LUISS

Department of Political Science

Master's Degree in International Relations

Chair of Crisis Communication

From Warning to Influence:
Intelligence in Crisis Anticipation and Decision-Making

A Comparative Case Study Approach

SUPERVISOR

Prof. Emiliana De Blasio

CO-SUPERVISOR

Prof. Marco Simoni

CANDIDATE

Nicola Vamerali

657672

Academic Year 2024/2025

Index

Introduction

Over the past two decades, the international system has been shaped by a series of crises that are more frequent, interconnected, and diffuse than those of earlier periods. Such transboundary shocks – pandemics, hybrid aggression, cyber operations against critical infrastructure, energy and financial disruptions, and climate-related emergencies – rarely fit neatly within traditional risk compartments. They develop across sectors and jurisdictions, compress decision time, and expose the limits of reactive governance. This context has intensified the demand for anticipatory capabilities: the capacity not only to detect deterioration early but also to translate foresight into preventive or mitigative action. Against this backdrop, intelligence is increasingly scrutinized not merely as a repository of secrets or a producer of retrospective situational awareness, but as an informational and strategic instrument capable of enabling earlier, better, and safer decisions.

This thesis builds on intelligence in its broad functional sense and examines its specific contribution to the anticipation of crises. It treats anticipation as a spectrum that runs from horizon scanning and weak signal detection to indications and warning, estimative judgement, and the use of tripwires to trigger predefined policy options. The central claim is that intelligence, when processed, communicated, and received under the right conditions, can shift authorities from a posture of reaction to one of prevention or pre-emption of harm. Yet, this potential is mediated by political incentives, institutional frictions, ethical constraints, and the perennial risk that closer proximity to power may corrode objectivity.

Accordingly, the study is guided by the following research questions: How does intelligence operate in the anticipation of crises, and what ethical and operational challenges arise when elevating intelligence from a marginal advisory role to a more influential and active position in decision-making? Is there a plausible future in which the figure of the intelligence practitioner replaces the decision-maker? These questions embed both an explanatory and a normative dimension. Explanatorily, the inquiry seeks to identify the mechanisms by which intelligence produces anticipatory value and the conditions under which that value is, or is not, converted into policy action. Normatively, it interrogates the boundary between influence and politicization, and the trade-offs between timely warning, proportional response, and democratic safeguards.

The working hypothesis is twofold. First, intelligence does possess appropriate tools in order to achieve anticipation. Second, the impact of these tools on real decisions remains uneven because of cultural skepticism toward probabilistic warnings, political risk-aversion in the face of false-alarm costs, organizational inertia, and ethical constraints surrounding intrusive collection or pre-emptive action. In short, intelligence can create decision advantage, but cultural, political, and ethical obstacles limit the degree to which that advantage is recognized, trusted, and operationalized.

Methodologically, the thesis employs a comparative qualitative design combining process-tracing within emblematic cases and cross-case comparison. Four contemporary episodes are selected for their variation in context and outcome and for their relevance to warning and policy uptake: the 9/11 attacks, the 2022 Russian invasion of Ukraine, the October 7 Hamas incursion in 2023, and the 2021 U.S. withdrawal from Afghanistan. The analysis triangulates scholarly literature, official and parliamentary inquiries, institutional documents, and credible open-source reporting. Indeed, given the inherent opacity of intelligence work, the study is constrained by limited access to classified materials; wherever possible, it mitigates this by prioritizing convergent findings across independent sources and by making inferential steps explicit. The temporal scope focuses on the period 2001-2024, while drawing selectively on earlier precedents where they illuminate enduring mechanisms of warning success or failure. Ethical considerations are vital: the discussion weighs the duty to warn against risks of alarmism, rights-infringing measures, and politicization.

Conceptually, the thesis advances three contributions. First, it systematizes the anticipatory instruments of intelligence and links each element to concrete policy needs related to decision-making. Second, it proposes a three-dimensional lens for assessing warning effectiveness that distinguishes analytical quality, communication and timing, and political receptivity. This interpretative angle helps locate where failures occur: analysts may be broadly correct yet unheard; messages may be clear yet ill-timed; leaders may be attentive yet constrained by incentives that penalize early action. Third, it elaborates the ethics of warning, clarifying thresholds for issuing alerts under uncertainty, proportionality in preventive measures, and the institutional guardrails required to sustain both effectiveness and legitimacy.

The question of elevating intelligence to a more central role in decision-making is treated with deliberate caution. On the one hand, earlier and more structured engagement with policy processes

– through joint exercises, agreed probability yardsticks, and pre-negotiated response playbooks – can increase the chances that warning alters behavior before the point of no return. On the other hand, over-integration may fuel role confusion, self-censorship, and the subtle pressures that have historically produced politicization. The thesis therefore tests not a binary choice between "unbiased oracle" and "co-decider," but a set of institutional designs that seek to preserve analytic autonomy while raising practical influence: for example, formal triggers linked to indicator thresholds, protected dissent channels, and reciprocal accountability whereby leaders must record and justify choices to accept or disregard high-confidence warnings.

In so doing, the structure of the thesis reflects this logic of inquiry. Chapter 1 clarifies core concepts for the ultimate understanding of the work – crisis typologies and dynamics, definitions of intelligence, predictive models and warning tools, and baseline conditions for effective warning. Chapter 2 investigates why intelligence is often an "unheard voice," analyzing the policy-intelligence gap, cognitive and organizational biases that suppress comprehension, the risks and mechanisms of politicization, and the ethical dilemmas that arise around the effort of acting. Significantly, Chapter 3 applies the framework to four case studies, tracing how anticipatory signals were generated, communicated, received, and acted upon, and drawing comparative lessons about the determinants of success and failure. Lastly, Chapter 4 turns to the future: it identifies contexts in which elevating intelligence would make a difference, examines new upcoming challenges, and formulates practical guidelines for fostering a concrete culture of anticipation.

In sum, this thesis explores how intelligence can move from warning to influence in anticipating and navigating crises. It argues that intelligence can provide genuine decision advantage, particularly in complex, ambiguous, high-impact environments, but that realizing this potential depends on reshaping the relationships, languages, and rules that connect analysts to decision-makers. Elevation of intelligence is thus reasonable where it improves public safety and reduces strategic surprise, and only to the extent that it remains tethered to analytic autonomy, legal bounds, and ethical restraint.

1. Anticipating Crises: Definitions, Models, and Theoretical Foundations

1.1 Defining "crisis": nature, typologies, and dynamics

In scholarly literature, a crisis is typically understood as an acute disruption or turning point that poses a severe threat to fundamental values or life-sustaining systems, and requires urgent decision-making under conditions of deep uncertainty. Classic definitions emphasize three structural elements: threat, urgency, and uncertainty. For example, Rosenthal et al. define a crisis as "a serious threat to the basic structures or fundamental values and norms of a social system, which – under time pressure and highly uncertain circumstances – necessitates the making of critical decisions"[1]. In other words, a crisis confronts leaders with high-stakes threats that demand immediate action despite incomplete information. As Hewitt adds, crises often have an "un-ness" quality – unfolding as unexpected, unpleasant events that are unprecedented in their implications and almost unmanageable[2]. These characteristics make crises extremely challenging to handle, as officials must respond quickly to contain harm while coping with ambiguity and stress.

Importantly, not all crises erupt in the same manner. Researchers distinguish between sudden crises and creeping or slow-burning crises as theoretical ideal types[3]. Sudden crises (also called fast-burning crises) are those that strike abruptly with little warning and evolve rapidly. Their onset is severe and decisive, as seen in events like natural disasters, terrorist attacks, or industrial accidents that unfold over hours or days.[4] Such crises demand rapid intervention and high-speed decision-making; if handled successfully the acute phase may pass quickly (albeit often leaving aftermath issues), whereas failure to respond can result in catastrophic loss. In contrast, slow-burning crises (often termed smoldering, creeping, or slow-onset crises) develop progressively over an extended period. Indeed, this type of crisis emerges gradually and then dissipates slowly rather than reaching

---

[1] Uriel Rosenthal, Michael T. Charles, and Paul 't Hart, *Coping with Crisis: The Management of Disasters, Riots, and Terrorism* (Charles C. Thomas, 1989).

[2] Kenneth Hewitt, *Interpretations of Calamity: From the Viewpoint of Human Ecology* (London: Allen & Unwin, 1983).

[3] Arjen Boin, Magnus Ekengren, and Mark Rhinard, "Hiding in Plain Sight: Conceptualizing the Creeping Crisis," *Risks, Hazards & Crisis in Public Policy* 11, no. 2 (2020): 116–138.

[4] Paul 't Hart and Arjen Boin, "Between Crisis and Normalcy: The Long Shadow of Post-Crisis Politics," in *Managing Crises: Threats, Dilemmas, Opportunities*, ed. Uriel Rosenthal, Arjen Boin, and Louise K. Comfort (Charles C. Thomas, 2001).

a definitive resolution, with a prolonged incubation phase during which warning signs accumulate[5]. Examples include climate change, protracted financial instabilities, or a public health threat that builds over months. Boin et al. conceptualize a creeping crisis as a threat to widely shared societal values or critical systems that grows over time and space, often foreshadowed by weak precursor events[6]. Because they arise slowly, creeping crises may initially receive inconsistent attention and inadequate responses from authorities, only culminating in a critical point following a protracted period of escalation. Managing such a crisis requires sustained attention and long-term commitment, yet paradoxically these crises are harder to galvanize action around due to their ambiguous, diffuse nature.

Beyond the fast-vs-slow distinction, scholars have identified other crisis types to capture different dynamics. Among them, total crises represent a crucial category. This term refers to crises that are systemic in scope: they threaten entire systems or societies rather than a single domain. Systemic crises often cut across geographical or sectoral boundaries (sometimes called transboundary crises) and involve major failures. For example, a global financial meltdown, a pandemic, or an energy grid collapse can be viewed as systemic crises – they affect multiple countries or critical sectors simultaneously and endanger the basic functioning of society at large[7]. Such crises are typically complex and interconnected, exhibiting high ambiguity and requiring coordinated responses on many levels[8]. Contemporary global crises – most notably the COVID-19 pandemic and climate change – are illustrative of phenomena characterized by high complexity, interpretative ambiguity, transnational implications, and gradual escalation. These features emphasize their deeply systemic nature and the extended temporal horizons over which they unfold. In sum, crises can take many forms – from sudden shocks to slowly-escalating "creeping" problems to far-reaching systemic disruptions – but all share the core features of looming threat, time pressure, and uncertainty.

Regardless of type, crises tend to induce highly dynamic and volatile situations. In a crisis, normal routines interrupt and actors face stress, confusion, and often need to operate under conditions of information vacuum. Uncertainty is pervasive: leaders may have an incomplete or misleading

[5] Boin, Ekengren, and Rhinard, "Hiding in Plain Sight," 122.
[6] Ibid., 116–138.
[7] Didier Wernli et al., "Understanding and Governing Global Systemic Crises in the 21st Century: A Complexity Perspective," *Global Policy* 14, no. 2 (2023): 207–28.
[8] David Omand, *How to Survive a Crisis: Lessons in Resilience and Avoiding Disaster* (London: Penguin Random House, 2023).

picture of what is happening, as critical facts can be unavailable or obscured amid the chaos[9]. Meanwhile, the need for urgency means that decisions – sometimes life-and-death in consequence – must be made faster than one would like, often with inadequate deliberation[10]. Another dynamic element is surprise: even in slow-developing crises, there can be triggering moments that catch actors off guard. However, it is worth noting the difference between situations of total surprise and of incomplete information. Indeed, the notion of surprise presupposes the existence of unknown possibilities, and therefore of ignorance. It represents the factor introducing the potential for genuine surprise, as it implies that certain scenarios lie entirely outside the scope of prior awareness. Within the rational choice paradigm, such ignorance is sufficient to explain the onset of crises, as it allows for the sudden emergence of unforeseen developments that demand immediate attention[11].

Crises also evolve through phases – typically an onset (or detection) phase, an acute response phase, and a post-crisis or recovery phase. The transition between these stages is not always definite, and misjudging the phase (e.g. failing to recognize that an emergency has begun, or prematurely thinking a crisis is "over") can lead to missteps. Furthermore, crises have feedback dynamics: initial responses (or non-responses) by decision-makers can either mitigate the situation or exacerbate it. A delayed or inadequate early reaction may allow a crisis to spiral, whereas effective early interventions can successfully contain the damage[12]. Finally, crises are social processes; they involve perception and interpretation. How leaders and the public perceive and frame a situation can influence the trajectory. A slowly-building problem might be ignored until a focusing event forces redefinition as a crisis. Overall, understanding these dynamics – the rapid tempo of decision-making, the information ambiguity, and the potential for escalation or de-

[9] Sniazhana Sniazhko, "Uncertainty in Decision-Making: A Review of the International Business Literature," *Cogent Business & Management* 6, no. 1 (2019).
[10] Lin-Xiu Hou et al., "Decades on Emergency Decision-Making: A Bibliometric Analysis and Literature Review," *Complex Intelligent Systems* 7 (2021): 2819–2832.
[11] Roger D. Congleton, "The Political Economy of Crisis Management: Surprise, Urgency, and Mistakes in Political Decision Making," in *The Dynamics of Intervention: Regulation and Redistribution in the Mixed Economy* (Emerald Group Publishing, 2004), 183–203.
[12] Uriel Rosenthal and Alexander Kouzmin, "Crises and Crisis Management: Toward Comprehensive Government Decision Making," *Journal of Public Administration Research and Theory* 7, no. 2 (1997): 277–304.

escalation – is crucial for anticipating crises and thus demonstrating readiness through effective responses.

1.2 Defining "intelligence": functions, cycle, and key actors

It is especially in the event of a crisis that information becomes crucial in order to act. Nonetheless, raw information is often misleading or pointless, as only once processed assumes value. In other words, only when information turns into intelligence. Several scholars and practitioners have tried to give a more or less objective definition of intelligence. However, often the challenge has been to understand the crucial role of intelligence both in the public and private sector. Therefore, definitions such as Warner's[13], stating that "Intelligence is secret, state activity to understand or influence foreign entities" seem only partially correct. Thus, Zegart[14] proposes a much more applicable concept of intelligence, assessing it as "information that gives policymakers an advantage over their adversaries". This definition highlights the true essence of intelligence, notably its ability to provide an advantage. The concept is also nicely reflected in Sims' work[15], which defines decision advantage as the chance for decision-makers to outperform adversaries by taking crucial decisions with a higher level of certainty. Indeed, according to him, intelligence is precisely what allows you to do so in a competitive scenario. This definition embraces the evolving field of private sector intelligence by considering a hypothetical decision maker as both a government policy maker and a CEO. Despite the debate, what is certain is that intelligence represents the result of a complex information processing scheme. This mechanism is conceptualized as intelligence cycle and includes the phases of direction, collection, collation, assessment, and dissemination – that we will discuss further later in the work. Sims successfully identifies the main steps in his definition. The intelligence nature of being a process is also described by Omand[16], who frames the matter as a "process in which decision-making is improved through understanding and situational awareness". Similarly, this broader conception is backed by

[13] Michael Warner, "Wanted: A Definition of Intelligence," *Studies in Intelligence* 46, no. 3 (2002): 21.
[14] Amy B. Zegart, *Spies, Lies, and Algorithms: The History and Future of American Intelligence* (Princeton: Princeton University Press, 2022), 8, 79.
[15] Jennifer E. Sims, *Decision Advantage: Intelligence in International Politics from the Spanish Armada to Cyberwar* (Oxford: Oxford University Press, 2022).
[16] David Omand, *How Spies Think* (New York: Penguin Random House, 2020).

Gill and Phytian. Additionally, they recognize that "a wide range of sub-state actors – political, commercial and criminal – also perceive a need to collect and analyze intelligence […] In today's world, this need even extends to sport teams"[17]. Within this context, the sphere of intelligence consumers is broadened, to encompass all modern actors operating not only with closed-access information but also and increasingly with open sources. A detachment from fallacious definitions limiting intelligence as a state prerogative is thus possible but not always necessary.

In the case of national security and organizational decision-making, intelligence refers to the process and product of collecting and analyzing information to support decision-makers in understanding complex situations, threats, and opportunities. A concise official definition from the U.S. Office of the Director of National Intelligence describes intelligence as "information gathered within or outside the U.S. that involves threats to our nation, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; and any other matter bearing on the U.S. national or homeland security"[18]. In essence, intelligence is knowledge and it is both a process and a product, meaning concrete reports or assessments delivered to leaders. Unlike raw information, intelligence has been evaluated for reliability and significance. The fundamental purpose of intelligence is to reduce uncertainty for decision-makers, especially on matters of security, defense, foreign policy, or competitive strategy[19]. As such, good intelligence can successfully provide decision advantages: warning of an emerging crisis, insight into an opponent's intentions, or factual basis for policy choices. It must sometimes be obtained clandestinely or through specialized means, since the most critical information is not usually freely available. Intelligence thus has a secretive aspect – involving espionage, surveillance, or data collection that rivals and challengers would prefer to conceal. However, intelligence is not exclusively secret: it increasingly incorporates open sources and advanced analytics (see discussion of OSINT in Section 1.3).

Overall, as intelligence is defined by its function (informing high-stakes decisions) rather than by any single method or type of data, we will now delve deeper into this aspect. Intelligence activities

---

[17] Peter Gill and Mark Phythian, *Intelligence in an Insecure World*, 3rd ed. (Cambridge: Polity Press, 2019).
[18] Office of the Director of National Intelligence (ODNI), "What Is Intelligence?", n.d., *https://www.dni.gov/index.php/what-we-do/what-is-intelligence*.
[19] Mandeep K. Dhami et al., "Improving Intelligence Analysis with Decision Science," *Perspectives on Psychological Science* 10, no. 6 (2015): 753–757.

are commonly divided into two levels corresponding to the scope of decisions they support. Strategic intelligence is the highest level, concerning broad, long-term issues of national policy, security, and strategy. The U.S. Department of Defense's (DoD) definition holds that strategic intelligence is "intelligence required for the formulation of strategy, policy, and military plans and operations at national and theater levels"[20]. In practice, strategic intelligence provides the "big picture" needed by top leaders – heads of state, senior policymakers, generals – to make informed decisions about war and peace, international relations, or major corporate direction. It deals with questions like adversaries' intentions, emerging global trends, or assessments of risks and opportunities in the environment.

Conversely, tactical intelligence is the most granular level, directly supporting immediate actions on the ground. In the military domain, tactical intelligence is the information a field commander or unit needs for combat operations in a specific locale – such as real-time intelligence on enemy forces in a battle, terrain and weather details, or imminent threats in an area of operations. More in general, the U.S. DoD defines it as "intelligence that is required for planning and conducting tactical operations"[21]. It is often time-sensitive and detail-rich, dealing with "here and now" questions to allow rapid decision and engagement. In policing, a rough analogue would be actionable tips that enable an arrest or prevent a crime about to occur. Tactical intelligence must be delivered quickly and be highly actionable, whereas strategic intelligence can be more analytic and forward-looking[22]. Both levels are interrelated: effective tactical intel can feed upward (as many strategic insights emerge from aggregated tactical reports), and strategic guidance flows downward to shape collection priorities at operational and tactical levels. Different intelligence organizations or units often specialize in one of these levels, though coordination among them is essential so that information flows properly. It is worth clarifying that for the sake of our analysis, closely related to the warning capabilities of intelligence, we will mainly refer to intelligence embracing its strategic purpose.

---

[20] U.S. Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: DoD, 8 November 2010), s.v. "Strategic Intelligence."

[21] U.S. Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: DoD, 8 November 2010), s.v. "Tactical Intelligence."

[22] Lewis Sage-Passant, "The Security Intelligence Services of the Private Sector" (Loughborough University, 2023).

At this point it becomes crucial to understand how information is transformed into actionable intelligence. This process is commonly described as a cycle with several key stages through which practitioners operate. While models vary slightly, a classic formulation is a five-step (or six-step) cycle: direction, collection, collation, assessment, and dissemination (with feedback as a looping mechanism that also allows to adjust direction)[23]. It begins with direction (or planning): decision-makers and intelligence managers establish priorities and requirements, asking questions that the intelligence apparatus needs to answer[24]. These requirements drive the collection phase, in which agencies gather raw information from various sources[25]. Collection methods span a wide range of "INTs," or intelligence disciplines: human intelligence (HUMINT) usually from spies or informants, signals intelligence (SIGINT) from intercepted communications, imagery intelligence (IMINT) from satellites or drones, open-source intelligence (OSINT) from public media and data, and others[26]. Each provides pieces of the puzzle. Once collected, the raw data undergo collation, through which all collected data coming from different sources is harmonized with the scope of verifying information and thus rating sources[27]. It may also involve translating foreign documents, decoding signals, data-mining large datasets, or filtering relevant bits from masses of information. The goal is to make the right information usable for analysis.

Next comes assessment (sometimes combined with processing and thus labeled "processing and analysis" or called production). Here, skilled analysts put pieces together, and interpret meanings – producing assessments, estimates, or final reports that address the initial questions. Assessment is at the heart of the intelligence function; it transforms disparate data into meaningful insight by applying contextual knowledge and analytic reasoning[28]. Through this step, intelligence teams are able to spot missing information by going beyond mere data. That is why critical thinking and creativity, alongside high capacity of judgement, often reward practitioners and their (theoretically) unbiased nature. Finally, the dissemination stage delivers the finished intelligence to the consumers

---

[23] Ibid.
[24] Mark Phythian, ed., *Understanding the Intelligence Cycle* (London: Routledge, 2013).
[25] Arthur S. Hulnick, "Intelligence Theory: Seeking Better Models," in *Understanding the Intelligence Cycle*, ed. Mark Phythian (London: Routledge, 2013), 149–160.
[26] Phythian, *Understanding the Intelligence Cycle.*
[27] John Hughes-Wilson, *Military Intelligence Blunders and Cover-Ups* (London: Robinson, 2004), 4–5.
[28] Mark Phythian, "Intelligence Analysis Today and Tomorrow," *Security Challenges* 5, no. 1 (2009): 67–83.

in a timely manner[29]. Dissemination can take many forms: written intelligence briefs, situation reports, oral briefings, podcasts, even phone calls etc., depending on the urgency and preference of the recipients[30]. Ideally, the process does not end there: a feedback loop ensues, wherein decision-makers might ask new questions or clarify requirements based on the intelligence, thus restarting the cycle. In practice, the intelligence cycle is not strictly linear – multiple activities often happen concurrently (collection and analysis run simultaneously on different issues), and the steps blend together in a continuous effort[31]. Nonetheless, the cycle model is a useful conceptual framework highlighting that intelligence is not a single event but an ongoing process aimed at meeting decision-makers' needs.

In the case of intelligence, decision-makers tend to be mostly governments. Indeed, traditionally, intelligence has been the domain of government agencies. Virtually every nation has established public intelligence services to safeguard national security and inform policy. For example, the United States Intelligence Community (USIC) is a federation of 18 government agencies and organizations (such as the CIA, NSA, DIA, FBI, and military intelligence units) working both independently and jointly to conduct intelligence activities ranging from foreign espionage to domestic counterintelligence[32]. These agencies collect secret information, analyze international developments, and brief policymakers from the President downward. Other countries have their own structures: the UK's intelligence community includes MI6 (foreign secret intelligence service), MI5 (domestic security intelligence), Government Communications Headquarters "GCHQ" (signals intelligence), and others; France relies on the Direction générale de la Sécurité extérieure "DGSE" and Direction Générale de la Sécurité Intérieure "DGSI"; Russia holds the same distinction with SVR and FSB. While the core functions (collection, analysis, covert operations, counter-intelligence) have parallels across nations, there are differences in how intelligence is organized and overseen. Some democracies separate domestic and foreign intelligence into different agencies, whereas others have more integrated services. National context also affects intelligence culture and methods – for instance, legal constraints and oversight in liberal

[29] Federation of American Scientists (FAS), "The Intelligence Cycle", n.d., https://irp.fas.org/cia/product/facttell/intcycle.htm.
[30] Sage-Passant, "The Security Intelligence Services of the Private Sector".
[31] Arthur S. Hulnick, "What's Wrong with the Intelligence Cycle," *Intelligence and National Security* 21, no. 6 (2006): 959–979.
[32] Office of the Director of National Intelligence (ODNI), "Members of the IC," n.d.

democracies versus more unchecked mandates in authoritarian regimes[33]. That said, in all contexts the primary actors of intelligence are those governmental units tasked with gathering sensitive information and advising the state's decision-makers.

In recent decades, however, private sector intelligence has grown in prominence. Therefore, despite this research will mainly develop on state activity and public intelligence, it is worth spending a few words for this rising branch. Private companies and organizations increasingly employ intelligence-like functions for their own security and strategic needs. This includes corporate security intelligence units, risk assessment firms, and consultancies that provide geopolitical or market intelligence. Such private intelligence entities perform analyses on terrorism, cyber threats, political instability, competitive business threats, and other issues that can affect companies' operations and assets[34]. They often hire former government intelligence professionals or train analysts in similar tradecraft. Private sector intelligence (PSI) operations differ in that they primarily use open sources (information lawfully and publicly available) and their goals are primarily business-centric rather than national defense[35]. For example, a multinational corporation might have an in-house intelligence team monitoring political violence in countries where it has plants, or tracking activist groups that could target the company's facilities. The methods used by PSI overlap with classical intelligence but tend to rely heavily on OSINT (including social media analysis) – in fact, it is estimated that open sources account for roughly 90% of the information collected in private sector intelligence[36]. Private intelligence firms (sometimes called OSINT vendors or risk advisory firms) now sell analysis to clients on topics like cybersecurity threats, kidnapping risks, or regulatory changes.

Differences across national contexts are also evident in the role of intelligence in policy. Some countries institutionalize strong intelligence-policy relations (e.g. the U.S. President receives a daily intelligence briefing), whereas in other states intelligence services might have less direct

---

[33] Michael M. Andregg and Peter Gill, "Comparing the Democratization of Intelligence," *Intelligence and National Security*29, no. 4 (2014): 487–497.

[34] Maria A. Robson Morrow, "Private Sector Intelligence: On the Long Path of Professionalization," *Intelligence and National Security* (2022).

[35] Sage-Passant, "The Security Intelligence Services of the Private Sector".

[36] Stevyn D. Gibson, "Exploring the Role and Value of Open Source Intelligence," in *Open Source Intelligence in the Twenty-First Century*, ed. Christopher Hobbs, Matthew Moran, and Daniel Salisbury (London: Palgrave Macmillan, 2014), 12.

influence or face more skepticism from leaders. The actors involved in producing and consuming intelligence thus range from government agencies (military, civilian, law enforcement intelligence units) to private sector analysts, and even non-governmental organizations in some humanitarian or conflict early-warning contexts. Each actor operates under its own mandates and constraints. Public agencies often have legal authority to collect classified information (including covertly), but they must navigate oversight and political expectations. Private intelligence actors lack government powers but can be more flexible in using open information and innovative analytic tools[37]. In summary, while "intelligence" historically refers to government secret services, today it encompasses a broader ecosystem of public and private actors all engaged in information collection and analysis to anticipate risks and inform decisions.

1.3 Predictive intelligence: models and warning tools

Now that we have introduced the fundamentals of both crises and intelligence, we are going to see in detail how these two fields are strictly related. A critical function of intelligence – and central theme of this thesis – is anticipating crises before they fully unfold. This is often termed warning intelligence or predictive intelligence. The idea is to detect emerging threats or instabilities early enough that decision-makers have time to prevent or mitigate disaster. Ever since strategic surprises like Pearl Harbor (1941) or the Yom Kippur War (1973), the intelligence community has devoted great effort to improving its early warning capabilities[38]. Warning intelligence differs slightly from basic intelligence: it is inherently forward-looking and probabilistic, dealing in indications and estimative judgments about the future[39]. To conduct predictive intelligence, analysts use a variety of models and tools designed to flag potential crises in advance. Key concepts in the warning analytic arsenal include indicators, tripwires, weak signals, and structured analytical techniques for hypothesis testing and scenario exploration.

---

[37] Stephanie Lizzo, "Intelligence Redefined: The Interplay of Private Companies and National Security," *Journal of International Affairs* (Columbia University), 2024, *https://jia.sipa.columbia.edu/news/intelligence-redefined-interplay-private-companies-and-national-security*.

[38] Erik J. Dahl, "Warning of Terror: Explaining the Failure of Intelligence Against Terrorism," *Journal of Strategic Studies*28, no. 1 (2005).

[39] Cynthia M. Grabo and Jan Goldman, *Handbook of Warning Intelligence: Complete Declassified Edition* (Lanham, MD: Rowman & Littlefield, 2015).

An indicator is an observable sign or data point that is hypothesized to correlate with escalating risk or a particular adversary activity. Analysts often develop indicators lists for specific contingencies – for example, indicators of an impending military invasion might include unusual troop movements, certain logistical measures, high-level command activity, and aggressive rhetoric. These serve as a systematic monitoring framework: by tracking whether indicators are lighting up, intelligence can assess how likely a crisis is becoming[40]. In the Cold War, the practice of Indications & Warning (I&W) was institutionalized, with analysts watching a dashboard of indicators for signs of surprise attack[41]. A tripwire is closely related: it usually refers to a specific indicator or threshold that, if tripped (i.e. crosses a set value), triggers a warning or predefined response. For instance, a government might declare that if a pandemic's infection rate exceeds a certain number, it will trigger a state of emergency – the infection rate indicator in this case acts as a tripwire for crisis response[42]. Tripwires can also be covert, such as clandestine sensors or human sources set to alert if an adversary does X or Y. Together, indicators and tripwires form an advance warning system: they translate diffuse information into concrete signals for decision-makers. As one scholar's analysis notes, "Indicators are at the heart of the warning data collection process, providing a systematic framework for monitoring the situation and creating an alert.[43]" By pre-defining which developments would be alarming, leaders can avoid being caught completely off-guard – assuming, of course, that those developments are reliably detected.

Unfortunately, though, not all crises come with clear, known indicators. Often the early signs of trouble are ambiguous whispers rather than loud alarm bells. The concept of weak signals refers to those subtle clues and preliminary anomalies that may foreshadow a coming disruption, though their relevance may only be recognized in hindsight[44]. H. Igor Ansoff, who introduced the term in a business context, suggested paying attention to weak signals to avoid strategic surprise[45]. In

---

[40] Grabo and Goldman, *Handbook of Warning Intelligence*, chap. 7.

[41] John A. Gentry and Joseph S. Gordon, *Strategic Warning Intelligence: History, Challenges, and Prospects* (Washington, DC: Georgetown University Press, 2019).

[42] Sage-Passant, "The Security Intelligence Services of the Private Sector".

[43] Peterlinus O. Odote, "Role of Early Warning Systems in Conflict Prevention in Africa: Case Study of the Ilemi Triangle" (PhD diss., University of Nairobi, 2016).

[44] Humbert Lesca and Nicolas Lesca, *Strategic Decisions and Weak Signals: Anticipation for Decision-Making* (John Wiley & Sons, 2014).

[45] H. Igor Ansoff, "Managing Strategic Surprise by Response to Weak Signals," *California Management Review* 18, no. 2 (1975): 21–33.

national-security warning, weak signals are the scattered pieces of evidence that something is brewing – a fragment of chatter, a minor incident, an emerging local conflict – which by themselves are easy to dismiss as irrelevant. The difficulty is that these signals are usually buried in a lot of noise[46]. Scholars therefore argue that in order to identify such weak signals, horizon scanning techniques are required: casting a wide informational net, looking at outliers and novel data sources, and employing creative thinking to imagine what those faint signals could imply. Intelligence agencies increasingly use data science and machine learning to help filter signal from noise – for example, monitoring social media or news patterns worldwide in real time for anomalies that might indicate an emerging crisis or a threat possibly developing even far away in the future[47]. Horizon scanning units might look for early signs of political instability (changes in tone of online discourse, unusual protest activity), public health concerns (upticks in disease symptoms reported on forums), or financial stress (sudden capital outflows). The aim is to catch the rise of trouble before they crescendo. This approach is inherently difficult, since by definition a weak signal is not a proven predictor, and many turn out to be false alarms. Nevertheless, developing methodologies to exploit weak signals is seen as crucial for dealing with today's hybrid threats and complex systemic risks.

Beyond monitoring indicators, predictive intelligence relies on structured analytical methods to imagine and evaluate future scenarios. One well-known tool is the Analysis of Competing Hypotheses (ACH), developed by Richards Heuer at the CIA. ACH is designed to overcome cognitive biases when weighing evidence about uncertain situations. Using ACH, an analyst explicitly lays out multiple alternative hypotheses or explanations for what might be happening or what might occur, and then systematically tests each hypothesis against the available evidence[48]. The idea is to avoid jumping to conclusions by forcing consideration of multiple possibilities in parallel. For example, in a warning context, hypotheses could be "Country X is intending to launch a surprise attack" vs. "Country X's military movements are a bluff" vs. "They are defensive." Analysts list indicators or evidence for and against each, and reject hypotheses that are contradicted by the majority of evidence. ACH encourages a refutational approach (eliminate hypotheses that

[46] Gentry and Gordon, *Strategic Warning Intelligence*.
[47] Ibid., 202.
[48] Richards J. Heuer Jr., *Psychology of Intelligence Analysis* (Center for the Study of Intelligence, CIA, 1999).

do not fit) rather than confirmation-seeking. By doing so, it helps highlight which scenario remains most consistent with the facts, hopefully leading to a more accurate warning judgment[49]. ACH and similar structured analytic techniques (SATs) – including "devil's advocacy", and quality of information checklists – have been increasingly taught in intelligence communities to improve predictive analysis. They add methodological rigor to thinking about the future, attempting to make analytic reasoning as explicit and evidence-based as possible.

Another critical methodology used in this field is scenario analysis or scenario building. This is a foresight technique in which analysts construct a set of plausible future scenarios (stories or sketches of how the future could unfold) to encompass uncertainty and challenge assumptions[50]. Rather than trying to predict a single outcome, scenario analysis explores a range of outcomes – e.g., best case, worst case – to ensure preparedness for each. In early warning, scenario exercises might ask, "How could this political crisis evolve over the next year? Let's imagine Scenario A: peaceful resolution, Scenario B: escalating protests but without leading to a regime change, Scenario C: coup d'état and civil war." By fleshing out these narratives and their indicators, intelligence officers clarify which developments to watch for that would steer reality toward one scenario or another. Scenario planning, pioneered in the corporate world by Shell during the 1970s, emphasizes preparing for multiple plausible futures rather than predicting a single outcome[51]. It encourages thinking about low-probability but high-impact outcomes that might otherwise be dismissed. War-gaming and simulations are related tools – they allow analysts and decision-makers to role-play scenarios (e.g., simulate a cyberattack on national infrastructure) to see how adversaries and our own side might behave. Such simulation exercises not only test crisis response plans but can also reveal indicators and branch-points for early warning. For instance, a simulation of a regional conflict might highlight that the adversary would likely prepare by doing X, Y, Z – which then become concrete indicators to monitor in the real world. These models, while never perfect and sometimes considered distinct from classic intelligence practices[52], help to anticipate possible futures in a systematic way.

---

[49] Ibid.
[50] Randolph H. Pherson and Richards J. Heuer Jr., *Structured Analytic Techniques for Intelligence Analysis*, 3rd ed. (CQ Press, 2020), 272–276.
[51] Pierre Wack, "Scenarios: Uncharted Waters Ahead," *Harvard Business Review* 63, no. 5 (1985): 72–89.
[52] Sage-Passant, "The Security Intelligence Services of the Private Sector".

Indeed, the rise of open-source intelligence (OSINT) and big data analytics has significantly expanded the toolkit for predictive intelligence. Traditionally, intelligence communities focused on secret sources, but now OSINT has gained respect as a rich source of indicators and context. In an era of global connectivity, valuable warning insights can often be gleaned from open data if one has the tools to aggregate and analyze it in real time. For example, social media platforms have on-the-ground eyewitness reports and local sentiment data that, if mined properly, can give early clues of emerging crises (such as an outbreak of violence or a sudden migration flow). Șușnea's study [53] described a real-time social media monitoring method as an OSINT early-warning platform: by capturing the immediate, unfiltered reactions of people during unexpected events, such a system can provide a portrait of a developing crisis and even help anticipate its evolution. The vast volume of social data requires "intelligent technologies" (like AI algorithms for pattern recognition and data mining) to filter relevant signals. For instance, during an earthquake or natural disaster, spikes in certain keywords or geotagged posts can indicate the severity and locations of damage in advance of official reports and therefore spread awareness. Even in disease outbreak monitoring, researchers now rely on web search trends and social media mentions of symptoms as early indicators of an epidemic (sometimes providing warning days before public health surveillance catches up). Big data analytics also enable trend analysis on a scale previously impossible: by crunching years of global data on conflicts, prices, weather, analysts can identify anomalous patterns or correlations suggestive of stress in a particular system.

Another benefit of OSINT and big data is the breadth of coverage. HUMINT or IMINT might be focused on a few targets deemed most critical, but open-source monitoring can cast a wider net across many countries and topics at a lower cost, increasing the chance of catching surprises in non-prioritized areas. Of course, open sources come with challenges: information overload, questions of reliability (mis/disinformation is rampant), and the need to verify and contextualize what is found. Yet, when used judiciously, OSINT can complement classified sources to improve warning. Modern early warning systems often integrate both classified intel and open data feeds into a fusion center. For example, to anticipate a humanitarian crisis, an analyst might combine

[53] Elena Șușnea, "A Real-Time Social Media Monitoring System as an Open Source Intelligence (OSINT) Platform for Early Warning in Crisis Situations," *The Knowledge-Based Organization* 24, no. 2 (2018): 427–431, *https://doi.org/10.1515/kbo-2018-0127*.

satellite imagery of crop conditions (commercial imagery as OSINT), local price data, social media reports of food shortages, and confidential diplomatic reporting – each source filling in part of the puzzle. In summary, OSINT and big data analytics serve as force-multipliers for predictive intelligence, enabling more comprehensive horizon scanning and faster detection of weak signals – from disease outbreaks to military buildups – thereby enhancing the intelligence community's ability to issue timely warnings.

1.4 Conditions for effective warning

Possessing and mastering early warning systems and predictive models is only half the challenge; the other crucial half is ensuring that warnings lead to effective decision-making. History is replete with cases where warnings were available but either not communicated clearly or not acted upon by policymakers – resulting in avoidable surprise or inadequate responses. This section examines the conditions under which warning intelligence is most effective, and conversely the inherent limits of forecasting. Key requirements for effective warning often cited in the literature include accuracy, timeliness, relevance, and credibility (or receptivity). Meanwhile, challenges such as ambiguity of information, cognitive biases, organizational inertia, and the problem of false alarms complicate the warning process.

Fundamentally, for a warning to be useful, it must be correct (or at least on target about the general threat) and it must reach decision-makers in time for them to do something about it. Accuracy in this context means that the warning correctly identifies the nature of the emerging threat – for example, warning that a specific actor will invade a neighbor and being right about it. Timeliness means the warning arrives neither too late (when the crisis has already struck) nor so early and uncertain that it cannot galvanize any action. These two factors can be in tension: a very early warning is often low in confidence (thus potentially inaccurate), whereas a very accurate warning might be one delivered at the last minute when the evidence is definitive. Intelligence scholars therefore view warning effectiveness along an analytical dimension of accuracy and timeliness[54]. High accuracy and timeliness give decision-makers the best chance to mitigate a threat. Achieving

[54] Grabo and Goldman, *Handbook of Warning Intelligence*.

both accuracy and timeliness is difficult; warnings are inevitably based on incomplete data and probabilistic judgments. Yet, intelligence agencies strive to improve analytic methods to get as close to "right, and early" as possible. They refine indicator lists, employ modeling, and constantly evaluate past performance to calibrate the balance between false alarm and missed warning. Delving deeper into the concept of timeliness, Omand distinguishes two crucial characteristics: latency and perishability[55]. The former indicating how fresh is the piece of intelligence at the moment it is transmitted to the decision-maker, while the latter referring to the period of time in which the intel received remains sensitive for the customer. These two elements efficiently highlight how critical the speed of communication is in such contexts.

Nonetheless, even the best and quickest analytic warning is inoperable if it is not effectively communicated to the people who must decide on a response. Thus, a second key dimension is the process of warning dissemination and communication. To be effective, warnings should be delivered through the proper channels, in a clear and persuasive manner, to the right recipients. This often means tailoring the message to the decision-maker's needs and framing it in policy-relevant terms. Intelligence officers talk about making intelligence "digestible" and action-oriented[56] – a warning should tell a policy official what is happening, why it matters, and perhaps what options or urgent actions could be taken. If the warning is buried in a lengthy, technical report or couched in vague language, it may easily be ignored or misunderstood. That is why explicit or previously agreed probability yardsticks matching the likelihood term with its percentage are key in order to always be on the same page and avoid vagueness about probabilities[57]. Gentry notes that successful warning communication requires not only accuracy but also skill in presentation[58] [59] – getting policymakers to pay attention amidst many competing issues. The warning must also be relevant to the recipient's responsibilities, and therefore practitioners must transmit it to the right

[55] Omand, *How to Survive a Crisis*, 56–58.
[56] Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Ithaca, NY: Cornell University Press, 2011).
[57] Tzur M. Karelitz and David V. Budescu, "You Say 'Probable' and I Say 'Likely': Improving Interpersonal Communication with Verbal Probability Phrases," *Journal of Experimental Psychology: Applied* 10 (2004): 25–41.
[58] John A. Gentry, "Intelligence Failure Reframed," *Political Science Quarterly* 123, no. 2 (2008): 247–270.
[59] Dennis J. King, *Channeling Cassandra: Humanitarian Intelligence and Decisionmaking in the Age of Complexity* (U.S. Department of State, National Intelligence University, Ann Caracristi Institute for Intelligence Research, 2024).

person[60]. If the warning does not clearly connect to the decision-maker's portfolio or interests, it may be discounted. Thus, intelligence professionals often frame warnings in terms of the decision-maker's objectives.

An imperative aspect of communication is also format and frequency. Warning may be conveyed as a special report, an urgent memo, a briefing in person, or even via direct phone call in extreme cases. Some organizations have dedicated warning bulletins or indicators dashboards for leadership, such as the U.S. with the President's Daily Brief[61]. Preserving an efficient warning system often entails regular drills or updates. If decision-makers are accustomed to seeing early warnings presented in a certain way, they are more likely to notice when a critical alert appears. Conversely, if warnings are sporadic or always formatted differently, they might be overlooked in a context where briefings are not a habit.

The final critical condition is whether the political or organizational leaders believe the warning and are willing to act on it. Scholars have identified a frequent political dimension to warning outcomes: the degree of decision-maker receptivity or willingness to heed the warning[62]. Sometimes intelligence has done its job – a timely, accurate warning was given – but leaders for various reasons may choose not to elevate the response. This "warning-response gap" can arise from psychological, bureaucratic, economic or political factors. Cognitive biases play a role. A famous hurdle is confirmation bias: if a warning does not fit the decision-maker's prior beliefs, expectations or agenda, they may subconsciously downplay it[63]. For instance, warnings about imminent threats are sometimes ignored because leaders assume the adversary "wouldn't dare" take such bold actions, or because preparing for seemingly unlikely but high-impact events, like pandemics, is perceived as economically inconvenient. For example, intelligence warnings before the 9/11 attacks were overlooked partly due to assumptions that such an unprecedented assault on U.S. soil was unlikely. Similarly, early alerts about the COVID-19 pandemic were downplayed because the global health crisis seemed improbable and costly to prepare for.

---

[60] Nikki Ikani, "Beyond the Binary: A New Typology for Evaluating Warning Success and Failure in Strategic Surprise," *International Studies Review* 27, no. 1 (2025).
[61] Adrian Wolfberg, "The President's Daily Brief: Managing the Relationship between Intelligence and the Policymaker," *Political Science Quarterly* 132, no. 2 (2017): 225–258.
[62] Ikani, "Beyond the Binary."
[63] Gentry and Gordon, *Strategic Warning Intelligence*.

A further issue concerns ambiguity intolerance. Policymakers often prefer certainty, and if an intelligence warning comes with uncertainty (as they usually do according to their inherent essence), officials may ignore it in favor of hoping the worst won't happen. To this, the problem of overload is added: in a complex environment, leaders get many warnings and risk assessments. As responding robustly to all would be disproportionally costly and hard to manage, triage happens and some warnings simply do not garner attention[64].

Organizational and political disincentives can further impede receptivity. Decision-makers might fear the political price of acting on a warning that turns out to be a false alarm, thus making them risk-averse and inclined to wait for more evidence. If intelligence swings too far toward sensitivity (to avoid missing anything), it will generate warnings too frequently, many of which inevitably prove to be incorrect. These false alarms can desensitize leaders. As one study noted, repeated false alarms jeopardize intelligence and policymakers' ability to react, resulting in a reduced capacity to effectively tackle threats[65]. A well-known witticism in the U.S. intelligence community captures this: "The CIA predicted twelve of the last four crises."[66] – an ironic sentence that Former Secretary of State Dean Rusk (1961-1968) used to highlight the tendency of intelligence agencies to forecast more crises than could realistically occur, thereby implying a pattern of excessive warning or overestimation. Every false alarm that results in costly preventive measures or mobilizations can reduce the credibility of future warnings. On the other hand, intelligence history is rich of examples of analysts feeling like "Cassandra," doomed to issue true warnings that no one believed until after the fact. Effective warning thus requires building trust and credibility between intelligence and policymakers over time. A certainty in the field is that when intelligence services have a reputation for reliability, leaders are more likely to listen. Conversely, if the intelligence community has cried wolf repeatedly, leaders will tend to act according to their beliefs. Indeed, one paradox noted by historians is that "most successful warnings appear to be false alarms"[67] – meaning if a warning leads to preventive action and the disaster is averted, it may look in retrospect as though the warning

[64] Omand, *How to Survive a Crisis*, 137–162.
[65] Euan G. Davis, "A Watchman for All Seasons," *Studies in Intelligence* 13, no. 2 (1969): 37–42.
[66] Loch K. Johnson, "Bricks and Mortar for a Theory of Intelligence," *Comparative Strategy* 22, no. 1 (2003): 1–28.
[67] Mary McCarthy, "The National Warning System: Striving for an Elusive Goal," *Defense Intelligence Journal* 3 (1994): 5–19.

was overblown. Thus, intelligence must strive for a balance: aggressive enough in warning to catch true threats, but not so hyperactive that it cries wolf and is ignored when it really matters. This is easier said than done. In practice, improvements in technology (e.g., better sensors, data analytics) and methodology are being pursued in order to sharpen accuracy, while training and dialogue with decision-makers are increasingly used as a way to improve communication and trust.

In the process of evaluating past failures and successes, experts have formulated multidimensional frameworks. For instance, Ikani (2025) suggests measuring warning success across analytical, communication, and political dimensions[68], as briefly anticipated above. A fully effective warning would score well on all three: analytically sound, well-communicated, and acted upon by leadership. In reality, partial failures occur: analysts might get it right but be ignored (political failure), or policymakers might be willing to act but were never informed clearly enough (communication failure). Understanding these dimensions helps diagnose where the breakdown lies and improve intelligence success rate. Nonetheless, it also highlights some intrinsic limits of forecasting. No forecast can ever be 100% certain, as the future is inherently contingent and often influenced by random or unknowable factors. Moreover, crises by their nature often involve novelty, as theorized by Hewitt (1973) through his "un-ness category" [69] that we mentioned at the beginning of Section 1.1. This means intelligence will most certainly face the issue of ambiguity forever: signals are open to multiple interpretations. Within this context, the analytical methods of Section 1.3 aim to mitigate such difficulties, but can never eliminate uncertainty.

In conclusion, effective warning is a socio-technical endeavor: it requires not only good data and models to foresee crises, but also savvy communication and receptive governance structures. Accuracy, timeliness, relevance, and credibility form the cornerstone criteria for success in warning intelligence. And yet, even with all criteria met, the fog of uncertainty means surprise can never be fully eliminated – only managed and reduced. Recognizing the limits of forecasting should instill humility and drive continuous refinement of the warning enterprise. As this chapter has laid out, the theoretical and conceptual foundations – from how we define a crisis and intelligence, to the tools for prediction and the conditions for their use – provide the basis for exploring how, in

[68] Ikani, "Beyond the Binary."
[69] Hewitt, *Interpretations of Calamity*.

practice, intelligence can move decision-makers “from warning to influence” in anticipating and navigating crises.

2. Intelligence as an Unheard Voice: Obstacles and Distortions in Policy-Making

As we briefly introduced in Chapter 1, intelligence organizations often find that even accurate, high-quality analyses do not translate into timely political action. This chapter delves into why intelligence – "the unheard voice" – frequently fails to influence decision-making and crisis prevention. Both theoretical models and real-world cases reveal a persistent policy-intelligence gap in which warnings are ignored or distorted. We will explore how communication breakdowns, power dynamics, cognitive biases, organizational culture, and politicization each contribute to this gap. Further, we will examine the ethical dilemmas inherent in warning: acting too early at the risk of false alarm, or too late (or choosing not to act at all) with potentially catastrophic consequences. The discussion engages with key intelligence scholarship and draws on lessons from notable cases. Ultimately, since overcoming the obstacles to intelligence influence requires not only better analytical tradecraft but also changes in the relationship between analysts and policymakers, the sections below address each dimension in turn.

2.1 The Policy-Intelligence Gap: A Communication Issue or a Matter of Power

Scholars have long noted a disconnect between intelligence producers and policy consumers. Stephen Marrin observes: "strategic intelligence analysis frequently does not influence the creation and implementation of foreign policy"[70], contrary to the ideal of evidence-based decisions. Therefore, the objective is to identify which of the three dimensions of warning production – analytical, communicative, or political – offer the greatest potential for improvement, with the aim of increasing the overall effectiveness of warning transmission.

One view is that misunderstandings and poor communication lie at the heart of the gap. Intelligence analysts and policymakers often seem to speak different languages or have misaligned expectations. Analysts pride themselves on nuance and are comfortable with uncertainty, whereas

[70] Stephen Marrin, "Why Intelligence Analysis Has Limited Influence on American Foreign Policy" (paper presented at the APSA Annual Meeting, 2014).

policymakers demand clear, actionable advice under time pressure. As Lowenthal notes, the two communities are "different tribes" – analysts are akin to scholars seeking truth, while policymakers are achievers focused on action[71]. This can lead to friction and messages lost in translation. For example, warnings couched in probabilistic terms or lengthy reports may not register amid policymakers' busy agendas[72]. Practical initiatives like CRIP (the common recognized information picture) have emphasized tailoring and timing of warning dissemination during crises, attempting to established a shared common knowledge among decision-makers and save time that could be crucial[73]. However, CRIP is usually applied during emergencies that are already in place and demanding advanced commitment. That is why such techniques are not particularly useful when dealing with warnings, as the key component of pressure is missing in the strategical sphere. Yet, better communication including clearer framing of threats and more direct engagement with policy needs, is seen as a solution to bridge the gap.

Yet, other experts argue that the core issue is not how intelligence is communicated but when and why it is ignored. Robert Jervis even asserted that conflict between intelligence officers and policymakers is virtually guaranteed because their requirements and positions differ so fundamentally[74]. Leaders are free to reject intelligence assessments, as they have no obligation to heed warnings if doing so would force undesired actions[75]. In some cases, ignoring a warning is a deliberate choice: acknowledging a looming crisis might compel costly preventative measures or admissions of policy failure that decision-makers are reluctant to undertake[76]. For instance, studies of disregarded warnings (such as the 1990 National Intelligence Estimate "NIE" on Yugoslavia's breakup) found that U.S. officials resisted the forecast partly because they feared it would become

[71] Mark M. Lowenthal, "Tribal Tongues: Intelligence Producers, Intelligence Consumers," in *Strategic Intelligence: Windows into a Secret World*, ed. Loch K. Johnson and James J. Wirtz (Los Angeles: Roxbury Press, 2004), 234–241.
[72] Rovner, *Fixing the Facts*.
[73] Omand, *How to Survive a Crisis*, 54–56.
[74] Robert Jervis, "Why Intelligence and Policymakers Clash," *Political Science Quarterly* 125, no. 2 (2010): 185–204.
[75] Rovner, *Fixing the Facts*, 34–38.
[76] Omand, *How to Survive a Crisis*, 137–162.

a "self-fulfilling prophecy" and undermine efforts at a diplomatic solution[77]. Here the gap arose not from miscommunication but from leaders' power calculations and reluctance to change course. Nonetheless, what can play a role in determining whether intelligence is heard is how it is positioned relative to policy. Three idealized relationship models appear in the literature. The first is rooted in Sherman Kent's philosophy, where analysts act as impartial custodians of truth, standing apart from politics and delivering objective assessments without advocacy[78]. This model prizes integrity and neutrality, but it risks intelligence being ignored as irrelevant or out-of-touch if analysts are too detached from policymakers' practical needs. At the opposite end is the model associated with Robert Gates' views, which urges close engagement and alignment with policymakers so that intelligence directly informs options and is seen as useful[79]. This can make intelligence more influential on a daily basis, but blurs the line between analysis and policy preference, potentially undermining objectivity. Between these poles lies a dysfunctional role all too common in practice: the "scapegoat". When crises erupt or policies fail, officials often point to "intelligence failures" to deflect blame[80]. The intelligence community thus becomes a convenient scapegoat. This adversarial dynamic corrodes trust: policymakers treat intel as an easy target rather than a partner, while analysts cultivate frustration as their work is misused or disused[81]. The scapegoating phenomenon highlights the power and responsibility imbalance of the relationship. As Betts dryly observed, "failures occur more often at the consuming than the producing end of intelligence"[82]. Yet, those failures still tend to be laid at the feet of intelligence agencies in hindsight.

A recurring theme is the ambivalence in how decision-makers use intelligence. Indeed, policymakers need sound intelligence to navigate uncertainty, and ideal relations are characterized

---

[77] Gregory F. Treverton and Renanah Miles, "Unheeded Warning of War: Why Policymakers Ignored the 1990 Yugoslavia Estimate," *Intelligence and National Security* 32, no. 4 (2016): 506–522.
[78] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949).
[79] Robert M. Gates, *From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War* (New York: Simon & Schuster, 2011).
[80] John Hollister Hedley, "Learning from Intelligence Failures," *International Journal of Intelligence and CounterIntelligence* 18, no. 3 (2005): 435–50.
[81] Richard K. Betts, "Policy-Makers and Intelligence Analysts: Love, Hate or Indifference?" *Intelligence and National Security* 3, no. 1 (1988): 184–189.
[82] Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (Columbia University Press, 2007).

by healthy collaborative interaction and challenge. In practice, however, institutional ambiguity and inconsistency are widespread. Sometimes policymakers treat intelligence as a genuine neutral input; other times they selectively excerpt or ignore it depending on convenience. Intelligence may warn of brewing crises – economic, military, societal – but if those warnings clash with dominant political narratives or entail undesirable policy trade-offs, they risk falling on deaf ears. Moreover, policymakers may neglect the influence of even accurate intelligence unless it aligns with what power-holders are predisposed to hear. Marrin concludes that the intelligence-policy nexus is beset by theoretical and institutional ambiguity: no clear rules govern how much weight intelligence should carry, leaving it vulnerable to ad hoc, power-driven use (or non-use) by decision-makers[83].

Beyond structural issues, cognitive factors also explain why warnings go unheeded. Jervis observed that leaders may perceive warnings through lenses of wishful thinking or denial – especially if acting on a warning involves high political cost. It is psychologically easier to downplay a threat than to grapple with costly preventive action. There is often a reluctance to believe bad news and a search for other explanations that dismiss alarming intelligence.

In sum, the policy-intelligence gap persists as both a communication problem and a power problem. On one hand, improving the clarity, relevance, and delivery of intelligence can help ensure warnings at least register with busy decision-makers. On the other hand, no amount of clear communication can overcome a willful refusal to listen, as power dynamics and political incentives greatly shape whether intelligence is heard. As long as policymakers are free to ignore inconvenient truths – and suffer little immediate penalty for doing so – intelligence will remain an "unheard voice" in many crises. Bridging the gap requires not only better messaging, but also changes in the culture and rules of decision-making: leaders must internalize that ignoring warning intelligence can carry grave costs, and institutional mechanisms must encourage genuine consideration of analytic input. The next sections seek to examine more closely the cognitive biases and organizational factors that compound this problem, as well as the deleterious effect of politicization in distorting intelligence before it ever reaches policymakers' ears.

[83] Stephen Marrin, "Intelligence, Policy and Politics: The Limited Role of the Expert Analyst," 2012.

2.2 Cognitive and Organizational Factors Hindering Intelligence Impact

If intelligence often fails to change policymakers' minds, part of the explanation lies in how humans and organizations process information. Even a rational message can be undermined by irrational biases or bureaucratic barriers. This section delves deeper into the psychological and organizational factors – from individual cognitive biases like confirmation bias, to institutional culture and inter-agency frictions – that impede intelligence from having its intended impact.

Indeed, extensive research in psychology shows that decision-makers are prone to cognitive biases that can distort their interpretation of intelligence, especially if they do not have a past as analysts[84]. The first and probably most relevant one is confirmation bias. It consists of the tendency to favor information that confirms one's preexisting beliefs and to downplay or dismiss contradictory evidence[85]. In intelligence contexts, confirmation bias is pernicious – a policymaker who believes an actor is unlikely to attack may subconsciously ignore multiple warning indicators while seizing upon any data that suggests the opposite. Heuer emphasized that both leaders and analysts must actively seek disconfirming evidence since the mind will accept plausible hypothesis more easily than rejecting them[86]. As Wason argues: "no confirming instance of a law is a verifying instance, but […] any disconfirming instance is a falsifying instance"[87]. Yet, policymakers under pressure may have neither the time nor inclination for such reflection, often denying, downplaying, or ignoring intelligence that challenges their prior view[88]. Within this context, Isenberg highlights how approaching unexpected developments and counterarguments with openness enables leaders to comprehend threats at an early stage and to interpret them with a mindset less constrained by entrenched assumptions or rigid preconceptions[89].

---

[84] Rovner, *Fixing the Facts*, 28–33.
[85] Raymond S. Nickerson, "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises," *Review of General Psychology* 2, no. 2 (1998): 175–220.
[86] Heuer, *Psychology of Intelligence Analysis*.
[87] Peter C. Wason, "On the Failure to Eliminate Hypotheses in a Conceptual Task," *The Quarterly Journal of Experimental Psychology* 12, no. 3 (1960).
[88] Heuer, *Psychology of Intelligence Analysis*.
[89] Daniel J. Isenberg, "How Senior Managers Think," in *Decision Making: Descriptive, Normative, and Prescriptive Interactions*, ed. David Bell, Howard Raiffa, and Amos Tversky (Cambridge: Cambridge University Press, 1988), 535.

There is also a temporal bias affecting decision-making: so long as a crisis is not yet at boiling point, leaders may optimistically assume more time remains or that the worst-case scenario will not materialize[90]. This is conventionally termed "the status quo bias" and helps explain several infamous warning failures. For instance, prior to the Yom Kippur War (1973), despite intelligence indicators of Arab preparations, both Israeli and U.S. decision-makers clung to an assumption that war was unlikely[91]. It represented a classic case of discounting warning signs due to premature cognitive closure, as they believed their existing policy posture was sound enough. Such cases demonstrate leaders' inclination to stick with established policies or assumptions until a crisis forces change. However, it is worth stating that their responsibility is sometimes only partial, as contemporary bureaucracies have standard operating procedures that are hard and take long to pivot, even when intelligence indicates those procedures are failing and decision-makers show intention to act.

A further category of bias encompasses personal or political preferences. Decision-makers often interpret ambiguous information in the manner most favorable to their desired outcome[92]. This is a subtle bias where either emotion or partisan predilection guide reasoning. Thus, leaders who are politically constrained from intervening in a foreign conflict might convince themselves that an intelligence warning is overblown, not purely out of analytical judgment but because accepting it would force an uncomfortable decision. As noted, Israeli authorities before October 2023 had strong political reasons to prioritize other theaters; this motivated them to treat Gaza invasion warnings as exaggerations[93]. Likewise, in the run-up to the COVID-19 pandemic, some governments were slow to act on intelligence about the virus's spread, arguably due to wishful thinking that drastic measures such as lockdowns could be avoided.

Furthermore, within policy councils or intelligence agencies, there is risk of groupthink, since usually both activities involve a wide series of participants. It consists of an unconscious collective

---

[90] William Samuelson and Richard Zeckhauser, "Status Quo Bias in Decision Making," *Journal of Risk and Uncertainty* 1 (1988): 7–59.
[91] Itai Shapira, "The Yom Kippur Intelligence Failure after Fifty Years: What Lessons Can Be Learned?" *Intelligence and National Security* 38, no. 6 (2023): 978–1002.
[92] Betts, *Enemies of Intelligence*, 75.
[93] Erik J. Dahl and David Strachan-Morris, "'Predictive Intelligence for Tomorrow's Threats': Is Predictive Intelligence Possible?" *Journal of Policing, Intelligence and Counter Terrorism* 19, no. 4 (2024): 423–435.

bias where dissenting voices are suppressed to maintain a facade of consensus[94]. Groupthink notoriously contributed to the 2002 U.S. National Intelligence Estimate on Iraqi weapons of mass destruction (WMD), where analysts across agencies converged on a firm (but largely wrong) judgment that Iraq had active WMD programs, partly due to mutual reinforcement and reluctance to challenge prevailing assumptions[95]. In policymaking circles, groupthink can mean an entire administration buys into a particular worldview and is deaf to intelligence that contradicts it.

An organization's culture can reinforce biases too: for instance, the organizational mindset in the CIA post-9/11 became overly attentive to worst-case terrorist threats, while potentially causing other nuanced intelligence to be underweighted. Indeed, many government organizations have long-standing cultures that shape how they view intelligence. Some militaries, for example, are known to have historically been skeptical of civilian intelligence, preferring their own channels or valuing operational intuition over analytic estimates. A hostile or dismissive culture can lead to systematic underuse of intelligence. If a cabinet or command staff regards intelligence analysts as academic naysayers, warnings are more likely to be left aside. On the other hand, organizational overconfidence in its own judgment can be dangerous too. For instance, prior to the Space Shuttle Challenger disaster (1986), NASA's culture discounted engineering risk warnings[96], an analogy outside pure intel but concretely and sadly illustrating how institutional pride can override expert caution. In intelligence, Jack Davis noted that a certain tension between analysts and policymakers is healthy in order to ensure rigorous debate and raise potential challenges, but too much rigidity or mistrust becomes debilitating[97].

Certainly, the key aspect is trust: decision-makers must trust the competence and objectivity of intelligence to give it weight. After major intelligence failures, a culture of skepticism can easily pervade, where officials quietly assume the intel might be wrong again and hence automatically discount it. This is paradoxical: previous intelligence failures (or perceived failures) hinder future

---

[94] Irving L. Janis, *Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascoes* (Houghton Mifflin, 1972).

[95] Richard Aldrich, "Whitehall and the Iraq War: The UK's Four Intelligence Enquiries," *Irish Studies in International Affairs* 16 (2005): 73–88.

[96] Howard S. Schwartz, "On the Psychodynamics of Organizational Disaster: The Case of the Space Shuttle Challenger," *Columbia Journal of World Business* 22, no. 1 (1987): 59–67.

[97] Jack Davis, "Intelligence Analysts and Policymakers: Benefits and Dangers of Tensions in the Relationship," *Intelligence and National Security* 21, no. 6 (2006): 999–1021.

intelligence from being believed, increasing the odds of new failures through inaction[98]. Building and maintaining trust is thus crucial. Regular, open communication and demonstrating value by answering the questions policymakers actually have, can help overcome cultural skepticism.

A further underlying organizational factor that potentially undermines the relation between policy and analysis is the lack of formal accountability on the policy side for ignoring warnings. If an analyst fails to provide a warning, the intelligence community faces investigations and criticism. Conversely, if a policymaker receives a valid warning and chooses not to act, rarely is there an analogous accountability mechanism to examine that decision. Commissions and inquiries tend to focus on intelligence performance[99], not on why policymakers did not heed intelligence. This asymmetric accountability incentivizes risk-aversion among analysts (to "cover their bases" with warnings) but does not comparably incentivize risk-aversion among policymakers (to err on the side of caution and heed warnings). As analysts have wryly noted, when warnings are ignored and disaster strikes, it still gets labeled an "intelligence failure" in public discourse[100]. This dynamic can breed cynicism and frustration within intelligence ranks. It also means policymakers do not feel a strong professional penalty for dismissing intelligence. Therefore, scholars argue that to improve intelligence impact, there must be greater shared accountability: policymakers should be expected to explain egregious cases of warning-dismissal, and oversight bodies ought to scrutinize policy failures in conjunction with intelligence ones[101].

Mechanisms to address this could include formal collective reviews in order to ensure decision-makers have explored what happens if warnings are right, or even legislation requiring that certain high-level warnings must be briefed to Congress or Parliament, creating pressure on the executive to respond. Hans Born and the Geneva Centre for Democratic Control of Armed Forces (DCAF) offered their contribution to this matter, emphasizing that effective democratic oversight of intelligence involves not only controlling intelligence agencies to prevent abuse, but also ensuring

---

98 Luis Garicano and Richard A. Posner, "Intelligence Failures: An Organizational Economics Perspective," *Journal of Economic Perspectives* 19, no. 4 (2005): 151–70.

99 Hans Born and Ian Leigh, *Democratic Accountability of Intelligence Services* (Geneva: Geneva Centre for the Democratic Control of Armed Forces, 2006).

100 Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Georgetown University Press, 2013), 7.

101 Julius A. Agwu and Zems Mathias, "The Policy-Maker Intelligence Interface: A Critical Vulnerability in the Intelligence Community," *GSJ: Global Scientific Journal* 11, no. 9 (2023).

intelligence advice is properly considered in policy processes[102]. In other words, accountability should cover whether governments use intelligence wisely, not just whether intelligence agencies stay within legal bounds. Some countries have tried innovative approaches: for instance, the UK's Joint Intelligence Committee (JIC) historically issues formal warning documents to which policymakers must respond, creating a quasi-requirement to acknowledge warnings[103]. Such practices, however, constitute the exception rather than the rule.

In summary, cognitive biases inside the human mind and bureaucratic frictions inside organizations significantly hinder the impact of intelligence. Meanwhile, organizational culture can foster skepticism or poor communication such that warnings are not truly heard. Overcoming these impediments requires conscious effort: analytic training to mitigate biases (e.g. Heuer's Analysis of Competing Hypotheses technique is one tool to fight confirmation bias), fostering a culture of dissent and openness in both intelligence and policy circles in order to encourage consideration of uncomfortable scenarios, and building trust through regular policy-intel dialogue. It also demands structural fixes, like streamlining dissemination in crises and enacting oversight that does not only punish intelligence after the fact but also questions policy judgment. Only by tackling the human and institutional sources of inertia can intelligence move from an "unheard voice" to a persuasive influence on decision-making.

2.3 The Risk of Politicization of Intelligence

The section we just concluded and the dilemma it carries around accountability raises numerous questions around the relation between analysts and decision-makers, suggesting that the entire intelligence community could not but benefit from an increased proximity. However, there is widespread concern that moving towards such condition could threaten intel in terms of ethics and transparency by eliminating the distinction that characterizes the interests that each role defends. Indeed, one of the gravest distortions in the intelligence-policy relationship is politicization, which represents the antithesis of objective intelligence: instead of speaking truth to power, intelligence

[102] Born and Leigh, *Democratic Accountability of Intelligence Services.*
[103] Michael S. Goodman, "The Dog That Didn't Bark: The Joint Intelligence Committee and Warning of Aggression," *Cold War History* 7, no. 4 (2007): 529–551.

is manipulated to tell power what it wants to hear. This section examines politicization in depth, drawing on theories and the notorious case of the 2002-2003 Iraq WMD assessments, where intelligence was instrumentalized in the run-up to war. We also consider how politicization, once it occurs, inflicts long-term damage on analytical credibility and the autonomy of intelligence institutions.

In simple terms, politicization in our case refers to the alteration or shaping of intelligence assessments in a manner that aligns them with the desired policy objectives or preferences of decision-makers[104]. It arises in many forms, from manifest to subtle. Richard Betts distinguishes two broad types: "top-down" politicization, when policymakers impose their views on intelligence (e.g., pressuring analysts to alter findings), and "bottom-up" politicization, when intelligence officers skew their own analysis (consciously or subconsciously) to please superiors or match what they think policymakers want[105]. Mark Lowenthal elaborates with several specific scenarios. Indeed, politicization in intelligence manifests in various ways, including deliberate alteration of assessments by analysts to favor specific policy goals. It also occurs when policymakers exert influence over intelligence processes and rules to shape outcomes in their favor. Additionally, analysts may modify their future reports in response to consistent negative feedback, aiming to evade criticism. Another common form involves policymakers selectively endorsing intelligence findings that align with their agendas while disregarding dissenting views. These mechanisms illustrate the multifaceted nature of politicization, where intelligence is both consciously and unconsciously molded through interactions between intelligence producers and policy consumers to serve particular political interests[106]. All these undermine the integrity of intelligence. As Rovner notes, neglect is a critical aspect, but "the most damaging pathology is politicization, meaning the manipulation of intelligence to reflect policy preferences"[107].

Partisan battles after intelligence controversies frequently involve each side claiming the other manipulated intelligence and history provides clear cases of politicization at work. For instance, the intelligence assessments of Iraq's alleged WMD programs in 2002-2003 are widely regarded

---

104 Joshua Rovner, "Is Politicization Ever a Good Thing?", *Intelligence and National Security* 28, no. 1 (2013).
105 Betts, *Enemies of Intelligence*, 76–77.
106 Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 9th ed. (Thousand Oaks, CA: CQ Press, 2023).
107 Joshua Rovner, "Fixing the Facts or Missing the Mark? Intelligence, Policy, and the War in Iraq" (paper presented at the APSA Annual Meeting, 2011).

as a textbook example of politicization, both direct and indirect. Multiple official inquiries (the U.S. Senate Intelligence Committee reports, the UK's Butler Report, etc.) documented pressures on intelligence in that period. Between 2002 and 2003, a critical low point occurred when intelligence agencies were effectively co-opted by policymakers to help overcome domestic skepticism about the threat posed by Iraq. During this period, intelligence assessments were shaped and selectively emphasized to support the case for war, as political leadership sought to convince both the public and the international community of the imminence of the Iraqi threat. This process was marked by a concerted effort to present intelligence in a way that justified military action, despite considerable doubts and contested evidence within the intelligence community itself[108].

Among the key components of such politicization, we find the procedure of selective promotion of conforming views. Indeed, senior U.S. officials highlighted intelligence reports that supported the existence of active Iraqi WMD programs and ties to terrorism, while omitting or suppressing dissenting evidence. For instance, in public presentations like Secretary of State Colin Powell's UN speech (Feb 2003) in which he stressed the reasons why a military operation was necessary, the intel used was carefully curated to be as incriminatory as possible. In so doing, no light was shed on crucial caveats such as the State Department intelligence bureau's dissent on the Iraqi aluminum tubes evidence that were likely for rockets and not for uranium enrichment[109]. This scrupulous selection meant that within the intelligence community, alternate assessments coming from skeptical agencies were effectively sidelined when it mattered most[110].

Politicized intelligence tends to display a tone of unwarranted certainty, since policymakers will always prefer definitive statements. In the Iraq NIE, language was more assertive (e.g. explicitly indicating that Iraq owned chemical and biological weapons[111]) than the evidence merited, and alternative explanations or uncertainties were downplayed. Internal intelligence drafts often contained ranges of opinion, but by the time estimates were finalized, much ambiguity had been

[108] Ibid.
[109] Senate Select Committee on Intelligence (SSCI), *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq* (U.S. Government Printing Office, 2004).
[110] Paul Pillar, "Intelligence, Policy, and the War in Iraq," *Foreign Affairs* 85, no. 2 (2006): 15–27.
[111] U.S. Intelligence Community, *Iraq's Continuing Programs for Weapons of Mass Destruction* [National Intelligence Estimate, October 2002], declassified.

eliminated[112]. However, it is also worth noting that this was partly self-driven by analysts eager to be part of the history and not appear irresolute in face of administration urgency. The result of it generated hyperbolic assessments that presented worst-case assumptions as likely facts, with an "unrealistic sense of certainty", as stated by Rovner[113].

Moreover, while the 2004 Senate review did not find explicit cases of analysts being ordered to change conclusions, considerable indirect pressure on practitioners and officials was later acknowledge[114]. Analysts at CIA and DIA knew the administration's keen interest in finding evidence of Iraqi WMD and terrorist links; this knowledge itself can shape analytic tone. Rovner explains that repeated high-level questioning on the same issues signaled to analysts what answers they had to look for, encouraging them to adopt worst-case interpretations of ambiguous data and to focus on specific leads[115]. Some analysts later described it as an atmosphere where to be taken seriously, one had to align with the prevailing policy narrative that Iraq was a grave, active threat[116]. In the UK, a similar environment led, as historian Richard Aldrich noted, to analysts developing "an ideological conviction" that dictators like Saddam must have or plan to acquire WMD[117]. Notably, at the Pentagon, the Office of Special Plans under Undersecretary Douglas Feith was even created, in order to produce analyses more in line with the policy goal of emphasizing an Iraq-Al Qaeda connection, bypassing ordinary intelligence channels[118].

The consequences of this politicization were dire. The Iraq WMD fiasco is often labeled one of the biggest U.S. intelligence failures. In truth, it was as much a policy failure and a politicization failure, as intelligence was set around policy[119]. The war went ahead on false pretenses, and when no WMD were found, the credibility of Western intelligence agencies suffered a devastating blow.

---

112 Robert Jervis, "Reports, Politics, and Intelligence Failures: The Case of Iraq," *Journal of Strategic Studies* 29, no. 1 (2006): 3–52.
113 Rovner, "Fixing the Facts or Missing the Mark?".
114 SSCI, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq.*
115 Rovner, "Fixing the Facts or Missing the Mark?".
116 Commission on the Intelligence Capabilities of the United States Regarding WMD, *Report to the President* (Washington, DC: GPO, 2005).
117 Richard J. Aldrich, "Whitehall and the Iraq War: The UK's Four Intelligence Enquiries," *Irish Studies in International Affairs* 16, no. 1 (2005): 73–88.
118 Tom Barry, "Decentralizing U.S. Intelligence: Office of Special Plans" (Silver City, NM: Interhemispheric Resource Center, 2004).
119 James P. Pfiffner, "Did President Bush Mislead the Country in His Arguments for War with Iraq?", *Presidential Studies Quarterly* 34, no. 1 (2004): 25–46.

Politicization, especially a high-profile case like Iraq, has demonstrated to produce ripple effects that last years, even decades. First, it skews threat perception going forward. In the wake of Iraq, analysts and leaders had to grapple with the opposite problem – being too cautious in assessments so as not to overestimate again. For example, intelligence estimates on Iran's nuclear program in subsequent years were arguably more reserved and heavily caveated in a conscious or subconscious reaction against the overconfidence of the Iraq estimate[120]. Nonetheless, such mild approach this time may even have the opposite effect of inhibiting forthright analysis in situations where a strong warning might actually be needed.

Second, politicization poisons the trust relationship between intelligence professionals and policymakers[121]. After Iraq, many analysts felt mistreated by politicians who had manipulated their work and then blamed the agencies for being inaccurate. Conversely, some policymakers grew more openly suspicious that intelligence officers might have their own agendas. Rovner observed that post-Iraq, frictions between the intelligence and policy communities intensified: analysts voiced concerns that their assessments had been subject to political manipulation, while some policymakers implied that analysts were obstructive or insufficiently aligned with policy objectives[122]. Such mistrust corrodes the healthy dialogue needed for effective warning. It can also lead intelligence officers to become excessively defensive, sticking strictly to data and refusing any interpretive leaps for fear of subsequent accusations, or conversely lead policymakers to shut intelligence out of sensitive deliberations.

Third, episodes of severe politicization often trigger institutional reforms aimed at restoring analytic autonomy and credibility, but these can be double-edged. In the U.S., the post-2003 period saw measures like the establishment of an analytic "Ombudsman" to report any politicization concerns, the issuance of the DNI's Analytic Integrity guidelines (ICD 203) emphasizing objectivity and prohibiting politicization, and a general encouragement of alternative analysis[123]. These reforms were designed to protect analysts from undue influence and ensure dissenting views get voiced. While they likely have had a positive effect on analytic tradecraft, they also formalized a kind of separation between intel and policy – a reminder of Sherman Kent's warning that too

---

[120] National Intelligence Council (US), *Iran: Nuclear Intentions and Capabilities* (Washington, DC: NIC, 2007).
[121] Rovner, *Fixing the Facts*.
[122] Rovner, "Fixing the Facts or Missing the Mark?".
[123] Alexandru Marcoci et al., "ODNI as an Analytic Ombudsman: Is Intelligence Community Directive 203 Up to the Task?", *Intelligence and National Security* 34, no. 2 (2019).

much closeness breeds politicization[124]. The semipermeable membrane dividing intel and policy that Lowenthal describes, where policymakers can give input but analysts must not become advocates[125], was thus reinforced. The unintended consequence is that intelligence may have retreated somewhat from policy engagement to guard its integrity, which in turn can reduce its immediate influence on policy (a reversion to the policy-intel gap). It is a difficult balance: intelligence must aim at being policy-relevant but not policy-driven. The Iraq case tilted the balance far toward policy-driven, and the corrective measures have tried to redirect it toward independence. Finally, politicization can hurt the morale and recruitment within intelligence institutions. Analysts join with a sense of mission to inform truthfully, and therefore seeing their work politicized or ignored can be demoralizing. Over time, if analysts come to believe their honesty will be subverted or that speaking truth is career-damaging, the community risks a culture of cynicism or self-censorship which might end up endangering national security.

Looking at another angle, politicization not only undermines credibility but can threaten institutional autonomy. When scandals erupt, intelligence agencies come under intense external scrutiny and reorganization[126]. In the U.S., the creation of the Director of National Intelligence (DNI) in 2004-2005 was partly a response to coordination failures, but also an attempt by Congress to impose more top-down guidance on the IC[127]. It is still a topic of debate whether the DNI can be seen as a successful remedy to politicization issues or it simply increased bureaucracy without providing a concrete answer.

Scholars and practitioners suggest a number of solutions to maintain the firewall between analysis and policy. These include strong professional ethics and training for analysts to "speak truth to power" even when inconvenient, as encapsulated in CIA's ethos and in IC Directive 203 requiring objectivity and omitting political considerations[128]. This highlights how internal culture can either succumb to or withstand external politicizing pressure. Indeed, a confident analytic culture that

---

[124] Kent, *Strategic Intelligence for American World Policy*.
[125] Lowenthal, *Intelligence: From Secrets to Policy*.
[126] Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton University Press, 2009).
[127] Richard A. Best Jr. and Alfred Cumming, *Director of National Intelligence Statutory Authorities: Status and Proposals*, CRS Report RL34231 (Washington, DC: Congressional Research Service, January 12, 2011).
[128] Office of the Director of National Intelligence (ODNI), *Intelligence Community Directive (ICD) 203: Analytic Standards* (Washington, DC: ODNI, 2007).

values accuracy over political convenience is the best fortification to preserve integrity and provide concrete decision advantage. Additionally, external oversight can deter overt politicization – knowing that later investigations might expose undue pressure acts as a check on policy officials. In the end, however, the line between responsive intelligence and politicized intelligence will always be thin. As Lowenthal quipped, within the policy-intelligence boundary, policymakers will continuously give feedback and pushback, but intelligence must not let that cross into dictating analytic conclusions[129]. Achieving that equilibrium is an ongoing challenge.

In conclusion, politicization is a fundamental threat to the integrity of intelligence and the quality of decisions. The Iraq case unambiguously illustrates how distorted intelligence can lead to strategic blunders and a loss of public trust. Rebuilding credibility after such episodes is arduous and preventing the next politicization requires vigilance: insulating the analytic process from advocacy, ensuring leaders value truth over confirmation, and fostering an environment where intelligence can provide the information or assessments that policymakers might find difficult, inconvenient, or counter to their preferences, yet essential to acknowledge and consider in order to make well-informed decisions[130]. Only then can intelligence serve as a real corrective to policy, rather than an echo chamber. Moreover, politicization deeply affects the intelligence ambition to mature and expand its influence by fostering closer integration with decision-makers. Indeed, as intelligence becomes increasingly subject to control and distortion, practitioners find it more challenging to effectively communicate critical information, thereby diminishing the timeliness and impact of their warnings. This significantly undermines the effectiveness of intelligence operations and raises concerns about the discipline's future viability, particularly since intelligence lacks the inherent authority and power that policy carries as a guiding force.

2.4 The Ethics of Warning: Acting Too Early, Too Late, or Not at All

We have thus analyzed how the intel field has to engage with a series of structural and psychological phenomena associated with cognitive processes. Nonetheless, warning intelligence is also fraught with profound ethical dilemmas. Unlike many governmental activities, intelligence

[129] Lowenthal, *Intelligence: From Secrets to Policy*.
[130] Betts, *Enemies of Intelligence*.

warnings can save lives and prevent disasters. This section explores the moral and ethical questions surrounding the issuance of warnings. Specifically, we will try to understand when intelligence analysts should raise the alarm and what are the responsibilities of intelligence when evidence is uncertain. Within the community, it is difficult to establish whether it is worse to raise a false alarm or to miss a real threat. We also consider how legal and civil liberty considerations factor into warning decisions, particularly in democratic societies where aggressive early warnings, and the actions taken on them, might conflict with individual rights.

Analysts and officials often have to deal with the problem of transforming an ambiguous signal into a noise in the context of warning. Issue a warning for every potential threat and you will inevitably produce many false positives – warnings about events that never occur. Yet, set a very high bar for certainty, to avoid embarrassment or panic, and you risk false negatives – failing to warn of a real impending disaster. Ethically, finding the right balance is challenging. Intelligence veteran Cynthia Grabo identified the reluctance to alarm and the fear of being wrong as two frequent impediments to warning[131]. For example, if intelligence wrongly warns of an imminent terrorist attack and drastic security measures are taken with economic and social costs, the backlash can be severe. Moreover, each false alarm will erode trust and thus feed the possibility that decision-makers or the public might ignore the next warning.

On the other hand, failing to warn can mean catastrophe. Morally, many would argue a false positive is preferable to a false negative. While we can recover from embarrassment or costs of a false alarm, we cannot undo lives lost from an un-warned attack. This view aligns with the precautionary principle. When stakes are high (war, terrorist attack, genocide), it may be more ethical to err on the side of issuing a warning with incomplete information than to stay silent until full confirmation, which might come only when the attack happens[132]. Roberta Wohlstetter, in her study of Pearl Harbor, noted innate human craving for definitive and unmistakable assurances from intelligence, a demand that is fundamentally unattainable[133]. Warning will always be probabilistic. The question then is how much uncertainty one is willing to tolerate in either direction. What is certain is that probability is hard to quantify, and even a low-probability event might merit warning

[131] Grabo and Goldman, *Handbook of Warning Intelligence*.
[132] Betts, *Enemies of Intelligence*.
[133] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford University Press, 1962).

if its impact would be devastating. Thus, analysts often face a moral decision under uncertainty: speak up early with partial information, or hesitate and wait until more evidence accumulates.

Furthermore, there is also an ethical duty embedded in the intelligence profession often worded as "duty to warn". This concept appears in different contexts – one being the duty to warn individuals if they are personally targeted and a broader sense of duty to warn the nation or leadership of looming harm[134]. Ethically, many analysts internalize that if they see indicators of a coming crisis (war, terrorist plot, etc.), they must do everything possible to raise attention. Once again, in cases of uncertainty over whether threat-related intelligence satisfies the duty to warn criteria, the principle is to err on the side of disclosure, ensuring that the potential victim is informed[135].
However, this duty can clash with political and bureaucratic realities. Analysts cannot themselves take action; they must persuade decision-makers. When superiors remain dismissive, the analyst faces the dilemma of determining the appropriate extent of action. The ethical tension lies in whether circumventing the chain of command or publicly communicating information could ever be justified as a means of alerting the nation to an impending disaster that leaders appear to be disregarding. This is a profound ethical dilemma. Whistleblowing in intelligence breaks procedures and trust, yet many could argue that in extreme situations, it might be justified by a higher duty to save lives. One historical parallel is the FBI agent Coleen Rowley, who before 9/11 urgently tried to get FBI HQ to pay attention to the "Phoenix memo" and Zacarias Moussaoui's flight training – she didn't go public beforehand, but after the fact blew the whistle on FBI's internal failures[136]. Her case shows the tension: she followed ordinary methods and the warning stayed buried. Had she ignored guidelines to warn higher authorities or media, perhaps things might have been different.
Another angle is timing and proportionality of action: it's always doubtful to determine how early is too early to act on a warning. However, this is crucial to analyze, as acting too early can cause the very harm you seek to prevent. For instance, if intelligence warns that a hostile power might attack, a decision to launch a preventive strike based on that warning raises questions of international law and moral responsibility for starting conflict. The 2003 Iraq invasion again is

[134] Office of the Director of National Intelligence (ODNI), *Intelligence Community Directive (ICD) 191: Duty to Warn* (Washington, DC: ODNI, 21 July 2015).
[135] Ibid.
[136] Lauren Robinson, "Protecting the Rights of Whistleblowers," *Social Education* 69, no. 6 (2005): 313.

instructive, as it was essentially a preemptive war based on flawed warning intelligence about WMD. Once the warning proved false, it was seen as not only a policy mistake but an ethical one. Thus, acting robustly on a warning is itself ethically perilous unless the warning is sound enough. Further, false positives might potentially lead to violations of rights. In democracies, the intelligence community must operate within legal frameworks that protect citizens' rights. Early warning often requires collecting information that might infringe on privacy or freedom if done without restraint. Amy Zegart, in a congressional statement, noted two principal dangers oversight must guard against: first, that "intelligence agencies become too powerful, violating the liberties, laws, and values that Americans hold dear". Second, that they fail to protect the nation as a result of being weak[137]. This extensively encapsulates the ethical dilemma. For this reasoning we will consider counterterrorism as an example: signals of a possible plot might be picked up via intrusive means such as monitoring communications. In the post-9/11 era, many countries expanded surveillance powers in the name of warning and prevention. This has provoked intense ethical and legal debates around data and privacy. The Patriot Act in the U.S., for instance, allowed far greater intelligence gathering domestically. Proponents argued it was necessary to prevent attacks evoking the duty to warn, while critics argued it overreached and violated privacy rights of millions[138]. The Edward Snowden revelations in 2013 about NSA surveillance highlighted this conflict: intelligence was essentially issuing warnings by collecting as much data as possible, but the program itself infringed legal and moral norms in the eyes of many[139].

Another civil liberties aspect is how warnings are actioned in law enforcement. If intelligence identifies a suspected terrorist, acting on that warning might mean detention or targeted killing before a crime is committed. Yet, preventive action challenges the legal principle of innocent until proven guilty. Cases like the targeted killing of Anwar al-Awlaki (a U.S. citizen deemed a terrorist) were justified by intelligence warning of his intent, but raised questions about due process[140]. More commonly, local authorities might use intelligence warnings to conduct raids or arrests on suspicion

---

[137] Amy B. Zegart, "Statement on Intelligence Oversight" (testimony, Senate Select Committee on Intelligence, November 13, 2007), https://irp.fas.org/congress/2007_hr/111307zegart.pdf.

[138] Patricia Mell, "Big Brother at the Door: Balancing National Security with Privacy under the USA PATRIOT Act," *Denver University Law Review* 80 (2002): 375.

[139] Cynthia Nolan, "The Edward Snowden Case and the Morality of Secrecy," *Catholic Social Science Review* 22 (2017): 291–310.

[140] Michael Ramsden, "Targeted Killings and International Human Rights Law: The Case of Anwar Al-Awlaki," *Journal of Conflict & Security Law* 16, no. 2 (2011): 385–406.

which, after careful investigation, result involving innocents and communities. Thus, the ethics of warning entail ensuring that protective actions do not unduly violate rights. That is why structured oversight bodies, as argued by Hans Born, aim to "insulate security and intelligence agencies from political abuse without isolating them from executive control"[141]. In practice, that means setting legal guardrails: requiring warrants, minimizing data collection on citizens, providing avenues for redress if an intelligence-led action was erroneous.

Finally, we should consider legal accountability in warning. In academic discourse, the notion that an intelligence agency could be found legally negligent for failing to warn of an attack it should have anticipated remains largely theoretical. Generally, this does not hold true in a court sense, even though official inquiries and commissions will most likely deliver strong criticism. Conversely, if an agency's warning leads to actions that harm people there may be legal liability or at least a need for redress. Asaf Lubin outlines such a duty of care in the context of International Humanitarian Law but acknowledges that litigation has yet to emerge in this domain[142]. Instead, accountability typically arises through official inquiries and commissions, as detailed by DeRosa, which deliver institutional criticism without judicial enforcement[143]. Moreover, despite policy directives like ICD-191 establish a formal duty to warn, they appear as policy guideline rather than legally enforceable acts. Notably, Lubin suggests that when intelligence warnings themselves cause harm, introducing civil liability may offer a path to redress in case of intelligence error[144] – though this remains at the moment a developing and largely theoretical proposal. This intricate scenario is exacerbated once more by the fact that intelligence officers themselves operate under legal guidelines that sometimes constrain warning dissemination. For instance, they cannot surveil certain populations or developments without cause, even if that makes warning harder. These legal norms reflect societal values aiming to strike a balance between security and a surveillance state. Amy Zegart in front of the U.S. Congress noted that robust oversight ensures agencies are powerful enough to protect the nation and its citizen but not so powerful as to infringe their values[145]. Today, intelligence agencies also coordinate with legal advisors to ensure their warning-related activities comply with law – maintaining the ethical-legal standard even under pressure. The involvement of

---

[141] Born and Leigh, *Democratic Accountability of Intelligence Services.*
[142] Asaf Lubin, "The Reasonable Intelligence Agency," *Articles by Maurer Faculty* 3034 (2022).
[143] Mary B. DeRosa, "Congressional Oversight of US Intelligence Activities," *Georgetown Law Faculty Publications and Other Works* 2575 (2021).
[144] Lubin, "The Reasonable Intelligence Agency".
[145] Zegart, "Statement on Intelligence Oversight."

oversight bodies and, where appropriate, international partners can provide a sanity check on both extremes: pushing agencies to not hold back important warnings, and conversely checking any tendencies toward overzealous or rights-infringing actions in the name of warning.

To navigate these dilemmas, intelligence communities develop their own codes of behavior related to warning. At this stage, the core ethos of intelligence professionals can be distilled into three guiding conservative principles: avoid politicization, avoid alarmism, stick to objective analysis. However, as we explored, such guidance sometimes conflicts with the urgency of warning. Mohr wrote about the need for analytic humility[146] – recognizing the limits of one's knowledge and the possibility of error. On the one hand, humility is important so that analysts do not become extremists convinced they are always right. On the other hand, analysts must have the courage of conviction when evidence strongly points to looming danger[147] – even if the evidence is incomplete or in progress. Indeed, if analysts have high confidence in a warning that could save lives, they must not remain silent out of fear. A balanced ethic thus leans toward giving warning with proper context, remembering that the costs of issuing a false alarm are usually far less severe than the consequences of failing to provide warning of a real threat.

In the end, the ethics of warning requires a delicate balance between boldness and restraint. Achieving this equilibrium means cultivating judgment in intelligence officers – to know when a threat is serious enough to justify potential false alarms – and ensuring that the system as a whole values risk and liberty in equal measure. Democratic societies entrust intelligence with a grave responsibility: anticipate dangers while upholding the very freedoms we seek to protect. Therefore, the true measure of success is not only in strategic surprise averted, but in doing so in a manner consistent with our laws and ethics.

---

[146] John S. Mohr, "A Call for More Humility in Intelligence Analysis," *Studies in Intelligence* 61, no. 4 (2017): 53–58.

[147] Janet M. Evans and Mark R. Kebbell, "The Effective Analyst: A Study of What Makes an Effective Crime and Intelligence Analyst," *Policing and Society* 22, no. 2 (2012): 204–219.

3. Comparative Case Studies: Intelligence Between Voice and Silence

The aim of this chapter is to test the models and conditions discussed until now by examining recent emblematic cases that involved both intelligence and decision-making. Each case will allow us to highlight the strengths and limits of the field in the prediction phase, opening a debate on intelligence's effectiveness and prospects for a more decisive role. The analysis emphasizes both positive and negative aspects and outcomes in each instance. Ultimately, a comparative discussion will address the central research question, trying to establish the level of maturity of the field and the challenges surrounding its possible elevation to a more influential role in policy. In particular, we will consider whether a future scenario is conceivable in which the intelligence practitioner becomes or replaces the decision-maker and the implications this process would involve.

3.1 Case 1 – 9/11 Attacks: The Tragedy of Non-Integration as a Turning Point

The September 11, 2001 terrorist attacks are often cited as an intelligence failure sui generis. It mainly consisted in a tragedy of non-integration, where plentiful warning signs were available but never effectively synthesized[148]. Prior to 9/11, various U.S. intelligence agencies each held pieces of the puzzle: the CIA had amassed intelligence on Osama bin Laden's growing terrorist network, the FBI had field reports about suspicious flight training activities, and the NSA intercepted communications hinting at a looming plot[149]. Strategic warning did exist – in fact, both intelligence analysts and top policymakers were aware by 2001 that al-Qaeda posed a serious, imminent threat[150]. As Daniel Byman noted, the intelligence community, particularly the CIA, was effective in delivering strategic warning regarding al-Qaeda, accurately identifying "the foe, its ambitious scale, and its lethality"[151]. High-level officials in both the Clinton and early Bush administrations

[148] Stephen Marrin, "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis," *Intelligence and National Security* (2011).
[149] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (Washington, DC: GPO, 2004).
[150] George J. Tenet and Bill Harlow, *At the Center of the Storm: My Years in the CIA* (New York: HarperCollins, 2007).
[151] Daniel Byman, "Strategic Surprise and the September 11 Attacks," *Annual Review of Political Science* 8 (2005): 151.

were fully cognizant of the danger[152]. Indeed, Benjamin and Simon highlight that the warning of a "new brand of terrorism that aimed at mass casualties" had effectively reached both legal and political authorities[153].

Despite this general awareness, the warnings were fragmented and never translated into a coherent tactical warning that could prompt preventive action. The lack of coordination and information-sharing among agencies was a decisive factor[154]. The 9/11 Commission found that institutional barriers – the infamous "walls" between foreign intelligence and domestic law enforcement, and between agencies – meant that vital indicators were not combined together[155]. In an eminent example, a CIA unit tracking al-Qaeda knew that known extremists, notably Nawaf al-Hazmi and Khalid al-Mihdhar, had entered the United States[156], but this information was not properly shared with the FBI in time for them to be located. Indeed, the Commission concluded that the foremost barrier to integrating intelligence from multiple sources, and thereby constructing a coherent picture, was organizational and cultural reluctance toward information sharing[157]. In short, no single agency had the complete picture; each possessed single warnings that in isolation seemed inconclusive. The intelligence community's siloed structure and poor information flow meant analysts failed to assemble these clues into an actionable forecast of the 9/11 plot. This represents a classic organizational failure, consistent with the reformist school of thought that blames bureaucratic stovepipes and rigid structures for intelligence failures, rather than individual actors[158]. Nonetheless, the intelligence sphere on the side of analysts suffered from a well-documented failure of imagination: only few practitioners anticipated terrorists would be able to turn airliners into suicide missiles[159]. Therefore, even explicit indicators like a 1998 report titled "Bin Ladin Preparing to Hijack US Aircraft" did not trigger sufficient alarm[160]. Yet, intelligence

---

[152] Tenet and Harlow, *At the Center of the Storm*.
[153] Daniel Benjamin and Steven Simon, *The Age of Sacred Terror: Radical Islam's War Against America* (New York: Random House Trade Paperbacks, 2003), 386.
[154] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*.
[155] Ibid.
[156] Ibid.
[157] Ibid.
[158] Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 11–13.
[159] U.S. Department of Defense, Paul Wolfowitz to Donald Rumsfeld, "Were We Asleep?" memo, 18 September 2001, cited in *The 9/11 Commission Report* (Washington, DC: GPO, 2004), 336.
[160] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*.

warnings lacked specificity about timing and method, and decision-makers struggled to believe that such an unprecedented attack could happen, illustrating how cognitive biases can lead to underestimation of unconventional threats.

Compounding these issues was a failure in communication to political leadership, though whether this was an intelligence shortcoming or a policy one is still debated. Some scholars argue that U.S. intelligence did ring alarm bells loudly and unequivocally to the White House – for instance, the CIA's repeated high-level briefings on al-Qaeda, including the notorious President's Daily Brief of August 6, 2001 titled "Bin Ladin Determined to Strike in US"[161], which warned of terrorist conspiracies. One interpretation is that this was a failure of policy response rather than of intelligence per se. According to this view, intelligence agencies fulfilled their duty by identifying the threat, but the consumer did not translate warning into preventative decision-making[162]. Another perspective, including the 9/11 Commission's, is that while policymakers knew terrorism was a grave danger, they did not have a clear warning of the specific 9/11 attack plan and therefore did not perceive the immediacy. The truth likely lies in between: multiple warnings were present, but they were either not effectively communicated or not sufficiently heeded, in favor of other concerns.

Paradoxically, the failure of 9/11 became a catalyst for positive change in the intelligence community. It "marked a turning point" by demonstrating, at terrible cost, the need for adjustment. Indeed, the shock generated by 9/11 spurred a thorough re-examination of U.S. intelligence practices and led to the most significant restructuring of the community since its founding. This is the reason why, in addition to considerations of chronological order, this case has been selected as the first in our analysis. Notably, reforms included the creation of a Director of National Intelligence (DNI) to coordinate across the 17 agencies, the establishment of an integrated National Counterterrorism Center, and the implementation of improved information-sharing protocols across federal and local levels[163]. These restructurings aimed to ensure that the single indicators found from different agencies would be connected in the future. In terms of intelligence-cycle

---

[161] "Bin Ladin Determined to Strike in US," *Presidential Daily Brief*, 6 August 2001, declassified, 9/11 Memorial & Museum, https://www.911memorial.org/sites/default/files/inline-files/Bin%20Ladin%20Determined%20to%20Strike%20in%20US.pdf.

[162] Marrin, "The 9/11 Terrorist Attacks."

[163] U.S. Congress, *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. 108–458, 118 Stat. 3638 (S. 2845) *https://www.congress.gov/108/plaws/publ458/PLAW-108publ458.pdf*.

practice, 9/11 raised awareness of strategic warning intelligence as a discipline. Culturally, agencies began breaking down turf barriers, aided by technology and evolution in mindset. While no system can guarantee success in foreseeing every attack, the post-9/11 reforms did address many structural deficiencies. It is no coincidence that the incidence of thwarted terrorist plots increased substantially, with interdiction rates rising from approximately 32% prior to 2001 to over 80% in the subsequent years[164]. In sum, the 9/11 case underscored that integration is key: when intelligence warnings are not pooled and conveyed with clarity and urgency, they may go unacted upon – with catastrophic results. It took a national tragedy for this lesson to be absorbed, marking 9/11 as both a devastating failure and a turning point that completely reshaped intelligence operations going forward.

3.2 Case 2 – 2022 Russian Invasion of Ukraine: A (Partially) Effective Public Warning

Moving to another crucial moment in our contemporary history, Russia's full-scale invasion of Ukraine in February 2022 offers a stark contrast to 9/11. In this case, intelligence warnings were largely accurate, timely, and even publicly disseminated, and they were used as a policy tool. Western intelligence – particularly from the United States and United Kingdom – correctly anticipated the Kremlin's war plans many weeks in advance and took the unusual step of sharing these warnings with the world. This is why it is currently cited as a model of (partial) success in crisis anticipation. U.S. secret services had been tracking Russia's military buildup around Ukraine through late 2021, and their alarm grew as they observed specific indicators of an imminent attack[165]. In early November 2021, President Biden dispatched CIA Director Bill Burns to Moscow to warn Russia's leadership that Washington was aware of unusual troop movements near Ukraine and was fearful of aggressive intentions[166]. By December, U.S. intelligence publicly revealed detailed assessments: for example, the Washington Post, citing intelligence sources from un

[164] Kevin J. Strom et al., *Terrorist Plots against the United States: What We Have Really Faced, and How We Might Best Defend against It* (Santa Monica, CA: RAND Corporation, 2016).
[165] Shlomo Shpiro, "Intelligence and the Ukraine War: Early Lessons and Research Roadmap," *National Security and the Future* 24, no. 1 (2023): 7–18.
[166] Natasha Bertrand, Jim Sciutto, and Kylie Atwood. "CIA Director Dispatched to Moscow to Warn Russia over Troop Buildup near Ukraine." *CNN*, November 5, 2021, *https://edition.cnn.com/2021/11/05/politics/bill-burns-moscow-ukraine*.

unnamed official, reported that Russia was preparing to launch a large-scale assault in early 2022, with an estimated deployment of as many as 175,000 soldiers and artillery[167]. This level of specificity – including attack axes from multiple directions – proved uncannily accurate in hindsight, as Russia did in fact invade from the north, east, and south with roughly the same force size. British intelligence was also vocal: the UK government warned in January 2022 of Russian plots to establish a pro-Kremlin government in Kyiv in the context of potential military action against Ukraine[168]. While some of these early warnings were met with skepticism or seen as outlandish at the time, they were part of a coordinated Western strategy to publicly raise awareness about the situation and thereby preempt Russian disinformation[169].

Western intelligence organizations demonstrated a high level of foresight and proactive use of warning intelligence in this crisis. These disclosures served multiple purposes. First, they alerted and convinced allied governments (and even Ukraine's own leadership) that the threat was real and imminent, overcoming initial doubts[170]. This helped unify NATO and EU countries, many of whom were hesitant due to economic ties with Russia or memories of flawed Iraq-war intelligence. Notably, U.S. officials have acknowledged that one primary goal of publicizing the intelligence was to galvanize a collective response: by the time the invasion happened on February 24, 2022, Western nations had already begun coordinating sanctions, military aid to Ukraine, and force posture adjustments[171]. In that respect, the warning intelligence was effectively used as a political and diplomatic lever. By facilitating the rapid alignment of international backing for Ukraine, the intelligence disclosures created conditions that enabled a faster response to Russia's aggression than would likely have occurred otherwise[172]. This transparency helped strip President Putin of a

---

[167] Shane Harris and Paul Sonne, "Russia Planning Massive Military Offensive against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns," *Washington Post*, 3 December 2021, *https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html*.

[168] Foreign, Commonwealth & Development Office and Elizabeth Truss, "Kremlin Plan to Install Pro-Russian Leadership in Ukraine Exposed," UK Government Press Release, 22 January 2022, *https://www.gov.uk/government/news/kremlin-plan-to-install-pro-russian-leadership-in-ukraine-exposed*.

[169] Joshua C. Huminski, "Russia, Ukraine, and the Future Use of Strategic Intelligence," *PRISM* 10, no. 3 (2023).

[170] Ibid.

[171] Joseph R. Biden, "Remarks by President Biden Providing an Update on Russia and Ukraine," The White House, 18 February 2022.

[172] Huminski, "Russia, Ukraine, and the Future Use of Strategic Intelligence."

key element of surprise and shaped the international narrative. In essence, intelligence became a tool of information warfare in defense of Ukraine: by exposing Russian intentions, the objective of Western strategy was to prevent adversarial misperceptions and to re-establish primacy in the information contest, an arena where Russia had traditionally held the advantage through its propaganda apparatus[173].

Second, the event showcased impressive integration of traditional classified intelligence with OSINT[174]. The U.S. government's claims about Russian deployments were rapidly validated by independent analysts using satellite imagery and social media, creating an external, thus enhancing credibility[175]. This synergy between secret and open information bolstered the warning's impact and is cited as an innovative model which set a precedent for future intelligence communications[176].

Another positive aspect was that the warnings, while public, generally maintained truthfulness and accuracy, avoiding the mistake of exaggeration that haunted the Iraq WMD case. In fact, the shadow of Iraq 2003 loomed large – allies like Germany and France were initially distrustful precisely because U.S./UK intelligence had been wrong before[177]. By proving right this time, the intelligence community has begun to restore some trust.

For all its successes, the Ukraine warning was only partially effective, as denoted. Crucially, it failed to deter the invasion itself, as Russia proceeded with the attack despite the world being warned. However, the release of intelligence served less as a deterrent and more as a means of strategic signaling. While it could complicate Russia's operational planning at the margins, few concretely expected it to dissuade the Kremlin from launching the assault[178]. Thus, the outcome underscores that even excellent intelligence cannot always prevent a crisis, especially when an adversary's decision is firmly made or immutable. Another limitation was audience skepticism and "warning fatigue." In Ukraine's case, some intended recipients of the warning did not initially act.

---

[173] Ibid.

[174] UK Ministry of Defence, "How Open-Source Intelligence Has Shaped the Russia-Ukraine War," GOV.UK, 9 December 2022, *https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war*.

[175] Huminski, "Russia, Ukraine, and the Future Use of Strategic Intelligence."

[176] Hannah van Beek and Sebastiaan Rietjens, "Open-Source Intelligence in the Russia–Ukraine War," in *Reflections on the Russia–Ukraine War*, ed. Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens (Leiden: Leiden University Press, 2024), 57–76.

[177] Huminski, "Russia, Ukraine, and the Future Use of Strategic Intelligence."

[178] Ibid.

The government in Kyiv, for example, was wary of causing panic or economic collapse and thus downplayed some U.S. warnings; President Zelenskyy, prior to the attack, voiced frustration that constant alarming intelligence was hurting Ukraine's economy and public morale[179]. Many Ukrainians could not believe an invasion of that scale would actually occur, given they had been in a quasi-war with Russia for years. This illustrates the perennial challenge that even accurate authoritative warnings can be met with disbelief or inaction. Western intelligence had to overcome not only foreign partners' doubts but also its own credibility issues. Memories of past intelligence errors meant that persuading allies involved sharing more evidence than usual, which U.S. agencies were initially reluctant to do due to source protection concerns. Indeed, the decision to release so much intel was ethically and operationally daring, as it risked compromising sensitive sources and methods in exchange for political effect. The White House opted to emphasize immediate strategic value at the expense of secrecy[180], calculating that the benefit of exposing Moscow's plans outweighed the cost of possibly losing some collection capabilities. In future, this ethical challenge will recur, concerning the extent to which intelligence should be employed openly to provide warnings or influence events, even at the potential cost of compromising sources, methods, and therefore long-term collection. The Ukraine case opened a debate on this trade-off. Moreover, the apparent success could encourage politicization of intelligence once more. Particularly, leaders might pressure agencies to release intel selectively to support a policy narrative. To avoid this, as we analyzed in Chapter 2, the creation of transparent standards to ensure a distinction between analytic judgment and policy persuasion is key, especially when using intelligence publicly[181]. Within this context, maintaining honesty and not overstating confidence is vital.

In summary, the 2022 Ukraine invasion case demonstrates the potential of intelligence when effectively integrated into decision-making and diplomacy. Western intelligence here was not marginalized or ignored; it was at the forefront, shaping global response. The case thus provides a counterpoint to the notion of intelligence as a silent voice in the wilderness. Instead, it was a loud voice that, while not preventing war, arguably saved lives by ensuring Ukraine was better prepared

---

179 Sarah Rainsford, "Ukraine Crisis: Don't Create Panic, Zelensky Tells West," BBC News, 28 January 2022, *https://www.bbc.com/news/world-europe-60174684*.
180 Huminski, "Russia, Ukraine, and the Future Use of Strategic Intelligence."
181 Committee of Privy Counsellors, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Counsellors* (Cm 6278), (London: The Stationery Office, July 2004).

and the West more united than they would have been in a surprise scenario. The strengths shown include accurate forecasting, inter-allied sharing, proactive public communication, and coordination with open sources. The limits, however, remind us that intelligence is not omnipotent: it can warn and inform, but policy action and adversary decision-making is what ultimately determines outcomes.

3.3 Case 3 – Israel–Hamas War (2023): Tactical and Strategic Surprise

On October 7, 2023, Israel suffered a shocking surprise attack by Hamas militants from Gaza – a multi-pronged onslaught that killed over 1,200 people and led to an extended war[182]. This event is arguably Israel's worst intelligence failure in decades, often compared to the surprise of the 1973 Yom Kippur War. It represents a case of both tactical surprise and strategic surprise. Indeed, there was neither a timely warning of the impending attack nor a clear recognition that Hamas possessed both the intent and the capability to mount such a massive operation[183]. The Israeli intelligence community, renowned for its technological capabilities and human intelligence networks, was caught unprepared that morning despite Hamas mobilizing thousands of fighters, rockets, and even paraglider units. To understand how this could happen, analysts point to a confluence of factors: overreliance on deterrence and technology, misreading of adversary intentions, and certain political and cognitive biases[184].

In the years leading up to 2023, Israeli leadership and intelligence agencies developed a flawed strategic conception regarding Hamas. Tel Aviv embraced a narrative that cast Hamas as restrained by Israel's deterrent power and only invested in the daily governance of Gaza and the pursuit of economic relief[185]. In line with this belief, Prime Minister Netanyahu's administration took steps that implicitly treated Hamas as contained: for example, allowing influxes of Qatari financial aid

---

[182] Human Rights Watch, "I Can't Erase All the Blood from My Mind," 17 July 2024, *https://www.hrw.org/report/2024/07/17/i-cant-erase-all-blood-my-mind/palestinian-armed-groups-october-7-assault-israel*.
[183] Amy B. Zegart, "Israel's Intelligence Disaster," *Foreign Affairs*, 11 October 2023.
[184] Michel Wyss, "The October 7 Attack: An Assessment of the Intelligence Failings," *CTC Sentinel* 17, no. 9 (2024).
[185] Ibid.

to Gaza as an incentive for calm[186]. This mindset led to an overly optimistic underestimation of Hamas's intentions and capabilities, as Israeli officials came to view Hamas as unwilling to risk its rule in Gaza through a full-scale confrontation. Essentially, both Israeli intelligence and leaders did not imagine that Hamas wanted or dared to initiate a major war at that time, believing the group was deterred by potential Israeli retaliation and preoccupied with its local administration[187]. This turned out to be a grave miscalculation. In reality, Hamas's leadership was ideologically committed to armed struggle and had been meticulously planning a large attack, training fighters and stockpiling arms under the radar.

Another critical factor was overreliance on technological intelligence and automated surveillance, at the expense of classical human intelligence. Israel's defense apparatus had invested heavily in monitoring Gaza's border with sensors, cameras, and the high-tech "Iron Dome" anti-rocket system[188]. These tools had successfully managed smaller outbreaks, perhaps breeding a sense of confidence that any Hamas aggression would be quickly detected and neutralized. However, Hamas operatives effectively exploited gaps in this tech-focused security blanket. They conducted careful operational security, avoiding electronic communications, using underground facilities, and practicing on mock targets out of sight, thus evading Israel's SIGINT[189][190]. The attackers even managed to take down border surveillance towers and jam communications on the day of the attack, blinding the Israeli forces at the critical moment[191]. Within this context, Israeli secret services may have under-prioritized traditional HUMINT penetration of Hamas or misinterpreted the signs due to confirmation bias.

---

[186] Ibid.

[187] Larry Hanauer and Michael P. Connell, *Political Priorities, Poor Intelligence Tradecraft, and the Suppression of Dissenting Views: Why Israel Failed to Warn of Hamas's October 7 Attack* (Institute for Defense Analyses, 2024).

[188] Peter Dombrowski, Catherine Kelleher, and Ethan Auner, "Demystifying Iron Dome," *The National Interest* (126) (2013): 49–59.

[189] Katie Bo Lillis et al., "US Intelligence Warned of the Potential for Violence Days before Hamas Attack," *CNN*, October 13, 2023, *https://edition.cnn.com/2023/10/13/politics/us-intelligence-warnings-potential-gaza-clash-days-before-attack*.

[190] Pamela Brown and Zachary Cohen, "Hamas Operatives Used Phone Lines Installed in Tunnels under Gaza to Plan Israel Attack over 2 Years," CNN, 25 October 2023, *https://edition.cnn.com/2023/10/24/politics/intelligence-hamas-israel-attack-tunnels-phone-lines*.

[191] Human Rights Watch, "I Can't Erase All the Blood from My Mind".

Compounding these issues were organizational and leadership failures in the Israeli intelligence and security establishment. Investigations revealed that some warning signs were present but were dismissed or lost in bureaucratic channels. For example, lower-level analysts and even the Israel Defense Forces (IDF) field observers had reported unusual indicators: increased training exercises by Hamas, simulations of breaching the border fence, and other anomalies that suggested preparation for a large-scale attack[192]. However, these reports were largely ignored by superiors, as they conflicted with the widespread presumption that Hamas would refrain from undertaking such an offensive[193]. Israeli intelligence lacked effective mechanisms for challenging established assumptions. Nonetheless, "devil's advocate" structures to poke holes in the conventional wisdom are present and eminent in the Israeli system. Notably, in the weeks prior to the attack, the Head of IDF Devil's Advocate unit distributed reports and gave presentations to top military and political leaders, contending that underlying changes in the strategic landscape pointed to an imminent offensive. Nevertheless, his warnings – contradicting the dominant conception that Hamas preferred stability in Gaza – were disregarded, illustrating the reluctance of senior officials to consider analyses that challenged their established assumptions[194]. This offset the effectiveness of tailored mechanisms for improving intelligence analysis and once again meant that dissenting views can be easily brushed aside by senior analysts or commanders who are confident in the existing paradigm. In addition, Israeli intelligence collection efforts had been partly reoriented away from Gaza in prior years, due to shifting priorities. The government's focus had tilted more towards threats like Iran's nuclear program and Hezbollah in the north. Domestically, there was political tumult and a controversial judicial reform debate consuming attention in 2023. These factors contributed to strategic myopia: Hamas was considered a secondary threat that was being managed, until it was not anymore. Reports indicate that even foreign intelligence services tried to warn Israel[195]. For instance, Egyptian officials allegedly informed Israel that Hamas was preparing

---

[192] Hanauer and Connell, *Political Priorities, Poor Intelligence Tradecraft*.
[193] Ronen Bergman and Adam Goldman, "Israel Knew Hamas's Attack Plan More Than a Year Ago," *The New York Times*, 30 November 2023, *https://www.nytimes.com/2023/11/30/world/middleeast/israel-hamas-attack-intelligence.html*.
[194] *Times of Israel*, "Head of IDF Devil's Advocate Unit Tried Repeatedly in September to Warn of Possible Hamas Attack," 6 January 2024, *https://www.timesofisrael.com/liveblog_entry/head-of-idf-devils-advocate-unit-tried-repeatedly-in-september-to-warn-of-possible-hamas-attack/*.
[195] Hanauer and Connell, *Political Priorities, Poor Intelligence Tradecraft*.

an operation of considerable magnitude shortly before October 7, but such warnings did not spur action[196].

When analyzing the failure, we can thus conclude it was not a single-point failure but a systemic breakdown involving both intelligence and decision-making lapses. In fact, some argue October 7 was not entirely an intelligence failure in the narrow sense – because pieces of intelligence did exist – but rather a failure of leadership to heed intelligence. Indeed, Israel had the capacity to collect and analyze the relevant information (and collected some of it), but institutional and cognitive issues prevented that information from being believed or acted upon in time. This mirrors the classic pattern identified in prior cases of surprise attacks: a mix of biases, indications that get misinterpreted or ignored, and poor information sharing and coordination between levels of command[197]. Israeli intelligence, like others before, fell victim to what scholars of warning intelligence call the fog of certainty, a perspective in which leadership becomes so certain of its paradigm that it overlooks contradictory signals until it's too late[198].

Nevertheless, attempts to extract constructive lessons have given rise to a thorough process of reflection in the aftermath of the attack, which could contribute to future improvements. For instance, Israeli authorities moved swiftly to acknowledge the failure. Major General Aharon Haliva, head of Aman (Military Intelligence), openly acknowledged that, during his tenure, the Military Intelligence Directorate did not succeed in anticipating the Hamas assault. He admitted that the directorate had fallen short in its core mission and accepted personal responsibility for this failure in his capacity as its head[199]. This level of accountability is the first step toward reform, and Israel has historically been good at learning from such debacles. The post-1973 Agranat Commission, for example, led to significant changes in the Israeli IC to avoid a similar trap. Already, intelligence professionals and scholars are emphasizing the need to revive the discipline of warning intelligence within the community. Notably, the U.S. abolished the position of National

---

[196] *Times of Israel*, "Egypt Intelligence Official Says Israel Ignored Repeated Warnings of 'Something Big'," 9 October 2023, *https://www.timesofisrael.com/egypt-intelligence-official-says-israel-ignored-repeated-warnings-of-something-big/*.

[197] Hanauer and Connell, *Political Priorities, Poor Intelligence Tradecraft*.

[198] Dror Michman and Yael Mizrahi-Arnaud, "The Fog of Certainty: Learning from Intelligence Failures of the 1973 War," Brookings Institution, 23 October 2017.

[199] *Times of Israel*, "IDF Intel Chief Says He 'Bears Full Responsibility' for Not Warning of Hamas Attack," 17 October 2023, *https://www.timesofisrael.com/idf-intel-chief-says-he-bears-full-responsibility-for-not-warning-of-hamas-attack/*.

Intelligence Officer for Warning, assuming that each analyst would handle warning in their area[200]. Another crucial aspect consists in reinvesting in specialist training for analysts to "think outside the box" and thus overcome groupthink in order to dispose of any kind of conceivable scenario. There is also a recognition that intelligence must integrate human insight with technology more efficiently. No matter how advanced electronic surveillance is, it must be paired with penetrating the adversary's inner decision circles to truly know intent. Israel should thus bolster its HUMINT efforts against groups like Hamas by trying to recruit sources inside, improving Arabic linguistic skills, and paying attention to enemy communications culture.

In sum, the Israel–Hamas 2023 case highlights the danger of strategic complacency. The primary positive dimension of this case lies not in the events themselves but in the aftermath, namely the opportunity it generated for institutional learning and reform. The attack has opened debate in Israel about reforming intelligence practices, much as 9/11 did in the U.S. While the surprise was devastating, it has forced a reckoning with biases and system weaknesses. Internationally, this case also serves as a cautionary tale: even world-class intelligence services can be damaging if they become victims of their own success and assumptions. The emphasis going forward will likely be on fostering a culture that values dissenting analysis, imaginative scenarios, and continuous re-examination of adversaries' intentions, ensuring that intelligence practitioners speak up even if their warnings challenge the prevailing view, and that policymakers listen when they do.

3.4 Case 4 – U.S. Withdrawal from Afghanistan (2021): Inconsistent Forecasts and Operational Deafness

For our last case we will deconstruct, from an intelligence point of view, the chaotic fall of Kabul in August 2021, during the final withdrawal of U.S. forces from Afghanistan. This represents a contemporary example where intelligence warning and policy execution misaligned, resulting in a major crisis. In this case, shared responsibility for the failure is evident: the intelligence community provided some warnings, though with significant uncertainty and inconsistency, while policymakers failed to fully heed or act on those indications. The outcome – the Taliban's rapid

[200] Hanauer and Connell, *Political Priorities, Poor Intelligence Tradecraft*.

sweep to power and the rushed evacuation from Kabul's airport – suggests a disconnect between analysis and decision, or what might be termed operational deafness on the part of leadership. This scenario is particularly illuminating because it did not materialize as a sudden surprise like 9/11 or the October 7 attack. Indeed, the crisis was a drawn-out collapse that many observers predicted in broad strokes yet unfolded faster and more disastrously than almost anyone anticipated.

In the months leading up to the withdrawal, U.S. intelligence analysts assessed that the Western-backed Afghan government and its military could fall to the Taliban, but their forecasts varied widely on timing and were often too optimistic[201]. Early assessments in 2021 generally predicted the Afghan National Defense and Security Forces might hold out for a considerable period after U.S. troops left. Yet as conditions on the ground worsened during July and August, intelligence assessments became progressively more pessimistic, though they continued to underestimate the rapidity of the Taliban's advance. For instance, by mid-August 2021, when Taliban fighters were at Kabul's gates, intelligence assessments were reportedly suggesting that Kabul could fall "within a month to 90 days"[202]. In reality, Kabul fell almost immediately – on August 15, a couple of days after those estimates were made. This indicates that while warning was given, it was imprecise and consistently undershot the speed of events, failing to provide the anticipation feature, considerably required in the context of crises. Different agencies were even in profound disagreement. The CIA allegedly presented more pessimistic forecasts about the Afghan army's will to fight[203], whereas other bodies were somewhat more confident that Kabul might stand longer. These inconsistencies diluted the urgency of the warning message reaching top decision-makers.

On the policy side, there was a noticeable reluctance to act on the worst-case warnings. President Biden's administration, committed to ending the 20-year war, appeared to discount the direst predictions of a rapid Taliban victory. Even as intelligence grew more alarmed in July 2021, the administration did not significantly change its withdrawal timeline or execute robust contingency

---

[201] Council on Foreign Relations, "The Taliban in Afghanistan," 15 August 2023, *https://www.cfr.org/backgrounder/taliban-afghanistan*.

[202] Claire Mills, *Afghanistan: Fall of the Government and the Transition of Power* (House of Commons Library Research Briefing no. 9299, August 17, 2021), *https://researchbriefings.files.parliament.uk/documents/CBP-9299/CBP-9299.pdf*.

[203] Julian Borger, Hugo Lowell, and Dan Sabbagh, "'A Massive Policy Fail': CIA Warned White House of Swift Taliban Takeover," *The Guardian*, 18 August 2021, *https://www.theguardian.com/world/2021/aug/18/massive-policy-fail-cia-warned-taliban-takeover*.

plans (such as the early evacuation of at-risk Afghan allies) until the very last moment[204]. In particular, A U.S. Senate Foreign Relations Committee review later criticized this behavior, stating: "Despite countless warnings that the Taliban had the ability to take the country swiftly, the Biden Administration failed to properly plan a coordinated evacuation […] The administration waited until less than a day before Kabul fell to make senior leadership decisions on organizing and executing a withdrawal, which proved to be too little too late"[205]. This quote underscores that numerous warnings coming from intelligence reports, diplomats in the field and military commanders, had signaled the Taliban's rapid advances, yet the planning for evacuation was delayed until essentially the eve of Kabul's collapse. Policymakers in Washington heard the warnings but seemingly did not trust them or failed to act with the urgency required – a case of what one might call "operational deafness." The main reason for this included overconfidence in the Afghan government. 38 days before Kabul fell, President Biden dismissed suggestions of an inevitable collapse, highlighting Afghanistan's sizeable and well-armed security forces, estimated at 300,000 personnel[206]. Moreover, perhaps a general fatigue after two decades of war which created an optimistic bias that getting out could be managed smoothly.

From an intelligence analysis perspective, this case reveals the challenge of forecasting collapse in a complex political and military context. The Taliban's victory was not an unpredictable event but a culmination of a long trend of insurgent gains once external support was withdrawn[207]. Yet, predicting the exact pace of collapse is notoriously difficult. As scholarly literature on warning notes, broad strategic warning often does not provide the actionable specifics in terms of timing and method that are essential for decision-makers to confidently preempt a crisis[208]. Indeed, in Afghanistan, analysts transmitted the strategic warning that without U.S. support, the regime could fall, but the tactical warning, indicating that it could all unravel in essentially a week, was absent.

---

[204] United States Senate Committee on Foreign Relations, *Left Behind: A Brief Assessment of the Biden Administration's Strategic Failures during the Afghanistan Evacuation.* Minority Report (Washington, DC: GPO, February 2022).
[205] Ibid.
[206] Madeleine Ngo, "Biden Defends Decision to Pull Out of Afghanistan," *The New York Times*, 16 August 2021. *https://www.nytimes.com/live/2021/08/16/us/politics-news*.
[207] Council on Foreign Relations, Center for Preventive Action, "Instability in Afghanistan," *Global Conflict Tracker*, 12 February 2025, *https://www.cfr.org/global-conflict-tracker/conflict/war-afghanistan*.
[208] James J. Wirtz, "Are Intelligence Failures Still Inevitable?", *International Journal of Intelligence and CounterIntelligence* 37, no. 1 (2024): 307–330.

This left a gray zone in which decision-makers could interpret the situation according to their hopes. Cognitive bias played a role too: U.S. officials, recalling that Kabul did not fall even in the face of major Taliban offensives earlier, might easily have fallen prey of mirror-imaging, thus assuming the Afghan side would at least put up a prolonged defense, as they themselves would in that position[209]. Additionally, organizational factors limited adaptability. Once the White House had set an end-of-August withdrawal date[210], the bureaucracy was slow to adjust that plan even as conditions changed.

Despite the disastrous outcome, there were some elements of this case that can be viewed in a positive or at least mitigating light when strictly analyzing the event from an intelligence point of view. First, some parts of the IC did anticipate the possibility of rapid Taliban gains and tried to raise alarms. This shows that the IC was not completely blindsided; there was diversity of views, and the most pessimistic, sadly, turned out to be closest to reality. Had those warnings been absent, the evacuation might have been an even greater disaster.

The second aspect to consider is accountability and learning. Much like other cases, the Afghanistan withdrawal fiasco has prompted reviews and debates in Washington about how to avoid such failures. Congressional committees held hearings, and reports have examined the episode to distill lessons. These include the importance of earlier contingency planning when intelligence hints at worst-case outcomes, and better coordination between intelligence predictions and policy decisions. In essence, the case is already influencing thinking on how future warning intelligence is handled in policymaking – a recognition that when multiple indicators point to a possible disaster, leaders should err on the side of preparation even if the timing is uncertain[211][212]. The U.S. government has since adjusted some processes for forecasting foreign stability and is

---

[209] Dahl, *Intelligence and Surprise Attack*, 9–11.

[210] U.S. House of Representatives, Committee on Foreign Affairs. *An Assessment of the Biden Administration's Withdrawal from Afghanistan by America's Generals.* Hearing Before the Committee on Foreign Affairs. 118th Congress, Second Session. March 19, 2024. Serial no. 118–89 (Washington, DC: U.S. Government Publishing Office, 2024).

[211] U.S. Senate Committee on Foreign Relations, *Left Behind.*

[212] U.S. House of Representatives, Committee on Foreign Affairs, *Willful Blindness: An Assessment of the Biden-Harris Administration's Withdrawal from Afghanistan and the Chaos that Followed* (Washington DC: U.S. House of Representatives, September 8, 2024), *https://foreignaffairs.house.gov/sites/evo-subsites/foreignaffairs.house.gov/files/migrated/uploads/2024/09/WILLFULL-BLINDNESS-An-Assessment-of-the-Biden-Harris_Administrations-Withdrawal-from-Afghanistan-and-the-Chaos-that-Followed.pdf*.

more actively monitoring so-called "critical warning problems" (cases where a friendly government could rapidly collapse, for example). This is reminiscent of past intelligence-policy lessons, echoing Richard Betts' famous argument that often the problem is not complete lack of warning, but decision-makers failing to believe or act on it[213]. Afghanistan 2021 will likely be a case study reinforcing that argument in future intelligence education.

In summary, the Afghanistan withdrawal exemplifies a situation where intelligence was marginal in influence – it provided a range of scenarios, including dire ones, but could not compel its consumers to prepare adequately. The forecasts were inconsistent and imprecise, which gave policymakers latitude to choose a rosier interpretation. When that proved erroneous, the resulting scramble was attributed to both intelligence failure and policy failure. The truth is that both sides share blame, hence shared responsibility. Ethically, it raises further questions of how intelligence officers can or should press their case when they see a disaster coming. Organizationally, it highlights the eternal challenge of warning: getting it exact at the precise time, and getting it heeded by the right people. After-action analyses have already called for strengthening the interface between analysts and decision-makers so that warning signs are communicated with greater clarity and urgency, perhaps even at the risk of "crying wolf." It is preferable, the lesson suggests, to have policymakers complain about false alarms than to have them deaf to real ones.

3.5 Comparative Analysis: Results and Conditions for Effective Intelligence

Examining these four cases side by side reveals recurring themes about when intelligence succeeds in influencing outcomes and when it fails. A clear pattern emerges: intelligence tends to be most effective when it is integrated, communicated, and trusted. Nonetheless, even when the stakes are high, it is systematically undermined by fragmentation, cognitive bias, and reluctance or inability of policymakers to act on it. Each case provides evidence for certain enabling or hindering conditions: first, the importance of integration, which is notably illustrated by 9/11. There, the failure to share and fuse intelligence across agencies was the single biggest factor that kept the

[213] Richard K. Betts, "Surprise despite Warning: Why Sudden Attacks Succeed," *Political Science Quarterly* 95, no. 4 (1980–81): 551–572.

warning signals from coalescing into a useful alert. Conversely, in the Ukraine 2022 case, integration across allied services and between classified and open-source intelligence bolstered the credibility of warnings. A key condition for effective use of intelligence, therefore, is having structures that promote all-source analysis and timely information exchange. Modern threats often cross jurisdictional lines (foreign/domestic, military/civilian), so a harmonizing system becomes fundamental. Additionally, the Israeli case shows that even working within a single country's IC, stovepipes or narrowed focus can develop and often lead to blind spots. The comparative lesson is that intelligence organizations must strive for holistic coverage and fight the instinct to work in silos. Horizontal communication (among agencies and analysts) and vertical communication (to political leaders) must be clear and unencumbered. Indeed, any systemic hindrance preventing sharing will inevitably reduce the chances of accurate prediction and prevention of crises.

Second, all cases underline the role of human factors in terms of cognitive and analytical rigor. Intelligence is ultimately a rational activity done by people, who can ultimately err. The 9/11 and October 7 failures both involved what psychologists call confirmation bias and groupthink. In 2001, there was a failure of imagination, assuming terrorists wouldn't do something as audacious as flying planes into buildings, and some mirror-imaging by thinking a non-state actor could did not have the means to strike so effectively on U.S. soil[214]. In Israel's case, groupthink around the "Hamas wouldn't dare" notion prevailed[215]. These show that an intelligence system is only as good as its capacity to challenge its own assumptions. Conditions that favor effective intelligence include fostering a culture of analytic dissent and periodic review of prevailing judgments. Where such a culture is lacking, systematic difficulties emerge: warning signs get rationalized away, and intelligence becomes an echo chamber. By contrast, in the lead-up to the Ukraine invasion, one could argue the U.S. IC had learned from past mistakes and actively questioned optimistic assumptions about Putin's intentions, thereby getting the analysis right. It's significant that the intelligence there was building on multiple sources, including presumably some excellent human sources close to the Kremlin, which gave confidence to challenge skeptics.

---

[214] U.S. Department of Defense, Wolfowitz to Rumsfeld, "Were We Asleep?" memo, cited in *9/11 Commission Report*, 336.
[215] Hanauer and Connell, *Political Priorities, Poor Intelligence Tradecraft.*

Third, even the best intelligence is futile if leaders ignore it. This is a consistent thread and our cases extensively echo that. In Afghanistan 2021, warnings of a Taliban takeover were largely acknowledged but not operationalized – the administration did not want to slow or reverse withdrawal plans, so warnings were psychologically discounted. In 9/11, as Marrin argues, policy leaders knew al-Qaeda was a grave threat yet did not elevate counterterrorism high enough on the agenda to force systemic fixes before disaster[216]. A similar episode occurred before the October 7 attack, when political leadership was arguably distracted and complacent, failing to prioritize the Gaza threat despite warnings from abroad and below. By contrast, in the Ukraine case, the political leadership were very receptive to intelligence; they chose to act on the warnings by sharing them and using them diplomatically. This impeccably showcases that a crucial condition for intelligence impact is the consumer's attitude. Effective use of intelligence occurs when decision-makers have trust in their intelligence community, have the willingness to hear unpleasant news, and are ready to take preventive or preparatory actions based on analysis. What hinders influence systematically is when leaders bring their own biases or policy agendas that cause them to dismiss or downplay intelligence that does not fit their hopes. Rebuilding and maintaining credibility is thus key. An ethical challenge here is ensuring intelligence is seen as apolitical and objective, so that when real warnings come, they are not met with cynicism.

Additionally, the cases we examined highlight that vague or broad warnings often fail to spur action. A systemic issue in intelligence is that analysts can usually identify dangers but struggle to pin down specifics like timing and method. As a result, policymakers, faced with ambiguity, may choose inaction by default, since taking drastic preventive action is costly and hard to justify without concrete evidence[217]. For example, intelligence told the U.S. leaders that Afghanistan might collapse eventually, but not "Kabul will fall on August 15," so preparation was insufficient. In Israel, there was a general sense that Hamas remained hostile, but not a pin-point warning about a detailed plan of Hamas. Without that level of accuracy, leaders often gamble that nothing immediate will happen. However, the Ukrainian case represents a rather successful warning in terms of specifics. Intel was unusually exhaustive in predicting the invasion window and force composition, which made it more compelling. This underscores that improving the specificity of

[216] Marrin, "The 9/11 Terrorist Attacks".
[217] Omand, *How to Survive a Crisis.*

warning (when possible) can favor its effectiveness. It also speaks to a need for decision-makers to be trained to appreciate even uncertain warnings – to actively build on intelligence assessments that indicate high risk, instead of waiting for near-certainty. Indeed, this may never arise, as in intelligence there is no crystal ball. Too often, a systemic hindrance is that bureaucracies reward certainty and clear signals, whereas warnings are mostly probabilistic. This can lead to inertia in the face of weak signals until those signals strengthen. Developing frameworks for "no regret" actions that can be taken in response to warnings, even if they do not materialize, is one approach to overcome this reluctance.

Finally, our research question posits whether intelligence might move from a marginal, advisory role to a more influential and active one, perhaps even to the point of the intelligence practitioner as decision-maker. The comparative evidence provides a mixed answer. On one hand, the case about the invasion of Ukraine shows intelligence can step into a very vigorous role: shaping public messaging, rallying allies, and essentially driving policy direction. This hints at a future where intelligence agencies are not just quiet advisors but integral players in the policy arena, engaging with media and international partners directly. On the other hand, such a role expansion raises ethical and accountability concerns. Indeed, in democratic systems, intelligence officers are not elected, therefore if they start making or heavily steering decisions, it could blur lines of responsibility. Imagine, for instance, intel officers deciding unilaterally to release sensitive information or to take covert action to preempt threats. There is also the danger of intelligence becoming politicized if it gets too entangled with advocating specific policies. The tradition has been that intel provides the input, and elected leaders make the call, thus maintaining a check and balance. Our cases, despite some promising results, reinforce why that separation exists. Consider the Iraq WMD tragedy, where intelligence was used to justify a policy and lost credibility. If intelligence leaders had direct decision power, a similar misjudgment could have even more dire consequences without political debate. Importantly, the Israeli and U.S. examples show that often after failures, intelligence professionals are brought into closer counsel with policymakers to ensure their warnings are front and center. Ultimately, a future scenario where an intelligence practitioner becomes the decision-maker might be conceivable in narrow domains. But generally, elevating intelligence's role means giving it a stronger voice within the decision process, not replacing the decision-makers. The comparative analysis thus suggests the best outcome is when intelligence and

policy operate in tandem – intelligence offering candid, unvarnished foresight and options, and policy actors willing to be guided by that insight while applying ethical and political judgment. Achieving this balance involves building and maintaining trust: policymakers must trust intelligence enough to factor it heavily into decisions, and intelligence officers must trust policymakers to use their product wisely and not as a political football. When that mutual trust and clear delineation of roles exists, intelligence can truly be a force-multiplier for national decision-making by helping anticipate crises before they explode and guiding leaders in navigating them ethically and effectively.

4. Intelligence as a Strategic Actor: Prospects and Limits

In this final chapter, we will assess how intelligence can assume a more influential role in political decision-making, despite lacking key features. Building on the obstacles and case studies discussed earlier, we consider the contexts in which elevating intelligence's voice would be most sensible, the new and future frontiers that could expand intelligence's strategic contribution, and the steps needed to foster a true culture of anticipation. Ultimately, despite determining that the figures of intel analysis and decision-makers cannot overlap, we find that intelligence can play a more central role in guiding policy. Yet, realizing this potential requires adapting institutions and mindsets. Thus, by exploring both prospects and limits, we aim to answer our research question and offer recommendations for better integrating foresight into governance.

4.1 Justifying a More Central Role for Intelligence

Not all policy decisions merit a heavier intelligence hand. In routine matters or low-stakes issues, political judgment and public values appropriately dominate. However, there are certain scenarios where, giving intelligence a louder voice could be crucial. These are typically complex, ambiguous, high-impact crises, in which early warning and expert risk assessment might spell the difference between disaster and mitigation. In the context of crisis management, there is broad agreement that "earlier equates with better"[218]. In other words, the earlier a potential crisis is detected and understood, the easier it is to diminish its scope or prevent it altogether. Consequently, high-impact, fast-moving threats like terrorist attacks or military invasions become obvious cases where intelligence warnings should carry great weight. As seen in our case studies, when such warnings are ignored, the consequences can be shocking (e.g., the 9/11 attacks). But beyond sudden threats, creeping crises also demand an elevated intelligence role. Consider global pandemics or emerging biosecurity dangers: well before COVID-19 struck, experts had warned of a high likelihood of a severe pandemic[219]. Yet those strategic warnings remained largely on the periphery of policy

[218] Florence Gaub, "Enhancing Early Warning and Preparedness," in *Crisis Rooms: Towards a Global Network?*, ed. Patryk Pawlak and Andrea Ricci (Paris: EU Institute for Security Studies, 2014), 78–82.
[219] Erik J. Dahl, *The COVID-19 Intelligence Failure: Why Warning Was Not Enough* (Washington, DC: Georgetown University Press, 2023).

agendas. When the coronavirus threat materialized, governments lacked timely, actionable intelligence on the outbreak's development, and many leaders were unreceptive even to the warnings that did arrive[220]. The result was a costly intelligence-policy failure. Had intelligence assessments of the novel virus's spread and lethality been given more urgent attention in early 2020, responses could have been mobilized even weeks sooner – and studies indicate that even few weeks in advance can massively reduce deaths and damage in a pandemic[221]. In short, complex crises marked by uncertainty but extreme stakes are prime candidates for a stronger intelligence role. When traditional political actors are prone to underestimating ambiguous threats or delaying action, an empowered intelligence voice advocating precaution can help overcome inertia. This applies to other "slow-burn" crises as well, such as climate-related security threats or financial system instabilities, where intelligence forecasts and indicators might prompt preventive measures that politics alone would neglect.

Another factor is when a crisis crosses technical or domain boundaries unfamiliar to policymakers. Health threats are again illustrative: bridging the gap between medical science and national security requires intelligence analysts who can translate epidemiological signals into national-level warnings. Some have even proposed creating specialized intelligence units for such domains. For example, one recommendation after COVID-19 was to elevate the U.S. National Center for Medical Intelligence to an independent national center discussing directly with top leadership, enhancing the visibility and clout of health-related warnings[222]. Countries like the UK and Canada have also launched dedicated health intelligence bodies to ensure pandemics trigger high-level alerts[223]. Elevating intelligence in these cases makes sense because traditional policy departments might not recognize the urgency of technical threats. Similarly, cyber security is an area where intelligence agencies often have superior situational awareness.

A related context is when dealing with hybrid transnational threats that no single institution can tackle alone. Issues like international terrorism networks, hybrid warfare, or global criminal syndicates benefit from intelligence-led coordination. If intelligence assessments indicate an

---

220 Ibid.

221 Sen Pei et al., "Differential Effects of Intervention Timing on COVID-19 Spread in the United States," *Science Advances* 6, no. 49 (2020).

222 Dahl, *The COVID-19 Intelligence Failure.*

223 Ibid.

imminent terrorist plot or a hostile influence campaign, there is a compelling case for those assessments to drive the agenda – perhaps even to temporarily guide policy response across agencies. In such multifaceted crises, intelligence agencies sometimes serve as de facto crisis managers by virtue of their information advantage. The goal is not for unelected intelligence officials to replace policymakers, but for their warnings and expertise to set the tempo of the response, as we noticed in the case of the 2022 invasion of Ukraine. The provided warnings, unusually, were even shared with the public and allies in an effort to galvanize action. Importantly, the intel was largely correct and prompted earlier preparations than would have occurred otherwise, such as sanctions and military aid. While the decision to publicly release those warnings was ultimately a political one, it shows intelligence taking a central role in shaping diplomatic and security strategy to mitigate the effects of an imminent crisis.

Finally, we must consider the rise of private intelligence and whether it is more suitable in some respects to play a more influential anticipatory and decisional role. In recent decades, a vast ecosystem of private-sector intelligence firms and in-house corporate analytic teams has emerged. These entities, though outside government, function very similarly, collecting information (mostly openly) and providing analysis to clients about threats ranging from geopolitical instability to cyber-attacks[224]. Although private intelligence firms do not possess the state's legal mandate to gather classified information, they often demonstrate greater adaptability in exploiting open sources and applying novel analytical methods. In contexts where much of the relevant data is open-source (social media, commercial satellite imagery, public health data), private outfits may actually have an advantage in agility. For instance, months before Russia's 2022 invasion, some corporate security firms correctly assessed the high risk of war and advised their clients accordingly. Notably, the firm Global Guardian recommended that its corporate clients withdraw staff from Ukraine a month prior to the outbreak of war and actively assisted by coordinating evacuations and providing protective resources[225]. Similarly, Sibylline cautioned of the impending invasion and broadened its outreach by openly sharing reports with all organizations operating in

[224] Sage-Passant, "The Security Intelligence Services of the Private Sector".
[225] Global Guardian, "Case Study: Emergency Response" (Ukraine, 2022), *https://www.globalguardian.com/case-studies_emergency-response-ukraine*.

the area, extending critical intelligence beyond its client base. These examples underscore that actionable warning is no longer the sole province of government agencies.

Furthermore, private firms often employ former government analysts and apply rigorous tradecraft, but with fewer bureaucratic constraints they might ring alarm bells faster. Moreover, they tend to maintain a close focus on specific risk portfolios (for a company or sector), meaning their warnings can be very tailored and concrete compared to broad governmental warnings. This democratization of intelligence means that decision-makers can benefit from a plurality of warning inputs, not just secret intelligence. However, private intelligence is not the ultimate remedy. These actors lack direct access to the highest levels of government where critical decisions are made, and their advice carries no official authority. They also may face commercial biases as firms answer to clients, which could skew priorities. Thus, while private intelligence can sharpen early warning and indeed should be integrated into an all-source warning system, ultimately governmental intelligence must still synthesize these inputs and present them in national decision forums. The rapid rise of private intelligence does, however, suggest that if state intelligence agencies are too slow or constrained, others will address the shortfall. In high-impact crises, it makes sense for governments to welcome credible outside analysis and perhaps even elevate some of these external voices into advisory roles. For example, tapping academic and private experts on emerging threats (pandemics, climate security, etc.) can enrich the intelligence picture and lend it greater influence.

In summary, elevating the role of intelligence is most warranted in scenarios where uncertainty is high but the cost of surprise would be catastrophic. In such cases, intelligence warnings and scenario assessments should be given primacy in policy deliberations. This could mean institutionalizing channels for urgent warnings to reach top leaders and for leaders to be obliged to respond. Intelligence may even at times drive policy for short periods, for example when an evacuation or preemptive action is clearly indicated by incoming intelligence, both in private and public crises. The key rationale is that professional intelligence personnel are trained to peer through ambiguity and imagine worst-case scenarios that political minds may discount. Still, this comes with a major caveat: if intelligence is to take on a more central role, policymakers must be willing to listen and act.

4.2 Present and Future for Intelligence in Emerging Crises

Alongside the rising number of actors involved in the intelligence process, the range of variables shaping the environment in which crises emerge continues to expand. As a result, the broader landscape of intelligence is undergoing rapid transformation. On one hand, more complex technology and the explosion of open information have empowered intelligence agencies with unprecedented tools. On the other hand, the world is facing hybrid threats and novel crisis domains that test the limits of traditional intelligence methods. Here we examine these new frontiers and how they could enable – or sometimes constrain – a more central role for intelligence in decision-making.

Technological advancements have greatly expanded intelligence capabilities. Over the past two decades, sensors like satellites and drones have become more numerous and less expensive, yielding constant streams of imagery and signals from every corner of the globe[226]. Big Data analytics and artificial intelligence are being applied to scrutinize massive volumes of information, helping detect patterns or anomalies that might signal an emerging crisis[227]. For example, machine-learning algorithms can monitor global news and social media in real time for early indicators of conflict or disease outbreaks. This has given rise to what some call "predictive analytics" in intelligence – attempts to forecast events by correlating trends in open data[228][229]. The promise of these technologies is that intelligence services can cast a much wider net and perhaps catch weak signals that humans would miss. Indeed, one positive lesson from recent successes is that integrating OSINT with secret intelligence can greatly enhance warning. In the Ukraine case, U.S. and UK agencies paired their classified findings with OSINT (like commercial satellite photos and social media posts) to convince allies of the threat, and independent OSINT researchers externally validated many of the governments' claims[230]. This synergy not only improved the accuracy of

[226] Zegart, *Spies, Lies, and Algorithms*.
[227] Ibid.
[228] Ibid.
[229] Patrick L. Bokonda et al., "Predictive Analysis Using Machine Learning: Review of Trends and Methods," in *2020 International Symposium on Advanced Electrical and Communication Technologies (ISAECT)* (2020): 1–6.
[230] Huw Dylan, "Kyiv, 2022 – Russia's Full-Scale Invasion of Ukraine," in *Contemporary Intelligence Warning Cases: Learning from Successes and Failures*, ed. B. E. M. Grønning and S. Stenslie (Edinburgh: Edinburgh University Press, 2024), 253–271.

analysis but also its credibility, showing a model for future crises where public and private data are fused for maximum impact.

Moreover, technology has democratized intelligence collection in surprising ways. We live in a world where "we are all intelligence officers now," as analyst Dan Geer quipped[231]. Consider that anyone with an internet connection can access real-time satellite imagery, track flights or ships, or analyze online chatter with free tools. The digital era has blurred the line between what is secret and what is knowable through open data. This means that intelligence as a function is no longer confined to government. A tech corporation like Microsoft, for example, monitored in 2024 over 78 trillion security signals per day across its networks, effectively making it one of the world's largest SIGINT collectors[232]. For governments and decision-makers, this new reality offers both opportunity and challenge. The opportunity lies in leveraging these external capabilities to enrich official intelligence. The challenge is the diminished monopoly of intelligence: agencies must assert their relevance in an environment where policymakers are courted by numerous competing sources of information[233]. Leaders today are flooded with data from news, social media, and private reports alongside traditional intel briefings. If an intelligence agency's insights are slow, overly secretive, or indistinguishable from what open sources provide, its influence will fade. Thus, to maintain a central role, agencies need to harness innovative tech and OSINT themselves, and provide value-added analysis.

At the same time, contextual developments may offset tech gains, making warning harder even with better tools. The rise of hybrid threats is a case in point. The European Commission defines them as such: "mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the

---

[231] Dan Geer, "We Are All Intelligence Officers Now," RSA Conference Speech, San Francisco, 2014, *https://docs.huihoo.com/rsaconference/usa-2014/exp-f02-we-are-all-intelligence-officers-now.pdf*.

[232] Microsoft, *Microsoft Digital Defense Report 2024: The Foundations and New Frontiers of Cybersecurity* (Redmond, WA: Microsoft, 2024), *https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024*.

[233] Bjørn Elias M. Grønning and Stig Stenslie, "Conclusion: Towards Better Warning – Lessons and Recommendations for Intelligence," in *Contemporary Intelligence Warning Cases*, ed. B. E. M. Grønning and S. Stenslie (Edinburgh: Edinburgh University Press, 2024), 288–292.

threshold of formally declared warfare"[234]. These threats often unfold in the gray zone between war and peace, testing the ability of standard intelligence and defense mechanisms to respond. For example, a state adversary might use cyber infiltrations and fake news to destabilize a country without ever sending troops, leaving policymakers unsure if a crisis is occurring or not. In such scenarios, intelligence agencies are on the front lines. The challenge is that hybrid operations are designed to be ambiguous and deniable. Thus, intelligence must not only detect these subtle, multi-domain aggressions but also persuade decision-makers of their reality and severity. While threats are becoming more transnational and multifaceted, intelligence cooperation across national and bureaucratic boundaries becomes essential. A cyber or pandemic threat does not respect borders or agency turf. New forms of international intel collaboration are needed, as noted by experts: issues like climate change, pandemics, and hybrid warfare necessitate the development of novel cooperative mechanisms among intelligence and security services[235]. Therefore, sharing information and analytic burden is the only viable path to cover the increasingly diverse threat spectrum[236].

In emerging crisis domains, intelligence agencies are also redefining their roles. Public health crises are a prime example. Historically, epidemic warning fell to health organizations and scientists. Nonetheless, after COVID-19, many governments realized that national security intelligence should also monitor health indicators – not to supplant medical experts, but to add global collection competency and to secure the attention of top leaders. We see nascent steps in this direction (e.g., Britain's Joint Biosecurity Centre) and calls for intelligence to work more openly with the medical community[237]. Similarly, on climate change, intelligence agencies have begun assessing how climate stress can spark conflicts or crises, feeding those insights to policymakers. This broadening of intel's remit to non-traditional threats supports a more anticipatory governance model. However, it also stretches intelligence thin. As one study observed, after 2001 many agencies focused so much on terrorism that they neglected other areas, contributing to failures like the unanticipated

---

[234] European Commission, *Joint Framework on Countering Hybrid Threats: A European Union Response* (Brussels: European Commission, 6 April 2016).
[235] Danny Pronk and Claire Korteweg, *Sharing the Burden, Sharing the Secrets: The Future of European Intelligence Cooperation* (Clingendael Report, Clingendael Institute, 2021), *https://docs.clingendael.org/sites/docs/files/2021-09/EU-intelligence-cooperation.pdf*.
[236] Ibid.
[237] Dahl, *The COVID-19 Intelligence Failure.*

2008 Russo-Georgia war[238]. Now, with an even wider array of concerns (health, climate, cyber, etc.), prioritization is difficult. Intelligence organizations will need to continually adapt, possibly with specialized units or partnerships for these new areas, to ensure depth of expertise. Indeed, the risk of information overload is real. More data does not automatically mean better insight. In fact, an excessive quantity of raw information can obscure warnings unless properly processed. Analysts can be overwhelmed by noise, and important weak signals might be lost in the confusion.

Furthermore, technology has introduced new vulnerabilities alongside capabilities. Adversaries can use the same open information and AI tools to spread sophisticated disinformation or even to deceive intelligence agencies. "Deepfake" videos or fake social media narratives can mislead analysts and the public, making it harder to discern truth and spreading misinformation. Thus, a core function of intelligence moving forward will be to serve as a reality check by verifying facts and providing an accurate picture amid the fog in order to achieve its aim of preventing crises. This is a role intelligence must play not just behind closed doors but at times in the public realm, to counteract false narratives. We saw a glimpse of this in 2022 when U.S. intelligence publicly released information to preempt Russian disinformation, thus seizing control of the narrative. This unconventional use of intel to fight an information war openly may therefore become more common in hybrid scenarios.

Lastly, even as we embrace high-tech solutions, the human element of intelligence remains irreplaceable. The 2023 Hamas surprise attack on Israel demonstrated that even the best technical surveillance and AI analytics can fail if analysts are working from flawed assumptions or lack human sources to reveal an adversary's intent. No matter how advanced electronic surveillance becomes, it must be paired with human insight to truly penetrate an opponent's plans. Technology can aid analysis, but it cannot substitute for creative, critical thinking. Therefore, a more central role for intelligence in decision-making will depend not just on tools and data, but on nurturing skilled analysts who can interpret ambiguous evidence and have the courage to voice

[238] Daniela Richterová, "Tbilisi 2008 – Russia Invades Georgia," in *Contemporary Intelligence Warning Cases: Learning from Successes and Failures*, ed. B. E. M. Grønning and S. Stenslie (Edinburgh: Edinburgh University Press, 2024), 61–77.

uncomfortable truths. In an age of algorithms, maintaining a culture of analytic rigor and imagination by avoiding overreliance on automated answers is a frontier challenge in itself.

In sum, the new frontiers of technology, OSINT, and hybrid threats offer both prospects and limits for intelligence as a strategic actor. Agencies equipped with big data analytics and plugged into open information flows can uncover emerging problems faster, giving them a stronger hand in guiding policy during crises. Within this context, the involvement of non-state intelligence actors can democratize and improve warning, holding governments to account and supplementing official efforts. However, these same trends increase complexity: intelligence must cut through information overload and compete with many voices to be heard. Hybrid threats and "unknown unknowns" mean intelligence will continue to deal with probabilities and broad warnings, not certainties – which frustrates policymakers expecting precise answers. The next section turns to how we can finally bridge this gap and embed an anticipatory culture in our institutions, so that early intelligence insights are not only produced but also acted upon.

4.3 Towards a Culture of Anticipation: Final Recommendations and Guidelines

If there is one overarching lesson from this study, it is that achieving a more influential role for intelligence depends as much on culture and process as on resources or prediction methods. Both the intelligence community and the political leadership must embrace a culture of anticipation, consisting of a mindset promoting foresight, open communication, and proactive action in the face of risk. Below, we present final recommendations and guidelines to cultivate such a culture. These suggestions address the intelligence-policy relationship, structural and training needs, and multi-level cooperation, building on the conducted analysis. Together, they aim to strengthen the integration of intelligence into decision-making without compromising democratic accountability.

First, breaking the warning-response disconnect requires more dialogue and mutual understanding between those who produce intelligence and those who consume it. Leaders should be regularly briefed not just on what analysts know, but how they know it and how confident they are. Conversely, analysts need insight into policymakers' concerns and constraints. The recommendation is to establish formal channels for frequent interaction, beyond the daily written

briefs. This could include weekly intel-policy forums or embedding intelligence liaisons within policy departments. The goal is to humanize the relationship so that when a crisis approaches, the intelligence warning comes from a known, trusted voice rather than a faceless report. Stronger personal relationships can help overcome the skepticism or indifference that sometimes greets intelligence warnings. Additionally, intelligence must communicate in a decision-useful way: avoiding jargon, clearly explaining uncertainties, and even offering possible response options. Policymakers, for their part, should give feedback to the intelligence community and indicate what information was helpful or what proved misleading, in order to refine the process. Trust is a two-way street: intelligence officers must trust leaders to handle sensitive information responsibly, and leaders must trust that intelligence is offered in good faith, not as bureaucratic turf protection or political manipulation.

One way to build mutual understanding is through joint training initiatives. Intelligence analysts and policymakers (and even military operators or diplomats) should periodically train together in crisis simulation exercises. By jointly addressing fabricated crises, each side can appreciate the other's challenges: analysts see the multitude of factors leaders manage, and leaders see how the intelligence cycle works under pressure. Such exercises also familiarize decision-makers to thinking in probabilistic terms and imagining low-probability/high-impact scenarios. For example, a simulation might force participants to respond to an unfolding pandemic or a hybrid attack, using intelligence reports as inputs. After action reviews would highlight if warning signs were missed or dismissed. This kind of experiential learning can instill a bias for early action. Educational exchanges are also endorsed: short-term rotations where intelligence officers work in policy roles and vice versa. When analysts and policymakers "speak the same language", intelligence is far more likely to inform policy rather than remain in a silo. Indeed, scholars argue that both sides will have to "judge and assess together"[239] which potential scenarios or threats merit alarm. Institutionalizing that collaborative assessment would thus foster the operationalization of an ethics to the work.

Second, to anticipate a wide array of crises, intelligence must draw on diverse sources of information and analysis. Thus, the idea is to invest in OSINT capabilities and partnerships with the private sector and academia. Intelligence agencies should make it standard practice to

[239] Pronk and Korteweg, *Sharing the Burden, Sharing the Secrets.*

incorporate credible outside analyses (e.g., think-tank reports, commercial satellite analyses, expert opinion) alongside classified reporting, since this plurality can help overcome blind spots. As we saw, sometimes an outside entity like a private firm or journalistic outfit might pick up on an emerging threat before government does. Rather than view that as a failure, agencies should treat it as an additional early warning layer. Within this context, creating channels for crowdsourced warning could augment official efforts. Moreover, inside intelligence organizations, analytic team diversity and structured debate should be encouraged. Devil's advocate units or "red teams" ought to challenge prevailing assumptions regularly. Further, leaders of analysis should foster a climate where dissenting views are not only accepted but rewarded, so that if someone sees a low-probability disaster on the horizon, they feel empowered to voice it loudly. The overall aim is to develop a collective system increasing the chance that at least someone flags an impending crisis.

Third, the hardest task is undoubtedly cultural. Both analysts and officials need to train their minds to expect the unexpected. Recommendations include that intelligence agencies implement regular horizon scanning sessions where analysts brainstorm even unplausible scenarios. The purpose is not to formulate alarmist fantasies, but to stretch thinking and develop contingency plans. Intelligence services are attempting to revive the old discipline of warning intelligence – dedicated analysts whose job is to constantly examine what piece of the puzzle is missing or what could happen next month that would shock the entire environment. Reestablishing roles like the U.S. National Intelligence Officer for Warning could prove extremely useful to coordinate such efforts. Likewise, governments can create interagency foresight units or assign a senior official as a "crisis anticipation officer" to ensure that early warnings are concretely given the right importance. Crucially, top political leaders must be the ones setting the tone: if they demand forward-looking analysis and are willing to hear uncomfortable truths, it will encourage the entire bureaucracy to think ahead. Leaders should make clear that warning superiors about potential threats is valued. The final step of imagination is bridging the gap to preventive action. It is not enough to envision a scenario; someone must decide to invest in averting it. Here, a culture of anticipation intersects with political will. The urge is to drive governments to create tangible contingency plans and trigger mechanisms linked to intelligence indicators, so that when warnings reach certain thresholds, pre-agreed preventive measures are automatically activated. In sum, both the intel and policy worlds

should prize anticipatory thinking as a core professional skill, rewarding those who anticipate and preventing the attitude that reacting to events is sufficient.

Finally, crises frequently spill across borders, so anticipating them cannot be solely a national endeavor. That is why intelligence cooperation should be strengthened at the regional and international level. The European Union, for instance, has developed a Conflict Early Warning System and other risk monitoring tools[240]; EU member states should actively support these by feeding in their national intelligence findings and jointly assessing emerging conflicts or hybrid threats, in the same way they have been cooperating in every other domain since the creation of the EU[241]. The logic is simple: pooling perspectives can compensate for one country's weakness with another's insight, exactly because many complex threats are now transnational. Concretely, this could mean expanding multinational intelligence fusion centers like EU Intelligence and Situation Centre (INTCEN) or NATO's intel units to focus on joint early-warning analysis. At the national level, a multilevel approach also means linking local, national, and global networks. For instance, local public health surveillance could connect to national intelligence assessment for pandemics, which in turn ties into global disease warning systems[242]. No level should operate in isolation. Multilevel resilience also implies involving multiple stakeholders: government, private sector, and civil society. For example, tech companies might be enlisted in an early warning network for cybersecurity (some countries already have such partnerships, where companies share threat data with intel agencies). Internationally, we support initiatives to create norms and agreements for sharing critical warning information – whether about an emerging virus, a looming famine, or an impending military strike – in a timely fashion. While national security often leads to secrecy, in many emerging crises a prompt collective response is more important than jealously guarding intel, and private sector intelligence is the leader in this[243]. Dismantling silos between

---

[240] European External Action Service, *Early Warning System: Factsheet* (Brussels: EEAS, August 2022), *https://www.eeas.europa.eu/sites/default/files/documents/Factsheet%20-%20EWS.pdf*.

[241] Björn Fägersten, "Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol," *Intelligence and National Security* 25, no. 4 (2010).

[242] Dahl, *The COVID-19 Intelligence Failure.*

[243] U.S. Department of Homeland Security, "The Importance of Private Sector Intelligence Programs," 2021, *https://www.dhs.gov/sites/default/files/publications/importance_to_private_sector_intelligence_programs.pdf*.

agencies, sectors, and nations is thus vital to build and promote an anticipatory, comprehensive ethos.

Yet, in advocating a more central role for intelligence, we must also heed the limits. Intelligence is not a perfect and unfailing tool, as we extensively argued. Decision-makers will often have to act on partial, moderate-confidence intelligence. This can be politically difficult but it is precisely what a culture of anticipation entails. It means having the courage to take out insurance against worst-case scenarios flagged by intelligence, even at the risk of false alarms. It also means remaining agile: if the warning eventually reveals to be incorrect, being willing to adjust the trajectory and not penalize the analysts. Another inherent limit is that intelligence personnel are not elected officials, therefore their remit is advice and in no way deciding policy. Elevating intelligence's role must not cross into undermining democratic control. We have stressed making policymakers more responsive to intel, not subordinate to it. Elected leaders will always need to weigh other factors (economic, political, ethical) that intelligence does not address. Thus, recommendations seek to embed intelligence as a strong advisor and early detector, not as an autonomous actor. Keeping that balance is important to avoid the risks of technocracy or the politicization of intelligence to serve agendas.

In conclusion, intelligence can indeed become a more strategic actor in governance – illuminating the path ahead so that policymakers are not surprised by the next crisis. The prospects for a more central role are evidenced by new technologies enabling broader situational awareness, the proven value of early warnings in saving lives, and the expanding intelligence activities in domains like health and cyber that directly inform policy choices. Nevertheless, our study demonstrates that intelligence inevitably operates within, rather than above, the realm of politics and decision-making, and its impact ultimately hinges on leaders' willingness to listen. By concretely implementing the guidelines developed above, the society can move closer to a genuine culture of anticipation. In such a culture, intelligence is not an "unheard voice" but rather a foundational pillar of decision-making in both daily governance and moments of crisis. Warnings would be neither overstated nor ignored, but thoughtfully integrated into prompt preventive action. This is an ambitious vision, and it will take continued reforms and learning from failures to achieve. Yet, as the crises of the 21st century continue to demonstrate, the cost of strategic surprise is simply too

high. Thus, creating the premises for intelligence to assume an enhanced role and be as influential as it should, is not merely plausible, but imperative for better safeguarding our future and facilitate decision-making processes.

Conclusion

This thesis aimed at addressing a dual problem. First, it examined how intelligence contributes to anticipating crises in environments defined by threat, urgency, and uncertainty. Second, it investigated the ethical and operational conditions under which intelligence can move from a peripheral, advisory function to a more influential role in decision-making, asking whether there are circumstances in which practitioners might edge toward quasi-decision authority without eroding analytic integrity or democratic accountability.

The analysis yields four principal findings. Conceptually, intelligence adds value to anticipation when it converts diffuse data into structured foresight and delivers judgments that are both timely and calibrated. Institutionally, influence hinges less on "what intelligence knows" than on "how systems hear": clarity of probability language, routinized channels for warning, and sustained trust between analysts and policymakers consistently determine commitment and outcome. Politically and psychologically, the main frictions lie on the receiving end: cognitive biases, organizational inertia, and incentive structures that punish false alarms more than missed warnings depress receptivity. Further, politicization distorts estimates and corrodes credibility over time. Empirically, the comparative cases underline that intelligence can shape results when analysis is early, specific, and communicated in policy-relevant terms, and when leaders have pre-agreed procedures for what to do as indicators light up. Whenever such conditions are absent, even accurate warning is easily sidelined.

Taken together, these findings support an articulated response to the research question. Intelligence can and should exercise greater strategic influence in crisis anticipation, but as a decision enabler, not a substitute decision-maker. Elevating intelligence is useful in high-ambiguity, high-impact contexts where lead time is decisive (pandemics, hybrid operations, systemic infrastructure risk), provided that three essential conditions are in place. Analytic integrity must be protected against advocacy and pressure; communication must be standardized (shared probability yardsticks, common operating pictures, pre-authorized response scenarios); and accountability must be mutual, so that ignoring a credible warning attracts scrutiny just as strongly as issuing a poor one. Within those bounds, limited forms of delegated authority are defensible because analysts

constantly face time, which is the scarcest resource in fast-approaching crises. Outside such predefined arrangements, the practitioner's role should remain to illuminate options and delineate constraints and risks, thus assisting power while resisting the pull to speak for it.

Indeed, the research presents manifest limitations. Methodologically, it relies on a qualitative comparison of recent, data-rich cases; findings may be sensitive to selection effects and hindsight bias. Substantively, the perspective is largely transatlantic and democratic, which may disregard the reality in which some intelligence agencies operate in specific countries, as lessons may travel imperfectly to other political systems. Evidentiary constraints are real: crucial details remain classified, and open-source reconstructions can overestimate coherence ex post. Moreover, the work mostly focused on public sector intelligence, but the increasingly developing field in the private sphere would certainly deserve more consideration. Finally, measuring influence is intrinsically hard and causal links between a warning and a non-event (a crisis averted) are rarely observable with precision.

The aforementioned constraints point to several paths for future study. First, develop metrics and datasets that evaluate warning performance across analytic, communicative, and political dimensions (e.g., timeliness–accuracy trade-offs; policy responsiveness indices). Second, pursue micro-level research on receptivity which may include field or lab experiments on how leaders interpret probabilistic language, and what formats increase the chance of heeding analysts. Third, compare oversight regimes cross-nationally to test which designs best deter politicization while preserving policy relevance. Finally, study the evolving boundary with the private sector, where risk advisory firms and platform operators now generate, fuse, and act on warning signals at scale, measuring its implications for legitimacy and accountability in anticipatory governance.

Despite leaving room for improvement, the takeaways of the thesis are straightforward. Intelligence is most effective upstream, not downstream; its comparative advantage lies in structuring uncertainty before it evolves into inevitability. Influence is earned less by dramatic secrets than by routine practices that make warning actionable. The chronic failure mode is not ignorance but inattention, meaning good analysis that arrives without a receiver prepared to hear it. Any form of barrier against politicization is a precondition for influence, not its enemy. And success will often

look like nothing happened, which is analytically demanding, politically unrewarded, and ethically necessary.

A concluding reflection, originally offered by my intelligence professor, encapsulates the underlying message of the thesis by highlighting this final point. Notably, intelligence is comparable to electronic countermeasures (ECM) used in military operations. ECM refers to defensive systems used by military forces deployed on the field to deceive enemy radar and targeting mechanisms. These devices are heavy, consume significant energy, and impose a constant burden on operators. They provide little or no immediate feedback: they never tell in real time whether the system is actively working. Most importantly, their value is almost invisible, since their success lies precisely in preventing an attack from ever materializing. When they function as intended, there is no spectacle of interception or retaliation but only the quiet non-occurrence of a danger that never appears.

In this sense, intelligence performs a similar function. It is costly to sustain, organizationally cumbersome, and often resented for its demands on resources and attention. Its outputs rarely provide the rhetoric of averted disaster. Instead, success manifests as silence, stability, or the persistence of normalcy. Precisely because both intelligence and ECM achieve their greatest victories in ways that remain unseen, they are prone to being undervalued, sidelined, or subjected to political neglect. Indeed, there is little acknowledgment for resolving problems that never happened. This invisibility underscores why institutions must create enduring habits, incentives, and professional norms that reward the work of prevention.

The broader implication is that moving from warning to influence is not about transferring decision-making authority to intelligence services, but about equipping political systems to recognize, trust, and act upon anticipatory insights. In doing so, societies can ensure that their hardest victories remain the ones the public never notices.

Bibliography

Agwu, Julius A., and Zems Mathias. "The Policy-Maker Intelligence Interface: A Critical Vulnerability in the Intelligence Community." *GSJ: Global Scientific Journal* 11, no. 9 (2023).

Aldrich, Richard J. "Whitehall and the Iraq War: The UK's Four Intelligence Enquiries." *Irish Studies in International Affairs* 16, no. 1 (2005): 73–88.

Andregg, Michael M., and Peter Gill. "Comparing the Democratization of Intelligence." *Intelligence and National Security 29*, no. 4 (2014): 487–497.

Ansoff, H. Igor. "Managing Strategic Surprise by Response to Weak Signals." *California Management Review* 18, no. 2 (1975): 21–33.

Barry, Tom. *Decentralizing U.S. Intelligence: Office of Special Plans*. Interhemispheric Resource Center, 2004.

Benjamin, Daniel, and Steven Simon. *The Age of Sacred Terror: Radical Islam's War Against America*. Random House Trade Paperbacks, 2003.

Bergman, Ronen, and Adam Goldman. "Israel Knew Hamas's Attack Plan More Than a Year Ago." *The New York Times*, November 30, 2023. https://www.nytimes.com/2023/11/30/world/middleeast/israel-hamas-attack-intelligence.html.

Bertrand, Natasha, Jim Sciutto, and Kylie Atwood. "CIA Director Dispatched to Moscow to Warn Russia over Troop Buildup near Ukraine." *CNN*, November 5, 2021. https://edition.cnn.com/2021/11/05/politics/bill-burns-moscow-ukraine.

Best, Richard A., Jr., and Alfred Cumming. "Director of National Intelligence Statutory Authorities: Status and Proposals." In *CRS Report RL34231*. Congressional Research Service, 2011.

Betts, Richard K. "Policy-Makers and Intelligence Analysts: Love, Hate or Indifference?" *Intelligence and National Security* 3, no. 1 (1988): 184–189.

Betts, Richard K. "Surprise despite Warning: Why Sudden Attacks Succeed." *Political Science Quarterly* 95, no. 4 (1980): 551–572.

Betts, Richard K. *Enemies of Intelligence: Knowledge and Power in American National Security*. Columbia University Press, 2007.

Biden, Joseph R. "Remarks by President Biden Providing an Update on Russia and Ukraine." The White House, February 18, 2022. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2022/02/18/remarks-by-president-biden-providing-an-update-on-russia-and-ukraine-2/.

"Bin Ladin Determined to Strike in US." In *Presidential Daily Brief*. Memorial & Museum, 2001. https://www.911memorial.org/sites/default/files/inline-files/Bin%20Ladin%20Determined%20to%20Strike%20in%20US.pdf.

Boin, Arjen, Magnus Ekengren, and Mark Rhinard. "Hiding in Plain Sight: Conceptualizing the Creeping Crisis." *Risks, Hazards & Crisis in Public Policy* 11, no. 2 (2020): 116–38.

Bokonda, Patrick L. "Predictive Analysis Using Machine Learning: Review of Trends and Methods." *2020 International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, 2020, 1–6.

Borger, Julian, Hugo Lowell, and Dan Sabbagh. "'A Massive Policy Fail': CIA Warned White House of Swift Taliban Takeover." *The Guardian*, August 18, 2021. https://www.theguardian.com/world/2021/aug/18/massive-policy-fail-cia-warned-taliban-takeover.

Born, Hans, and Ian Leigh. *Democratic Accountability of Intelligence Services*. Geneva Centre for the Democratic Control of Armed Forces, 2006.

Brown, Pamela, and Zachary Cohen. "Hamas Operatives Used Phone Lines Installed in Tunnels under Gaza to Plan Israel Attack over 2 Years." *CNN*, October 25, 2023. https://edition.cnn.com/2023/10/24/politics/intelligence-hamas-israel-attack-tunnels-phone-lines.

Byman, Daniel. "Strategic Surprise and the September 11 Attacks." *Annual Review of Political Science* 8 (2005): 151.

Commission on the Intelligence Capabilities of the United States Regarding WMD, Report to the President. GPO, 2005.

Committee of Privy Counsellors, Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Counsellors (Cm 6278). The Stationery Office, 2004.

Congleton, Roger D. "The Political Economy of Crisis Management: Surprise, Urgency, and Mistakes in Political Decision Making." In *The Dynamics of Intervention: Regulation and Redistribution in the Mixed Economy*. Emerald Group Publishing, 2004.

Council on Foreign Relations. "The Taliban in Afghanistan." August 15, 2023. https://www.cfr.org/backgrounder/taliban-afghanistan.

Council on Foreign Relations. Center for Preventive Action, "Instability in Afghanistan." *Global Conflict Tracker*, February 12, 2025. https://www.cfr.org/global-conflict-tracker/conflict/war-afghanistan.

Dahl, Erik J. "Warning of Terror: Explaining the Failure of Intelligence Against Terrorism." *Journal of Strategic* Studies, 28, no. 1 (2005).

Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond*. Georgetown University Press, 2013.

Dahl, Erik J. *The COVID-19 Intelligence Failure: Why Warning Was Not Enough*. Georgetown University Press, 2023.

Dahl, Erik J., and David Strachan-Morris. "'Predictive Intelligence for Tomorrow's Threats': Is Predictive Intelligence Possible?" *Journal of Policing, Intelligence and Counter Terrorism* 19, no. 4 (2024): 423–435.

Davis, Euan G. "A Watchman for All Seasons." *Studies in Intelligence* 13, no. 2 (1969): 37–42.

Davis, Jack. “Intelligence Analysts and Policymakers: Benefits and Dangers of Tensions in the Relationship.” *Intelligence and National Security* 21, no. 6 (2006): 999–1021.

DeRosa, Mary B. “Congressional Oversight of US Intelligence Activities.” *Georgetown Law Faculty Publications and Other Works* 2575 (2021).

Dhami, Mandeep K. “Improving Intelligence Analysis with Decision Science.” *Perspectives on Psychological Science* 10, no. 6 (2015): 753–757.

Dombrowski, Peter, Catherine Kelleher, and Ethan Auner. “Demystifying Iron Dome.” *The National Interest* 126 (2013): 49–59.

Dylan, Huw. “Kyiv, 2022 – Russia’s Full-Scale Invasion of Ukraine.” In *Contemporary Intelligence Warning Cases: Learning from Successes and Failures*, edited by B. E. M. Grønning and S. Stenslie. Edinburgh University Press, 2024.

European Commission. *Joint Framework on Countering Hybrid Threats: A European Union Response*. Brussels: European Commission, 2016.

European External Action Service, *Early Warning System: Factsheet*. EEAS, 2022. https://www.eeas.europa.eu/sites/default/files/documents/Factsheet%20-%20EWS.pdf.

Evans, Janet M., and Mark R. Kebbell. “The Effective Analyst: A Study of What Makes an Effective Crime and Intelligence Analyst.” *Policing and Society* 22, no. 2 (2012): 204–219.

Fägersten, Björn. “Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol.” *Intelligence and National Security* 25, no. 4 (2010).

Federation of American Scientists. “The Intelligence Cycle.” https://irp.fas.org/cia/product/facttell/intcycle.htm.

Foreign, Commonwealth, Development Office, and Elizabeth Truss. *Kremlin Plan to Install Pro-Russian Leadership in Ukraine Exposed*. UK Government Press Release, 2022. https://www.gov.uk/government/news/kremlin-plan-to-install-pro-russian-leadership-in-ukraine-exposed.

Garicano, Luis, and Richard A. Posner. "Intelligence Failures: An Organizational Economics Perspective." *Journal of Economic Perspectives* 19, no. 4 (2005): 151–170.

Gates, Robert M. *From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War*. Simon & Schuster, 2011.

Gaub, Florence. "Enhancing Early Warning and Preparedness." In *Crisis Rooms: Towards a Global Network?*, edited by Patryk Pawlak and Andrea Ricci. EU Institute for Security Studies, 2014.

Geer, Dan. "We Are All Intelligence Officers Now." *RSA Conference Speech, San Francisco*, 2014. https://docs.huihoo.com/rsaconference/usa-2014/exp-f02-we-are-all-intelligence-officers-now.pdf.

Gentry, John A. "Intelligence Failure Reframed." *Political Science Quarterly* 123, no. 2 (2008): 247–270.

Gentry, John A., and Joseph S. Gordon. *Strategic Warning Intelligence: History, Challenges, and Prospects*. Georgetown University Press, 2019.

Gibson, Stevyn D. "Exploring the Role and Value of Open Source Intelligence." In *Open Source Intelligence in the Twenty-First Century*, edited by Christopher Hobbs, Matthew Moran, and Daniel Salisbury. Palgrave Macmillan, 2014.

Gill, Peter, and Mark Phythian. *Intelligence in an Insecure World*. 3rd ed. Polity Press, 2019.

Global Guardian. "Case Study: Emergency Response." Ukraine, 2022. https://www.globalguardian.com/case-studies_emergency-response-ukraine.

Goodman, Michael S. "The Dog That Didn't Bark: The Joint Intelligence Committee and Warning of Aggression." *Cold War History* 7, no. 4 (2007): 529–551.

Grabo, Cynthia M., and Jan Goldman. *Handbook of Warning Intelligence: Complete Declassified Edition*. Rowman & Littlefield, 2015.

Grønning, Bjørn Elias M., and Stig Stenslie. "Conclusion: Towards Better Warning – Lessons and Recommendations for Intelligence." In *Contemporary Intelligence Warning Cases*, edited by B. E. M. Grønning and S. Stenslie. Edinburgh University Press, 2024.

Hanauer, Larry, and Michael P. Connell. *Political Priorities, Poor Intelligence Tradecraft, and the Suppression of Dissenting Views: Why Israel Failed to Warn of Hamas's October 7 Attack*. Institute for Defense Analyses, 2024.

Harris, Shane, and Paul Sonne. "Russia Planning Massive Military Offensive against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns." December 3, 2021. https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.

Hedley, John Hollister. "Learning from Intelligence Failures." *International Journal of Intelligence and CounterIntelligence* 18, no. 3 (2005): 435–450.

Hewitt, Kenneth. *Interpretations of Calamity: From the Viewpoint of Human Ecology*. Allen & Unwin, 1983.

Hou, Lin-Xiu. "Decades on Emergency Decision-Making: A Bibliometric Analysis and Literature Review." *Complex Intelligent Systems* 7 (2021): 2819–2832.

Hughes-Wilson, John. *Military Intelligence Blunders and Cover-Ups*. Robinson, 2004.

Hulnick, Arthur S. "Intelligence Theory: Seeking Better Models." In *Understanding the Intelligence Cycle*, edited by Mark Phythian. Routledge, 2013.

Hulnick, Arthur S. "What's Wrong with the Intelligence Cycle." *Intelligence and National Security* 21, no. 6 (2006): 959–979.

Human Rights Watch. "I Can't Erase All the Blood from My Mind." July 17, 2024. https://www.hrw.org/report/2024/07/17/i-cant-erase-all-blood-my-mind/palestinian-armed-groups-october-7-assault-israel.

Huminski, Joshua C. “Russia, Ukraine, and the Future Use of Strategic Intelligence.” *PRISM* 10, no. 3 (2023).

Ikani, Nikki. “Beyond the Binary: A New Typology for Evaluating Warning Success and Failure in Strategic Surprise.” *International Studies Review* 27, no. 1 (2025).

Isenberg, Daniel J. “How Senior Managers Think.” In *Decision Making: Descriptive, Normative, and Prescriptive Interactions*, edited by David Bell, Howard Raiffa, and Amos Tversky. Cambridge University Press, 1988.

Janis, Irving L. *Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascoes*. Houghton Mifflin, 1972.

Jervis, Robert. “Reports, Politics, and Intelligence Failures: The Case of Iraq.” *Journal of Strategic Studies* 29, no. 1 (2006): 3–52.

Jervis, Robert. “Why Intelligence and Policymakers Clash.” *Political Science Quarterly* 125, no. 2 (2010): 185–204.

Johnson, Loch K. “Bricks and Mortar for a Theory of Intelligence.” *Comparative Strategy* 22, no. 1 (2003): 1–28.

Karelitz, Tzur M., and David V. Budescu. “You Say ‘Probable’ and I Say ‘Likely’: Improving Interpersonal Communication with Verbal Probability Phrases.” *Journal of Experimental Psychology: Applied* 10 (2004): 25–41.

Kent, Sherman. *Strategic Intelligence for American World Policy*. Princeton University Press, 1949.

King, Dennis J. *Channeling Cassandra: Humanitarian Intelligence and Decisionmaking in the Age of Complexity*. U.S. Department of State, National Intelligence University, Ann Caracristi Institute for Intelligence Research, 2024.

Lesca, Humbert, and Nicolas Lesca. *Strategic Decisions and Weak Signals: Anticipation for Decision-Making*. John Wiley & Sons, 2014.

Lillis, Katie Bo. "US Intelligence Warned of the Potential for Violence Days before Hamas Attack." *CNN*, October 13, 2023. https://edition.cnn.com/2023/10/13/politics/us-intelligence-warnings-potential-gaza-clash-days-before-attack.

Lizzo, Stephanie. "Intelligence Redefined: The Interplay of Private Companies and National Security." *Journal of International Affairs*, 2024. https://jia.sipa.columbia.edu/news/intelligence-redefined-interplay-private-companies-and-national-security.

Lowenthal, Mark M. "Tribal Tongues: Intelligence Producers, Intelligence Consumers." In *Strategic Intelligence: Windows into a Secret World*, edited by Loch K. Johnson and James J. Wirtz. Roxbury Press, 2004.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 9th ed. CQ Press, 2023.

Lubin, Asaf. "The Reasonable Intelligence Agency." *Articles by Maurer Faculty* 3034 (2022).

Marcoci, Alexandru, Ans Vercammen, and Mark Burgman. "ODNI as an Analytic Ombudsman: Is Intelligence Community Directive 203 Up to the Task?". *Intelligence and National Security* 34, no. 2 (2019).

Marrin, Stephen. "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis." In *Intelligence and National Security*. 2011.

Marrin, Stephen. "Why Intelligence Analysis Has Limited Influence on American Foreign Policy." *APSA Annual Meeting*, 2014.

McCarthy, Mary. "The National Warning System: Striving for an Elusive Goal." *Defense Intelligence Journal* 3 (1994): 5–19.

Mell, Patricia. "Big Brother at the Door: Balancing National Security with Privacy under the USA PATRIOT Act." *Denver University Law Review* 80 (2002): 375.

Michman, Dror, and Yael Mizrahi-Arnaud. "The Fog of Certainty: Learning from Intelligence Failures of the 1973 War." *Brookings Institution*, October 23, 2017.

Microsoft. *Microsoft Digital Defense Report 2024: The Foundations and New Frontiers of Cybersecurity*. Microsoft, 2024. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024.

Mills, Claire. "Afghanistan: Fall of the Government and the Transition of Power." House of Commons Library Research Briefing no. 9299, August 17, 2021. https://researchbriefings.files.parliament.uk/documents/CBP-9299/CBP-9299.pdf.

Mohr, John S. "A Call for More Humility in Intelligence Analysis." *Studies in Intelligence* 61, no. 4 (2017): 53–58.

Morrow, Maria A.Robson. "Private Sector Intelligence: On the Long Path of Professionalization." In *Intelligence and National Security*. 2022.

National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report. GPO, 2004.

National Intelligence Council (US), Iran: Nuclear Intentions and Capabilities. NIC, 2007.

Ngo, Madeleine. "Biden Defends Decision to Pull Out of Afghanistan." *The New York Times*, August 16, 2021. https://www.nytimes.com/live/2021/08/16/us/politics-news.

Nickerson, Raymond S. "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises." *Review of General Psychology* 2, no. 2 (1998): 175–220.

Nolan, Cynthia. "The Edward Snowden Case and the Morality of Secrecy." *Catholic Social Science Review* 22 (2017): 291–310.

Odote, Peterlinus O. "Role of Early Warning Systems in Conflict Prevention in Africa: Case Study of the Ilemi Triangle." (PhD diss.), University of Nairobi, 2016.

Office of the Director of National Intelligence (ODNI), "What Is Intelligence?". https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

Office of the Director of National Intelligence (ODNI). *Intelligence Community Directive (ICD) 191: Duty to Warn*. ODNI, 2015.

Office of the Director of National Intelligence (ODNI). *Intelligence Community Directive (ICD) 203: Analytic Standards*. ODNI, 2007.

Omand, David. *How Spies Think*. Penguin Random House, 2020.

Omand, David. *How to Survive a Crisis: Lessons in Resilience and Avoiding Disaster*. Penguin Random House, 2023.

Pei, Sen. "Differential Effects of Intervention Timing on COVID-19 Spread in the United States." *Science Advances* 6, no. 49 (2020).

Pfiffner, James P. "Did President Bush Mislead the Country in His Arguments for War with Iraq?" *Presidential Studies Quarterly* 34, no. 1 (2004): 25–46.

Pherson, Randolph H., and Richards J. Heuer Jr. *Structured Analytic Techniques for Intelligence Analysis*. 3rd ed. CQ Press, 2020.

Phythian, Mark, ed. *Understanding the Intelligence Cycle*. Routledge, 2013.

Phythian, Mark. "Intelligence Analysis Today and Tomorrow." *Security Challenges* 5, no. 1 (2009): 67–83.

Pillar, Paul. "Intelligence, Policy, and the War in Iraq." *Foreign Affairs* 85, no. 2 (2006): 15–27.

Pronk, Danny, and Claire Korteweg. *Sharing the Burden, Sharing the Secrets: The Future of European Intelligence Cooperation*. (Clingendael Report), 2021. https://docs.clingendael.org/sites/docs/files/2021-09/EU-intelligence-cooperation.pdf.

Rainsford Sarah. "Ukraine Crisis: Don't Create Panic, Zelensky Tells West." *BBC News*, January 28, 2022. https://www.bbc.com/news/world-europe-60174684.

Ramsden, Michael. "Targeted Killings and International Human Rights Law: The Case of Anwar Al-Awlaki." *Journal of Conflict & Security Law* 16, no. 2 (2011): 385–406.

Richterová, Daniela. “Tbilisi 2008 – Russia Invades Georgia.” In *Contemporary Intelligence Warning Cases: Learning from Successes and Failures*, edited by B. E. M. Grønning and S. Stenslie. Edinburgh University Press, 2024.

Robinson, Lauren. “Protecting the Rights of Whistleblowers.” *Social Education* 69, no. 6 (2005): 313.

Rosenthal, Uriel, Michael T. Charles, and Paul ’t Hart. *Coping with Crisis: The Management of Disasters, Riots, and Terrorism*. Charles C. Thomas, 1989.

Rosenthal, Uriel, and Alexander Kouzmin. “Crises and Crisis Management: Toward Comprehensive Government Decision Making.” *Journal of Public Administration Research and Theory* 7, no. 2 (1997): 277–304.

Rovner, Joshua. “Is Politicization Ever a Good Thing?” *Intelligence and National Security* 28, no. 1 (2013).

Rovner, Joshua. *Fixing the Facts: National Security and the Politics of Intelligence*. Cornell University Press, 2011.

Samuelson, William, and Richard Zeckhauser. “Status Quo Bias in Decision Making.” *Journal of Risk and Uncertainty* 1 (1988): 7–59.

Schwartz, Howard S. “On the Psychodynamics of Organizational Disaster: The Case of the Space Shuttle Challenger.” *Columbia Journal of World Business* 22, no. 1 (1987): 59–67.

Senate Select Committee on Intelligence (SSCI). “Report on the U.S.” In *Intelligence Community’s Prewar Intelligence Assessments on Iraq*. U.S. Government Printing Office, 2004.

Shapira, Itai. “The Yom Kippur Intelligence Failure after Fifty Years: What Lessons Can Be Learned?” *Intelligence and National Security* 38, no. 6 (2023): 978–1002.

Shpiro, Shlomo. “Intelligence and the Ukraine War: Early Lessons and Research Roadmap.” *National Security and the Future* 24, no. 1 (2023): 7–18.

Sims, Jennifer E. *Decision Advantage: Intelligence in International Politics from the Spanish Armada to Cyberwar*. Oxford University Press, 2022.

Sniazhko, Sniazhana. "Uncertainty in Decision-Making: A Review of the International Business Literature." *Cogent Business & Management* 6, no. 1 (2019).

Strom, Kevin J. *Terrorist Plots against the United States: What We Have Really Faced, and How We Might Best Defend against It*. RAND Corporation, 2016.

Șușnea, Elena. "A Real-Time Social Media Monitoring System as an Open Source Intelligence (OSINT) Platform for Early Warning in Crisis Situations." *The Knowledge-Based Organization* 24, no. 2 (2018): 427-431. https://doi.org/10.1515/kbo-2018-0127.

't Hart, Paul, and Arjen Boin. "Between Crisis and Normalcy: The Long Shadow of Post-Crisis Politics." In *Managing Crises: Threats, Dilemmas, Opportunities*, edited by Uriel Rosenthal, Arjen Boin, and Louise K. Comfort. Charles C. Thomas, 2001.

Tenet, George J., and Bill Harlow. *At the Center of the Storm: My Years in the CIA*. HarperCollins, 2007.

Times of Israel. "Egypt Intelligence Official Says Israel Ignored Repeated Warnings of 'Something Big.'" October 9, 2021. https://www.timesofisrael.com/egypt-intelligence-official-says-israel-ignored-repeated-warnings-of-something-big/.

Times of Israel. "Head of IDF Devil's Advocate Unit Tried Repeatedly in September to Warn of Possible Hamas Attack." January 6, 2024. https://www.timesofisrael.com/liveblog_entry/head-of-idf-devils-advocate-unit-tried-repeatedly-in-september-to-warn-of-possible-hamas-attack/.

Times of Israel. "IDF Intel Chief Says He 'Bears Full Responsibility' for Not Warning of Hamas Attack." October 17, 2023. https://www.timesofisrael.com/idf-intel-chief-says-he-bears-full-responsibility-for-not-warning-of-hamas-attack/.

Treverton, Gregory F., and Renanah Miles. "Unheeded Warning of War: Why Policymakers Ignored the 1990 Yugoslavia Estimate." *Intelligence and National Security* 32, no. 4 (2016): 506–522.

UK Ministry of Defence. "How Open-Source Intelligence Has Shaped the Russia-Ukraine War." *GOV.UK*, December 9, 2022. https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war.

U.S. Congress. "Intelligence Reform and Terrorism Prevention Act of 2004." *Pub* 3638, S. 2845. December 17, 2004. https://www.congress.gov/108/plaws/publ458/PLAW-108publ458.pdf.

U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (Washington*. DoD), 2010.

U.S. Department of Defense. Paul Wolfowitz to Donald Rumsfeld, "*Were We Asleep?" Memo, 18 September 2001, Cited in The 9/11 Commission Report*. GPO, 2004.

U.S. Department of Homeland Security. "The Importance of Private Sector Intelligence Programs." 2021. https://www.dhs.gov/sites/default/files/publications/importance_to_private_sector_intelligence_programs.pdf.

U.S. House of Representatives, Committee on Foreign Affairs. *An Assessment of the Biden Administration's Withdrawal from Afghanistan by America's Generals.* Hearing Before the Committee on Foreign Affairs. 118th Congress, Second Session. March 19, 2024. Serial no. 118–89. Washington DC: U.S Government Publishing Office, 2024.

U.S. House of Representatives. Committee on Foreign Affairs. "Willful Blindness: An Assessment of the Biden-Harris Administration's Withdrawal from Afghanistan and the Chaos That Followed." Washington DC: U.S. House of Representatives, September 8, 2024. https://foreignaffairs.house.gov/sites/evo-subsites/foreignaffairs.house.gov/files/migrated/uploads/2024/09/WILLFULL-BLINDNESS-An-Assessment-of-the-Biden-Harris_Administrations-Withdrawal-from-Afghanistan-and-the-Chaos-that-Followed.pdf.

U.S. Senate Committee on Foreign Relations. *Left Behind: A Brief Assessment of the Biden Administration's Strategic Failures during the Afghanistan Evacuation.* Minority Report. GPO, 2022.

van Beek, Hannah, and Sebastiaan Rietjens. "Open-Source Intelligence in the Russia–Ukraine War." In *Reflections on the Russia–Ukraine War*, edited by Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens. Leiden University Press, 2024.

Wack, Pierre. "Scenarios: Uncharted Waters Ahead." *Harvard Business Review* 63, no. 5 (1985): 72–89.

Warner, Michael. "Wanted: A Definition of Intelligence." *Studies in Intelligence* 46, no. 3 (2002): 21.

Wason, Peter C. "On the Failure to Eliminate Hypotheses in a Conceptual Task." *The Quarterly Journal of Experimental Psychology* 12, no. 3 (1960).

Wernli, Didier. "Understanding and Governing Global Systemic Crises in the 21st Century: A Complexity Perspective." *Global Policy* 14, no. 2 (2023): 207–228.

Wirtz, James J. "Are Intelligence Failures Still Inevitable?" *International Journal of Intelligence and CounterIntelligence* 37, no. 1 (2024): 307–330.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford University Press, 1962.

Wolfberg, Adrian. "The President's Daily Brief: Managing the Relationship between Intelligence and the Policymaker." *Political Science Quarterly* 132, no. 2 (2017): 225–258.

Wyss, Michel. "The October 7 Attack: An Assessment of the Intelligence Failings." *CTC Sentinel* 17, no. 9 (2024).

Zegart, Amy B. "Israel's Intelligence Disaster." *Foreign Affairs*, October 11, 2023.

Zegart, Amy B. "Statement on Intelligence Oversight." Testimony Before the Senate Select Committee on Intelligence, November 13, 2007. https://irp.fas.org/congress/2007_hr/111307zegart.pdf.

Zegart, Amy B. *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Vol. 8. Princeton University Press, 2022.

Zegart, Amy B. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton University Press, 2009.

Note on the use of AI tools

Artificial intelligence tools were employed to support brainstorming and to assist in paraphrasing selected critical passages. The analysis and arguments presented remain entirely the author's own.