Prof.dr Baha' Aldeen Raed Suliman Almomani
Universiti Sultan Zainal Abidin - UniSZA/ Faculty of Language and Communication, Kuala Terengganu, Malaysia
Email: Almomanibaha5@gmail.com

Prof.dr Mohd Nazri Bin Latiff Azmi
Universiti Sultan Zainal Abidin - UniSZA/ Faculty of Language and Communication, Kuala Terengganu, Malaysia
Email: mohdnazri@unisza.edu.my

DOI: https://doi.org/10.37458/ssj.6.2.5
Review Paper
Received July 2, 2025
Accepted: November 1, 2025

ESPIONAGE AND SECURITIZATION IN THE AGE OF GLOBAL CONFLICT: INTELLIGENCE, PERCEPTION, AND PEACEBUILDING

Abstract: *This study provides a comprehensive analysis of the evolving role of espionage and intelligence sharing through the lens of securitization theory, with a particular focus on contemporary international conflicts. It demonstrates how espionage, especially in its digital and AI-enabled forms, has become a strategic tool for shaping state behavior, influencing threat perceptions, and guiding international discourse, while historically perceived as secretive and destabilizing. Using qualitative methods, including critical discourse analysis and historical comparative case studies, the study illustrates how intelligence diplomacy—intentional, legally informed, and ethically constrained intelligence sharing—can transform espionage into a stabilizing instrument. Evidence from historical reforms in Greece, contemporary intelligence partnerships such as SIGINT and Five Eyes, and emerging cyber operations supports this argument. The study highlights three key implications: the need for modern legal and normative frameworks to regulate AI and cyber espionage; the potential for trust-based intelligence alliances to function as infrastructures for peace; and the reconceptualization of espionage as a strategic signaling mechanism rather than solely a covert threat. These insights offer practical guidance for pre-conflict planning, international security cooperation, and responsible state conduct in the digital age.*

Keywords: *Espionage, Cyber Intelligence, Securitization theory, Intelligence diplomacy, Peacebuilding.*

Introduction

In the contemporary international arena, espionage has evolved far beyond traditional intelligence gathering, becoming a central instrument in diplomacy, national security, and the management of global conflicts. No longer confined to covert human intelligence operations, modern espionage encompasses cyber intrusions, algorithmic surveillance, and digital information manipulation, blurring conventional boundaries between war and peace (Corbett & Danoy, 2022). States now employ intelligence sharing and strategic warning mechanisms as proactive tools to anticipate threats, prevent attacks, and coordinate diplomatic responses (Grabo, 2002; Corbett & Danoy, 2022). In this digitally contested and fragmented global order, espionage functions as both a shield and a sword—a mechanism for safeguarding national interests while simultaneously influencing international power dynamics.

Historically perceived as destabilizing, espionage today occupies an institutionalized and normalized role in statecraft. By integrating intelligence practices into formalized structures, states can leverage espionage for perception management, risk mitigation, and peacebuilding, transforming covert operations into instruments that support transparency, responsible state behavior, and cooperative security norms. Yet, the rise of AI-enabled cyber espionage presents novel challenges: attribution difficulties, escalatory risks, and a lack of international regulation create conditions where states must navigate high levels of uncertainty while pursuing strategic objectives (Obioha-Val et al., 2025; Pereira & Silva, 2025).

Intelligence sharing emerges as a critical conduit linking situational awareness with proactive conflict prevention. By pooling knowledge across states and alliances, such as SIGINT and Five Eyes, governments can transform raw intelligence into actionable strategies, enhance collective resilience, and promote stability (Herman, 1996). Nevertheless, gaps in international legal frameworks and norms continue to permit exploitation, eroding bilateral trust and constraining the potential of intelligence diplomacy (Dmytrenko, 2024; Pereira & Silva, 2025).

This study examines the dual role of espionage as both a risk and a stabilizing force, demonstrating how intelligence practices can operationalize securitization narratives, influence state behavior, and contribute to peacebuilding strategies. By analyzing historical precedents, contemporary alliances, and cyber-enabled intelligence operations, it highlights the potential for intelligence diplomacy to reconcile strategic imperatives with normative obligations, offering actionable insights for enhancing security, fostering trust, and sustaining global peace in an era of technologically driven conflict.

Statement of Problem

In the contemporary global security environment, intelligence simultaneously functions as a defensive tool and a potential source of risk. The increasing prevalence of hybrid warfare, AI-enabled cyber-espionage, and rapidly shifting geopolitical alignments has created a paradoxical challenge for states: they must safeguard sensitive intelligence collection methods while participating in collaborative intelligence sharing to counter shared threats. This tension is particularly acute in active conflict zones, where the precision, speed, and coordination of intelligence operations can decisively shape both the course of hostilities and opportunities for de-escalation. However, existing structures for intelligence sharing are constrained by fragmented legal frameworks, inconsistent policy guidance, and technological discontinuities. As Corbett and Danoy (2022) highlight, stringent classification regimes—such as the "NOFORN" rule—often prevent or delay the timely dissemination of actionable intelligence, even among allied partners. These structural limitations are compounded by organizational cultures of risk aversion and excessive caution (Zegart, 2013), which frequently override the imperatives of strategic collaboration.

Securitization theory posits that framing an issue as an existential threat legitimizes extraordinary political and legal measures (Buzan, Wæver, & de Wilde, 1998). Yet, for such securitizing moves to maintain credibility, they must be underpinned by accurate, timely, and transparent intelligence. When intelligence flows are obstructed or filtered inconsistently, the legitimacy and persuasive power of securitizing acts are undermined, potentially distorting threat narratives. A pronounced legal and normative gap persists regarding the regulation of peacetime espionage, particularly in cyberspace, which Stritzel (2007) identifies as a key driver of mistrust between state and non-state actors, creating conditions conducive to escalation that impede peacebuilding. While AI and machine learning enhance operational efficiency in intelligence collection, they simultaneously

generate challenges related to attribution, opacity, and interpretive uncertainty, increasing the risk of miscalculation (Obioha-Val et al., 2025; Egloff & Smeets, 2023). Even within well-established intelligence alliances such as SIGINT, AUKUS, and Five Eyes, internal disagreements stemming from divergent legal mandates, conflicting strategic objectives, and technological limitations hinder decision-making and delay responses to emerging threats (Jacobs, 2020; Corbett & Danoy, 2022).

These dynamics highlight that modern espionage is not merely a covert operation but a sophisticated instrument of statecraft, requiring ethical frameworks, legal transparency, and diplomatic foresight. Without a reevaluation of intelligence practices, sharing mechanisms are likely to remain reactive, fragmented, and inadequate in supporting long-term peacebuilding objectives. This study addresses this critical gap by examining how espionage, when strategically integrated, can inform securitization processes, shape national policy, and contribute to conflict prevention and resolution.

Research Question

How does modern espionage contribute to the processes of securitization and conflict resolution in contemporary international conflicts?

Research Objectives

1. To examine how espionage shapes security narratives and informs national policies during global conflicts.
2. To evaluate the role of intelligence operations in either escalating or mitigating conflict.
3. To analyze the ethical, legal, and political consequences of intelligence use in securitization and peace processes.
4. To explore opportunities for intelligence cooperation as a mechanism for de-securitization and peacebuilding.

Contribution to Security Science

This research makes an original contribution to security science by demonstrating how historical intelligence practices and contemporary digital espionage intersect with securitization theory to influence both conflict dynamics and peacebuilding strategies. It highlights practical implications for intelligence agencies, including the integration of AI and cyber capabilities in a legally and ethically informed framework, the role of trust-based

intelligence alliances in supporting stability, and the strategic use of espionage as a tool for signaling and de-escalation. By connecting intelligence studies with peacebuilding, this study offers insights that can inform operational decision-making, policy design, and international cooperation in a digitally complex and politically contested environment.

Literature Review

Espionage as a Strategic Instrument in the Digital Age

In referring back to the Greek experience, the study demonstrates the vital role of perception management and the integration of intelligence into national and international security structures. Greek military history, as demonstrated in works like Kyriakidis (2025), shows a long product timeline of adjustment from irregular militia tactics to professional military techniques and practices. Evidence of how the transformational trajectory to formal military intelligence operations reflects the transition of national securitization discourse and practice as part of twentieth-century reform processes, where threats are constructed, co-constructed, or resisted with meanings defined and acted on based on intelligence apparatuses. Digital espionage, while historically being a central component in intelligence operations during the Cold War, has quickly become a strategic opportunity in international relations. As Devanny et al. (2021) note, states now face some level of uncertainty about what to do when they are publicly revealed as victims of digital espionage at a time when states increasingly venture into cyberspace as an arena for inter-state competition. Digital espionage has become so normalized as a tool of statecraft that states' assertions of normative behavior in cyberspace are often presented in diplomatic platforms, leaving digital espionage as the unaddressed “elephant in the room.”

What sets digital espionage apart from traditional intelligence operations is that it is incorporated into strategic approaches, where intelligence gathering becomes an action not simply of national security, but a willful exercise of power and ultimately shaping power relations and perceptions globally. Digital espionage is also a tactical and psychological means of achieving political intelligence, in that it obtains sensitive state information while exerting stress on the resolve, trust, and vulnerabilities of one’s adversaries. It is also significant in that it is securitizing—creating a situation whereby digital surveillance alone could elicit a defensive or escalatory reaction (Devanny et al., 2021).

The strategic utility of cyber-enabled espionage is rooted in its ambiguity. As Buchanan (2018) notes, cyber operations are often dual-use. The same access to legitimate networks can be used for offensive attacks, such as sabotage or disruption, that rely on the data exfiltration of espionage. This dual-use nature increases strategic ambiguity and leads states to calibrate their responses according to assumptions about the state's intent, capabilities, and possible future threats. The ambiguity creates a dynamic feedback loop where espionage acts not just as a passive tool for acquisition and knowledge of other states, but is an active agency in state behavior that can ultimately exacerbate diplomatic resolution and global stability of cyberspace.

In the past, responses to espionage, such as publicly condemning a state or expelling its diplomats, were established and followed tacit norms based upon state practice. But digital espionage in particular, especially the more public instances of espionage, such as the Snowden leaks (2013), the Office of Personnel Management breach (2015), and the SolarWinds operation (2020), highlights the inadequacies of these older norms in administering cyber-enabled threats (Devanny et al. 2021). Digital espionage and cyber-enabled threats were not just intelligence collection, but the attempt to create strategic signals, psychological pressure, and redefine the landscape of inter-state relations.

When we consider espionage in terms of strategic interaction, it is more than just a secret instrument of monitoring; it can be considered a strategy of state power. Devanny et al. (2021) point out that victim states must evaluate any response in terms of strategic variables such as the longer-term impact on bilateral relations, the perceived intent of adversaries, and their intelligence practices. Responses based on considered and principled responses may provide greater strategic stability (even if paradoxically) rather than destabilizing it, if the parties perceive the use of intelligence operations as being a form of informal diplomacy (or a mechanism to build confidence). Espionage, in this sense, functions as both a risk management tool and a strategic tool: It gives states the ability to manage uncertainty and develop their preferred security environment while also allowing for the potential for escalation if used improperly, and in a manner that does not uphold an established understanding of limitations (Danesy, 2024). This highlights the need for inter-state intelligence diplomacy (similar to cyber diplomacy), which recognizes espionage as a persistent, albeit "dirty" form of power projection and strategic signaling in world politics (Zuboff, 2019).

The advent of espionage is largely preceded by leaps in technology and later in state behavior. From the telegraph to biometric and digital surveillance, technology always plays a role in how intelligence is collected and acted upon (Obioha-Val et al., 2025). Espionage, which used to be reliant on face-to-face exchanges and covert human interactions, now finds itself in an environment where exchanges of information are being gathered, recorded, and dealt with regularly. While Lyon (2022) claims that cell phones and the advancement of innumerable data networks that claim to assist intelligence operations in some ways actually increased the vulnerability of traditional clandestine human exchanges of intelligence (HUMINT). Governments like the U.S., China, and Russia have designed systems of biometric and digital surveillance to track movements of potential foreign agents in transportation hubs, reducing the likelihood that clandestine meetings, formal or informal, occur (Amoore, 2013; Lyon, 2022). Intelligence services have had to reconsider and retool their recruitment and handling strategies to operate in a new world of surveillance and inquiry (Bauman et al., 2014).

Securitization Theory and Espionage

Securitization theory originated from the Copenhagen School (Buzan et al., 1998) and explains how political actors can discursively transform issues of a political nature into issues of existential threat, thereby allowing the state to take de facto extraordinary measures. Furthermore, while the theory has had a significant influence on security studies since its inception, particularly in the early 2000s, on how to unpack the security agenda beyond conventional military threats, ongoing issues regarding its empirical application persist, with scholars believing that these issues vary widely. Stritzel (2007) reported a significant degree of inconsistency between theoretical aspirations in securitization research and its range of actual empirical applications. They pointed out that the gap between the Copenhagen School's securitization model and its empirical utilization was widening (Balzacq, 2011).

The convergence of security and espionage, with the rise of digital tools, has found new salience, as cyber operations increasingly blur the lines of national defense, sovereignty, and legality (Rid, 2020). The theory of securitization, as suggested by the Copenhagen School, posits that security is not just an objective condition; rather, it is a discursive practice whereby political actors securitize issues as existential threats that demand exceptional measures (Buzan et al, 1998). Espionage, as a clandestine act of the

state, has undergone a massive shift in the era of cybersecurity. Obioha-Val et al. (2025) note that cyber espionage constitutes a "new frontier" of cyber warfare, threatening national critical infrastructures while heightening the risk of systemic failure. In this context, it is necessary to rethink espionage as a securitized practice, one frequently framed in the language of existential threat but lacking normative specificity or legal consensus.

Espionage and Peacebuilding

The legality and definition of espionage — especially in peacetime — have attracted scholarly debate because the activities are often ambiguous, as the legality in international law is unclear. Stritzel (2007) notes that the lawfulness of espionage in wartime is clear in international law as it would be subject to law such as the Hague Convention of 1907; however, there is no relevant international treaty covering espionage in peacetime other than the Vienna Convention on Diplomatic Relations (1961) granting immunity to members of a diplomatic mission while performing official tasks. Without the structure of international law, a law that has a certain context, such as military personnel or contractors, for evidence of economic espionage, it could be routinely accepted as espionage in times of peace.

With increasing frequency, cyber espionage has mutated into one of the most important challenges to national and global security, particularly regarding Critical National Infrastructures like the financial markets, defense units, energy grids, and election platforms (Obioha-Val et al., 2025). With the expansion of the digital economy and the convergence of new technologies, espionage has been dramatically reformulated, and actors now seek to engage in espionage outside of normed statecraft, or in cyberspace. Scholars such as Schmitt (2013) and Fjäder (2014) point out that cyber espionage has problematic implications for the conventional interpretation of state responsibility due to its transnational, covert, and anonymized environment. Traditional espionage was firmly situated in the corporeal; agents physically entered enemy territory (Warner, 2014). However, modern-day espionage uses artificial intelligence (AI), drones, and botnets to obtain access and, in some instances, influence democracy (Baker et al, 2023; Liebetrau, 2023). Moreover, this approach does not just affect geopolitical stability; it violates international law and the practice of peacemaking, as attribution is commonly fraught with politics and complexities (Egloff & Smeets, 2023).

Espionage, as a covert source of information, has been part of global political relations and a key component of national defense (Andrew, 2018). Rauch (1982) identifies three major forms of covert intelligence sources as: aerial and space reconnaissance, electronic eavesdropping, and the human agent. Espionage is accepted as an act of belligerency and is legitimate during armed conflict. Yet, the legitimacy of espionage in peacetime is less clear. Rauch (1982) argues that international law is, for the most part, deafeningly silent about peacetime espionage, but that silence may just be tacit acceptance due to its long tradition among states and its role in keeping a balance and right to self-defense.

More recent investigations turn the focus of investigation toward internal threat. Danesy (2024) considers insider espionage as a destabilizing threat to governments, economies, and public confidence, and makes the argument that deterrence and detection are no longer enough. He frames the Five-Factor Model as a model of the insider threat risk factor, which is based on years of research across sectors. His Five-Factor model offers a predictive risk model to identify internal risk and assist in mitigation - a required risk evolution to the precarious balance between state secrecy and societal transparency in today's digital world. At the same time, Dmytrenko (2024) stresses the need for comprehensive legal and strategic frameworks to address changing espionage strategies. In his comparative study of the global legal systems, he points out how many countries, particularly those with older or under-resourced institutions, cannot combat the espionage threats they face. He views espionage not only as a national security concern but a real challenge for peacebuilding, especially where states are fragile and public trust is tenuous.

Intelligence Sharing and State Security

During the Cold War, strategic warning intelligence developed as a way to counter the fear of surprise attacks from the Soviet Union (Grabo, 2002). Over time, this idea grew into detecting the plans and abilities of adversaries, which has become vital in today’s world of cyber threats. The Copenhagen School’s securitization theory helps explain how intelligence shifts potential risks into important political focus areas (Buzan et al. 1998). Alliances like FVEY show that shared histories and mutual values make exchanging intelligence information stronger (Corbett & Danoy, 2022). AUKUS strengthens Indo-Pacific security by combining defense tech and signals intelligence (Australian Government

2022). The European SIGINT group proves that even connected partnerships can succeed in cryptanalysis and interception through shared trust and skills (Jacobs 2020).

Sharing intelligence takes on two major roles in making something a security issue. It makes threats seem bigger and justifies extreme policies, but it also helps to ease tensions by building shared understanding. Barriers like scattered authority, tricky legal rules, and tech that doesn't work together often slow the flow of critical information (Corbett & Danoy, 2022). Human concerns, like being cautious or afraid of legal trouble, add more challenges to teamwork (Herman 1996; Zegart 2009). Although artificial intelligence could improve how data is analyzed and warnings are flagged, it struggles with classified data, making human judgment and trust between agencies vital (Corbett & Danoy, 2022). To make intelligence sharing effective, we need to link technology well, align narratives, and show boldness at the institutional level.

Methodology

This study used a qualitative research approach based on analytical dimensions and investigates how intelligence sharing and espionage serve as weapons of securitization, strategic communication, and maybe conflict resolution in modern global disputes. The methodological strategy reveals the study's main interest in knowing how governments employ intelligence—especially in its digital and AI-enabled forms—not just to justify unusual measures but also to influence security narratives and de-escalation plans. Emphasizing the dynamic and discursive character of intelligence activities inside changing geopolitical settings, the approach is therefore interpretive as well as explanatory. Using mostly critical discourse analysis (CDA) and historical-comparative case study analysis, the study investigates the function of espionage and intelligence diplomacy in contemporary conflict zones. Using the analytical lens that securitization theory, as expanded by Buzan, Wæver, and de Wilde (1998), offers, whereby the study evaluates how threat narratives are constructed and legitimized using language, symbols, and planned communication. Simultaneously, the study examines three major domains historically-comparatively: the contemporary intelligence-sharing dynamics; the evolution and function of the Five Eyes and SIGINT coalitions; and the modernization of Greek intelligence during times of geopolitical conflict. The historical case of Greece is investigated to show how early forms of intelligence securitization and national resilience were made possible by state capacity, reform, and pedagogy in intelligence operations. The examination of Five Eyes and SIGINT

alliances reveals insights into long-lasting models of trust-based intelligence cooperation, therefore providing institutional proof for how ordered alliances can change to support peace-oriented initiatives. The comparative emphasis permits a contextual assessment of how modern events include the operationalization of espionage and intelligence sharing as tools of conflict containment, diplomatic signaling, and narrative war. This multi-method approach improves the depth and dependability of results by allowing data triangulation across historical, discursive, and institutional facets. By guaranteeing that all publicly available intelligence materials are properly handled and that sensitive content is understood in its relevant geographic and historical context, the study upholds moral strictness. The study aims to provide empirical insights and theoretical innovation to the sectors of intelligence studies, international security, and peacemaking via this integrated methodological framework.

Discussion

Espionage as Securitizing Practice

This study demonstrates that Greece's historical evolution of intelligence and military structures offers a valuable model for understanding how states can use espionage as an instrument of strategic resilience. By examining the development of military academies and the professionalization of intelligence in Greece, it becomes evident that the integration of intelligence education into national defense was not merely administrative but constitutive of the state's ability to anticipate and manage complex security challenges (Kyriakidis, 2025). These historically grounded practices reveal how espionage functions as a proactive mechanism in shaping perceptions, informing policy, and guiding state responses to both domestic and international pressures (Karyotis, 2012). This approach advances security science by demonstrating that intelligence activities are not neutral tools for information collection but active components in the construction of strategic narratives, deterrence strategies, and adaptive security planning (Stritzel, 2007; Rid, 2020). The transition from traditional espionage to digital and AI-enabled intelligence illustrates how statecraft has been transformed into a securitizing activity that directly influences inter-state competition (Valeriano & Maness, 2015). Contemporary digital espionage combines human judgment with algorithmic processes to produce actionable intelligence, shaping political and operational decision-making under conditions of uncertainty (Devanny et al., 2021). High-profile cases such as the Snowden leaks (2013), the OPM breach (2015), and

SolarWinds (2020) reveal both the strategic potential of cyber-enabled intelligence and the regulatory void that amplifies risk. Unlike conventional espionage, digital operations exert immediate, performative pressures on states, generating political incentives for rapid retaliation while simultaneously challenging traditional norms of attribution, proportionality, and accountability. This dual-use nature of cyber espionage complicates the management of state relationships and illustrates the intersection between intelligence practice, securitization theory, and peacebuilding considerations. Furthermore, the hybridization of espionage practices—combining human networks with digital surveillance and machine learning—demonstrates the evolution of intelligence into a proactive, anticipatory process (Buchanan, 2020; Aldrich, 2010). Recruitment and asset management are no longer purely interpersonal but are informed by digital profiling, metadata analysis, and predictive algorithms, enhancing precision while maintaining the human dimension of intelligence work. By positioning espionage as an integrated element of strategic signaling, states can shape perceptions, reduce uncertainty, and enhance trust in intelligence-sharing partnerships. This synthesis of historical insights, technological innovation, and theoretical framing contributes to security science by offering a model for operationalizing intelligence diplomacy, guiding cyber-norm development, and informing strategies for conflict prevention and peacebuilding in the contemporary era.

Covert Securitization: The Role of Intelligence in Framing Threats and Justifying Conflict Escalation and Peacebuilding

Recent scholarship highlights a persistent tension between the conceptual clarity of securitization theory and its practical operationalization. Stritzel (2007) argues that this gap arises from two sources: inherent limitations of the theory and methodological limitations of researchers. The Copenhagen School's requirement for "strong" empirical evidence, along with the multi-layered progression from non-politicization to securitization, creates obstacles for empirical work. Scholars often fail to demonstrate all necessary conditions of securitization when applying the framework, leading to partial or inconsistent applications (Stritzel, 2007). These challenges underscore a broader issue in international relations research, where complex phenomena such as espionage, intelligence politics, and conflict narratives present empirical and conceptual difficulties that complicate the development of critical security frameworks (Buchanan, 2020).

Framing espionage as a securitizing practice provides a lens to examine its public, legal, and strategic dimensions in the era of AI. Obioha-Val et al. (2025) emphasize that AI-enabled espionage accelerates covert monitoring, data extraction, and system intrusion to an unprecedented scale. These developments mirror classic processes of securitization, in which states construct narratives of existential threat to justify extraordinary technological and legislative powers. Yet, Stritzel (2007) notes, securitization remains conceptually vague, particularly when addressing unpredictable, diffuse vulnerabilities. Attribution in cyberspace is inherently challenging, while changes to cross-border jurisdiction complicate the legitimacy of securitized acts (Hansen & Nissenbaum, 2009; Deibert, 2013). Digital architectures used for surveillance or security operations may simultaneously erode claims of democratic accountability and politicize securitization narratives among online communities (Monsees, 2019). Therefore, cyber espionage functions not only as a technical instrument but as a performative act of securitization, with broad normative and political implications (Buchanan, 2020). Espionage in peacetime presents multifaceted challenges across legal, strategic, and ethical domains. Stritzel (2007) suggests that peacetime espionage—particularly targeting non-diplomatic actors—operates under tacit acceptance, as no formal treaties prohibit it. However, this tacit acceptance undermines trust in peacebuilding, where legal transparency and respect for sovereignty are foundational. Industrial espionage, as described by Nasheri (2005), demonstrates organized and clandestine intelligence-gathering that violates legal and ethical norms, contrasting with competitive intelligence, which relies on legal methods. The state frames espionage as a national security activity, while private actors use civil, commercial, or corporate justification, producing divergent interpretations of acceptable risk and loss (Walsh, 2010).

The interplay of state and commercial espionage further complicates peacebuilding. State-sponsored espionage, when seen as competition rather than hostile interference, can still undermine trust and affect the efficacy of peacebuilding initiatives (Walsh, 2010; Borghard & Lonergan, 2017). Understanding the classification, operational methods, and legal status of various espionage activities is critical for developing international norms and enhancing cooperative legal frameworks (Dmytrenko, 2024).

Cyber espionage intensifies these challenges, eroding inter-state trust and destabilizing civilian infrastructure essential for post-conflict recovery (Rosli, 2025). AI technologies amplify the scale and precision of cyber operations, allowing state and non-

state actors to execute intelligence activities without physical presence (Obioha-Val et al., 2025). The covert and technologically mediated nature of espionage complicates diplomatic engagement, attribution, and accountability. Moreover, cyber-enabled espionage blurs the distinction between war and peacetime operations, raising ethical dilemmas for sustainable peace (Schmitt, 2013; Byman, 2023).

Historically, espionage and peacebuilding have been conceptualized as opposites: espionage is covert and adversarial, while peacebuilding is cooperative and restorative. Yet espionage can paradoxically support peace by maintaining strategic awareness and preventing surprise attacks (Rauch, 1982). At the same time, espionage may erode trust, a core component of peacebuilding, particularly through insider threats that compromise operational security and institutional integrity (Danesy, 2024). Predictive models for insider threat management illustrate that intelligence activities can proactively strengthen resilience and preserve social trust, functioning as a peacebuilding mechanism in their own right. Comparative legal analyses also show that states with adaptable legal frameworks are better positioned to mitigate espionage-related crises, whereas legal deficiencies can transform espionage into a destabilizing force that hinders negotiations and fosters distrust (Dmytrenko, 2024). Consequently, the modernization of espionage countermeasures serves both national defense and long-term peacebuilding objectives.

Findings

This study reveals that Greece's adaptation of naval and intelligence structures was central to navigating both external threats and internal fragmentation. The professionalization of espionage and counter-espionage allowed the state to respond with agility to regional pressures. Moreover, the fusion of military and intelligence pedagogy anticipates modern securitization practices, illustrating how education, intelligence, and statecraft coalesce to reinforce national resilience. These findings highlight the strategic utility of historically grounded intelligence systems for perception management, institutional stability, and peacebuilding.

In contemporary digital contexts, espionage has been fully normalized as a tool of statecraft, yet its operational instability reflects the complex intersection of intelligence, signaling, and state behavior. States struggle to manage cyber espionage in part because no universal norms define acceptable conduct, and public disclosures often provoke politically driven responses rather than rational strategic decision-making. When approached with

accountability, digital espionage can stabilize inter-state relations by clarifying intentions, strengthening trust, and enabling strategic signaling, demonstrating the dual function of intelligence diplomacy alongside conventional cybersecurity.

Despite the proliferation of digital technologies, espionage remains fundamentally human. Human judgment, endurance, and operational creativity remain irreplaceable, particularly in high-security environments such as tightly controlled nuclear facilities. Hybrid intelligence operations now blend physical access with digital capabilities, requiring operatives to master both fieldcraft and cyber literacy, including ethics, cybersecurity, and digital awareness. Modern intelligence entities thus operate as hybrid human-technical systems, integrating real-time cyber and physical operations. Applying securitization theory to espionage illuminates how states frame threats, but practical application is often limited by secrecy. Nonetheless, when cyber espionage is treated as an existential security threat, securitization processes reveal how states construct consensus and legitimize extraordinary measures. Three outcomes are notable: (1) cyber espionage has transitioned from secondary intelligence activity to central threat narrative, driving cyberspace securitization; (2) AI-enhanced espionage amplifies operational effectiveness and uncertainty, escalating state responses; (3) the absence of comprehensive legal frameworks underscores the gap between securitization discourse and enforceable international norms (Obioha-Val et al., 2025).

Legal and ethical considerations further clarify espionage's operational landscape. Legitimacy is contingent on both the actor and the target, with industrial, economic, and corporate espionage presenting systemic risks, sophisticated tools, and potential for irreparable harm. Establishing clear legal definitions and accountability frameworks is essential for fostering trust, transparency, and global peace (Pereira & Silva, 2025). Cyber espionage now poses major implications for sovereignty, critical infrastructure, and conflict escalation, revealing how digital operations are intertwined with modern strategic environments (Harknett & Smeets, 2022; Egloff & Smeets, 2023).

Integrating espionage with peacebuilding theory generates three critical insights. First, intelligence operations can act as implicit mechanisms of conflict prevention by monitoring threats and reducing the likelihood of escalation (Rauch, 1982). Second, effective management of insider threats requires predictive and proactive processes that safeguard institutional integrity and public trust (Danesy, 2024). Third, counter-espionage efficacy is closely linked to the robustness of legal and economic infrastructure, directly

influencing states' capacity to maintain peace amid evolving security challenges (Dmytrenko, 2024).

The study identifies actionable principles for improving intelligence sharing in global conflicts: cultivating trust, harmonizing legal frameworks, integrating technology, decentralizing authority while maintaining coordination, prioritizing training and leadership engagement, and implementing adaptive classification and sharing mechanisms (Jacobs, 2020). Historical and contemporary examples—including post-9/11 intelligence surges and operations in Ukraine—demonstrate that flexible intelligence alliances can both mitigate threats and enhance diplomatic outcomes (Corbett & Danoy, 2022; Jacobs, 2020).

This study makes several important contributions to security science by demonstrating the enduring strategic relevance of historically informed intelligence practices, showing how past adaptations continue to shape modern national resilience. It also advances understanding of cyber espionage within the securitization framework, revealing operational, technological, and legal gaps that influence state behavior and threat narratives. Furthermore, the study bridges intelligence studies and peacebuilding by illustrating how proactive, accountable espionage practices and effective intelligence sharing can prevent escalation, build trust, and support diplomatic engagement. Overall, the findings position espionage as both a potential risk and a stabilizing instrument, integrating historical, technological, and theoretical insights to inform contemporary intelligence practice, securitization strategies, and efforts to strengthen international peace and security.

Conclusion

This study demonstrates that espionage—both traditional and digitally enabled—functions as a complex, adaptive instrument in contemporary security environments, with implications that extend beyond information collection into strategic signaling, statecraft, and peacebuilding. Historical evidence, exemplified by Greece's military reforms and intelligence professionalization, illustrates how structurally organized intelligence practices can enhance national resilience, strengthen perception management, and shape strategic responses to both domestic and regional pressures. These cases underscore the enduring value of historically informed intelligence for modern security planning and highlight the importance of embedding intelligence within professional military and educational structures. The analysis further reveals that digital espionage, amplified by AI and cyber capabilities, has transformed the operational and ethical landscape of state intelligence.

States increasingly rely on cyber-enabled operations to manage uncertainty, assert influence, and securitize threats, yet the absence of clear international norms complicates accountability and risk management. This study emphasizes that intelligence diplomacy—an ethically guided, legally informed, and strategically deliberate approach to espionage and information sharing—can mitigate destabilizing effects, transform covert operations into tools of strategic stability, and foster cooperative frameworks for peacebuilding. From a theoretical standpoint, the findings advance securitization theory by demonstrating how intelligence activities operationalize threat narratives and legitimize extraordinary state actions in both traditional and digital arenas. Espionage emerges not merely as an ancillary or reactive function but as a performative, anticipatory, and normative instrument capable of influencing state behavior, managing risk, and reinforcing trust among actors. Cyber espionage, in particular, illustrates the duality of opportunity and risk: while it enhances monitoring and situational awareness, it also creates potential for misperception, escalation, and erosion of trust, necessitating legally and ethically accountable intelligence practices.

Finally, this study bridges the study of intelligence and peacebuilding, showing that espionage, when governed by transparency, accountability, and strategic foresight, can support conflict prevention and stability. Trust-based intelligence sharing, proactive counterintelligence measures, and robust legal frameworks can transform covert activities from sources of instability into mechanisms that preserve social cohesion, reinforce institutional integrity, and facilitate diplomacy. By integrating historical precedents, contemporary technological developments, and theoretical insights, this study positions espionage as both a risk and a stabilizing instrument, offering actionable guidance for intelligence practitioners, policymakers, and scholars seeking to navigate the evolving challenges of national and international security.

References

1. Aldrich, R. J. (2010). *GCHQ: the uncensored story of Britain's most secret intelligence agency*. http://ci.nii.ac.jp/ncid/BB09497532
2. Amoore, L. (2013). *The politics of possibility: Risk and security beyond probability*. Duke University Press.
3. Andrew, C. (2018). *The secret world: A history of intelligence*. Yale University Press.
4. Australian Government. (2022). *AUKUS: Partnership for the Indo-Pacific*. https://www.defence.gov.au
5. Baker, M. S., Baker, J., & Burkle, F. M., Jr. (2023). Russia's hybrid warfare in Ukraine threatens both healthcare & health protections provided by international law. *Annals of Global Health, 89*(1), 1–6.
6. Balzacq, T. (2011). *Securitization theory: How security problems emerge and dissolve*. Routledge.
7. Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology, 8*(2), 121–144. https://doi.org/10.1111/ips.12048
8. Borghard, E. D., & Lonergan, S. (2017). The logic of coercion in cyberspace. *Security Studies, 26*(3), 452–481. https://doi.org/10.1080/09636412.2017.1306396
9. Buchanan, B. (2018). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.
10. Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.
11. Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.
12. Byman, D. (2023). How to think about state sponsorship of terrorism. *Survival, 65*(4), 101–121.
13. Corbett, S., & Danoy, J. (2022, October 31). *Beyond NOFORN: Solutions for increased intelligence sharing among allies* (Issue Brief). Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/
14. Danesy, F. (2024). *Predicting insider espionage: A five-factor model*. Peter Lang. https://doi.org/10.3726/b22175
15. Deibert, R. (2013). *Black code: Surveillance, privacy, and the dark side of the internet*. Signal Books.
16. Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy, 6*(1), 1–22. https://doi.org/10.1080/23738871.2021.2000628
17. Dmytrenko, S. (2024). Espionage counteraction as national security paradigm of 21st century. *FOREIGN AFFAIRS*, 57–62. https://doi.org/10.46493/2663-2675.34(1).2024.57

18. Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: A framework. *Journal of Strategic Studies, 46*(3), 502–533. https://doi.org/10.1080/01402390.2021.1895117
19. Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalisation. *Resilience, 2*(2), 114–129. https://doi.org/10.1080/21693293.2014.914771
20. Grabo, C. (2002). *Anticipating surprise: Analysis for strategic warning*. University Press of America.
21. Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x
22. Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies, 45*(4), 534–567. https://doi.org/10.1080/01402390.2020.1732354
23. Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press.
24. 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
25. Karyotis, G. (2012). Securitization of migration in Greece: Process, motives, and implications. *International Political Sociology, 6*(4), 390–408.
26. Kyriakidis, M. (2025). Military education and professionalization in modern Greece: The Evelpidon Military Academy and the impact of foreign military doctrines (1828–20th century). *ISRG Journal of Arts Humanities & Social Sciences (ISRGJAHSS), 3*(1), 253–264. https://doi.org/10.5281/zenodo.14738407
27. Liebetrau, T. (2023). Organizing cyber capability across military and intelligence entities: Collaboration, separation, or centralization. *Policy Design and Practice, 6*(2), 131–145. https://doi.org/10.1080/25741292.2022.2127551
28. Lyon, D. (2022). *Pandemic surveillance: Privacy, security and public trust*. Polity Press.
29. Monsees, L. (2019). *Crypto-Politics*. https://doi.org/10.4324/9780429456756
30. Nasheri, H. (2005). *Economic espionage and industrial spying*. Cambridge University Press.
31. Obioha-Val, O., Olaniyi, O., Gbadebo, M., Balogun, A., & Olisa, A. (2025). Cyber espionage in the age of artificial intelligence: A comparative study of state-sponsored campaign. *Asian Journal of Research in Computer Science, 18*(1), 184–204. https://doi.org/10.9734/ajrcos/2025/v18i1557
32. Pereira, A., & Silva, C. (2025). The legality of international espionage based on the nature of the target and the perpetrator. *Expeditions with MCUP*. https://doi.org/10.36304/ExpwMCUP.2025.06
33. Rauch, E. (1982). Espionage. In *Encyclopedia of Public International Law*. Elsevier. https://doi.org/10.1016/B978-0-444-86234-1.50064-3

34. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
35. Rosli, W. R. W. (2025). Waging warfare against states: The deployment of artificial intelligence in cyber espionage. *AI and Ethics, 5*(1), 47–53. https://doi.org/10.1007/s43681-024-00628-x
36. Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.
37. Stritzel, H. (2007). Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations, 13*(3), 357–383. https://doi.org/10.1177/1354066107080128
38. Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.
39. Walsh, J. I. (2010). *The international politics of intelligence sharing*. Columbia University Press.
40. Warner, M. (2014). *The rise and fall of intelligence: An international security history*. Georgetown University Press.
41. Zegart, A. (2009). *Spying blind: The CIA and the origins of 9/11*. Princeton University Press.
42. Zegart, A. B. (2013). *Eyes on spies: Congress and the United States Intelligence Community*. Hoover Press.
43. Zuboff, S. (2019). *The age of surveillance capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019*. Profile Books.