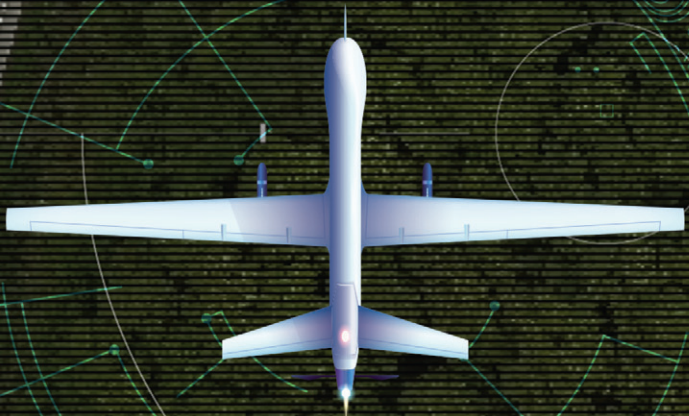
INTELLIGENCE FAILURES AND STRATEGIC SURPRISES IN COMPLEX GEOPOLITICAL ENVIRONMENTS



FREDERIC LEMIEUX

Intelligence Failures and Strategic Surprises in Complex Geopolitical Environments

This page intentionally left blank

Intelligence Failures and Strategic Surprises in Complex Geopolitical Environments

BY

FREDERIC LEMIEUX
Georgetown University, USA

United Kingdom – North America – Japan – India – Malaysia – China

Emerald Publishing Limited
Emerald Publishing, Floor 5, Northspring, 21-23 Wellington Street, Leeds LS1 4DL

First edition 2025

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-83608-611-6 (Print)
ISBN: 978-1-83608-610-9 (Online)
ISBN: 978-1-83608-612-3 (Epub)

To Ophelia and Rose-Lynn, may this work contribute to a safer and more stable world for your future.
Papa

This page intentionally left blank

Contents

Chapter 1

Intelligence and Intelligence Failures

The world is becoming increasingly unstable and complex. It has significantly reshaped the landscape of international relations as the current world order continues under relentless pressure from various state and nonstate actors. In this unstable environment, intelligence has become indispensable, both for national security and for maintaining stability around the globe. With politics, economy, and technology changing constantly, different actors are competing and cooperating in ways that expand their reach. These changes are changing global security, unveiling new threats and opportunities that require ongoing attention.

Within this rapidly evolving geopolitical landscape, the risk of intelligence failures has taken on even greater significance. The potential consequences of these failures, whether in the form of misinterpreted data, overlooked warning signs, or complete blindness to emerging threats, pose substantial risks to national security and the broader international community. Intelligence failures have always carried grave consequences, but their impact can be even more catastrophic in today's interconnected and high-stakes environments. Misjudgments or oversights in intelligence analysis can lead to strategic surprises that destabilize entire regions, ignite conflicts, or enable the proliferation of threats that could have otherwise been prevented.

The book is inspired by the fact that the current global environment has become increasingly complex and making it extremely difficult to detect and counter new threats. The sophistication of emerging threats and the quantity and pace of data and evolution make it more challenging for intelligence services to anticipate and prepare for such threats in real time. The failure to accurately identify such risks can have profound consequences for national security, global stability, and global tensions. One of the principal drivers of this increased risk is the unpredictable geopolitical winds. Relationships that have been established for generations are under scrutiny, emerging centers of power are being forged, and disaffected figures are taking on increasingly global roles. The proliferation of nonstate actors, including terrorist groups and global criminal syndicates, adds to the intelligence picture and renders it increasingly uncertain what the next threat could be. These threats tend to work behind the scenes, finding loopholes in traditional security architectures and learning fast to adapt to a response that

Intelligence Failures and Strategic Surprises in Complex Geopolitical Environments, 1–12

doi:10.1108/978-1-83608-610-920251001

eliminates them. Intelligence agencies are, therefore, always racing to keep up with an ever-evolving threat landscape.

The second is the rapid growth of technology, which has reshaped both the intelligence capabilities and the threat itself. On one side, emerging technologies like artificial intelligence (AI) and data analytics offer unprecedented possibilities for improving intelligence. These technologies help process vast data, allowing analysts to identify trends and patterns that would otherwise have been hard to discern with older methods. On the other hand, adversaries can use those same intelligence-enabled tools to cover up, disseminate, or launch highly sophisticated offensive operations that undermine national security and bring systems to chaos.

Other than technological and geopolitical problems, intelligence failures can stem from the internal processes of intelligence agencies. Cognitive biases, collective mentality, and institutional bias contribute to distorted data interpretations. Even if there are data, interpretations of that data can be obscured by assumptions or pressure to follow popular narratives. Moreover, intra-agency competition and the politicization of intelligence can further cloud judgment, resulting in erroneous conclusions and missed opportunities for early action.

Intelligence failures have far-reaching implications. History tells us repeatedly that when we underestimate potential threats, disaster follows. The Japanese bombing of Pearl Harbor in 1941, the terrorist attacks of 9/11 in 2001, and even the recent Russian invasion of Ukraine are just a few examples of the destructive nature of intelligence failures. Such instances highlight the need for robust, flexible intelligence systems to anticipate and address real-time threats. Failure to identify and anticipate vulnerabilities in the geopolitical climate that we now face can be regionally, if not globally, disruptive. The global interdependence of today means that a crisis in one region of the world can cause an outflow of instability in other regions, triggering economies, emigration, and cross-border warfare. All this interdependence heightens the risks of intelligence failures and makes it more pressing to develop methods to make intelligence more accurate, faster, and flexible.

Meanwhile, the scope for strategic surprises and geopolitical shifts has only expanded considerably. Strategic surprises arise when intelligence agencies do not foresee a destabilizing attack or a major geopolitical shift that changes the global power equation, breaks alliances, or establishes new battlegrounds. Such surprises are often caused by not taking warning signals seriously or underestimating an opponent's abilities and intentions. As international security grows increasingly fragmented, strategic surprises become even more probable, which makes it crucial for intelligence agencies to hone their predictive tools.

The chapter is structured in three parts. The first section examines the intelligence cycle and activities it is engaged in, to introduce fundamental concepts within the intelligence field. The second section discusses intelligence failures and how they relate to the intelligence cycle and intelligence operations at multiple levels. Finally, the third section discusses why this book matters to the general intelligence community and summarizes the major topics and arguments explored in the following chapters.

Conceptualizing Intelligence Activities

Intelligence typically represents the product of a process cycle with multiple steps (Lemieux, 2024): (1) prioritization and priorities and intelligence requirement (PIR); (2) gathering data; (3) collation of data; (4) interpretation of data; and (5) disseminating intelligence. Secondly, the intelligence cycle also includes the (6) analysis of the intelligence product (Peterson, 2005). Although many specialists typically view the evaluation as the last step of the cycle, Lemieux (2006) contends that assessment steps are conducted all the way through. Keeping this in mind, Fig. 1 puts evaluation at the center of the cycle because of its significance in ensuring the integrity and accuracy of the intelligence product. The intelligence cycle, widely acknowledged in professional circles, mirrors the methodological workflow of academic research in its structured approach but diverges significantly in its objectives. While intelligence aims to produce actionable decision-making information, academic research primarily focuses on developing theories and advancing knowledge. Each phase of the intelligence cycle will be examined in greater detail to better understand roles, functions, and activities.

Priorities and Intelligence Requirements Phase (PIRs)

PIRs can arise from two primary sources: (1) intelligence consumers, including customers or stakeholders, and (2) from ongoing or completed intelligence operations.

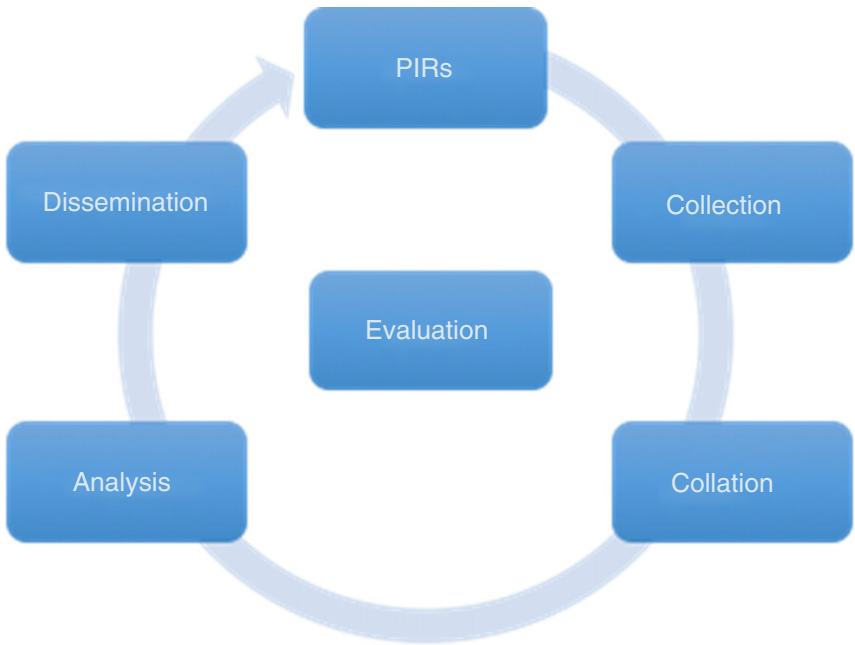


Fig. 1. The Intelligence Cycle (Lemieux, 2024).

The intelligence users use accurate information to make informed decisions, and early in the process, it is essential to decide what kind of intelligence is needed. Intelligence officers must assess whether the required knowledge will be strategic or tactical. In other words, the officer needs to know what the consumer wants. Some stakeholders need tactical intelligence to make day-to-day decisions, while others need strategic intelligence to plan for the long term. During this early PIRs phase, we develop the central question/hypothesis that the intelligence operation needs to resolve/validate. Identifying PIRs is a delicate responsibility because customers can only sometimes express exactly what they need. Close coordination between intelligence officers and stakeholders is critical to ensure the questions or theories are correctly formulated and match the consumer's intentions. It is a critical stage of validation in the intelligence cycle because it ensures that the intelligence needed is accurate and actionable.

The Collection Phase

Intelligence officers create a collection strategy in advance of initiating data collection. This plan usually includes what questions and hypotheses will be sought, intelligence fields to be researched, the sources to be used (primary and secondary), and any legal limitations on the collecting. It also lists the estimated duration for each source to be accessible and the deadlines for each activity. An essential part of this phase for intelligence officers is evaluating the credibility of each source (ascertaining whether it is accurate and credible). This review goes very closely with the ongoing review that ensures officers know who will most likely deliver an authentic intelligence product early on. Reliability of sources is critical for producing valuable and accurate intelligence.

Collection strategies vary widely based on source and intelligence field (interviews, wiretaps, and public records). By meticulously structuring the collection phase, the process becomes more streamlined and predictable, significantly reducing the risk of delays or obstacles within the intelligence cycle. Rapid collection is essential for timely, helpful intelligence to stakeholders. However, data collection plans and processes differ at every intelligence agency based on jurisdiction and mandate. Each agency tailors its collection activities to specific needs and directs the intelligence collected toward its strategic direction and regulatory environment.

According to Lowenthal and Clark (2015), collection activities can be categorized into five major disciplines. Intelligence activities used to be concentrated in two main areas: Human Intelligence (HUMINT) and Open Source Intelligence (OSINT). HUMINT involves obtaining data from humans, like spies or secret agents, who have details of target information. OSINT, meanwhile, refers to data openly available through the news media, government reports, databases, books, journals, and the Internet. In the 20th century, technologies diversified intelligence to create new fields: Measurement and Signature Intelligence (MASINT), Imagery Intelligence (IMINT), Geospatial Intelligence (GEOINT), and Signals Intelligence (SIGINT). In MASINT, data are collected and analyzed using electro-optical,

nuclear, geophysical, radar, radiofrequency, and material analysis, to name a few. IMINT is image-meaning and is made out of photos and images. GEOINT is composed of imagery (IMINT) and geospatial information related to physical features, structures, and human activity on a target of interest. Finally, SIGINT refers to the interception of communication, electronic communications, and telemetry signals. The information that these fields have gathered can be structured or unstructured. Structured data: DATA in a standard format like relational databases or spreadsheets (MASINT, GEOINT). Unstructured information, usually in text form, is descriptive information with some structure like dates, phone numbers, or bank account information (used to identify SIGINT, HUMINT, and OSINT).

The Collation Phase

During this phase, the intelligence officer standardized and organized the collected information in preparation for the analysis. Data Collation entails presenting the data in a format that reflects the analytical approach, either qualitative or quantitative. The intelligence officer also provides a preliminary data analysis to check for its validity and reliability. Part of this process involves matching the data collected with similar information sources to check for discrepancies or inconsistencies with existing knowledge. This step is essential to the success of the entire intelligence process because it is linked to the ongoing assessment process. By examining data correctly, the intelligence officer ensures that the following analysis is grounded in sound and valid data, maintaining the quality and credibility of the intelligence cycle.

The Analysis Phase

In this stage, the analyst reviews the collected data and applies various analysis tools, taking raw data and converting it to real-time intelligence. This phase is essential for implementing the identified priorities and intelligence needs. Two different types of analyses can be performed based on the PIRs, strategic and tactical. Strategic analysis is used to identify long-term trends, inform policy formulation, and provide techniques for managing security risks over time. In contrast, tactical analysis considers immediate tactical purposes, for example, to characterize the person or act, to detect patterns of incidents, and to analyze social media, time-series data, networks, communications, and the movement of items, like drugs, weapons, or people. During the analysis stage, the results are usually reviewed by peers and managers to ensure that the analytic procedures are effective and that the findings or recommendations do not suffer any flaws. This feedback ensures the integrity and quality of the intelligence that gets delivered and meets the stakeholder requirements.

The Dissemination Phase

During this phase, intelligence agencies present results to stakeholders based on the queries or hypotheses created in the early stages. Diffusion processes vary from agency to agency but usually have standard outlines of warning and watch, intelligence briefs, bulletins, reports, and assessments. The primary purpose of this phase is to disseminate information needed to enable stakeholders to make a tactical or strategic decision. For analysts and intelligence officials, an intelligence mission is best judged by how much their findings impact stakeholder decisions and how much action is guided by the intelligence provided. An intelligence product that has been well designed can have a positive impact on the decision-making process and can be leveraged by stakeholders to mitigate short-term or long-term security risks.

However, real-time intelligence dissemination is critical during crises, allowing decision-makers to respond rapidly to emerging threats. Historical examples, like the Cuban Missile Crisis, illustrate the importance of timely and accurate intelligence in averting catastrophe (Allison & Zelikow, 1999). Developing crisis-specific intelligence dissemination protocols can enhance decision-making and minimize the impact of unforeseen events.

Evaluation Phase

This phase includes internal and external evaluation of the intelligence product. Inside, errors or limitations spotted earlier in the process should be accounted for and rectified for better intelligence production in the future. From outsiders, they are the people who tend to provide intelligence with value in context and use-case insights to help refine suggestions and increase the value of the product.

Finality of Intelligence Products

Strategic, operational, and tactical intelligence are different levels of intelligence used in different decision-making processes. *Strategic intelligence* is used for longer-term, big-picture information that drives high-level policymaking. It comprehensively analyzes global threats, opportunities, or issues that could influence national or organizational strategies. Strategic intelligence helps policymakers develop foreign, defense, or economic policies. It enables managers to make decisions about future patterns and risks, thus maintaining an organization's sustainability or stability in the long run. Strategic intelligence systems, for example, allow decision-makers to collect and process data to make decisions that align with long-term national objectives (Huff, 1979).

Operational intelligence, by contrast, focuses on specific missions or zones. It involves data that are relevant to the operations of a given region or department. Such intelligence enables current activity to be linked to overall strategic goals. Commanders and mid-level managers often use operational intelligence to direct near-term and intermediate-term decisions, adjusting policies accordingly as new intelligence is received (Schmidt, 2015).

Tactical intelligence provides short-term, valuable data, typically in real time. It aids decision-making in the context of short-term activities, like war crimes or police actions. Tactical intelligence is used for decisions requiring instantaneous, field-based actions that support active units, allowing them to respond to developments rapidly. Tactical intelligence focuses on action from the front line and optimizes specific actions, such as counterinsurgency or fighting engagements (Mitchell, 2012).

The difference between policymakers and decision-makers also explains how intelligence gets consumed (Lowenthal, 2021). Government policymakers typically think strategically, drawing on intelligence to define long-term strategies and formulate domestic or foreign policies. Decision-makers can think at multiple levels (strategic, operational, or tactical) and draw on intelligence to make granular, sometimes tactical, decisions. These might be generals, diplomats, or business leaders who use intelligence for a short-term decision, mainly when things are critical or in crisis. Actionable intelligence is essential to the consumer because it gives them the power to make informed, timely decisions directly affecting strategic and operational goals. Without actionable intelligence, decision-makers risk acting based on partial or outdated data and ineffective or misleading policies and actions that do not effectively or appropriately mitigate existing threats or opportunities (Calof et al., 2015; Solano, 2019).

Intelligence Failures

Despite its importance in security and defense, intelligence remains complex and must often be better defined. This section discusses definitions, origins, and impacts of intelligence failures involving fundamental breakdowns in intelligence operations that lead to strategic surprises.

Definition

However, despite all the activity in intelligence, there is no general theory behind the subject (Gill & Phythian, 2013). As Warner (2019) explains, intelligence as a science needs help making itself understood and its role. Likewise, Pili (2019) highlights how "intelligence" is incomprehensible and requires philosophical treatment to get there. He is pushing for a philosophically and practically helpful definition of intelligence research. There are those who, like Breakspear (2017), might suggest that intelligence is a business ability that allows one to predict and act promptly in the face of change. It is an orientation of prescience and foresight, looking ahead and spotting opportunities or dangers before they happen. Others – such as Lowenthal (2021) – are more practical, attributing intelligence to policymaking and national security and drawing attention to its procedural and operational aspects in the government.

This approach is because there is no theoretical framework or definition of intelligence for why intelligence might fail. Despite no prevailing structure, intelligence agencies and analysts work with very different notions of intelligence.

This opaqueness renders it unable to detect and evaluate intelligence failures reliably and thus to provide standardized approaches and measures for intelligence operations. Thus, processes and results vary – and "intelligence failure" remains a fuzzy concept with different definitions by researchers and practitioners. This asymmetry makes it hard to identify the source of breakdowns and build effective plans for avoiding them, making intelligence work less reliable and effective.

Causes of Failures

The logic of intelligence failure has gradually come to be seen as inevitable, shaped by inherent challenges such as the tension between evidence and diligence, the ambiguity of judgment, and the constraints of institutional capabilities. They are more than just a matter of lousy tradecraft but of unsustainable expectations on the part of decision-makers and of using or abandoning intelligence. The three factors that most often contribute to intelligence failures are problems with precision, randomness, and complexity of the intelligence process and decision-making process (Jensen, 2012). There are inner and external causes of intelligence failure.

Intellectual deficits and a dearth of empathy from others, in turn, often contribute to intellectual misfiring, demonstrating the psychological component of analytic failure (Botts, 2018). Furthermore, mistakenness often arises from the psychological dispositions of leaders, not from analyst blindness to essential data (Betts, 2008). Jensen (2012) analyzed the subjective aspect of intelligence failure based on the analysis of fact versus judgment, and inaccurate prediction. In addition, intelligence failures are compounded by preventable issues like poor analysis techniques, ineffective intelligence operation coordination, and weak dissemination efforts.

The causes of intelligence breakdowns can be identified along different stages of the intelligence cycle. Regarding direction, most pitfalls come from unclear or lousy policy direction. Intelligence production and policy formulation can be ambiguous, and work needs to be clarified (Abdalla & Davies, 2021). Second, it fails at the collection level when the intelligence operations are misguided. The intelligence cycle often needs to be tuned to catch up to the rapidly changing requirements of the times, with policymakers providing scant collection advice (Hulnick, 2004). At the processing and analysis stage, confirmation bias, overconfidence, and other mental errors affect the analysis and can lead to wrong results (Belton & Dhami, 2020; Heuer, 1999).

Moreover, internal system faults like noise and bias errors in intelligence information systems play a crucial role in failures. For example, Labib et al. (2022) discovered that gaps in analysts' evaluation, which were caused by information overload, led to poor performance in UK Military Signals Intelligence (SIGINT). There is also a breakdown at the dissemination phase when inadequate communication and coordination thwart effective intelligence sharing. The Boston Marathon bombing case exemplifies the issues around federal, state, and local agencies sharing information (Garber, 2015). For these to be prevented, stronger strategic, operational, and tactical level coordination is essential (Trafton, 1994).