documents Show', 4 December 2024. [Accessed 26 May 2025].

60 Xhoi Zajmi, *'AI-Driven Russian Disinformation Campaign Targets German Elections'*, *Euractiv*, 5 February 2025. [Accessed 26 May 2025]; Chris Lunday, *'Russia-Linked Fake Videos Spread German Election Fraud Claims, Authorities Warn'*, *Politico*, 21 February 2025. [Accessed 26 May 2025].

61 Alexej Hock, Max Bernhard, Till Eckert, and Sarah Thust, *'Influence Operation Exposed: How Russia Meddles in Germany's Election Campaign'*, *Correctiv*, 24 January 2025. [Accessed 26 May 2025].

62 Republic of Latvia Constitutional Protection Bureau, *'2024 Annual Report'*, 2024. [Accessed 26 May 2025].

63 Nette Nöstlinger, *'German Spy Chief: Russia Could Test NATO Loyalty to 'Mutual Defense' Clause'*, *Politico*, 28 November 2024. [Accessed 26 May 2025].

64 Forsvarets Efterretningstjenste, *'Opdateret vurdering af truslen fra Rusland mod Rigsfællesskabet'*, 11 February 2025. [Accessed 26 May 2025].

65 Niklas Nilsson, Mikael Weissmann, and Björn Palmertz, *'Hybrid Threats and the Intelligence Community: Priming for a Volatile Age'*, *International Journal of Intelligence and CounterIntelligence* (2025).

66 Huminski, 'Russia, Ukraine, and the Future Use of Strategic Intelligence'.

67 Riemer, 'Politics is not everything'.

68 Niklas Nilsson, Mikael Weissmann, Björn Palmertz, Per Thunholm, and Henrik Häggström, 'Security Challenges in the Grey Zone: Hybrid Threats and Hybrid Warfare' in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm (eds) (London & New York: I.B. Tauris, 2021).

69 Amy Zegart, *'Open Secrets: Ukraine and the Next Intelligence Revolution'*, *Foreign Affairs* 102 no 1 (2023). [Accessed 26 May 2025].

70 Phythian and Strachan-Morris, 'Intelligence & the Russo-Ukrainian War'.

71 Michael Raska, *'The Sixth RMA Wave: Disruption in Military Affairs?'*, *Journal of Strategic Studies* 44 no 4 (2021).

72 Gundars Bergmanis-Korāts, Tetiana Haiduchyk, and Artur Shevtsov, *AI in Precision Persuasion. Unveiling Tactics and Risks on Social Media* (Riga: NATO Strategic Communications Centre of Excellence, 2024). [Accessed 26 May 2025].

73 Tahereh Saheb, Mouwafac Sidaoui, and Bill Schmarzo, *'Convergence of Artificial Intelligence with Social Media: A Bibliometric & Qualitative Analysis'*, *Telematics and Informatics Reports* 14 (2024). [Accessed 26 May 2025].

74 Christine S. Pitt, Anjali Suniti Bal, and Kirk Plangger, *'New Approaches to Psychographic Consumer Segmentation: Exploring Fine Art Collectors Using Artificial Intelligence, Automated Text Analysis and Correspondence Analysis'*, *European Journal of Marketing* 54 no 2 (2020). [Accessed 26 May 2025].

75 Priya Bhatt, Amanrose Sethi, Vaibhav Tasgaonkar, Jugal Shroff, Isha Pendharkar, Aditya Desai, Pratyush Sinha, Aditya Deshpande, Gargi Joshi, Anil Rahate, Priyanka Jain, Rahee Walambe, Ketan Kotecha, and N. K. Jain, *'Machine Learning for Cognitive Behavioral Analysis: Datasets, Methods, Paradigms, and Research Directions'*, *Brain Informatics* 10 no 18 (2023). [Accessed 26 May 2025].

76 Gundars Bergmanis-Korāts, Giorgio Bertolin, Yukai Zeng, and Adele Pužule, *AI in Support of StratCom Capabilities* (Riga: NATO Strategic Communications Centre of Excellence, 2024). [Accessed 26 May 2025].

77 Tess Horlings, *'Dealing with Data: Coming to Grips with the Information Age in Intelligence Studies Journals'*, *Intelligence and National Security* no 38 (2023).

78 Damien Van Puyvelde and FernandoTabárez Rienzi, *'The Rise of Open-Source Intelligence'*, *European Journal of International Security* (2025). [Accessed 26 May 2025].

79 Amy Zegart, *Spies, Lies and Algorithms: The History and Future of American Intelligence* (Princeton & Oxford: Princeton University Press, 2022).

80 David P. Oakley and Jeff Rogg, *'Spreading the "Smog of War": The Impact of Propaganda, Social Media, and OSINT on U.S. Civil-Intelligence Relations'*, *Intelligence and National Security* 39 no 3 (2024).

81 Allison Carnegie and Austin Carson, *'The Disclosure Dilemma: Nuclear Intelligence and International Organizations'*, *American Journal of Political Science* 63 no 2 (2019).

82 Mikael Weissmann and Niklas Nilsson, *'Current Intelligence and Assessments: Information Flows and the Tension Between Quality and Speed'*, *International Journal of Intelligence and CounterIntelligence* 37 no 4 (2024).

83 Stevyn D. Gibson, 'Exploring the Role and Value of Open Source Intelligence', in *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities*, Christopher Hobbs, Matthew Moran, Daniel Salisbury (eds) (London: Palgrave Macmillan, 2014).

84 Damien Van Puyvelde, *Outsourcing US Intelligence: Contractors and Government Accountability* (Edinburgh: Edinburgh University Press, 2019).

85 Takashi, *Weaponized Disclosure*

86 Carnegie and Carson, 'The Disclosure Dilemma'.

87 Gioe and Morell, 'Spy and Tell'.

88 Riemer, 'Politics is not everything'.

89 Dylan and Maguire, 'Secret Intelligence and Public Diplomacy'.

90 Ibid.

91 Elsa Hedling and Hedvig Ördén, *'Disinformation, Deterrence and the Politics of Attribution'*,

International Affairs 101 no 3 (2025).

92 Dylan and Maguire, 'Secret Intelligence and Public Diplomacy'.

93 Buluc, Arcos, and Ivan, 'When spies go public!'.

94 Huminski, 'Russia, Ukraine, and the Future Use of Strategic Intelligence'.

95 Gioe and Morell, 'Spy and Tell'.

96 Dylan and Maguire, 'Secret Intelligence and Public Diplomacy'.

97 Buluc, Arcos, and Ivan, 'When spies go public!'.

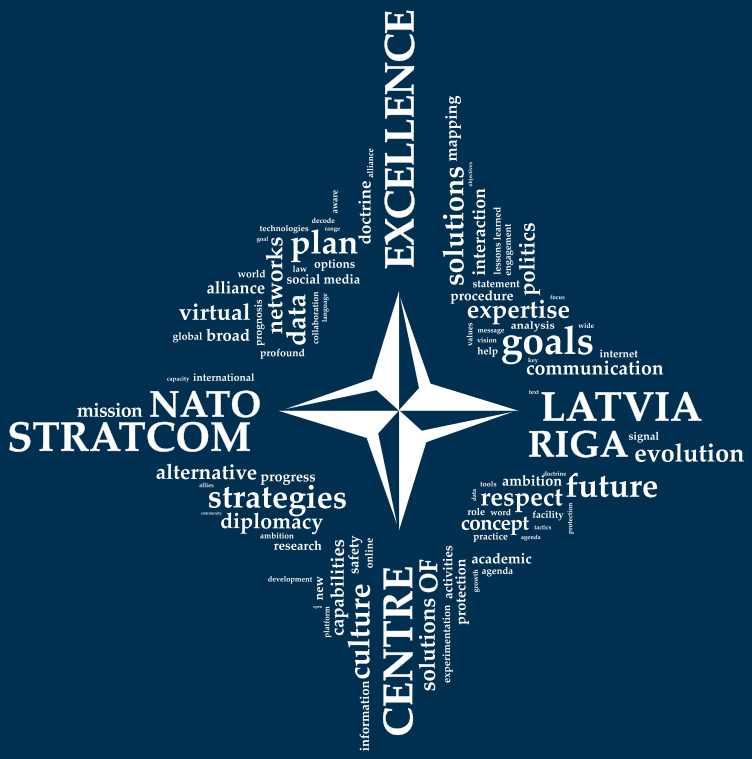
98 Kristian Gustafson, Dan Lomas, and Steven Wagner, ***'Intelligence Warning in the Ukraine War, Autumn 2021 – Summer 2022'***, *Intelligence and National Security* 39 no 3 (2024).

99 Julian E. Barnes and Adam Entous, ***'How the U.S. Adopted a New Intelligence Playbook to Expose Russia's War Plans'***, *New York Times*, 23 February 2023. [Accessed 26 May 2025].

100 Säkerhetspolisen, ***'Beslag av misstänkt fartyg för kabelbrott hävs'***, 3 February 2025. [Accessed 26 May 2025].

101 Huminski, 'Russia, Ukraine, and the Future Use of Strategic Intelligence'.

102 Ibid.



Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org