Eight Principles for Intelligence Sharing: A Holistic and Strategic Approach

Gazmend Huskaj[1,2]
[1]Geneva Centre for Security Policy (GCSP), Geneva, Switzerland
[2]Department of Computer and Systems Sciences, Stockholm University, Kista, Sweden
g.huskaj@gcsp.ch

Abstract: This paper reviews the strategic use of warning intelligence to pre-emptively address threats in complex geopolitical scenarios through rapid intelligence sharing. Specifically, the paper reviews the question How, based on research and experience, can a set of principles be applied by states to enhance situational awareness and tackle threat actors through a holistic and collaborative approach to intelligence sharing? The paper examines historical and contemporary alliances like the Five Eyes and reviews a Signals Intelligence Alliance as a case in point, highlighting the importance of collaborative approaches to enhance situational awareness and tackle threat actors. The study, grounded in the philosophical paradigm of interpretivism, adheres to the principles for transparent science when researchers use tools such as large-language-models as grammar editors or research assistants. The paper also acknowledges limitations such as the generalisability of the SIGINT model and the need for continuous adaptation of intelligence sharing practices. The results discuss policy, process, and people challenges to intelligence sharing. The paper concludes that successful intelligence sharing should follow eight general principles. Future research directions include exploring the impact of emerging technologies, human aspects of intelligence sharing, and context-based intelligence sharing alliances.

Keywords: Intelligence Sharing Principles; Strategic Warning Intelligence; SIGINT Alliance

[1]*The views expressed in this research product are only those of the author, and do not represent the Geneva Centre for Security Policy (GCSP), nor the Department of Computer and Systems Sciences, or any other party.*

1. Introduction

The current geopolitical security situation can be summarised by increased uncertainty and a shift from the traditional world order toward an indeterminate future (European Commission, 2023; Lazard, 2023). Threat actors are actively engaging in offensive cyberspace operations (Huskaj & Axelsson, 2023a) and cyber-enabled disinformation campaigns (Huskaj & Axelsson, 2023b) to achieve their tactical, operational, and strategic objectives. These activities include ransomware attacks, cyber-espionage, sabotage, destruction, and the employment of artificial intelligence (AI), such as deepfakes, to manipulate the perceived realities of societies by targeting individuals' fears and sowing distrust (Huskaj, 2024). Mitigating such attacks is crucial, and one effective approach involves the use of indicators and warnings—an intelligence-driven process that entails the identification of threat actors, along with their intentions and capabilities (Grabo, 2002).

How can the intent and capabilities of threat actors be discerned in a complex environment like today's geopolitical landscape, where state actors utilise their full arsenal? According to Meyer and Otto (2016), as cited in Rietjens (2020), “The idea of warning is that it enables a timely response so that harm is prevented or at least reduced by appropriate action. Effectively communicating the warning to decision-makers or the population at large is therefore of great importance. From Warner’s perspective, key communication requirements include source credibility, message content, and mode of communication.” Cynthia Grabo (2002) notes that strategic warning is a post-World War II innovation, developed in response to the perceived threats from the Soviet Union and other communist states to the security and interests of the “Free World” during the Cold War—actions that could potentially lead to unexpected conflict or direct aggression. In summary, the strategic application of warning intelligence aims to pre-emptively address threats in complex geopolitical scenarios through rapid sharing of intelligence.

The research question is: How, based on research and experience, can a set of principles be applied by states to enhance situational awareness and tackle threat actors through a holistic and collaborative approach to intelligence sharing?

Answering this question necessitates a short review of the literature on intelligence sharing and an understanding of past and current intelligence alliances. These alliances and partnerships include the Five Eyes, AUKUS, and the Signals Intelligence Alliance.

The Five Eyes (FVEY) alliance is one of the oldest and most comprehensive intelligence-sharing partnerships in the world. It consists of Australia, Canada, New Zealand, the United Kingdom, and the United States. Originating from World War II cooperative efforts, FVEY was formalized in the aftermath of the war through the UKUSA

Agreement in 1946 (Farrell, 2013; NSA, n.d.). This alliance focuses primarily on Signals Intelligence (SIGINT) and involves extensive sharing of intelligence gathered by each member's respective intelligence agencies. The unique strength of FVEY lies in its members' shared language, legal systems, and strong historical ties, which facilitate seamless collaboration (Corbett & Danoy, 2022). The geographical spread of the FVEY partners also enhances their global intelligence collection capabilities, providing access to diverse regions and intelligence sources that would be challenging for any single country to achieve alone.

AUKUS is a trilateral partnership announced in September 2021 between Australia, the United Kingdom, and the United States (U.S. DoD, n.d.). While it primarily focuses on enhancing Australia's naval capabilities through the acquisition of nuclear-powered submarines, AUKUS also encompasses broader aspects of defence and security cooperation, including cyber capabilities, artificial intelligence, quantum technologies, and additional undersea capabilities (Australian Government, 2022). This partnership signifies a strategic effort to strengthen security and stability in the Indo-Pacific region, addressing emerging threats and fostering greater interoperability among the three nations' defence forces. The AUKUS agreement underscores the shared commitment of its members to uphold international norms and maintain a balance of power in a region marked by increasing geopolitical competition (The White House, 2022).

The Signals Intelligence Alliance, as described by Bart Jacobs (2020), involves Denmark, France, Germany, the Netherlands, and Sweden. Initiated by Denmark in 1976, the alliance was formed to collaboratively address the challenges posed by signals intelligence, particularly with the advent of satellite communications. Germany and Sweden joined Denmark initially, followed by the Netherlands in 1978 and France in 1985. This alliance focuses on two main areas: signals analysis and cryptanalysis. Signals analysis involves coordinating interception mechanisms and sharing intercepted messages, which are discussed in multilateral meetings. Cryptanalysis, on the other hand, is handled bilaterally, with each country responsible for decrypting the messages it intercepts. The alliance is characterized by strong personal ties among its members and a high level of technical and cryptanalytical expertise, making it a successful model for intelligence sharing.

The main contributions of this research product can be summarised as follows:

- A set of principles for successful intelligence sharing (Section 4);
- A case study analysis of how the U.S. Intelligence Community can increase its intelligence sharing with allies, and based on this identified framework, review the SIGINT Alliance as a successful case, which leads to a set of principles for successful intelligence sharing (Section 3);
- A discussion on technological advancements, like AI and ML, and their impact on intelligence sharing (Section 3).

The remainder of this research product is organised as follows: Section 2 describes the methods and materials, Section 3 presents the results, while Section 4 presents the discussion. Finally, the conclusions are in Section 5.

2. Methods and Materials

This research is founded on the philosophical paradigm of interpretivism (Oates, 2005; Saunders et al., 2016). Interpretivism, a qualitative approach, posits that "the primary focus of research undertaken within this paradigm is the way we as humans attempt to make sense of the world around us" (Saunders et al., 2016, p. 134). Therefore, it can be argued that understanding intelligence sharing is influenced by examining the subjective interpretations and motivations of individuals.

The base of this research product is a systematic review of the scientific literature on intelligence sharing using Elsevier's Scopus abstract database. Scopus was selected due to its extensive coverage of peer-reviewed journals across various disciplines, ensuring a wide range of relevant articles. The search strategy was using a search query designed to capture articles related to intelligence sharing. The search query in Scopus was {intelligence sharing}. The curly bracers force the search engine to only provide research articles having both words in sequence. The results included many articles that were beyond the scope of this research, such as blockchain. Therefore, the decision to use additional sources was taken. Alongside the Scopus database, professional sources such as government reports, policy papers, and white papers were incorporated to provide a practical perspective on intelligence sharing. Notable sources included publications from the U.S. Department of Defence, NATO, various intelligence agencies, and books. The references section provides a list of relevant sources.

Although many instances of intelligence sharing are introduced in the initial section, only two cases are examined in depth: the enhancement of intelligence sharing by the U.S. Intelligence Community (Corbett & Danoy, 2022),

and the SIGINT Alliance (2020) as a successful example. The challenges and opportunities of intelligence sharing are analysed and discussed in the discussion section, from which a set of general principles for successful intelligence sharing is deduced and presented.

Additionally, this research aligns with the principles of transparent science as upheld by Nature and Springer Nature journals, utilising tools such as ChatGPT (Nature, 2023). In this study, ChatGPT4 has been employed both as a grammar editor and a research assistant. The editorial in Nature posits that trust in science is founded on researchers' transparency regarding their methods and materials—a position with which this author concurs. Moreover, the author believes that leveraging technological advancements is essential for enhancing information collection, processing, analysis, synthesis, production, and dissemination. Researchers who neglect to utilise these technologies risk falling behind, as discussed thoroughly by Mortenson & Vidgen (2016) in their discussion section.

This research has limitations. While the study describes a successful intelligence sharing strategy exemplified by the SIGINT Alliance, inherent limitations must be considered. First, the generalizability of the SIGINT model may be constrained by unique historical, geopolitical, and cultural contexts absent in other intelligence sharing environments. Additionally, while the focus on technical and cryptanalytical skills is beneficial, it could overshadow other crucial aspects such as human intelligence and open-source intelligence, which are equally vital to a comprehensive intelligence sharing strategy.

Moreover, the reliance on strong personal ties and leadership commitment can be a double-edged sword; while these factors enhance trust and efficiency, they may also introduce vulnerabilities if key individuals depart or if there is a shift in political priorities. Additionally, although technological interoperability is ideal, it often confronts practical challenges such as funding disparities, differing technical standards, and the rapid pace of technological changes, which might surpass the adaptability of alliances. Finally, while streamlined processes can reduce bureaucracy, they may compromise thorough oversight and accountability, potentially leading to ethical and legal dilemmas. These limitations highlight the imperative for continuous evaluation and adaptation of intelligence sharing practices to ensure their efficacy and relevance to evolving circumstances.

3. Results

The first case to review is the U.S. intelligence community. According to former Director of National Intelligence Lt. Gen. James Clapper, “Governments quite rightly protect their intelligence sources, methods, and collection capabilities as critical national assets.” However, “this must be balanced against the need to share high-quality intelligence with allies and partners to ensure a compelling and united imperative to act” (Clapper, as cited by Corbett & Danoy, 2022).

Sean Corbett and James Danoy (2022) state that “the Ukraine crisis and the US-led counterterrorist response to 9/11 have both demonstrated an ability to surge intelligence sharing, even with non-traditional partners, where political will exists at the highest level, and it is imperative to address a serious contemporary security challenge. This indicates that restrictive information-sharing practices and policies are not immutable but rather self-imposed and malleable.” According to them, the Five Eyes alliance is considered the optimum model for intelligence sharing. The reason for this is “predominantly due to shared values, standards, national interests, and language, but also because the muscle memory already exists—the FVEY relationship has developed over a considerable period.” Additionally, “The geographical spread of the FVEY partners also facilitates greater access to intelligence collection opportunities not readily available to all.” However, as challenges increase, there is a need to share intelligence with individual nations and coalitions beyond the Five Eyes, depending on security requirements and levels of trust.

The challenges to intelligence sharing stem from various factors, including policy, legal issues, security concerns, processes, technology, and people, as well as institutional and organisational culture. For instance, Jeffery Richelson (2016) highlights the complexity of coordinating multiple agencies within the U.S. intelligence community, which can hinder timely intelligence sharing. Additionally, the complexity of intelligence alliances increases with the number of entities involved: more participants in an alliance make it more difficult to share intelligence and heighten the associated risks. In coalition environments, when individuals become aware of exclusive small group meetings, feelings of exclusion can lead to hurt and a loss of trust (Corbett & Danoy, 2022).

According to Corbett and Danoy (2022), the policy challenges include a federated authority and decentralised control, where the authority to share intelligence is distributed among various bodies within the Intelligence Community and the Department of Defence. Furthermore, numerous intelligence community directives and

other policy documents govern intelligence sharing, often leading to policy overlap and sometimes contradictory mandates. This is compounded by a prevalent culture of risk aversion, which prioritises information security over sharing.

Policies that default to non-disclosure unless explicitly authorised perpetuate a cultural bias towards restricting the flow of information. Additionally, approval processes are complex, requiring multiple approvals and interagency coordination, which can be time-consuming and impact time-sensitive actions (Corbett & Danoy, 2022). Some policies also need to be updated to reflect the current operational environment or technological advancements. Moreover, there is always a balance to be struck between security and sharing—the need to protect intelligence, sources, and methods versus the benefits of sharing them.

One way to address the policy challenge is to shift from a default of "NOFORN" to the Australian model, which adopts a default classification of "Releasable FVEY," as noted by Corbett & Danoy (2022). Another approach could involve granting dual citizenship to staff serving in each country's intelligence services during their tenure. Furthermore, policy could be framed to default to stating that information sharing should occur at the broadest possible level with coalition and approved partner countries, and intelligence products should be drafted with a presumption of release to allies, coalitions, and international organisations (Corbett & Danoy, 2022).

Some challenges related to processes and technology include complex approval and coordination chains across different agencies and bodies, often resulting in delays and inefficiencies. For instance, a multi-source intelligence agency, such as the Defense Intelligence Agency, would need to contact each single-source agency to authorise the release of intelligence (Corbett & Danoy, 2022). Additionally, inconsistencies across agencies, with varying comfort levels and policies regarding intelligence sharing, complicate efforts to standardise sharing processes. The technological challenges arise because organisational structures and existing technologies do not keep pace with advancements in artificial intelligence (AI) and machine learning (ML). Moreover, while applying AI and ML can help streamline processes, these technologies cannot be applied to sensitive intelligence, making sharing a significant challenge (Corbett & Danoy, 2022).

The challenge of intelligence sharing related to people includes a cultural trait of risk aversion and fears of potential repercussions, such as criminal, civil, and administrative sanctions, which discourage proactive intelligence sharing. Additionally, workplace and institutional cultures must be integrated and aligned with policies and processes that encourage sharing; otherwise, overall effectiveness is reduced (Herman, 1996). Encouraging sharing also necessitates education and training for staff that highlights the mutual benefits of intelligence sharing and increased situational awareness. Finally, effective intelligence sharing requires strong support from leadership at all levels, who must align policies, processes, and cultural elements and be willing to assume risks on behalf of their teams (Zegart, 2009; Zegart, 2011).

The second case to review is the signals intelligence sharing alliance between Denmark, France, Germany, the Netherlands, and Sweden, as described by Bart Jacobs (2020) in his research article. According to Jacobs (2020), the alliance was initiated by Denmark in 1976, with Germany and Sweden joining initially. The Netherlands was invited to join in 1977 and formally did so in 1978, while France requested to join in 1983, received an invitation in 1984, and became a member in 1985.

The motivations for establishing broader cooperation were twofold. Firstly, the advent of signals intelligence via satellites necessitated substantial investment. Secondly, there was a need to address technical interception challenges and exchange methods collaboratively. The strategy was to combine forces and divide tasks to reduce costs and enhance effectiveness. The cooperation encompassed both cryptanalysis and signals analysis (Jacobs, 2020).

The signals analysis component focused on coordinating interception mechanisms and efforts to exchange intercepted (encrypted) messages. This aspect of the work was discussed in multilateral meetings involving the entire SIGINT Alliance (Jacobs, 2020). Cryptanalysis, in contrast, was addressed only bilaterally, with each participating country responsible for its own decryption efforts. According to Jacobs (2020), maintaining such division is common practice within the intelligence community to prevent the dissemination of manipulated information.

In essence, the intelligence alliance between these five countries was founded on close contacts among leading figures; the cooperation was bottom-up and relied on close personal ties and a shared high level of technical and cryptanalytical skills. Jacobs (2020) notes that certain countries were deliberately excluded from joining because they were considered to lack the relevant signal or crypto-analytical expertise and/or experience.

4. Discussion

The answer to the research question—How, based on research and experience, can a set of principles be applied by states to enhance situational awareness and tackle threat actors through a holistic and collaborative approach to intelligence sharing—comprises a set of eight general principles. These principles were derived from a detailed analysis of the SIGINT Alliance and challenges faced by the U.S. intelligence community, supported by various sources.

4.1 Policy Challenges

Regarding policy challenges, the SIGINT Alliance was formed based on close contacts between leading figures and close personal ties. A second important aspect is the skill set: these countries share a high level of technical and cryptanalytical skills. Additionally, these close ties likely streamlined policies through bilateral discussions and agreements, establishing a framework that accommodated the specific requirements of each country. An example of this framework, as suggested, focuses the cooperation on two parts: signals analysis and cryptanalysis. While signals analysis was discussed in multilateral meetings, cryptanalysis and decryption were the responsibility of each participating country and were discussed only bilaterally. Thus, it is plausible that shared classification protocols were developed to facilitate intelligence sharing, while cryptanalysis, discussed only bilaterally, suggests a security protocol based on the sensitivity of decryption methods. Finally, considering how the alliance was developed, the collaborative approach likely led to a distribution of decision-making authority that was aligned through common goals and regular communication.

4.2 Process Challenges

The SIGINT Alliance's small size and focused membership likely facilitated quicker consensus-building and decision-making processes. The alliance likely benefited from streamlined approval processes, enabled by the trust and operational compatibility developed among the members. The alliance probably invested in compatible technology platforms for sharing intelligence. It is reasonable to suggest that the SIGINT Alliance emphasised technological interoperability and possibly the joint development of tools, which would reduce disparities and enhance real-time data exchange. The SIGINT Alliance was almost certainly focused on efficiency, likely minimising bureaucratic overhead through simplified processes, particularly in secure communications and data handling.

4.3 People Challenges

The shared professional culture of cryptology and SIGINT among the member states likely helped align risk management strategies and operation security, thereby reducing the excessive risk aversion typically seen in larger and more diverse intelligence communities. It is conceivable that a culture of shared risk and mutual benefit was promoted to encourage more open-sharing practices. Given the technical nature of the alliance’s work, the SIGINT Alliance likely placed a strong emphasis on specialised training and professional development to ensure that all members were well-versed in the tools and protocols necessary for collaboration. The alliance might have developed a recognition system that acknowledged contributions and successful collaborations, thereby fostering a more proactive sharing environment. This would likely involve clear communication of the benefits of sharing, such as enhanced collective security. Strong leadership and committed support from all levels of the participating intelligence agencies are likely factors in the alliance’s success. Leadership possibly played a critical role in maintaining focus on the alliance’s objectives and ensuring that operational priorities were aligned.

4.4 The Eight General Principles for Successful Intelligence Sharing

Based on all of the above, the following general principles can be deduced for successful intelligence sharing:

1. Establish strong personal and institutional ties—Build an alliance based on strong personal relationships and close contacts between key figures. This helps streamline decision-making and enhance trust among the members.
2. Develop compatible and streamlined policies—Create mutually agreed-upon frameworks that cater to the specific needs and security requirements of each member country, with shared

classification protocols that allow for seamless intelligence sharing. Policies should be clear, consistent, and as much as possible free from contradictions.
3. Emphasise technical and analytical skills - Encourage developing and sharing high-level technical and cryptanalytical skills within the alliance and provide continuous training and professional development to keep pace with advancements in technology and analytical methods.
4. Foster technological interoperability and joint tool development - Invest in compatible technology platforms that facilitate secure and efficient data exchange and collaborate on developing joint tools and technologies that enhance the capabilities of all members, thereby reducing technological disparities.
5. Streamline processes to reduce bureaucracy - Minimise bureaucratic overhead by simplifying approval processes and enhancing operational compatibilities and develop efficient protocols for secure communications and data handling to prevent delays and ensure timely sharing of intelligence.
6. Cultivate a culture of shared risk and benefit—Promote a culture where risk management strategies are aligned, there is a collective responsibility for security and sharing outcomes and encourage a perspective that values intelligence sharing as beneficial for the collective security and success of all members.
7. Implement incentives and recognition systems - Develop recognition systems that acknowledge and reward successful collaborations and contributions to the alliance's objectives and clearly communicate the benefits of sharing intelligence, such as enhancing collective security and operational effectiveness.
8. Ensure strong and committed leadership—Secure committed support and leadership at all levels within the participating agencies. Leadership should actively maintain the focus on the alliance's objectives and ensure that operational priorities are synchronized and met.

5. Conclusions & Future Research

In conclusion, successful intelligence sharing in the current geopolitical security situation hinges on strategic collaboration that efficiently circumvents common barriers associated with policy, process, and people. The SIGINT Alliance exemplifies a model where close personal ties, a high degree of technical and cryptanalytical expertise, and a concerted effort towards streamlined operational processes effectively enhance intelligence sharing capabilities among member states. This alliance underscores the importance of mutual trust and the alignment of strategic goals across different national entities, facilitated by an agreed framework that accommodates the varied requirements and security protocols of each country.

By focusing on creating a conducive environment for intelligence sharing through compatible technological platforms, minimised bureaucratic processes, and a shared professional culture, intelligence sharing alliances can likely manage to mitigate the risks associated with complex intelligence sharing. These efforts are supported by strong leadership, continuous training, and a clear understanding of the shared benefits of collaboration, which are crucial for maintaining the operational integrity and effectiveness of intelligence operations.

The general principles derived from the SIGINT Alliance provide a first step for other intelligence sharing initiatives. These principles advocate for the establishment of strong foundational relationships, the development of cohesive and flexible policy frameworks, and the cultivation of a supportive operational culture. Together, these strategies empower intelligence communities to respond more dynamically and effectively to emerging global threats, thereby enhancing international security and cooperation.

Future research can explore several areas to further understand and enhance intelligence sharing, such as a potential prioritisation between the sharing principles. While this study mentions the Five Eyes and the AUKUS, these are not covered here. As the Five Eyes intelligence sharing alliance has worked to date, the AUKUS trilateral partnership highlights how an intelligence sharing alliance is established based on a specific context (the Indo-Pacific), and with specific capabilities (e.g. submarines, nuclear power and propulsion). Future research can include these intelligence sharing alliances as well as military operations. Next, the impact of emerging technologies should be examined, focusing on the impact of AI and ML. Additionally, ethical, legal and security implications should be reviewed. Additional areas may include cultural and organisational structures and how they influence trust-building, risk perception and cooperation among allies.

The role of policy evolution and harmonisation within a rapidly changing geopolitical security situation may be further investigated. Studies focusing on how policies are adapted and harmonised among diverse international

partners are crucial, particularly in responding to emergent threats such as malicious cyber operations and disinformation. Additionally, there is a significant need to delve into the human aspects of intelligence sharing. Future research may explore the impact of training programs, personnel exchanges, and establishing a common linguistic and professional standard among allies. Understanding how these factors either facilitate or impede effective intelligence sharing could offer valuable insights into enhancing collaborative intelligence sharing. A good start could be to review the NATO standardisation agreements (STANAG).

Longitudinal research is also essential to gauge the long-term efficacy of intelligence sharing agreements. Such studies could provide a deeper understanding of the sustainability and adaptability of these agreements to evolving threats. They may track the progression and outcomes of intelligence sharing initiatives over time, offering a comprehensive view of their effectiveness.

Moreover, incorporating quantitative methods can augment research of intelligence sharing. By applying empirical data to evaluate aspects such as response times to threats, the accuracy of shared intelligence, and the cost-effectiveness of cooperative operations, research can provide data-driven conclusions.

Finally, comparative studies can provide additional understanding of different intelligence sharing frameworks and agreements. Researchers can identify best practices and common challenges by comparing and contrasting various alliances, including those that are, for example, military-led versus civilian-led. These comparisons may highlight effective intelligence sharing strategies and help recognise areas that require improvement or adjustment to better meet contemporary security demands.

References

Australian Government, Department of the Prime Minister and Cabinet. (2022). FACT SHEET: Implementation of the Australia – United Kingdom – United States Partnership (AUKUS). Retrieved from: https://pmtranscripts.pmc.gov.au/sites/default/files/AUKUS-factsheet.pdf.

Corbett, S., & Danoy, J. (2022). Beyond NOFORN: Solutions for increased intelligence sharing among allies. Atlantic Council. Retrieved from: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/.

Defence Research and Development Canada. (2020). Standards for Evaluating Source Reliability and Information Credibility in Intelligence Production. Retrieved from: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc351/p812555_A1b.pdf.

Department of the Army. (2006). Human intelligence collector operations (FM 2-22.3 [FM 34-52]). Retrieved from: https://irp.fas.org/doddir/army/fm2-22-3.pdf.

European Commission. (2023). Shift in the geopolitical landscape. Retrieved from: https://knowledge4policy.ec.europa.eu/foresight/shift-geopolitical-landscape_en.

Grabo, C. M. (2002). Anticipating Surprise: Analysis for Strategic Warning. ISBN: 0-9656195-6-7.

Farrell, P. (2013). History of 5-Eyes – explainer. The Guardian. Retrieved from: https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

Herman, M. (1996). Intelligence Power in Peace and War. Cambridge University Press.

Huskaj, G., & Axelsson, S. (2023a). A state-of-the-art of scientific research on disinformation. Proceedings of the 22nd European Conference on Cyber Warfare and Security, 22(1).

Huskaj, G., & Axelsson, S. (2023b). A whole-of-society approach to organise for offensive cyberspace operations: The case of the smart state Sweden. Proceedings of the 22nd European Conference on Cyber Warfare and Security, 22(1).

Huskaj, G. (2024). Future Elections and AI-Driven Disinformation. The Defence Horizon Journal. https://doi.org/10.5281/zenodo.11140806.

Jacobs, B. (2020). Maximator: European signals intelligence cooperation, from a Dutch perspective. Intelligence and National Security, 35(5), 659-668. https://doi.org/10.1080/02684527.2020.1743538.

Lazard. (2023). The Global Geopolitical Landscape in 2023. Retrieved from: https://www.lazard.com/research-insights/the-global-geopolitical-landscape-in-2023/.

Mortenson, M. J., & Vidgen, R. (2016). A computational literature review of the technology acceptance model. International Journal of Information Management, 36(6), 1248–1259. https://doi.org/10.1016/j.ijinfomgt.2016.07.007.

Nature. (2023). Tools such as ChatGPT threaten transparent science; here are our ground rules for their use. Nature. Retrieved from: https://www.nature.com/articles/d41586-023-00191-1.

NSA-National Security Agency/Central Security Service. (n.d.). UKUSA Agreement Release. Retrieved from: https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/UKUSA/.

North Yorkshire. (2020). Intelligence Sharing Guide for the Partnership Information Sharing Form. Retrieved from: https://www.safeguardingchildren.co.uk/wp-content/uploads/2020/02/NYSCP-NYCSP-Intel-sharing-OMG-2020-06-15.pdf.

Oates, B. J. (2005). Researching Information Systems and Computing. Sage Publications, Inc.

Richelson, J.T. (2016). The U.S. Intelligence Community (7th ed.). Routledge. Retrieved from: https://doi.org/10.4324/9780429494321.

Rietjens, S. (2020). A warning system for hybrid threats – is it possible? Hybrid CoE. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2020/06/Strategic-Analysis_22_WarningSystem-1.pdf.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2016). Research Methods for Business Students. Financial Times/Prentice Hall.

U.S. Department of Defense. (2016). Evaluation of U.S. intelligence and information sharing with coalition partners in support of Operation Inherent Resolve. Retrieved from: https://media.defense.gov/2020/Aug/07/2002472951/-1/-1/1/DODIG-2016-081.PDF (Report No. DODIG-2016-081).

The White House. (2022). FACT SHEET: Implementation of the Australia – United Kingdom – United States Partnership (AUKUS). Retrieved from: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/.

Zegart, A. (2009). Spying Blind: The CIA, the FBI, and the Origins of 9/11. Princeton University Press.

Zegart, A. (2011). Implementing Change: Organizational Challenges. In Fischhoff, B., In Chauvin, C., & National Research Council (U.S.). Intelligence analysis: Behavioral and social scientific foundations. Washington, DC: National Academies Press.