Dean&Francis
ISSN 2959-6149

Convergence, Coordination, and Cybersecurity in Global Intelligence Sharing

Yichen Guo

McCourt School of Public Policy, Georgetown University, Washington, D.C., 20001, United States
yg380@georgetown.edu

Abstract:

This paper explores the critical importance of cooperation and trust in global intelligence sharing, drawing from historical and contemporary examples to highlight the complexities and challenges involved. The success of Operation Overlord during World War II exemplifies the power of effective intelligence collaboration, while the Snowden leaks reveal the fragility of trust within the intelligence community. The paper examines the challenges posed by fragmented and overlapping systems, as illustrated by the 9/11 attacks and the Boston Marathon Bombing, and underscores the need for streamlined communication and coordination among intelligence agencies. It also addresses the growing threat of cyber attacks, emphasizing the necessity of robust cybersecurity measures to protect shared intelligence. The discussion extends to the importance of rebuilding trust among allies, enhancing coordination, and developing unified cybersecurity standards. By addressing these key issues, the paper argues that intelligence agencies can better safeguard national and global security interests, ensuring a more secure and cooperative international environment.

Keywords: Global Intelligence Sharing, Cybersecurity, Snowden leaks reveal

1. Introduction

In American history, intelligence sharing plays an important role. In Operation Overlord, the successful intelligence cooperation between the US and the UK played a pivotal role in deceiving the German forces. The well-designed scenario at the military base, including the presence of General George Patton walking his dog and inspecting the FUSAG, served as a strategic diversion [1]. Simultaneously, MI5 played a crucial role as well. MI5 skillfully employed double agents who served Germany to mislead Germans about the FUSAG order of battle and the actual invasion plans, which contributed significantly to the success of Operation Overlord [1]. This is such a successful intelligence sharing and cooperation among countries in intelligence history.

Nevertheless, as the interconnectedness of global

ISSN 2959-6149

threats requires collective vigilance, the imperative for intelligence sharing and collaboration among allies has become even more pronounced. An increasing number of allies is needed against challenges such as cyber threats, terrorism, and geopolitical uncertainties. In an era where information is both a strategy and a potential vulnerability, fostering trust and reliability in intelligence partnerships becomes not just a historical lesson but a pressing necessity for safeguarding shared interests and addressing shared threats.

This paper explores the complexities of intelligence sharing in the modern era, focusing on the convergence of trust and national interest, the challenges posed by fragmented and overlapping systems, and the critical importance of cybersecurity. By examining these key issues, the paper aims to highlight the importance of coordinated efforts and robust security measures in maintaining effective global intelligence cooperation.

2. Matter 1: Convergence of Trust and National Interest in Intelligence Partnerships

The convergence of trust and national interest is crucial for effective intelligence sharing and international cooperation. Historical events, such as the revelations by Edward Snowden, underscore the complexities involved. The Snowden leakage raised serious concerns about the extent and scope of surveillance activities conducted by the NSA. This led to trust concerns between the US and its allies, as well as within the international intelligence community. Allies began to question the reliability and intentions behind the shared intelligence, fearing overreach and potential privacy violations [2].

Following the disclosures, many countries became cautious about sharing sensitive information, concerned about how their intelligence contributions might be used or exposed. One notable example is the skepticism directed towards the Five Eyes agreement, which faced criticism for its lack of transparency and the potential for unchecked government surveillance. After the Snowden disclosure, concerns were not only about national security but also about protecting the information of citizens. European courts, in particular, brought up skepticism towards the surveillance of Five Eyes nations, urging a shift towards more democratic accountability and transparency in surveillance and intelligence-sharing practices.[3] This shift requires less intrusive government surveillance practices. Therefore, trust concern has a profound impact on how international intelligence-sharing agreements were perceived and conducted after the Snowden disclosures.

Concerns about privacy and overreach have made countries more conscious about sharing sensitive data, which is crucial for effectively combating global terrorist threats [3]. This change marked a significant shift in the landscape of international intelligence cooperation. In the Snowden case, technological disparities can be a factor that impacts trust and reliability. There is the significant technological disparity in the Five Eyes alliance that is heavily dominated by US contributions. The advanced surveillance techniques used by the NSA, as revealed by Snowden, can make the allies feel over-relying on US intelligence, potentially undermining trust and raising concerns about relying on one dominant partner for intelligence.

In the context of national interests, the EU's relationship with China and the US illustrates the complexities of intelligence partnerships. China's sanctions on Lithuania for setting up the Taiwanese Representative Office in Vilnius led to significant economic impacts and a reevaluation of relationships with China [4]. To counter such threats, Baltic States should coordinate a collective European response to economic security, uniting democratic powers to defend against Chinese coercion.

The attitudes of small states, aligned with their national interests, play a crucial role in intelligence sharing for several reasons. Small states like Lithuania need to balance their national interests with the broader objectives of intelligence alliances. Strategic ambiguity—adopting a cautious and non-committal stance on sensitive issues like Taiwan—can be an effective approach for these countries [5]. China's Wolf Warrior Diplomacy is to legitimize the CCP's leadership by inflating nationalism and pushing Chinese ideas to other regions in the world aggressively [6]. It is obvious that China is "killing the chicken to scare the monkey," and the monkeys are big powers that support Taiwan [7]. Powerful states, such as Germany, may not entirely abandon economic cooperation with China but will adopt strategic measures to prevent over-dependence and potential sanctions. For small states, maintaining strategic ambiguity allows them to navigate the complex geopolitical landscape without provoking China while still fostering close economic ties with Taiwan and securing support from other democratic regions.

This approach is critical for intelligence sharing because it ensures that small states can continue to contribute valuable intelligence without jeopardizing their national interests or relationships with major powers. In 2023, China was the third-largest partner for EU exports of goods and the largest partner for EU imports of goods [8]. China tried to coerce Baltic states to follow the Chinese rules, not recognizing Taiwan as a sovereign state and lessening economic ties with Taiwan. China's sanction to Lithuania

shows that if any state violates China's rule, it would be sanctioned for cutting down on economic cooperation, forcing states like Lithuania to withdraw from their policies and affairs with Taiwan. Therefore, as each country prioritizes its national interests in intelligence cooperation, there is a tendency to withhold or selectively share information, treating the same intelligence differently based on their strategic objectives. An example of this selective sharing can be seen in the varying degrees of cooperation and intelligence sharing within the EU regarding migration and counter-terrorism efforts. Countries with different threat perceptions and national interests often approach the same intelligence data in diverse ways, affecting the overall efficacy of collective intelligence operations.

In conclusion, achieving convergence between trust and national interest in intelligence partnerships is essential. Trust issues stemming from surveillance practices and technological disparities must be managed to ensure effective cooperation. Additionally, aligning national interests, such as responding to economic coercion and adopting strategic ambiguity where necessary, is crucial for maintaining robust and reliable intelligence-sharing partnerships. By fostering trust, enhancing transparency, and strategically aligning national interests, countries can better safeguard their shared security and economic well-being.

3. Matter 2: Fragmented and Overlapped System

Despite the trust and reliability among allies, an excess of cross-national organizations can lead to fragmentation and overlap, resulting in a lack of coordination. Systemic communication breakdowns and delayed responses become significant consequences of this lack of coordination. A glaring example was in the event of 9/11, critical delays in communication occurred between the Federal Aviation Administration (FAA) and NORAD. The FAA failed to promptly notify NORAD of the hijackings, and when NORAD did receive the information, it struggled to swiftly assess and respond to the rapidly evolving situation [9]. This breakdown in communication and coordination directly contributed to the inability to intercept the hijacked planes before reaching their targets, highlighting the urgent need for streamlined and efficient communication channels within the intelligence and defense network.

Also, prior to 9/11, there was a lack of effective information sharing and integration among US intelligence and defense agencies, including NORAD. Important intelligence that could have alerted NORAD to the possibility of an attack using aircraft as weapons was not effectively shared or acted upon.[9] However, with too many agencies, the information for each agency may not be effectively shared among agencies. For example, there are assumptions that in the 2013 Boston Marathon Bombing, Tamerlan was considered to be an FBI informant, and Tamerlan and Jahar, whose identities were on the terrorist list, should have been informed at the POE [10]. Therefore, the effectiveness and clarity of roles in the intelligence agencies are matters of intelligence sharing and cooperation.

4. Matter3: Cybersecurity Concerns

In an era of digital intelligence, there's a threat of cyber attacks. Therefore, ensuring the secure transmission and storage of shared intelligence is a critical challenge. Cyber threats not only target individual nations but also the intricate network of international intelligence sharing. Therefore, the secure transmission and storage of shared intelligence are thus critical, demanding robust cybersecurity measures to protect data from unauthorized access while ensuring its integrity and availability. Additionally, establishing common standards and protocols for cybersecurity in intelligence sharing can enhance the overall security posture of allied nations.

Besides the Snowden incident, the OPM breach, where sensitive personal information of millions of US government employees was stolen, and the SolarWinds attack exposed the vulnerabilities in the software supply chain security. In the case of the OPM breach, the personal information obtained from the hackers could be used for blackmail, coercion, or to identify individuals in sensitive positions, thereby impacting their safety and the security of covert operations and military actions.[11] Such breaches also expose the techniques used in intelligence gathering, potentially rendering them ineffective. Over time, these breaches can erode the strategic advantage held by intelligence agencies, necessitating the development of new methods and technologies for intelligence gathering and analysis.

Developing unified cybersecurity standards and protocols is a significant challenge to international intelligence sharing. Addressed in Matter 1, diverse technological capabilities among allies mean that some nations may not be equipped to implement or maintain high-level cybersecurity measures. Additionally, there are different legal frameworks and cultural attitudes regarding privacy and data protection across countries. These disparities can create hindrances in aligning policies and practices, leading to potential vulnerabilities in shared intelligence networks. Overcoming these challenges requires a concerted effort to regulate cybersecurity standards, possibly through international agreements or collaborative frameworks that

ISSN 2959-6149

consider these diverse legal and technological landscapes. To summarize, from the historical experience of Operation Overlord to the modern-day concerns after the Snowden leakage, there is still a robust need for cooperation and trust among allies has never been more evident. The terrorist attacks underscore the consequences of systemic inefficiencies in intelligence coordination, while the digital era's cybersecurity challenges highlight the need for sophisticated and collaborative defense mechanisms. The future of effective global intelligence cooperation faces challenges such as rebuilding trust, enhancing coordination, and fortifying cybersecurity defenses. Intelligence agencies can better safeguard national and global security interests if policies can help make the intelligence-sharing system more organized and trusted, thus ensuring a more secure and cooperative international environment.

5. Conclusion

From the historical experience of Operation Overlord to the modern-day concerns highlighted by the Snowden leaks, the importance of cooperation and trust among allies in intelligence sharing remains evident. The challenges of fragmented and overlapping systems, along with the ever-present threat of cyber-attacks, underscore the need for sophisticated and collaborative defense mechanisms. The future of effective global intelligence cooperation hinges on rebuilding trust, enhancing coordination, and fortifying cybersecurity defenses. By addressing these key issues, intelligence agencies can better safeguard national and global security interests. Through a commitment to transparency, strategic alignment of national interests, and the establishment of robust cybersecurity measures, the global intelligence community can ensure a more secure and cooperative international environment. This collaborative approach is essential for addressing the complex and evolving threats of the modern era, ultimately contributing to a safer and more stable world.

References

[1] Woodward, John D., ed. "Lectures #11, 12, 13, 14, 15, & 16." Essay. In Spying--From the Fall of Jericho to the Fall of the Wall: An Intelligence Primer Based on the Lecture Notes of Professor Arthur S. Hulnick Lectures. Waynesburg, Pennsylvania: Waynesburg University Press, 2022.

[2] Turak, Natasha, and Dan Murphy. "WORLD NEWS America's Allies 'Can't Trust Us' after 'Disaster' Intelligence Leak, Former Intel Officers Say." CNBC, April 14, 2023. https://www.cnbc.com/2023/04/14/pentagon-intelligence-leaks-damage-trust-among-allies-former-intel-personnel-say.html.

[3] Reed, Betsy, ed. "NSA Files: What's a Little Spying between Old Friends?" The Guardian, December 2, 2013. https://www.theguardian.com/world/2013/dec/02/nsa-files-spying-allies-enemies-five-eyes-g8.

[4] Barros, Bryce, and Krystyna Sikora. "China's Sanctions Regime and Lithuania: Policy Responses for European Institutions." Hinrich Foundation | Advancing sustainable global trade, August 16, 2022. https://www.hinrichfoundation.com/research/wp/trade-and-geopolitics/china-sanctions-lithuania-european/.

[5] Clarke, Michael, and Matthew Sussex. "Why 'Strategic Ambiguity' Trumps 'Strategic Clarity' on Taiwan." RUSI, November 24, 2021.

[6] Nawrotkiewicz, Joanna, and Peter Martin. Understanding Chinese "Wolf Warrior Diplomacy." Other. The National Bureau of Asian Research, October 22, 2021.

[7] Higgins, Andrew. "In an Uneven Fight With China, a Tiny Country's Brand Becomes Toxic." The New York Times, February 21, 2022. https://www.nytimes.com/2022/02/21/world/europe/china-lithuania-taiwan-trade.html.

[8] "Translate China-EU - International Trade in Goods Statistics." Eurostat Statistics Explained, February 2024. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=China-EU_-_international_trade_in_goods_statistics.

[9] "Chapter 1 We Have Some Planes." Essay. In 9/11 Commission Report: The Official Report of the 9/11 Commission and Related Publications. Washington, D.C.: U.S. G.P.O., 2004. https://9-11commission.gov/report/.

[10] McPhee, Michele R. Mayhem: Unanswered Questions about the Tsarnaev Brothers, the U.S. Government, and the Boston Marathon Bombing, 2020.

[11] Woodward, John. "Intelligence and Homeland Security." Lecture, 2022.