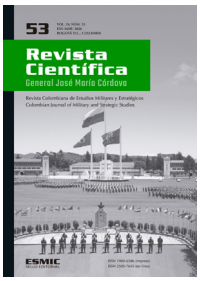

Revista Científica General José María Córdova
Colombian Journal of Military and Strategic Studies)

Bogotá D.C., Colombia
ISSN 1900-6586 (print), 2500-7645 (on line)
https://doi.org/10.21830/19006586.1485

RESEARCH ARTICLE

Intelligence Failures: An Exploration of Key Theories

Fallos de inteligencia: una exploración de teorías clave

Luigi Martino
University of Bologna, Italy
luigi.martino3@unibo.it

Claudio Paya-Santos
Valencia International University, Spain
claudio.paya@professor.universidadviu.com

How to cite in APA: Martino, L. & Paya-Santos, C. (2026). Intelligence Failures: An Exploration of Key Theories. *Revista Científica General José María Córdova, 24*(53), 105-132. https://doi.org/10.21830/19006586.1485

Published online: January 26, 2026

Revista Científica General José María Córdova
Colombian Journal of Military and Strategic Studies

Bogotá D.C., Colombia
Volume 24, Issue 53, January-March 2026, pp. 105-132
https://doi.org/10.21830/19006586.1485

RESEARCH ARTICLE

Intelligence Failures: An Exploration of Key Theories

Fallos de inteligencia: una exploración de teorías clave

Luigi Martino
University of Bologna, Italy
Claudio Paya-Santos
Valencia International University, Spain

ABSTRACT. This paper examines the organizational and structural factors that contribute to intelligence failures, with particular emphasis on institutional coordination challenges. Recent events, including the October 7 attacks in Israel and the 2022 Russian invasion of Ukraine, illustrate persistent vulnerabilities in early warning systems and inter-agency collaboration. The analysis reveals that contemporary intelligence failures stem not from information scarcity but from problems of signal-noise discrimination, institutional fragmentation, and the politicization of intelligence processes. The expanding scope of national security, encompassing cybersecurity, economic stability, public health, and climate risks, demands enhanced coordination across agencies, disciplines, and international partners. Drawing on foundational intelligence studies and recent case analyses, the research demonstrates how open-source intelligence integration, cognitive biases, and bureaucratic dysfunctions systematically undermine effective threat anticipation and strategic warning capabilities.

Keywords: cybersecurity; hybrid warfare; intelligence activities; intelligence failures; national security

RESUMEN. Este artículo examina los factores organizativos y estructurales que contribuyen a las fallas de inteligencia, con especial énfasis en los desafíos de coordinación institucional. Eventos recientes, como los atentados del 7 de octubre en Israel y la invasión rusa de Ucrania en 2022, ilustran vulnerabilidades persistentes en los sistemas de alerta temprana y la colaboración interinstitucional. El análisis revela que las fallas de inteligencia contemporáneas no se derivan de la escasez de información, sino de problemas de discriminación señal-ruido, fragmentación institucional y politización de los procesos de inteligencia. El alcance cada vez mayor de la seguridad nacional, que abarca la ciberseguridad, la estabilidad económica, la salud pública y los riesgos climáticos, exige una mayor coordinación entre agencias, disciplinas y socios internacionales. Basándose en estudios fundamentales de inteligencia y análisis de casos recientes, la investigación demuestra cómo la integración de inteligencia de código abierto, los sesgos cognitivos y las disfunciones burocráticas socavan sistemáticamente la anticipación efectiva de amenazas y las capacidades de alerta estratégica.

Palabras clave: actividades de inteligencia; ciberseguridad; fallos de inteligencia; guerra híbrida; seguridad nacional

Received: April 2, 2025 • **Accepted:** January 16, 2026

Contact: Claudio Paya-Santos ✉ claudio.paya@professor.universidadviu.com

Introduction and Key Concepts

National security now emphasizes safeguarding populations and critical infrastructure against increasingly interconnected challenges, from global pandemics to hybrid warfare tactics (Mazurier & Payá-Santos, 2018). In democratic states, the focus has shifted toward protecting individuals and their rights, recognizing vulnerabilities at the state and community levels (Luque-Juárez et al., 2023). Recent threats, such as cyberattacks targeting essential services or the impacts of economic crises, highlight how deeply national security is intertwined with global systems and individual well-being (Dobák, 2021; Kaldor, 2007; Neri et al., 2023).

The role of intelligence in safeguarding national security has undergone a profound transformation, shaped by the complexity and interdependence of the modern world. Today, intelligence is not only an organizational function but also a strategic tool for analysis, forecasting, and risk mitigation. Its scope has widened considerably in recent decades, driven by two key factors: the digital revolution, which has exponentially increased the volume and speed of available information, and the compression of decision-making timeframes in crisis and policy contexts.

As intelligence agencies are now expected to address multiple, concurrent threats—ranging from terrorism and cyberattacks to disinformation and economic coercion—they must strike a delicate balance between the speed and depth of analysis. This tension became evident in the aftermath of the 9/11 attacks. In response, the United States implemented the Intelligence Reform and Terrorism Prevention Act of 2004, which sought to correct systemic coordination failures among agencies, enhance information sharing, and improve analytic capabilities. While this example pertains specifically to the US, it illustrates a broader international trend: the growing recognition that intelligence services must evolve structurally and cognitively to keep pace with the speed and complexity of current global risks.

However, a persistent challenge remains: obtaining the correct information at the right time and interpreting it correctly. As Roberta Wohlstetter observed in her analysis of Pearl Harbor, intelligence failures often result not from a lack of data but from the inability to distinguish signal from noise, that is, to filter and prioritize relevant indicators within an abundance of low-quality or distracting inputs (Wohlstetter, 1962).

This dilemma is magnified in the digital age. Intelligence now increasingly depends on open-source intelligence (OSINT), a trend supported by the rising allocation of resources and training within Western intelligence communities to exploit open data. According to NATO and EU intelligence reports, up to 80–90% of actionable intelligence originates from open sources, including news media, social networks, satellite imagery, and commercial databases (NATO Strategic Communications Centre of Excellence, 2023). While this abundance offers new opportunities, it also introduces analytical overload, making it harder to isolate meaningful patterns, trends, and causal relationships.

Thus, the core of modern intelligence work lies not merely in information collection but in the processing, synthesis, and contextual interpretation of data to produce timely, actionable, and relevant insights for decision-makers. This expands the traditional boundaries of intelligence, which still include espionage and counterintelligence operations, but now also encompass complex domains such as economic influence, geopolitical risk, and technological competition (Payá-Santos & Luque-Juárez, 2021; Payá-Santos, 2023). Intelligence must adapt its methods accordingly, moving from secrecy-centric paradigms to knowledge-centric ecosystems, if it is to remain effective in anticipating and shaping strategic realities.

Through the analysis of specialized literature—such as the foundational works of Sherman Kent (1949), Michael Warner (2002), and Jennifer Sims (1995), intelligence is broadly understood as a set of systematic and coordinated processes by which information is collected, analyzed, and disseminated to support the protection of national interests and the anticipation of threats. Rather than equating intelligence with raw data or generic news content, its core lies in transforming information into actionable knowledge through critical interpretation, contextualization, and strategic relevance.

In this framework, the concept of "information" is not passive or neutral. It is structured, evaluated, and prioritized to serve as a basis for situational understanding. Intelligence, then, is meant to enhance the decision-maker's capacity to discern emerging risks and potential opportunities. This function distinguishes it from other forms of information, such as journalistic reporting, academic analysis, or bureaucratic reporting. Authors like Kent (1949) and Lowenthal (2017) emphasize that intelligence must bridge the gap between information abundance and policy relevance.

Nonetheless, it is important to recognize, especially in the context of open-source dominance, that intelligence is not the only source of strategic information. In situations such as global economic crises, public health emergencies, or climate-related risks, decision-makers are increasingly supported by a constellation of expert systems: economic forecasting agencies, scientific advisory panels, think tanks, intergovernmental bodies, and, significantly, open-source intelligence platforms. Indeed, modern intelligence must coexist with and complement these alternative sources, integrating open-source intelligence (OSINT) with classified material to provide a holistic, comparative advantage in decision-making.

The role of intelligence is not to monopolize information, but to ensure coherence, reliability, and strategic alignment in the flow of insights that reach the upper echelons of decision-making. This process operates within what is commonly referred to as the "intelligence cycle"—a dynamic sequence of planning, collection, processing, analysis, and dissemination, subject to continuous feedback from both producers and consumers of intelligence.

As shown in Figure 1, this cycle is not linear but adaptive, shaped by external policy priorities and internal reassessments of threats and vulnerabilities over time. Ultimately, intelligence provides a structured perspective within the broader ecosystem of knowledge

production, offering anticipatory, decision-oriented analysis that enhances the quality and timing of strategic choices.

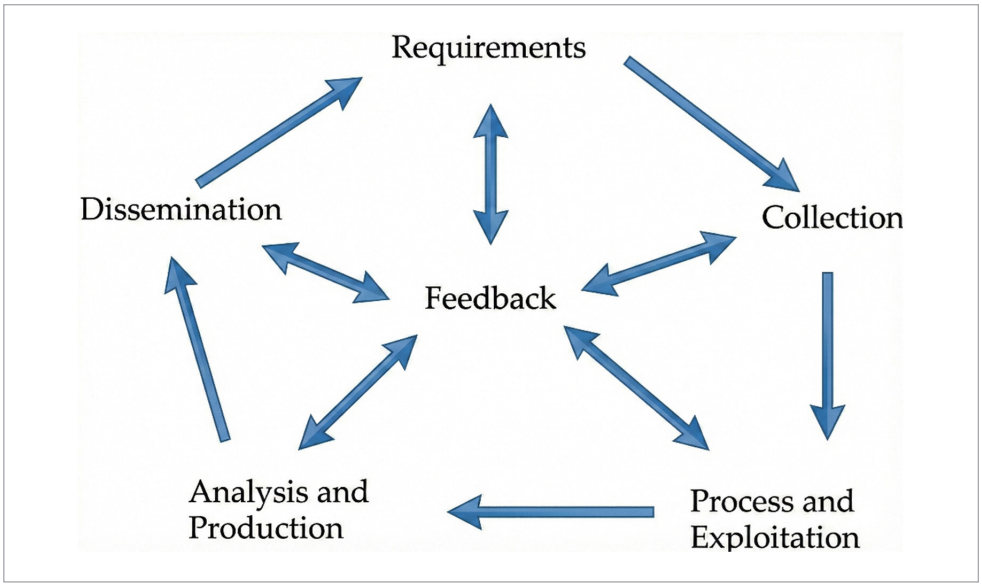

Figure1. Intelligence cycle
Source: own elaboration

However, this cycle can sometimes fail to yield the desired outcomes, resulting in genuine failures (Barnea, 2020). Disruptions in decision-making can arise from errors or deficiencies by analysts or political leaders, as well as dysfunctional dynamics between intelligence agencies and decision-makers. Despite extensive examination by researchers and industry professionals, no universally accepted definition of intelligence failure remains in the literature. Mark Lowenthal, a former CIA official, describes an intelligence failure as the inability of agencies to deliver accurate and timely information or analysis regarding a matter of national importance (Lowenthal, 1985).

Conversely, Abram Shulsky and Gary Schmitt characterize it as a fundamental misunderstanding of a situation that compels a government or its military to undertake actions misaligned with its interests (Shulsky & Schmitt, 2002). By analyzing these definitions, three primary views on intelligence failures emerge: the first posits that a failure is confirmed only when intelligence agencies err; the second argues the opposite, suggesting that a failure occurs solely when the decision-maker is at fault; the third perspective, which we believe is the most comprehensive, acknowledges that a failure can stem either from the intelligence services' inability to produce necessary information for decision-makers or the decision-makers failure to act correctly on the information they receive.

Specifically, the issue lies not only in the fact that each intelligence service in question was unable to predict these events, but also in their complete unexpectedness. This failure hindered intelligence agencies from fulfilling their vital role: influencing the future to avert serious outcomes based on available information. While hindsight might suggest that these events were preventable, it is clear that intelligence systems had access to warning signs beforehand. However, they either failed to act on them or ignored their warnings, leaving decision-makers unprepared.

The primary advocate for the third perspective is Erik J. Dahl (2013), who challenges the conventional view that intelligence failures occur when critical warnings are overlooked amid noise. In contrast, Mark M. Lowenthal's definition aligns more closely with the first perspective. He discusses this in "The Burdensome Concept of Failure," where he examines the complexities of defining intelligence failure. For a comprehensive understanding of intelligence failure, refer to Gustavo Díaz Matey's "Methodological Approaches to the Concept of Intelligence Failure" (2005), which offers an in-depth analysis. Additionally, Richard J. Aldrich's (2000) provides valuable insights into the historical context of intelligence failures.

Drawing insights from the latest literature on the issues affecting the relationship between decision-makers and intelligence, along with empirical evidence from multiple case studies, including the January 6 United States Capitol Attack, as well as the October 7 Hamas Attacks on Israel, the following paragraph will briefly outline the key theories on intelligence failures.

Explanatory Frameworks for the Failure of Intelligence Services

Since the publication of Roberta Wohlstetter's seminal Pearl Harbor: Warning and Decision (1962), the study of intelligence failures has become a crucial subfield within intelligence studies. While her work laid the groundwork by examining how key warnings were lost in the "noise" of abundant information, subsequent literature has expanded considerably, particularly through the contributions of scholars like Betts, Jervis, and more recently, Díaz Matey (2005), who has systematized key concepts such as capability, intention, and strategic deception—not simply as abstract ideas, but as operational variables that affect the structure and effectiveness of intelligence processes.

However, it is important to note that much of the canonical literature reflects a predominantly U.S.-centric perspective, focusing on high-profile failures within American intelligence history. This narrative, while valuable, can be enriched by incorporating non-Western and comparative case studies that highlight how structural, cultural, and political factors affect intelligence outcomes in other contexts. For example, Israel's surprise in the 1973 Yom Kippur War, India's lack of anticipation of the Kargil conflict in 1999, or the Argentine miscalculations prior to the Falklands War all demonstrate the global nature of strategic surprise and the diverse institutional responses to early warning breakdowns.

During the Cold War, the primary concern was detecting imminent conventional or nuclear attacks, which led to the institutionalization of early warning methodologies. Among these, the Indications and Warning (I&W) model emerged as a structured analytical framework for identifying precrisis anomalies and behavioral patterns of potential aggressors. This model did not aim solely to forecast attacks, but to minimize decision-making delays, enhance readiness, and reduce false negatives through a more formalized system of alerting (Delgado-Morán et al., 2019a).

From the 1980s onward, the scope of "strategic surprise" has expanded well beyond the military domain. Events such as the Iranian Revolution (1979) or the collapse of the Soviet Union (1991) caught many intelligence services off guard—not necessarily because of a lack of data, but because of institutional biases, cognitive rigidity, or politicized environments that dulled analytic foresight. It is precisely in this period that comparative intelligence studies begin to gain traction, analyzing structural weaknesses in intelligence organizations across multiple national contexts.

After the attacks of September 11, 2001, academic and operational focus shifted toward the analysis of failures in counterterrorism, with new emphasis placed on interagency coordination, information sharing, and the dangers of intelligence silos. These discussions have catalyzed reforms in numerous countries and have fed a body of literature that critiques the over-reliance on technical collection over human intelligence (HUMINT), the lack of cultural expertise, and the operational limits of predictive analysis.

In reviewing this body of work, three broad explanations tend to dominate scholarly and practitioner discussions of intelligence failure. First, organizational or structural flaws: including bureaucratic inertia, poor interagency communication, and fragmented responsibilities. Second, cognitive and psychological biases, such as mirror imaging, confirmation bias, or groupthink, distort threat perception. Third, political interference or pressure: when intelligence is shaped or filtered to align with the policy preferences of decision-makers. Understanding these dimensions not only enriches the study of intelligence failure but also reinforces the need for plural, comparative, and critical approaches that go beyond any single national experience.

The Traditional View of Intelligence Failures

The first of these, defined as the "Traditional View", referenced by authors such as Robert Jervis, Roberta Wohlstetter, and Richard Betts, considers intelligence failures natural and, to some extent, inevitable. From this viewpoint, intelligence failures occur either during the analytical phase, typically due to cognitive limitations inherent to human nature and therefore never entirely avoidable, or during the reception and absorption of information by decision-makers, who may either be disinclined to accept the intelligence or fail to act appropriately. Michael Handel writes that most failures occur because intelligence analysts

or decision-makers refuse to adapt to "new information" (Betts, 1978; Handel, 1984; Heuer, 1999; Latham, 2012).

In addition to having solid intellectual references in the psycho-cognitive approach within the field of International Relations (Cashman, 2013; Jervis, 1985), the line of argument of the traditional school finds specific evidence in studies on the pathologies affecting the relationship between intelligence analysts/officers and decision-makers, particularly in the phenomena of neglect and excessive harmony.

Neglect occurs when decision-makers dismiss intelligence reports that contradict their views, often exemplified by Stalin's disregard for warnings before Operation Barbarossa (Andrew, 2009). This behavior may stem from rejecting unsettling information, aligning with the "theory of selective attention," in which leaders interpret adversary intentions based on preconceived notions rather than actual behavior. Organizational dynamics within intelligence communities can exacerbate neglect, as a focus on redundancy overshadows analytical synthesis, allowing decision-makers to seek information that supports their beliefs.

This environment can stifle minority opinions and contribute to *groupthink*, where dissenting views struggle to be heard. This is what may have happened in July 1990 when Walter Lang, an analyst officer at the US Defense Intelligence Agency for the Middle East and Southeast Asia, forwarded to his (skeptical) superiors a report suggesting that Iraqi troop movements along the Kuwaiti border, combined with Saddam Hussein's personality, indicated a probable imminent invasion of Kuwaiti territory (Jordan et al., 2009).

Excessive harmony arises when intelligence officers' perspectives align too closely with those of decision-makers, leading to uncritical acceptance of ideas. This can create a self-reinforcing cycle, as illustrated by cases such as the Vietnam War, where mutual agreement hindered critical analysis. On this, Morton Halperin (1971) writes:

> As information is collected and passed up through the system, some are highlighted, and many are discarded. Inferiors often provide information according to what they believe their superiors want to hear. The result of this filtering process for decision-makers is often a narrow set of options and a distorted view of the issue. For years, intelligence reports on Vietnam presented a rosy view that victory was just around the corner, that with more troops, firepower, and bombing, the communists would be defeated. The reality was just the opposite. How did this intelligence distortion develop? President Johnson made it clear in his statements and actions that this was the result he wanted. Thus, key officials at various levels in the intelligence community filtered out any information that ran counter to the administration's preferred narrative. The Navy and the Air Force, in particular, exaggerated the effectiveness of their respective bombing campaigns, hoping the president would favor one branch over the other. However, the chief effect may have been to convince Johnson that he could win the war through bombing (pp. 80-81).

In the case of the Vietnam War, the US intelligence community supported Johnson primarily because it had few doubts (at least for some years) about the main world power's

ability to win a conflict, however atypical, against much weaker actors (Gomez del Prado, 2010). For this reason, analyses contrary to this view remained a long minority and marginal, rarely making it into the information flows intended for political leadership. Particularistic interests, tied to various sectors of the American military-industrial complex, may have certainly contributed to the escalation, even as it became clear that victory was far from certain (a "psychologically unsettling" fact), but, from a predominantly psychological standpoint, they did not represent the primary cause.

A similar dynamic of excessive harmony contributed to Israel's surprise in the 1973 Arab-Israeli War. Israeli intelligence and leadership, over-reliant on a trusted source within Egypt, adhered to a rigid assumption, the "Concept", that Egypt would not attack without sufficient air capabilities and Syria would only act in tandem. This unwavering adherence blinded them to clear indications of an impending offensive, leaving Israel vulnerable to the coordinated attack by Egypt and Syria. In Western contexts, excessive harmony also influenced intelligence assessments about major geopolitical shifts, such as the collapse of the Soviet Union. Few analysts or decision-makers anticipated this event, often dismissing contrarian views as out of step with prevailing paradigms.

An example of excessive harmony closer in time occurred during the lead-up to the 2003 Iraq War. Intelligence agencies in the United States and the United Kingdom accepted and amplified the political narrative that Iraq possessed weapons of mass destruction (WMDs). Despite the lack of concrete evidence, reports increasingly aligned with this assumption, driven by bureaucratic pressures and the influence of senior political figures. This convergence of political will and intelligence assessments, described by some as deliberate manipulation, underscores intelligence's vulnerability to political interests.

Oliver Latham's research provides a theoretical lens for understanding this pathology. He suggests that, during the Cold War, mainly ideologically driven leadership and analysts' reluctance to dissent due to career concerns contributed significantly to excessive harmony. Deeply rooted in psychological and organizational factors, these behaviors were often unconscious and difficult to eliminate (Bzostek, 2008).

Both neglect and excessive harmony, while damaging, are not always driven by intentional political motives. Instead, they arise from psychological and organizational dynamics that are inherently challenging to mitigate. Traditionalist scholars argue that while intelligence performance can be improved through better training and awareness, failures are ultimately unavoidable. For example, following 9/11, experts concluded that while preventing all terrorist attacks is impossible, preparing for their aftermath may be a more realistic and practical strategy (Betts, 2007; Handel, 1984; Heuer, 1999; Jervis, 2010; Marrin, 2004; Wohlstetter, 1962). This perspective reflects the traditional school's pragmatic, if somewhat pessimistic, stance, which largely downplays errors or limitations in intelligence collection.

The Reformist View of Intelligence Failures

The reformist school of thought on intelligence failures contrasts with the traditional perspective by holding a more optimistic view about improving intelligence systems. While traditionalists accept a certain error level as inevitable, reformists argue that failures stem mainly from organizational weaknesses that can be addressed through specific structural reforms. They emphasize that intelligence failures often result from insufficient agency coordination and a lack of information sharing across departments - issues rooted in flawed institutional frameworks.

In his 1985 study, Glenn Hastedt identified the rigid, hierarchical, and centralized nature of bureaucratic organizations as a key limitation to effective communication, contributing to intelligence failures. According to this view, bureaucracies often hinder collaboration, as agencies or individuals within them may prioritize institutional prestige or adopt narrow perspectives, aligning with the principle of "where you stand depends on where you sit" or Miles' Law (Hastedt, 2013; Martino & Merenda, 2021).

As early as 1967, in a famous organizational theory essay, Harold Wilensky argued that if anything is clear from this book, it is that intelligence failures are built into complex organizations (Allison & Zelikow, 1999; Hastedt, 1985; Wilensky, 1967). In the late 2000s, this thesis was taken up by Amy Zegart regarding the events of 9/11, highlighting how bureaucratic reorganizations have been the preferred solutions recommended by all governmental and expert commissions established to examine the strategic failures of Washington's Intelligence Community. Indeed, the majority of the 340 proposed reform interventions between 1991 and 2001, from twelve study commissions, were organizational (Zegart, 2007). In contrast to traditionalist authors who believe that American intelligence services have performed well, the scholar evaluates their activities as severely deficient in several respects, essentially because the entire intelligence system suffers from ineffective organization (Zegart, 2007).

Reformists also critique the systemic issue of politicization, where intelligence is intentionally skewed to align with political objectives. Politicization undermines the integrity of intelligence analysis, distorting decision-making processes. This pathology can take three forms: direct manipulation, indirect manipulation, and intelligence-driven manipulation. In direct manipulation, decision-makers exert explicit pressure on intelligence officials to produce analyses that support their political agendas or appoint individuals to key positions predisposed to align with their views (manipulation by appointment). Indirect manipulation involves subtler signals, often coupled with implicit incentives or threats, that influence agencies to align their outputs with leadership's preferences.

As in direct manipulation, in indirect manipulation, the selective use of information primarily results from the policymaker's activity aimed at shaping the analytical approaches and positions of intelligence agencies for purposes tied to policy preferences. If the policymaker tended to favor selective use of information without interfering in the analytical

production of the agencies; for instance, only to obtain temporary support or address a specific contingency, then this would be termed neglect. Intelligence-driven manipulation occurs when agencies distort information to support or undermine political decisions.

A well-documented case of politicization is the Reagan administration's handling of intelligence on the Soviet Union. CIA analysts were pressured to overestimate Soviet military expenditures, legitimizing massive US defense spending, including the Strategic Defense Initiative. Despite these efforts, evidence later revealed that Moscow's spending had declined. Still endowed with a certain degree of structural autonomy from the executive, particularly in democratic systems, intelligence services may be incentivized to manipulate information, today more than in the past, due to the growing presence of private competitors (e.g., fearing losing relevance to the executive compared to the latter, intelligence services might politicize information to please decision-makers or, in the worst case, blackmail them).

This functional model is opposed in the literature by the "objectivity' model, which holds that intelligence agencies should strive as much as possible to remain impartial in their activities and assessments, maintaining a bureaucratic detachment from political leadership (even at the risk of becoming politically irrelevant themselves). This model, inspired by Sherman Kent, a Yale academic and one of the first senior intelligence officials in the US, remains a foundational element of the CIA's institutional culture, to the point that its analysts' school is named after Kent (1949). It appears that the two models can blur or overlap in reality, though one may clearly prevail at times.[1] Similarly, in the lead-up to the Iraq War in 2003, intelligence agencies in the United States and the United Kingdom faced pressure to substantiate claims that Iraq possessed weapons of mass destruction (WMDs), which were later proven false. This contributed to a war based on distorted intelligence assessments, with long-lasting geopolitical consequences.

Politicization is especially prevalent in non-democratic regimes (Vanhanen, 2000), where intelligence agencies operate with limited institutional oversight. In such contexts, political leaders often exploit intelligence services to consolidate domestic power or legitimize external aggression, even when this leads to strategic miscalculations. This phenomenon helps explain why authoritarian regimes may initiate asymmetric conflicts against stronger adversaries, underestimating risks or overestimating their own capabilities (Liz-Rivas, 2023). A notable example is Russia's 2022 invasion of Ukraine, where politicized intelligence may have contributed to critical misjudgments, not only in underestimating Ukrainian resistance, but also in overlooking the scale and cohesion of Western support. These failures highlight the dangers of intelligence shaped by political imperatives rather than grounded, objective analysis.

This can occur not only in regimes where one or a few decision-makers can fully impose a specific political will, however irrational, but also, if not mainly, in systems where

1 For an in-depth explanation of these aspects, see Betts (2007, pp. 76-77) and Nester (2001, p. 130).

the executive is heavily influenced by small domestic groups (including actors belonging to or linked with intelligence services) with economic or political interests in a state of war - and where the political leadership owes its rise and maintenance in power to these groups, e.g., consider Jack Snyder's cartelized systems (1991). A well-known example of asymmetric warfare is the Falkland-Malvinas conflict, in which Argentina, despite being weaker than the United Kingdom, occupied the islands to divert attention from its domestic issues through a bold foreign policy move, albeit underestimating the British response.[2]

Even in democratic systems, politicization is not uncommon. For example, during the Reagan administration, CIA analysts complained about senior officials tailoring intelligence to justify controversial policies or clandestine operations. A former CIA director, Robert Gates, admitted that during the 1980s, intelligence on Soviet military capabilities and expenditures was deliberately exaggerated to support President Reagan's defense agenda (Gates, 1996). This manipulation led to unnecessary increases in US defense spending, including vast investments in the Strategic Defense Initiative, which contributed to a ballooning national deficit without significantly impacting Soviet policies.

Unlike neglect and excessive harmony, which stem from psychological or relational factors, politicization is driven by rational calculations on both sides. Politicization can be explained by two main independent variables: public commitment to a political goal and the emergence of a political entity (a critical constituency) capable of effectively opposing the decision-maker's policies (Martino, 2024). A political leader who has publicly declared their intentions is exposed to significant damage in the event of failure. This risk is even higher if commitment, especially on controversial issues, has given rise to strong opposition. Under such conditions, the decision-maker may find it challenging to accept dissent from intelligence services and may seek favorable analyses, potentially even making them public.

Conversely, intelligence agencies might be incentivized to support competing positions and actors if such a choice better safeguards their preferences.[3] Decision-makers seek to secure their power and advance their agendas, sometimes by pressuring intelligence agencies to align with their objectives. Conversely, intelligence agencies may seek to protect their bureaucratic influence, even at the cost of undermining political leadership. These dynamics are not unique to any one regime type and can create cycles of distrust and hostility. Once revealed, politicization often leads to mutual alienation: intelligence officials may withdraw from the decision-making process, while political leaders may limit their reliance on intelligence services to avoid accusations of manipulation.

Addressing politicization requires structural and procedural remedies. Keeping sensitive intelligence confidential can reduce the temptation to manipulate it for public or political

2 On asymmetric conflicts and their various causes, see Paul (1994).

3 For theories about the pathologies of the intelligence-decision-maker relationship, particularly politicization, see Rovner (2011).

purposes. Enhancing coordination and information-sharing mechanisms within intelligence systems can also be a self-check against manipulation. In democratic contexts, robust parliamentary oversight of intelligence agencies and their relationships with political leaders can provide an additional layer of accountability. For instance, reforms in the US following the 9/11 Commission Report included creating the position of Director of National Intelligence to improve inter-agency coordination and reduce the likelihood of manipulation (National Commission on Terrorist Attacks Upon the United States, 2004). While not foolproof, such measures help mitigate the risk of politicization and preserve the integrity of intelligence operations.

The Contrarian View of Intelligence Failures

The third school of thought on intelligence failures diverges from traditionalist and reformist perspectives, thus getting the name "contrarian". While reformists emphasize organizational shortcomings and traditionalists focus on cognitive limitations and decision-makers' reception of intelligence, contrarian scholars such as David Kahn and Ariel Levite shift the focus to the collection phase of the intelligence cycle. Unlike traditionalists, they argue that intelligence failures stem from informational deficiencies rather than analytical errors or bureaucratic inefficiencies. According to this school, the absence of sufficient or relevant data during the collection phase prevents intelligence agencies from generating timely warnings or alarms (Kahn, 1991; Levite, 1987).

This view also stands apart from the previous schools in its theoretical and empirical underpinnings. It lacks significant ties to established theoretical frameworks, making it appear less comprehensive when closely examined. While the distinction between the collection and analytical phases can serve as a valuable heuristic for describing the intelligence cycle, it becomes less convincing when applied to explaining failures. This is because analytical processes are inherently embedded in the collection phase, as certain analytical assumptions or orientations often precondition the data-gathering process.

It is not coincidental that within professional intelligence practice, the term *collection* is frequently qualified as *informative*, highlighting its purpose as a foundational step in producing an actionable intelligence product. In some contexts, however, *informative collection* is also used—as perhaps more precisely a synonym for *informative research* —a term that encompasses not only the acquisition of raw data but also the early stages of processing and preliminary analysis (Phythian, 2013).

Theoretically, the contrarian perspective offers originality but contributes limited value beyond what the other two schools provide, as it fails to address the organizational bureaucratic factors underlying intelligence operations. In the digital age, attributing failures solely to the absence of specific indicators, rather than to an inability to recognize, integrate, or interpret them, poses theoretical and empirical risks. This perspective could suggest that one

intelligence system's failure stems from another's success, or that the lack of clarity in identifying the required indicators undermines the explanatory power of both.

It may be the case, for example, where the intelligence services of one state, through a successful deception activity, completely mislead the intelligence of another country. While some failure of the latter cannot be denied, the outcome of the "contest" may be more attributable to the merits of the former than to the shortcomings of the latter. The international literature on deception is quite extensive, and this concept now extends well beyond the strategic-military domain (Bruce, 2010).

The contrarian school sets the stage for a related perspective known as the "theory of preventive action". Developed by Erik J. Dahl and inspired by Deborah Barger's earlier work, "Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond" (Dahl, 2013), this theory builds on the contrarian emphasis on collection while focusing specifically on the absence of tactical-level warnings as a primary cause of intelligence failures. Unlike strategic analysis, which offers broader assessments of long-term trends, tactical intelligence is centered on immediate, actionable insights. According to this theory, intelligence failures often stem from the lack of detailed tactical analysis rather than from issues in strategic interpretation. As the discussion progresses, the distinction between tactical and strategic intelligence analysis will be further elaborated, using specific case studies to test the logic of the theory of preventive action. These examples will clarify how emphasizing tactical intelligence could prevent inevitable failures while acknowledging the risks of underweighting strategic considerations.

A New View: Preventive Action. Theoretical Framework and Case Studies

Erik J. Dahl, a professor of National Security at the Naval Postgraduate School in Monterey, introduces his theory of preventive action by critically examining the dominant schools of thought in international intelligence literature. Dahl argues that traditional and reformist schools have significant limitations, particularly their ability to translate theoretical insights into practical applications for intelligence operations.

The traditional school, often sympathetic to intelligence practitioners, is rooted in the belief that intelligence failures are "inevitable" due to human beings' inherent cognitive limitations. According to Dahl, this perspective is overly pessimistic and offers little opportunity for meaningful improvement. It assumes that even significant failures are unavoidable, regardless of advancements or efforts within intelligence systems. Moreover, this school focuses almost exclusively on the analytical phase of the intelligence cycle, neglecting the potential for errors or shortcomings in the collection phase.

In contrast, the reformist school takes a more optimistic view. Reformists argue that intelligence performance can be significantly improved through extensive bureaucratic

restructuring, such as enhancing inter-agency coordination and ensuring better information sharing. This approach, while reassuring the public, has its shortcomings. Dahl critiques the reformist school for its implicit rigidity, as it attributes failures solely to organizational and administrative issues. By narrowing its focus to structural solutions, this perspective disregards other potential causes of failure that fall outside the bureaucratic domain.

Dahl's critique of prevailing theories goes even deeper. According to the US professor, three significant shortcomings can be identified in studies of intelligence failures. The first is the lack of comparative analysis between failure and success cases. Studies typically focus only on failures, that is, cases in which a surprise attack was successful, and intelligence failed. There is no analysis of cases in which intelligence successfully prevented a surprise attack. Erik Dahl (2013) writes.

> In the terminology of the social sciences, these studies are guilty of selecting on the dependent variable or choosing cases to study based on how those cases turned out. For this reason, although existing studies may help us understand some of the many reasons why intelligence can fail, they do little to tell us how it can succeed (p. 15).

One major limitation in analyzing intelligence operations stems from the difficulty of accessing documentary evidence on successful cases. This challenge is understandable, as intelligence agencies are strongly incentivized to keep their achievements confidential. Even when they do share information about successes, they rarely disclose operational methods, sources, or the details of their activities, making comprehensive analysis difficult.

A second limitation, frequently observed among reformist scholars, is the prevalence of "Hindsight Bias," also known as the "*Monday-morning quarterbacking syndrome*." This bias involves the tendency to reinterpret information available before an event but overlooked at the time. When reviewed after the fact, such information is often perceived as indicative of what was to come, even though it may not have appeared before the event.

The third limitation relates to the scope of existing studies on intelligence failures. Most analyses focus heavily on military-related shortcomings, particularly those related to surprise attacks during the Cold War. There remains a notable lack of research addressing non-military intelligence failures or those from more recent periods, especially in the post-Cold War context, leaving significant gaps in the broader understanding of intelligence shortcomings. In his research, Erik Dahl attempts to overcome these limitations by developing the first research framework in specialist literature to enable a comparative analysis of both successful and failed cases (Dahl, 2013).

Dahl's theory of preventive action is tested across both types of cases (Dahl, 2013, p. 19) and over a period that extends beyond the Cold War into subsequent years. However, it is essential to clarify that Dahl's analysis concerns only surprise attacks, which, while a critical category, constitute only a subset of the broader genus of intelligence failures. The same

American professor invites the academic research community to test the theory of preventive action on further case studies.

When is it appropriate to speak of an intelligence failure, and when of success? Dahl adopts an approach that involves both actors in the process: the agencies and the decision-maker. An "intelligence failure" occurs either when the agencies fail to provide the decision-maker with the necessary intelligence or when the decision-maker errs by failing to act appropriately based on the information received from the agencies. For intelligence to be successful, both actors must act correctly: the agencies must provide the required information and analyses, and the decision-maker must act appropriately based on these. Specifically, the information provided to the decision-maker must be *actionable* ("actionable intelligence"), a term lacking a precise definition even in the US intelligence system but generally referring to intelligence that is "useful" to the decision-maker. Such information must be accurate and timely to be actionable. It must be specific and linked to the immediate needs of decision-makers. In other words, this intelligence must be tactical rather than strategic.

Moving on to the concepts of "tactical intelligence" and "strategic intelligence", according to Dahl, tactical intelligence is shorter-term, more narrowly focused (often on specific events), and most likely to be used by junior-level officials engaged in planning or directing individual operations. In contrast, strategic intelligence "tends to be longer-term, broader in focus, and of interest to senior-level policymakers who make decisions concerning the most important national and international issues" (Dahl, 2013, p.22).

Thus, tactical intelligence provides the decision-maker with more specific, detailed, and short-term information than strategic intelligence (which instead covers medium- to long-term timelines and develops complex overall scenarios without delving into the details of specific and circumstantial events). Simplifying, while a strategic-level warning informs the decision-maker that a particular actor has the intention and means to attack, a tactical warning provides detailed information on the presumed location of the attack and the enemy forces ready to engage.

If a strategic-level warning alerts national security leadership that a terrorist group intends to attack the country, a tactical warning provides specific details about the ongoing plot.

In the US national security culture and in accordance with the prevailing approach in the literature, strategic intelligence is considered valuable for preventing surprise attacks. Only through strategic-level analyses and information can intelligence thwart terrorist attacks or military assaults by hostile forces. This approach holds that tactical intelligence is inherently insufficient and unsuitable for this role. On the other hand, good strategic intelligence provides the decision-maker with a comprehensive overview of future threats; only with strategic-level information can national decision-makers effectively protect the country.

The theory of preventive action takes a distinct approach to understanding and preventing surprise attacks. According to Erik Dahl, two critical factors influence success in thwarting such attacks: the specificity of the warning and the decision-maker's recep-

tiveness. For intelligence to be practical, it must generate specific, tactical-level warnings (the first factor) and rely on decision-makers who are open to them (the second factor). Tactical warnings, rather than strategic ones, capture decision-makers' attention and prompt timely action to counter imminent threats.

Dahl's comparative analysis of successful and unsuccessful cases suggests that decision-makers are more likely to act on tactical intelligence, which contains actionable specifics such as the "where," "when," and sometimes the "who," whereas strategic warnings typically lack them. While strategic warnings may accurately identify potential threats, their generality often fails to create the urgency for decisive action.

Dahl wrote in his book "Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond" that, on the contrary, strategic intelligence does little to prevent surprise attacks. In many cases, strategic warnings before attacks have been very imaginative, and analysts have often been able to forecast threat scenarios that proved to be highly prescient. However, these warnings have done little good because they did not give specific information about who, what, where, or when that was needed to create the sense of urgency that would have compelled decision makers to act and enable them to know what action to take. Conversely, when a warning has been specific, and policymakers have been receptive, attacks have been successfully prevented," (Dahl, 2013, p. 176).

Simply put, strategic warnings often fail to "wake up" decision-makers, prompting them to take politically challenging actions. Dahl, however, does not downplay the significance of strategic intelligence. Drawing from earlier arguments by Jack Davis (2006), Dahl asserts that practical strategic analysis is essential for laying the foundation for precise tactical intelligence. Strategic intelligence is crucial for identifying medium- to long-term trends and for ensuring adequate resources are allocated to developing tactical alerts.

However, only detailed tactical warnings can prevent imminent threats. Even so, tactical intelligence alone is insufficient. For intelligence to avert failures, decision-makers must trust their intelligence sources and the presented threat. The combination of high-quality tactical intelligence (specific, timely, and actionable) and a decision-maker's trust in this information determines the effectiveness of intelligence operations and reduces the likelihood of failure.

Dahl's analysis further reveals that the relative importance of these factors - tactical intelligence and decision-maker receptiveness - varies depending on the type of threat. In the context of conventional military attacks, where a wealth of intelligence data is generally available, decision-maker receptiveness is often the determining factor. Conversely, in cases of terrorist threats, decision-makers in the United States and other countries tend to be more attuned to and willing to act on warnings, making the availability of tactical intelligence the most decisive factor in preventing an attack.

Two case studies help illustrate the theory of preventive action. The first is the September 11, 2001, terrorist attacks carried out by Al Qaeda against the United States. Various commissions have extensively investigated this event, and it has become one of

the most analyzed examples of intelligence failure in history. Available evidence suggests that the failure stemmed not from a lack of tactical information but from gaps in strategic intelligence that did not adequately prepare decision-makers to anticipate or counter the attack. This case underscores the importance of balancing strategic and tactical intelligence to address complex threats effectively. Dahl (2013) writes in his book:

> The first major official study of the 9/11 attacks—the Congressional Joint Inquiry (2002)—concluded that although no specific intelligence predicted the exact time or method of the attacks, important warning signs were mishandled by the intelligence community. The report highlighted a lack of strategic analysis on al-Qaeda and an insufficient understanding of the broader threat. Its findings anticipated those of the later 9/11 Commission, whose widely accepted report emphasized that, despite numerous tactical warnings, there was no integrated assessment of bin Laden's overall strategy between 1998 and 2001 (p. 130).

The 9/11 Commission Report posits that the primary shortcoming in the US national security apparatus was the absence of strategic-level analyses capable of conveying the severity of the al-Qaeda threat to political and strategic leadership. This view has become the prevailing interpretation of the intelligence failure leading to the September 11 attacks. However, Erik Dahl challenges this interpretation. An examination of the intelligence circulating within US national security circles reveals that considerable strategic information and analyses were available.

From the mid-1990s to just days before the attacks, the American intelligence community issued numerous warnings regarding the increasing threat of jihadist terrorism, notably from al-Qaeda and its leader, Osama bin Laden. For instance, the August 6, 2001, President's Daily Brief titled "Bin Laden Determined to Strike in US", prepared by CIA analysts at President George W. Bush's request, clearly outlined the ongoing threat, stating, "Clandestine, foreign government and media reports indicate Bin Laden since 1997 has wanted to conduct terrorist attacks in the US." Such intelligence clearly highlighted the threat's existence and origins.

Despite strategic warnings, Dahl questions why these did not lead to preventive action. He argues that while awareness of the strategic threat was widespread, tactical-level details were missing. The intelligence community failed to produce actionable intelligence on the specifics of the planned attack, including when, where, and how it would occur. While the strategic context was well understood, the lack of tactical warnings meant decision-makers lacked the precise information needed to act decisively.

According to Dahl's theory of preventive action, strategic intelligence alone is insufficient to prevent surprise attacks. Detailed, specific, and actionable tactical intelligence creates the urgency to prompt preventive measures. However, Dahl also emphasizes that the second factor in his theory, decision-maker receptivity, was equally deficient in the lead-up to 9/11. Within both the Clinton and Bush administrations, only a small number of officials fully grasped the seriousness and immediacy of the al-Qaeda threat. This dual failure - insuf-

ficient tactical intelligence and a lack of decision-maker receptivity - contributed to one of US history's most significant intelligence failures.

Similarly, January 6, 2021, storming of the US Capitol highlights another significant intelligence failure rooted in ignored warnings and analytical biases. According to the bipartisan Senate report "Examining the U.S. Capitol Attack: A Review of the Security, Planning, and Response Failures on January 6" (US Senate Committee on Homeland Security and Governmental Affairs & Committee on Rules and Administration, 2021), both the FBI and the Department of Homeland Security were aware of potential threats of violence, but these were not adequately acted upon. The report describes the agencies' failure as ignoring a "massive amount of intelligence," emphasizing a systemic underestimation of the severity of the threat. Analysts were criticized for a "failure of imagination," reminiscent of critiques following 9/11, which prevented them from fully appreciating the scale and uniqueness of the impending crisis.

Moreover, indicatively, the October 7, 2023, attack by Hamas on Israel, according to a report published a year after the event by the Combating Terrorism Center at West Point, highlights a critical intelligence failure rooted in the neglect of tactical intelligence in favor of strategic analyses. Although Israeli intelligence agencies had accumulated extensive strategic knowledge about Hamas's long-term objectives and overall capacity, they failed to act on specific, actionable tactical warnings that signaled an imminent threat. Intelligence reports had flagged suspicious activity, including unusual movements and communications among Hamas operatives, which should have raised alarms about an impending offensive. However, according to author Wyss, these indicators were downplayed or dismissed, as decision-makers prioritized the broader strategic assessment that Hamas was unlikely to launch a significant attack due to its perceived lack of preparedness and deterrence by Israeli military strength (Wyss, 2024).

This overreliance on strategic intelligence, characterized by its long-term focus and emphasis on broader trends, created a blind spot for tactical intelligence's actionable, time-sensitive insights. Tactical intelligence, by its nature, focuses on specific details such as the "when," "where," and "how" of an attack, offering a granular level of detail necessary for preventive measures. In the case of Hamas, such tactical warnings were overlooked due to a systemic bias within the intelligence apparatus. This bias was reinforced by Israel's reliance on technological surveillance over human intelligence, a choice that limited the contextual understanding of Hamas's operational intentions. Human intelligence could have provided corroborating details about the scope and timing of the attack, but its underutilization left Israeli decision-makers with incomplete situational awareness.

This failure reflects a broader issue identified by Erik Dahl's preventive theory: the need to integrate tactical intelligence into decision-making processes to complement strategic insights. While strategic intelligence provides the overarching framework for understanding threats, tactical intelligence ensures timely and actionable responses to immediate dangers.

The October 7 attack demonstrates how an imbalance between these two levels of intelligence can leave a nation vulnerable to surprise attacks. In this case, the overconfidence in strategic deterrence and the dismissal of tactical alerts allowed Hamas to exploit operational blind spots, resulting in one of the most devastating security breaches in Israeli history.

A notable and contrasting example of successful counterterrorism intelligence occurred in June 1993, when US authorities successfully dismantled a coordinated plot by Islamic extremists to launch multiple attacks in New York City. The group, linked to Sheikh Omar Abdel Rahman—commonly known as the "Blind Sheikh"—had been planning to strike symbolic infrastructure targets, including the United Nations headquarters, the Lincoln and Holland Tunnels, and the George Washington Bridge (Dahl, 2013, pp. 110–127).

The operation's success was the result of long-term intelligence gathering led by the FBI in collaboration with the New York City Joint Terrorism Task Force (JTTF). Monitoring of the group began as early as 1989 and intensified with the introduction of an Egyptian informant in 1992, who infiltrated the conspirators' inner circle. On June 23, 1993, US authorities launched a coordinated intervention, arresting the individuals involved and thereby preventing a potentially devastating series of attacks on American soil. This case highlights the value of human intelligence (HUMINT), inter-agency cooperation, and persistent surveillance in pre-empting terrorist operations—elements that are often absent in intelligence failure scenarios. It also serves as a counterpoint in the broader discourse on intelligence, where most academic focuses tend to revolve around failures rather than successes.

An analysis of the intelligence leading to this success highlights the crucial role of tactical information. Although strategic analyses underestimated the broader threat of international terrorism at the time - assessing it as "low" even after the February 1993 World Trade Center bombing - the FBI and JTTF had access to specific and actionable intelligence regarding the planned attacks. Detailed tactical warnings, including information on the "how, where, and when" of the plot, enabled authorities to act in time. This case demonstrates how high-quality tactical intelligence, even without robust strategic assessments, can be decisive in preventing terrorist attacks. Erik Dahl (2013) writes:

> This case is especially relevant because it validates the theory of preventive action. The "Day of Terror" plot was not stopped by strategic intelligence or analysts connecting distant clues. In fact, national assessments underestimated the terrorist threat even after the World Trade Center bombing. What prevented the attack was timely, tactical intelligence from an FBI informant. However, the case also shows that even accurate intelligence must be matched with responsive decision-makers for it to result in effective action (p. 126).

To conclude, the theory of preventive action shifts the focus from the analytical phase to the collection phase of the intelligence cycle, emphasizing the importance of tactical intelligence over strategic intelligence. Unlike the contrarian theory, which attributes intelligence failures to an objective lack of valuable data, the theory of preventive action identifies the

root problem as the intelligence community's failure to identify and collect the necessary information. According to Dahl, intelligence services must prioritize strengthening their tactical-level collection capabilities to generate actionable intelligence - detailed, specific tactical warnings that receptive decision-makers can effectively utilize.

Dahl's theory, supported by comparative analyses of success and failure cases, represents a significant innovation in intelligence study. After the catastrophic failure of US intelligence during September 11, 2001, attacks, the dominant scholarly opinion has emphasized the importance of strategic intelligence. While indispensable for robust intelligence operations, strategic intelligence alone cannot prevent surprise attacks, whether conventional or unconventional.

A practical takeaway from Dahl's theory is the recommendation to enhance tactical-level intelligence collection efforts to reduce the likelihood of such failures. The following section will explore how improving tactical capabilities can and must coexist with adaptations inspired by other theoretical perspectives examined in this paper. Indeed, the solutions proposed by the traditional and reformist schools are not mutually exclusive and can be integrated to reduce intelligence failures. For instance, restructuring intelligence systems can incorporate strategies to improve organizational efficiency and personnel training, ensuring a more holistic approach to enhancing intelligence performance.

Conclusions

In this paper, we outlined the main explanatory perspectives on intelligence failures, focusing mainly on the theory of preventive action. By focusing on the analytical phase, the traditional school highlights errors and pathological phenomena tied to the cognitive limits of human nature and the psychological dynamics involving the relationship between analysts and decision-makers. Conversely, the reformist school focuses primarily on poor performance stemming from organizational dysfunctions, which are possible in intelligence systems as well as in bureaucracies and complex organizations more generally. The contrarian theory, however, attributes failures to shortcomings in the intelligence cycle's collection phase, i.e., deficiencies in gathering material that the analytical phase of the same cycle should then evaluate and process.

While the first two schools exhibit clear connections to more general and established theoretical approaches widely used in various areas of Political Science, the third view appears less convincing due to its theoretical indeterminacy and more significant empirical challenges (Bar-Joseph, 1988). Consequently, concerning operational recommendations, the first two schools of thought prove more fruitful. The first school partially addresses the problem of intelligence failures by suggesting continuous technical training for practitioners. In contrast, the second aims to reduce such failures almost entirely through the organizational analysis of intelligence systems (Sanz-Gonzalez et al., 2024).

The intuition of the contrarian theory - namely, the possibility of failure rooted in factors unrelated to analytical or organizational errors of intelligence - has, however, been partially incorporated (and "rescued") by the theory of preventive action. Unlike the first, this theory attributes intelligence failures not to a problematic objective lack of valuable raw data (a relatively lenient perspective towards analysts and decision-makers) but rather to a shortage of tactical-level intelligence. As the case studies and the case studies examined below demonstrate, an intelligence failure, understood as the inability to prevent a significant event threatening national security, may depend on a lack of tactical early warnings.

In other words, preventing a harmful event, such as a surprise attack, requires more than just knowing its most likely cause (the actor and their motive); it involves understanding, as precisely and in as much detail as possible, how, where, and when that cause will produce its (most feared) effects. This is also because decision-makers, despite cognitive limitations or organizational characteristics of the systems they operate in, tend to act (i.e., adopt defensive-preventive measures) if the benefits outweigh the costs. If the threat is not specific and imminent, taking serious measures to neutralize it may be technically challenging and politically risky - even in counterterrorism.

To safeguard national security from military, terrorist, or economic-financial attacks, decision-makers may (and will) act preventively much more in response to tactical warnings than to strategic ones, which are more general and vaguer. The 9/11 attacks provide a textbook example: before the attacks, US intelligence knew that al-Qaeda posed a significant threat to America and the world. However, to prevent those attacks, it was not enough for American decision-makers to understand what al-Qaeda was, nor was it sufficient to be informed about its ideological, structural, and operational characteristics or the generic presence of its supporters on US soil.

In the absence of specific indications about the timing, methods, locations, and probable perpetrators of a potential attack, decision-makers failed to act - they did not take the measures that could have averted the worst-case scenario (even though within American intelligence there had been, albeit speculatively and generically, some warnings a few months before the attacks about the possible use of commercial airplanes as weapons) (Delgado-Morán et al., 2019b). The low receptivity of decision-makers (or their limited propensity to act based on intelligence), within the theory of preventive action, should not be confused with the pathology of negligence, which most often occurs because the decision-maker tends to reject information that is "psychologically unsettling" or otherwise inconsistent with their worldview (or, more rarely, because they place more trust in their own analytical abilities than in those of the Services). In other words, the former appears to respond more to a rational perspective than the latter. This does not absolve American decision-makers of all responsibility, partly because the lack of tactical analysis may stem from their tendency to request more strategic than tactical intelligence, even though they are more receptive to the latter.

This would be, in Erik Dahl's own words, the paradox of strategic warning (Dahl, 2013, p. 177), also because, not infrequently (and in various countries far more than in the USA), the connection between medium- to long-term (or otherwise non-contingent) decision-making and strategic warnings from intelligence would be relatively weak in absolute terms. However, we should remember that, regarding the quantitative relationship between demands for strategic intelligence and other types of intelligence, certain scholars hold positions that differ from those expressed by Dahl; for example, the aforementioned Thomas Fingar (Payá-Santos & Delgado-Morán, 2017). It is interesting to note how the analytical-professional profiles of the two authors might partly reflect this divergence of views, with the latter being highly specialized in strategic analysis, while the former also engages in tactical analysis (having practiced as an intelligence officer in the US Navy, where he served for more than twenty years).

As noted in the previous paragraph, intelligence did not fail when it provided and forwarded specific tactical early warnings to decision-makers. This was true in cases of terrorist actions comparable to 9/11 (except in outcomes) as well as in instances of conventional military attacks (Dahl, 2013, pp. 1–86). In most situations where there was no significant shortage of tactical analysis, intelligence performed well - or rather, the relationship between intelligence and decision-makers produced favorable results. When decision-makers were aware of the strategic picture and tactical information consistent with it, they were more likely to adopt necessary measures to prevent significant threats to national security.

The theory of preventive action undoubtedly has some original features, including its apparent ambition to explain intelligence failures and its performance more generally (at the tactical level). The theory is formulated not only to be applicable (both empirically and operationally) across various sectors of intelligence (to explain or prevent military or terrorist attacks as well as economic-financial offensives. For example, let us hypothesize here that, to prevent a speculative surprise attack (against currencies, markets, etc.), it would be necessary to anticipate not only its potential perpetrators (actors + motive = strategic level) but also its most probable methods/tools and timing (tactical level) but also, and especially, to require testing both in cases of failure and success (even though the latter may pose more significant empirical challenges due to the confidentiality of the activities/operations involved). For this reason, it is also often argued that, in general, the Services' work is more likely to become known externally in cases of failure than in cases of success.

Compared to previous literature on intelligence failures, this theory has the merit of highlighting the importance of tactical intelligence as an independent variable. The main operational implication of this perspective is that tactical analysis is undoubtedly a worthwhile investment to improve intelligence performance. More broadly, every information system should strive for a constant balance between strategic-level and tactical-level intelligence, using both synergistically and complementarily.

While underestimating strategic intelligence can mean failing to understand the essence of various threat factors, with serious repercussions for the medium- to long-term

measures needed to neutralize them thoroughly and definitively, neglecting tactical intelligence can result in unexpected violent manifestations of threats, with all the ensuing damage. Moreover, there can be no strategic analysis without tactical analysis and vice versa. Suppose the former without the latter can be of limited use. In that case, the latter without the former can be nonsensical - or, in other terms, blind (and, in turn, futile or misleading) - since in intelligence analysis, the tactical level is guided by the strategic level (and not vice versa, at least in general terms).

However, like other explanations of failures, the theory of preventive action is not without external and internal criticisms. Externally, the theory may have a "limited" view of intelligence failures: it is less equipped than others to explain strategic failures. Examples include the USA failing to foresee their debacle in Vietnam when they began the military escalation (almost a decade earlier) and in the immediately following years, or (to a much lesser extent) the collapse of the Eastern Bloc when, in the early 1980s, signals of its possible implosion began to surface, hypothesized by Randall Collins in 1975 and 1998, or Italy entering the war alongside Germany in 1940. Many other examples could be drawn from more contemporary events, ranging from the 2003 military intervention in Iraq to the outbreak of the Arab revolutions in 2011, up to the current global economic-financial crisis.

This means that, compared to competing theories, its lower level of generality narrows its empirical reference field regarding both "failures" and "successes" (though this is not necessarily a disadvantage). Furthermore, even fully accepting the assumptions and conception of failures proposed by the theory, one could argue that the empirical evidence supporting it is (still) limited, quantitatively and qualitatively.

Apart from the partial validation provided in this paper, the theory of preventive action has undergone an empirical examination over a perhaps satisfactory temporal framework, but almost exclusively in relation to the US system, and, in truth, without a very systematic comparison with other theories. Moreover, on the empirical level, the distinction between strategic intelligence and tactical intelligence may not always be so clear, with the result that researchers may be tempted to claim excessive discretion in assigning the respective qualifications to the various warnings used on a historical-documentary basis to prove (or disprove) the theory - bearing in mind that establishing causation between the presence of tactical warnings and the decision-maker's behavior should require both indirect verification strategies (e.g., the method of covariations) and direct ones (e.g., process tracing). Finally, difficulties may arise concerning the comparability of the cases used to test it, especially as it inherently requires testing "in parallel" (i.e., on examples of both success and failure), making it necessary to select cases with great care to balance pair homogeneity and sample heterogeneity.

Similarly, intelligence failures (or successes) do not always depend on the absence (or presence) of tactical intelligence. Having a reasonably sufficient amount of tactical warnings is useless (if not counterproductive) if they are substantively incorrect, especially when they

converge. For instance, if an actor (be it a regular army, an economic operator, or a cyber-warrior) can deceive an opposing intelligence system through disinformation, causing the system not to ignore or underestimate a potential threat but rather to anticipate an event that will never occur - or one that unfolds differently than expected - then failure may still be attributed to analytical error or organizational dysfunction.

Therefore, it is essential not only to consider all the theories reviewed in this paper as plausible (albeit to varying degrees) but also to see them as mutually informing, at least to a certain extent. For example, if the contrarian theory and the theory of preventive action can be seen as partially "communicating", the traditional and reformist schools do not entirely disagree, as they both highlight the causal impact of standard variables - albeit according to different priorities. To simplify greatly, we could say that the primary (or independent) causal variables of the reformist school act as secondary (or, if you will, "intervening") causal variables in traditional theory (and vice versa).

Following this perspective, the remedies proposed by the various schools of thought should be complementary rather than alternatives in reducing intelligence failures (Kerbel, 2014). For instance, the prescriptions of the reformist and traditionalist schools are not antithetical, as the restructuring of an intelligence system can be based on guidelines aimed at improving both its organization and staff training. Countries such as France, the USA, and the UK, as evidenced by the number of publicly available, specific training materials on intelligence analysis used within and outside institutional agencies, dedicate recurring sections to cognitive biases and techniques to mitigate their impact, following the traditionalist school of thought (Heuer, 1999).

As such, reflecting on potentially useful measures for a nation's intelligence system, and establishing integrative "anti-paradigmatic" cells within analytical divisions to foster internal debate and creative thinking, would help mitigate the errors and "pathologies" identified by the traditionalist school. From the reformist perspective, an inter-ministerial security committee should be created. In line with the theory of preventive action, an intelligence service should enhance tactical intelligence through stronger collaboration with other countries' security services, extensive local informant networks, long-term surveillance, and, where appropriate and possible, direct infiltration (not at the expense of strategic intelligence or corrective measures derived from other theories, with which such enhancement is essentially conceptually compatible).

Disclaimer

The authors declare no potential conflict of interest related to the article. No artificial intelligence content generation tools were used in its preparation.

Funding

The authors do not declare any source of funding for this article.

About the author

Luigi Martino is assistant professor in the Department of Political and Social Sciences at the University of Bologna. He earned his PhD from the Scuola Superiore Sant'Anna, Pisa, with a research project on Improving cybersecurity for critical infrastructure in Italy: the public-private partnership model against cyberattacks. His research interests include cybersecurity, security studies, international relations theories, and the dynamics of cyberspace in the international system.

https://orcid.org/0000-0002-7417-2898 - luigi.martino3@unibo.it

Claudio Paya-Santos is full professor accredited by ANECA. Senior Researcher, PhD (with honors and international distinction) in Social Sciences, Humanities and Law, Universitat Internacional de Catalunya. PhD in Political Theory, Libera Università Internazionale degli Studi Sociali Guido Carli.

https://orcid.org/0000-0002-1908-9960 - claudio.paya@professor.universidadviu.com

References

Aldrich, R. J. (2000). *Intelligence and the war against Japan: Britain, America, and the politics of knowledge*. Cambridge University Press.

Allison, G., & Zelikow, P. (1999*). Essence of decision: Explaining the Cuban missile crisis*. Longman.

Andrew, C. (2009). *The defence of the realm: The authorized history of MI5*. Allen Lane.

Bar-Joseph, U. (1988). Methodological Magic. *Intelligence and National Security*, *3*(4), 134–155. https://doi.org/10.1080/02684528808431976

Barnea, A. (2020). Strategic intelligence: A concentrated and diffused intelligence model." *Intelligence and National Security, 35*(5), 701–716. https://doi.org/10.1080/02684527.2020.1747004

Betts, R. K. (1978). Analysis, War, and Decision: Why Intelligence Failures are Inevitable. *World Politics*, *31*(1), 61–89. https://doi.org/10.2307/2009967

Betts, R. K. (2007). *Enemies of intelligence: Knowledge and power in American national security*. Columbia University Press.

Bruce, J. B. (2010). Countering denial and deception in the early 21st century: An adaptation strategy when all else fails. *American Intelligence Journal, 32*(2), 17–24.

Bzostek, R. (2008). *Why Not Preempt? Security, Law, Norms and Anticipatory Military Activities*. Routledge. https://doi.org/10.4324/9781315547213

Cashman, G. (2013). *What Causes War? An Introduction to Theories of International Conflict*. Rowman & Littlefield Publishers.

Collins, R. (1975). *Conflict Sociology*. Academic Press.

Collins, R. (1998). *The Sociology of Philosophies*. Harvard University Press

Dahl, E. J. (2013). *Intelligence and surprise attack: Failure and success from Pearl Harbor to 9/11 and beyond*. Georgetown University Press. https://doi.org/10.1353/book26551

Davis, J. (2006). Strategic warning: Intelligence support in a world of uncertainty and surprise. In L. K. Johnson (Ed.), *Handbook of Intelligence Studies* (pp. 173-188). Routledge.

Delgado-Morán, J., Jiménez, J., & Jiménez, R. (2019b). Transporte Aéreo Estratégico Militar en las Operaciones Militares Modernas. *Ciencia y Poder Aéreo, 14*(1), 114-147. https://doi.org/10.18667/cienciaypoderaereo.625

Delgado-Moran, J., Mazurier, P.A., & Paya Santos, C. A. (2019a). The race to securitize the arctic in a post-cold War scenario. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 4(1), 59-64. http://hdl.handle.net/10272/17180

Díaz Matey, G. (2005). *Methodological Approaches to the concept of intelligence failure*. UNISCI Discussion Papers.

Dobák, I. (2021). Thoughts on the evolution of national security in cyberspace. *Security and Defence Quarterly, 33*(1), 75–85. https://doi.org/10.35467/sdq/133154

Gates, R. M. (1996). *From the shadows: The ultimate insider's story of five presidents and how they won the Cold War*. Simon & Schuster.

Gomez del Prado J. L. (2010). *The Privatization of War: Mercenaries, Private Military and Security Companies*. Global Research.

Halperin, M. (1971). Why bureaucracies play games. *Foreign Policy,* (2), 70-93. https://doi.org/10.2307/1147860

Handel, M. (1984). Intelligence and the problem of strategic surprise. *Journal of Strategic Studies, 7*(3), 229–281.

Hastedt, G. (1985). Organizational foundations of intelligence failures. In A. Maurer, M. Tunstall & J. Keagle (Eds.), *Intelligence: Policy and Process* (pp. 148-160). Westview Press.

Hastedt, G. P. (2013). *Understanding the intelligence community*. Routledge.

Heuer, R. J. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence, Central Intelligence Agency. https://tinyurl.com/3stutep3

Jervis, R. (1985). Perceiving and coping with threats. *Political Psychology, 14*(3), 547–558.

Jervis, R. (2010). *Why intelligence fails: Lessons from the Iranian revolution and the Iraq war*. Cornell University Press.

Jordan, A. A., Taylor, Jr., W. J., Meese, M. J., & Nielsen, S. C. (2009). *American National Security*. Johns Hopkins University Press

Kahn, D. (1991). The Intelligence Failure of Pearl Harbor. *Foreign Affairs, 70*(5), 138–152. https://doi.org/10.2307/20045008

Kaldor, M. (2007). *Human security: Reflections on globalization and intervention*. Polity Press.

Kent, S. (1949). *Strategic Intelligence for American World Policy*. Princeton University Press

Kerbel, J. (2014). *The U.S. intelligence community's Kodak moment*. The National Interest. https://tinyurl.com/bddwrrhh

Latham, O. (2012). *Politicization of intelligence reporting: Evidence from the Cold War*. University of Warwick.

Levite, A. (1987). *Intelligence and strategic surprises*. Columbia University Press.

Liz-Rivas, L. (2023). La agresión sexual en los conflictos prolongados. Derecho de intervenir y obligación de proteger. *Cuadernos de Res Publica en derecho y criminología*, (1), 71–84. https://doi.org/10.46661/respublica.8044

Lowenthal, M. (2017). *The Future of Intelligence*. Polity Press

Lowenthal, Mark. M. (1985). The burdensome concept of failure. In A. C. Maurer et al. (Eds.), *Intelligence: Policy and Process*. Westview Press.

Luque-Juárez, J. M., Payá-Santos, C. A., & Arenas Morales, F. (2023). Contexto de las políticas de seguridad ciudadana. *Cuadernos de Res Publica en derecho y criminología*, (2), 69–82. https://doi.org/10.46661/respublica.8293

Marrin, S. (2004). Preventing intelligence failures by learning from the past. *International Journal of Intelligence and CounterIntelligence, 17*(4), 655–672. https://doi.org/10.1080/08850600490496452

Martino, L. (2024). *Cybersecurity in Italy. Governance, Policies, and Ecosystem*. Springer Nature. https://doi.org/10.1007/978-3-031-64396-5

Martino, L., & Merenda, F. (2021). Artificial intelligence: A paradigm shift in international law and politics? Autonomous weapon systems as a case study. In G. Giacomello, F. N. Moro & M. Valigi (Eds.). *Technology and International Relations* (pp. 89-107). Edward Elgar Publishing. https://doi.org/10.4337/9781788976077.00012

Mazurier, P. & Payá-Santos, C. A. (2018). *Amenazas híbridas: teoría de la hibridez y nuevo orden internacional*. Thomson Reuters Aranzadi.

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks Upon the United States*. W. W. Norton & Company.

NATO Strategic Communications Centre of Excellence (2023). *About strategic communications*. NATO. https://tinyurl.com/4r7ntzdv

Neri, M., Niccolini, F., & Martino, L. (2023). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information & Computer Security*. 32. https://doi.org/10.1108/ICS-05-2023-0084

Nester, W. (2001). *International relations: Politics and economics in the 21st century*. Wadsworth.

Paul, T. V. (1994). *Asymmetric Conflicts: War initiation by weaker powers*. Cambridge University Press. https://doi.org/10.1017/CBO9780511598746

Payá-Santos, C. A. (2023). El desempeño de la inteligencia en España en el ámbito público, empresarial y académico. *Revista Científica General José María Córdova*, *21*(44), 1029–1047. https://doi.org/10.21830/19006586.1222

Payá-Santos, C., & Delgado-Morán, J. J. (2017). Uncertainty of dimensional analysis of intelligence. *URVIO. Revista Latinoamericana de Estudios de Seguridad,* (21), 225–239. https://doi.org/10.17141/urvio.21.2017.2962

Payá-Santos, C., & Luque-Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. *Revista Científica General José María Córdova, 19*(36), 1121–1136. https://doi.org/10.21830/19006586.855

Phythian, M. (2013). Understanding the intelligence cycle. Routledge. https://doi.org/10.4324/9780203558478

Rovner, J. (2011). *Fixing the facts: National security and the politics of intelligence*. Cornell University Press. https://doi.org/10.7591/cornell/9780801448294.001.0001

Sanz-González, R., Luque Juárez, J. M., Martino, L., Liz Rivas, L., Delgado Morán, J. J., & Payá Santos, C. A. (2024). Artificial Intelligence Applications for Criminology and Police Sciences. *International Journal of Humanities and Social Science, (14)*2, 139-148. https://doi.org/10.15640/jehd.v14n2a14

Shulsky, A. N., & Schmitt, G. J. (2002). *Silent Warfare: Understanding the World of Intelligence*. Potomac

Sims, J. (1995). What is Intelligence? Information for Decisionmaking. In R. Godson, E. R. May, & Gary Schmitt (Eds.). *U.S. Intelligence at the Crossroads: Agendas for Reform* (pp. 3-17). National Strategy Information Center Inc.

Snyder, J. (1991). *Myths of empire: Domestic politics and international ambition*. Cornell University Press.

US Senate Committee on Homeland Security and Governmental Affairs & Committee on Rules and Administration. (2021). *Examining the U.S. Capitol attack: A review of the security, planning, and response failures*. United States Senate.

Vanhanen, T. (2000). A new dataset for measuring democracy, 1810-1998. *Journal of Peace Research, 37*(2), 251–265. https://doi.org/10.1177/0022343300037002008

Warner, M. (2002). Wanted: A Definition of Intelligence. *Studies in Intelligence* (46), 1-13. https://tinyurl.com/yypcxb98

Wilensky, H. L. (1967). *Organizational Intelligence: Knowledge and Policy in Government and Industry*. Basic Books.

Wohlstetter, R. (1962). *Pearl Harbor: Warning and decision*. Stanford University Press. https://doi.org/10.1515/9781503620698

Wyss, M. (2024). *The October 7 attack: An assessment of the intelligence failings*. *CTC Sentinel, 17*(9), 1-9.

Zegart, A. (2007). *Spying blind: The CIA, the FBI, and the origins of 9/11*. Princeton University Press. https://doi.org/10.2307/j.ctt7s790