Beyond the binary: a new typology for evaluating warning success and failure in strategic surprise

Ikani, N.

International Studies Review (2025), viaf009

ANALYTICAL ESSAY

Beyond the Binary: A New Typology for Evaluating Warning Success and Failure in Strategic Surprise

Nikki Ikani
Leiden University, The Netherlands
NATO Defense College, Italy

Why do some intelligence warning processes succeed in anticipating surprise while others fail? This article challenges the binary perspective on warning success and warning failure prevalent in extant analyses, which it contends ignores the complexity of warning processes and their outcomes. Its main thesis is that warning success rather exists on a spectrum of outcomes from full success to complete failure. To support this argument, this article introduces a novel, multidimensional typology that captures warning outcomes on such a spectrum, aligning with approaches to measuring (foreign) policy success within political science and public administration. It dissects warning effectiveness into three dimensions: the analytical (accuracy and timeliness of threat understanding), process (effectiveness of warning communication), and political dimensions (degree of decision-maker receptivity). Inherent tensions and challenges within these dimensions are expected to produce trade-offs, where success in one dimension may not ensure success in others. By applying this typology to three illustrative case studies—the COVID-19 pandemic warning in the United Kingdom, the Russian interference in the 2016 US election campaign, and the EU's warning process preceding the Crimea annexation—this paper demonstrates that warning performance often varies significantly across the three dimensions, highlighting the trade-offs and conflicts that can occur. This typology challenges existing binary paradigms and enables a more comprehensive understanding of warning effectiveness. This may inform targeted, adaptive, and effective security policy responses, in addition to improving our understanding of strategic surprise anticipation and warning strategies.

¿Por qué algunos procesos de alerta de inteligencia logran anticipar la sorpresa mientras que otros fracasan en esta tarea? Este artículo desafía la perspectiva binaria sobre el éxito y el fracaso de las advertencias que prevalece en los análisis existentes, y sostiene que esta perspectiva ignora la complejidad de los procesos de alerta y sus resultados. Su tesis principal es que el éxito de la advertencia existe más bien como un espectro de resultados que van desde el éxito total hasta el fracaso completo. Con el fin de apoyar esta hipótesis, este artículo presenta una tipología novedosa y multidimensional que captura los resultados de las advertencias en dicho espectro y se

Ikani, Nikki. (2025) Beyond the Binary: A New Typology for Evaluating Warning Success and Failure in Strategic Surprise. *International Studies Review*, https://doi.org/10.1093/isr/viaf009

alinea con los enfoques para medir el éxito de la política (exterior) dentro de la ciencia política y la administración pública. El artículo disecciona la eficacia de estas advertencias en tres dimensiones: la analítica (precisión y puntualidad de la comprensión de las amenazas), la del proceso (eficacia de la comunicación de las alertas) y las dimensiones políticas (grado de receptividad por parte de los responsables de la toma de decisiones). Se espera que las tensiones y los desafíos inherentes a estas dimensiones produzcan equilibrios, en los que el éxito en una dimensión puede no garantizar el éxito en otras. Este artículo aplica esta tipología a tres estudios de caso ilustrativos (la alerta sobre la pandemia de COVID-19 en el Reino Unido, la injerencia rusa en la campaña electoral estadounidense de 2016 y el proceso de alerta por parte de la UE que precedió a la anexión de Crimea) y demuestra que es frecuente que el funcionamiento de las advertencias varíe significativamente en las tres dimensiones, destacando las compensaciones y los conflictos que pueden ocurrir. Esta tipología desafía los paradigmas binarios existentes y permite una comprensión más completa de la efectividad de las advertencias. Esto puede proporcionar información para elaborar respuestas en materia de política de seguridad específicas, adaptables y eficaces, además de mejorar nuestra comprensión de las estrategias estratégicas de anticipación y alerta por sorpresa.

Pourquoi certains processus d’avertissement par les renseignements réussissent-ils à anticiper une surprise quand d’autres échouent ? Cet article remet en cause la perspective binaire sur la réussite et l’échec d’un avertissement qui prévaut dans les analyses existantes. Selon lui, elle ignore la complexité des processus d’avertissement et de ses résultats. Sa thèse principale est que la réussite d’un avertissement se situe plutôt sur un spectre de résultats, qui s’étend de la réussite totale à l’échec complet. Pour étayer cet argument, l’article présente une typologie multidimensionnelle inédite qui représente les résultats des avertissements sur un tel spectre, conformément aux approches de la mesure de la réussite de la politique (étrangère) au sein des sciences politiques et de l’administration publique. Il dissèque l’efficacité d’un avertissement selon trois dimensions : la dimension analytique (précision et rapidité de la compréhension d’une menace), processuelle (efficacité de la communication de l’avertissement) et politique (degré de réceptivité des décideurs). Des tensions et défis inhérents à ses trois dimensions devraient produire des compromis, si bien qu’une réussite au sein d’une dimension pourrait ne pas assurer la réussite dans d’autres. En appliquant cette typologie à trois études de cas d’illustration (l’avertissement de la pandémie de Covid-19 au Royaume-Uni, l’interférence russe dans la campagne électorale américaine de 2016 et le processus d’avertissement de l’UE avant l’annexion de la Crimée), cet article démontre que les performances d’un avertissement diffèrent souvent de façon importante au sein des trois dimensions, ce qui met en évidence les compromis et les conflits éventuels. Cette typologie remet en question les paradigmes binaires existants et permet de comprendre de façon plus exhaustive l’efficacité d’un avertissement. Ainsi, l’on pourrait apporter des réponses plus ciblées, adaptatives et efficaces en politique de sécurité, en plus d’améliorer notre compréhension de l’anticipation de la surprise stratégique et des stratégies d’avertissement.

Introduction: An Evolving Threat Landscape and the Need for Warning

Strategic surprises, those significant, unforeseen events that disrupt the status quo in (international) politics, occur frequently (Grabo 2002; Dahl 2020; Gray 2005; Betts 1981). In the last 3 years, the October 2023 Hamas attack on Israel, the fall of Kabul, and (to some actors) the 2022 Russian invasion of Ukraine stand out as notable examples. The volatility of the international geopolitical landscape requires states and international organizations to devote significant funds to developing systems that can provide advance threat warnings. For instance, from 1978 to 2011 the US federal government had a National Intelligence Officer for Warning to provide explicit warning on developments of major concern (Central Intelligence Agency 1978). In the United Kingdom, the Cabinet Office Assessments Staff provides warnings of threats to UK interests (UK Ministry of Defence 2023, 12–3). The North Atlantic Treaty Organization (NATO) developed its Intelligence Warning System to provide long-term crisis anticipation, in addition to various tactical warning units. The warnings these systems produce can be strategic, concerning the emergence of important threats that require action in order to deter or defend against (Grabo 2002; Gentry and Gordon 2019), or tactical: related to specific timings, modalities, perpetrators, and targets of near-term events or attacks (Davis 2006). Warning processes, and the need to continuously improve these, have recently gained considerable traction on policy agendas at the domestic and the international level, as the perception exists that we live in a time of unprecedented strategic surprise (US Department of Defense 2020; European Union 2022; NATO 2022; Republique Francaise 2023).

In parallel, the literature both on the origins of strategic surprise and the challenges of accurately predicting and warning for these events has expanded considerably over the past decades. This happened across the domains of international relations, public administration, and intelligence studies (Nye 1994; Parker and Stern 2002; Wirtz 2003; Byman 2005). While traditionally (in predominantly US-focused literature), strategic surprise was associated with military attacks (Ben-Zvi 1976; Betts 1981, 1982; Kam 2004), slower-burning, indirect, and nonkinetic threats by state and nonstate actors have received increasing attention as instances of strategic surprise (Dahl 2018, 2023; Wirtz 2023). Through a vast array of historical case studies, this body of work demonstrates how in practice, the warning processes and systems preceding these surprise events are riddled with problems. Even under the best of circumstances, issuing accurate, and timely warnings is highly challenging. Signals indicating impending upheaval are often weak or drowned out by a flood of noise. Warnings that are generated might stumble on bureaucratic roadblocks or might be held back by unwilling superiors. Even if a warning about an imminent threat manages to make it to the top of the organization, decision-makers might be too busy, might not trust the warner, or may be politically motivated to discard the message (Wohlstetter 1962; Kent 1966; Betts 1978; Ben-Zvi 1990; Grabo 2002; Zegart 2005; Jervis 2010b; Bar-Joseph and McDermott 2017; Gentry and Gordon 2019).

Despite the proliferation of warning systems over the past decades and the rich literature detailing instances of warning failure, there remains an academic emphasis on isolated cases of failure. This produced an ambiguous understanding of what defines “success” and “failure” within warning contexts. The frequent application of these unspecified labels underscores that a scholarly definition of warning success and warning failure is still lacking. The extant literature also shows a tendency towards a binary categorization of warning effectiveness, simplifying a spectrum of warning outcomes into clear-cut successes or failures. History, the literature attests, is particularly replete with the latter.

The issue is, this article contends, that this overwhelming tendency towards binary, oppositional categories of failure and success fails to capture the interplay of diverse factors that might contribute to or undermine the effectiveness of warnings. It also falls short in capturing the more nuanced realities and intermediate outcomes that characterize the warning process. Warning success should be a matter of degree. “To set up a distinction in binary form when the things referred to vary by degree or in some other fashion,” Levy (1970, 95) argued, “is not only the classic misuse of the law of the excluded middle, it also guarantees the begging of important questions." It equally overlooks warnings that led to a partial mitigation of threats or that result in heightened preparedness without completely averting a crisis—for these are neither outright successes nor total failures.

This paper argues that warning success exists on a spectrum of outcomes rather than in binary. The traditional binary perspective of "warning success" and "warning failure" oversimplifies the complexities of the warning process and its outcomes. To address this limitation, this article's primary contribution is a novel typology that allows for a systematic and multidimensional evaluation of warning success and failure along a continuum. In doing so, it aligns with earlier efforts to reconceptualize policy success (McConnell 2015) and foreign policy success (Levy 1970; Dahl 1976). Informed by both the IR and intelligence studies literature, this typology dissects warning effectiveness across three dimensions: (1) the analytical dimension, concerning the ability to produce clear, actionable and timely warnings in order to provide a basis for decision-making; (2) the process dimension, concerning the effectiveness of the warning communication channels within organizations to ensure warnings reach the intended recipients; and finally, (3) the political dimension, concerning decision-maker receptivity and response to the warnings they receive. It thus integrates the myriad reasons the extant body of work has identified as contributing to warning failure into a single framework capturing the main overarching dimensions of such failure. The typology assesses warning failure and warning success across these dimensions on a spectrum, recognizing that warning success is a matter of degree. By allowing for varying levels of success or failure within each dimension, this typology provides a more nuanced and multifaceted understanding of what constitutes a "successful" warning process.

This approach can shift our focus away from asking whether the warning has been successful or unsuccessful, to explaining warning performance: where and how the warning process may not reach the desired outcome, as well as potential frictions and trade-offs within the warning process. This improves our understanding of strategic surprise, as in an ideal scenario, timely warnings precede and potentially prevent strategic surprises. "At its essence," contend Wirtz et al. (2023), "warning in the 21st century is warning of the impending failure of strategy, that the threat of war is growing and that the strategy of deterrence could soon be rendered superfluous." Identifying the various pathways to warning success and failure thus offers an improved understanding of how strategic surprises arise and the ways in which they can be anticipated or mitigated. In addition, this typology categorizes and synthesizes the myriad factors that contribute to warning failures that earlier, often isolated case studies identified. Organizing these into three dimensions provides a structured lens through which both failures and successes in intelligence warning can be assessed.

The remainder of this article proceeds as follows. First, it examines how warning processes are generally studied in binary in the extant literature, highlighting the conceptual and practical issues of this pervasive binary conception of success and failure. It then introduces a novel, multi-dimensional typology, which offers a more nuanced framework to map and understand the various dimensions and outcomes of warning success and failure. Following this conceptual groundwork, it applies this framework to three illustrative case studies: the warning process leading up to the COVID-19 pandemic in the United Kingdom, the Russian interference in the 2016 US election campaign, and finally the EU's warning process preceding the 2014 Crimea annexation. It concludes by underscoring the broader implications of such a refined typology of warning success and failure, emphasizing how its analytical scope can enhance our understanding of the effectiveness of warning systems as well as our understanding of strategic surprise.

This paper employs three illustrative case studies to demonstrate how the typology of warning success and failure applies to a real-world context. These case studies are not intended for comparison but serve to showcase the value of a spectrum-based approach to warning performance (Seawright and Gerring 2008; Yin 2017). Primarily, they illustrate how warning processes may result in varying degrees of success along the three different dimensions, highlighting the advantage of the spectrum-based approach over the traditional, binary approach.

These case studies were selected based on several criteria. First, they represent different types of strategic surprise, spanning from a global health crisis (the COVID-19 pandemic in the United Kingdom), a cyber and disinformation campaign (Russian interference in the 2016 US election), and a geopolitical conflict (the 2014 Crimea annexation). All three cases presented critical scenarios which had a significant impact on national and international security as they transpired. Second, the cases involve different entities: national governments (United Kingdom and United States) and a multilateral organization (EU), each with distinct structures. The United States has a highly professionalized, yet decentralized intelligence community. Multiple agencies with significant manpower, budget, and specialized functions can and must collaborate in the warning process. The UK intelligence community, in contrast, has a much more centralized structure and culture of intelligence and decision-making (Davies 2012). Finally, the EU disposes of the Single Intelligence Analysis Capacity, which combines civilian intelligence (EU INTCEN) and military intelligence (EUMS INT), but does not possess any primary intelligence-collecting powers, and is reliant on what is fed to it by its member-states (Ikani et al. 2020). The UK-COVID-19 case study adds additional value not just because of this organizational variation but also because COVID-19 was a health crisis involving a wide range of actors beyond the intelligence services. It highlights how nontraditional threats travel through warning systems. This diversity between the entities involved in the case studies demonstrates how the three dimensions of warning effectiveness manifest, enhancing the utility and applicability of the typology proposed. The cases also show varying degrees of success across the three different dimensions in the warning process, as well as how they may conflict and necessitate trade-offs. Finally, all three cases were well-documented.

To explore the warning process in the three selected cases this paper draws on historical process tracing techniques. This implies it investigates how the warning processes unfold over time. It involves identifying the mechanisms that shaped the warning process in these three case studies, primarily using documentary analysis (Bowen 2009; Mahoney 2015). The main evidence consists of the material "left behind" in the warning process, used to pinpoint specifically which warnings or alerts were issued, when, and to whom. Twenty-three public records were analyzed, from the United Kingdom on COVID-19 (8), the United States on the election interference by Russia (9), and the EU on the Crimea annexation (6). These records span official texts, public inquiries or investigations as well as leaked classified documents in which these warnings were discussed. This evidence is corroborated with publicly available secondary material, allowing for a thick description of the political context in which the three warning processes took place.

Through these diverse cases, the article demonstrates the utility of a spectrum-based analysis over the traditional binary model, providing a richer explanation of the outcomes observed. The cases illustrate how varying degrees of warning success across the analytical, process, and political dimensions can exist in various "high stakes" strategic surprise scenarios. They also show how the different dimensions of warning failure may conflict and result in trade-offs. By encompassing such a wide range of contexts and entities, the case studies illustrate the robustness of the proposed typology and how can be applied in diverse situations.

The Limitations of the Success–Failure Binary in Strategic Surprise

The binary understanding of warning success and warning failures is in part rooted in the way our brains are wired. Humans are biased toward perceiving information in binary terms (Fisher and Keil 2018). Binary constructs are thus a pervasive part of how we perceive wealth, power, and politics, to name a few. Political conflicts enter history books as victories or defeats (Johnson and Tierney 2006). Economic sanctions either "work" or do not (Pape 1998). The same applies to our assessment of cybersecurity regimes (Atkins and Lawson 2021) or international peacekeeping operations. When conducting inquiries into past crises and whether they could have been avoided, we see that institutions engage in similar, dualistic terminology of success and failure (Boin et al. 2008). Binary conceptions of warning success and failure of course have advantages: They allow for straightforward feedback and facilitate allocating praise, or blame. Binary assessments of past performance also provide easier pathways toward policy recommendations. Gray, ambiguous areas of partial success, or partial blame, complicate the process of policy prescription.

In the field of intelligence studies, "intelligence failures" are a major topic of study as they examine warnings from intelligence and foreign policy services on matters that could affect national security, both tactical and strategic. Landmark cases include the failure of US intelligence to warn of the Japanese attack on Pearl Harbor in 1941, the 1973 Yom Kippur War, the 1982 Falklands War, and the 9/11 terrorist attacks (Wohlstetter 1962; Bar-Joseph 2005; Parker and Stern 2005). This body of literature has identified what exactly frustrates this process. Explanations range from psychological factors, the politicization of the warning process, bureaucratic inhibitions, or the inability of intelligence services to distinguish crucial signals from the ubiquitous noise (Kent 1966; Handel 1980; Ben-Zvi 1990; Grabo 2002; Davis 2003; Zegart 2005; Dahl 2013b; Gentry and Gordon 2019). However, and with some key exceptions (Handel 1984; Wirtz 2003; Dahl 2013a) the central focus on dissecting predominantly single cases of failure long fostered a lack of conceptual clarity on what specifically constitutes "success" and "failure" in the context of warning. Intelligence successes are discussed only occasionally, though much more infrequently since they are much less visible and often tend to remain classified. Moreover, partial successes remain underexplored (Levite 1989; Marrin 2004; Jervis 2010a; Dahl 2013a; Bar-Joseph and McDermott 2017).

The conflict studies scholarship has, in its turn, contributed to our understanding of the so-called "warning–response gap." This refers to the tendency of policymakers not to take early warning seriously, let alone act upon it (George and Holl 1997). These studies place particular emphasis on early warnings regarding human security and human rights violations (George and Holl 1997; Meyer et al. 2020; Adelman and Suhrke 1996; Ackermann 2003). The concept of the warning–response gap presents an important step beyond the static binary conception of warning toward a more dynamic view of warning as a process, yet also insufficiently specifies what successful or failed warnings exactly entail (Meyer et al. 2020, 31).

Two issues emerge from the pervasive success–failure binary. The first is conceptual. "Success" and "failure" "are not inherent attributes, but labels retrospectively applied to evaluate past performance. Such labels can obscure more than they clarify. Crucially, the frequent claim that warning processes have failed—even if underpinned by a rich analysis of past failures—presupposes an underlying criterion for evaluation which is rarely defined. "As a result of these limitations in the literature," posits Dahl (2013a, 15), we have fundamentally misunderstood the reason why intelligence fails to help us prevent surprise attacks, failures, and other disasters. It is therefore important not to "hasten to label particular historical episodes as warning successes or failures" (Chan 1979, 173), without a nuanced understanding of where and how the warning process broke down. The political scientist Robert Dahl once argued that a common error was that power was seen as an attribute actors would possess or not possess—instead of exploring the variations in the degree of power, they may have (1976). This tendency to "ignore gradations in effectiveness" (Baldwin 2000, 174) has persisted in assessments of warning. Explaining how and why certain warnings fail requires an evaluation of the degree to which the warning process has indeed failed, including those instances where the warning was perhaps partially successful in some respects.

More practically, this black-and-white categorization can potentially result in misdiagnosed pathologies in the warning process due to a superficial understanding of this process. For example, if both the detection of threats as well as the communication of the warning upwards in the hierarchy were effective, but decision-makers simply ignored the warnings, it would be remiss to label the entire warning process as a failure. Jervis (2022, 1) identified that in the assessment of warning success or failure, people are guided by outcomes when guiding the appropriateness of the warning process, and "ignore the fact that people may be right for the wrong reasons and wrong for the right ones." Such blanket labeling can produce scapegoating, blame games, or misdirected attempts at reform (Brändström and Kuipers 2003). There is a related potential danger of "overcorrections" when we overlook partial successes and partial failures that do not neatly fit into the categories—and any potential specific lessons these can yield.

The lead-up to Russia's invasion of Ukraine in 2022 serves as a recent example of how detrimental a binary lens of success and failure can be. Despite persistent warnings from the United States, Paris, and Berlin remained unconvinced Russia would invade Ukraine—to the point where the head of the German foreign intelligence service was stuck in Kyiv when the Russians invaded and had to undertake an arduous overland journey to get back. A significant factor in this dismissal of American warnings was the shadows cast by past failures, notably with regard to Iraq two decades earlier, dubbed "the perfect intelligence failure" (Phythian 2006). This was further fuelled by the US surprise at Kabul's fall just months prior (The New York Times 2021). A French insider reflecting on this perception of previous failures explained that "American intelligence [was] not considered to be a naturally reliable source. It was considered to be prone to political manipulation" (Harris et al. 2022). Success and failure, we learn, are no absolute or dichotomous outcomes. Rather, there exists a spectrum between the two ends, and this is where most of the lessons to avoid these failures may be found (McConnell 2015).

A New Typology for Evaluating Warning Success and Failure

"Success is a slippery concept," Baldwin wrote about foreign policy success (2000, 171), "it makes little sense to describe someone as pursuing success without specifying success in doing what." Based on a review of the corpus on strategic surprise and warning research in IR and intelligence studies, this typology dissects warning effectiveness into three critical dimensions: the analytical, procedural, and political (Wohlstetter 1962; Betts 1978; Grabo 2002; Parker and Stern 2005; Fitzgerald and Lebow 2006; Zegart 2007; Gentry 2008; Jervis 2010b; Dahl 2013a).

The first stage of any warning process concerns the detection and ***analysis*** of threats. The ability to produce accurate and timely inferences on threats to security, in order to provide a basis for decision-making, is a necessary but not sufficient ingredient to warning success (Chan 1979; Betts 2010; Mandel 2015). Warning pathologies within this analytical dimension frequently stem from the intrinsic diagnostic challenges that warning processes present. Predicting the course of a variety of actors and factors in our volatile and complex world, and how they might potentially interact to combust, is challenging. Especially in complex regions of vital interest, "the data are abundant, but they do not point unambiguously to a single outcome" (McCarthy 1994). The result is a tendency to simplify assumptions, to rely on broad and abstract conceptions about how the world works, and so-called "factor wars": attempts to find a singular explanatory factor, rather than considering the complexity of events (Herrmann and Choi 2007, 153). Analytical failures are arguably avoidable, as more data, more information, and more "connecting the dots" could potentially mitigate them. Yet realism is needed: nonlinear events, black swans, or bolts from the blue do occur and they present severe diagnostic challenges for analysts (Chan 1979; Taleb and Blyth 2011). Strategic surprises are by their very nature drastic departures from the status quo and therefore very difficult to forecast and warn for appropriately.

"Warning that exists only in the mind of the analyst is useless," wrote Grabo (2002, 14). Warnings need to travel to decision-makers. The ***process*** dimension of warning concerns the path warnings must navigate within organizations to reach the right end-points. This "warning journey" is a challenging one: successful warnings must flow through a host of units and stages, each with potential veto points and with numerous stakeholders before the right decision-makers are even reached. Bureau politics, complex organizational structures, and other structural organizational forces have been identified as core factors that affect the effectiveness with which warnings are communicated and acted upon (Wilensky 1967; Cohen and Gooch 1990; Zegart 1999, 2007). An effective procedural dimension involves ensuring that accurate warnings are not just generated, but also prioritized, effectively communicated upwards in the organizational hierarchy, and delivered to decision-makers able to act (Snyder et al. 1962; Allison and Halperin 1972; Parker and Stern 2005). Warnings that thrive in the system tend to be tailored and digestible, allowing the warning to be communicated swiftly (Lowenthal 2012). Warning effectiveness is also subject to temporal constraints. Wirtz (1991, 6) discusses the phenomenon of "diminishing returns" of warning, using the Tet Offensive as an example. He posits that in any warning scenario, there exists a critical point after which the effectiveness of any warning issued begins to yield diminishing results, even if they even when warnings reach the right decision-makers. This diminishing effectiveness stems from the time required to mobilize defense measures or mitigate outcomes. The window for effective action can close rapidly, especially as warnings need to journey through bureaucratic systems to reach all relevant decision-makers in a timely manner. For example, by the time the last-minute warning messages on a Japanese attack on Pearl Harbor arrived in the morning of December 7, 1941, effective military and naval action may no longer have been feasible. (Wohlstetter 1962, 12).

Process failures occur when the warning chain breaks down due to organizational and classification barriers, causing warnings based on accurate signals and pattern detection not to travel to the right places (Marrin 2004). Particularly organizational factors play a role in causing them, as flawed institutional design and a tendency towards "group think" (Janis 1972) cause systemic biases that impede the flow and handling of the warning. In recent years, more attention is paid to facilitating the transmission of potentially discordant views, to facilitate bottom-up warnings that may go against the "organizational line." Examples are the creation of "Red Teams," or "devil's advocate" positions. Yet proliferating numbers of foreign and intelligence agencies providing warning can create institutional rivalry and trigger turf wards among them, leading to limited information exchange. Warnings may be scattered across institutions, with each providing only part of the picture, or lacking effective and credible communicators.

The ***political*** dimension of the warning process is concerned with how receptive decision-makers are to warnings. This receptivity is a crucial last step in the warning process (Dahl 2013b, 70). The analytical and process dimensions were both about the *presence* of critical elements in the warning process. The presence of the appropriate tools, capabilities, and knowledge to identify and interpret threat patterns and formulate a warning. Or the presence of effective procedures and channels for communicating and delivering these warnings to the appropriate decision-makers.

Contrastingly, success in the political dimension is not just about the presence of receptivity, but crucially also about the *absence* of detrimental political interference, bias, or expediencies that interfere with or undermine political receptivity to warning. A politically successful warning does not equate that all warnings always directly influence policy decisions, but necessitates an environment where warnings are received, taken seriously, considered, and duly prioritized—or indeed dismissed—on substance.

Political failures occur when the warning process is inhibited by political nonreceptivity to warnings issued, or due to an inability among political actors to agree on the significance or urgency of issues. Generally, once warnings, policy, or other issues reach the political domain, they meet the "usual suspects" of conflicting interests, decision-maker careerism, or a lack of political will, which creates political nonreceptivity. They may stumble across decision-makers "who project their own personal or policy desires, character flaws, or mental disorders onto those around them" (Wirtz 2023, 326). This is exacerbated by the fact that decision-makers are known to have a status-quo bias, making them particularly hesitant to listen to warnings about events that would significantly disrupt this status quo (Samuelson and Zeckhauser 1988). Especially since warnings are often of "uncertain accuracy," and the action in response to the warning may be costly (Wirtz 2023, 326). Prior to the Yom Kippur War, for example, Israeli decision-makers did receive warning, but were reluctant to call for a mobilization as not only could it actually encourage the Egyptians and Syrians to prepare for war, but it would also have detrimental effects on the Israeli economy (Handel 1977). Adequate analysis, effective process, and political receptivity are the necessary and sufficient conditions for the realization of warning success, which is not just about whether threats are accurately and timely detected, but also about how this information is subsequently managed, communicated, and received.

The interplay between these dimensions means that each can affect the outcomes of the others: success in the process dimension is facilitated by clear and timely warnings, whereas the clarity of communication in the process dimension may shape political receptivity in the political dimension. However, this interdependence can also introduce challenges and negative feedback loops, producing tensions, contradictions, or frictions, with success in one dimension not translating into success in another, or problems in one dimension exacerbating issues in the other (McConnell 2010, 357). For example, accurate warnings (analytical dimension) can be undermined by poor communication channels (process dimension) or distorted by political biases (political dimension). Political agendas may shape analytical priorities and focus, but equally potentially alter communication pathways due to increased urgency.

The prioritization of one dimension may equally compromise another. Streamlining the process dimension by making sure warnings are communicated in clear terms and quickly, might lead to the sacrificing of analytical accuracy by shortening the timeframe for assessing the threat. Also, in their attempt to persuade policymakers for increased political receptivity, analysts might simplify their findings. Political success might also be achieved at the expense of analytical success. We saw this in the case of 9/11, where various signals and warnings about potential terrorist attacks by al-Qaida did not resonate with decision-makers, who had made a ballistic missile defense system the centerpiece of their security policy and were not receptive to nonstate actor terrorism warnings (Parker and Stern 2005). Understanding the three dimensions as well as their interdependencies is thus critical for developing mitigation strategies aimed at enhancing the warning process.

Full warning success is achieved when the entire warning process across its dimensions—from the initial identification and analysis of a threat, through its communication to decision-makers, to the warning reception and understanding by decision-makers—is completed optimally, culminating in the consideration of appropriate policy action (Betts 1978; McCarthy 1994; Hedley 2005; Johnson 2009; Jervis 2010b; Lowenthal 2012; Marrin 2012; Wirtz et al. 2023). Paradoxically, "most successful warnings appear to be false alarms" because they provide decision-makers with enough time to avert, mitigate, or deter the threat (McCarthy 1994). However, full warning success does not transform regions or scenarios into ideal states. It merely means that (1) decision-makers receive warnings prior to the critical point after which warnings yield diminishing returns; (2) are receptive to the warnings; (3) comprehend the particular outcome they are being warned about; and (4) understand it is their responsibility to consider appropriate policy options. The US intelligence community, for example, successfully warned US decision-makers that Russia could invade Ukraine in February 2022 and that this would be a last-minute decision by Russian President Putin. Their warnings outlined what later transpired "in extraordinary detail" and were fully accepted by the Biden Administration, exemplifying a warning success (Harris et al. 2022). This holds true even if the warning did not stop the invasion.

A *near success* occurs when decision-makers receive nearly comprehensive warnings with minor details either omitted or inaccurate. They may experience minor delays but remain well within the timeframe to take effective action. The warnings are generally well-understood by decision-makers, with slight ambiguities remaining which do not hamper action. Decision-makers may have some uncertainty about the right course of action, or may disagree, but will have enough effective policy options available. *Moderate success/failure* concerns a mix of success and failure within the warning process. Analytically, warnings may be incomplete or include inaccurate interpretations. Suboptimal communication within the process dimension may cause noticeable delays or confusion, narrowing the window for an effective response. And even though some warnings will still reach the decision-makers, they may lack context or detail. Political bias or reduced receptivity constrains policy options, meaning the response may be the lowest common denominator. A *significant failure* occurs when decision-makers receive incomplete, inaccurate, or vague warnings, which arrive too late to allow for a full spectrum of policy options. Warnings may still yield some insights which could aid in either mitigating the threat or improving the warning process for future, similar threats. Politically, warnings prompt limited preventative action due to biases, competing interests, or highly constrained policy options. Finally, *complete warning failure* occurs when a warning is not issued or not issued in time, or critical signs are misunderstood or misinterpreted leading to a failure to provide any meaningful warning. Warnings may also be not communicated timely and effectively for decision-makers to act, or decision-makers simply do not understand the warning they receive. Even when they receive and understand the warning, they may still have either no policy options or lack agreement on policy options to mitigate the threat, due to entrenched biases or overriding foreign policy priorities, resulting in delayed or absent responses that do not manage the threat effectively. Table 1 summarizes the multidimensional, spectrum-based approach this paper proposes. This conceptualization underlines that reality involves trade-offs and frictions within and among these dimensions, thus resulting in varying levels of success or failure, as the case studies below illustrate.

Table 1. A typology of warning performance from success to failure

	Analytical dimension	Process dimension	Political dimension
Full success	Threat judged and analyzed accurately	Warning formulated and communicated effectively to decision-makers	Warning received, accepted, and considered for policy action by decision-makers. Decision-makers have enough time to avert, mitigate, or deter the threat.
Near success	Nearly comprehensive warnings with minor inaccuracies	Warnings may arrive with minor delays but within actionable timeframe	Warnings generally well-understood with slight ambiguities not hampering action. Some uncertainty about the right course of action but effective policy options are available.
Moderate success/failure	Warnings may be incomplete or include inaccurate interpretations	Suboptimal communication causes noticeable delays or confusion, limiting effective response time and options	Warning reaches decision-makers but may lack detail. Political bias or reduced receptivity constrains policy options, yet some action is undertaken.
Significant failure	Incomplete, inaccurate, or vague warnings	Warnings arrive too late for a full spectrum of policy options	Warnings prompt limited policy action due to biases, unclear responsibilities to act, competing interests, or highly constrained policy options.
Complete failure	No meaningful warning issued in time	Failure to communicate warnings timely and effectively for decision-makers to act	Decision-makers do not understand the warning, have no policy options or lack political agreement to mitigate the threat, resulting in delayed or no response.

Applying the Typology: Case Studies of Strategic Surprise

COVID-19 in the United Kingdom

The COVID-19 outbreak that started in late 2019 precipitated a multifaceted global crisis, directly affecting the health and well-being of individuals worldwide. Experts had long warned for the probability of a global health crisis or a pandemic, particularly from zoonotic diseases (Morse et al. 2012). As far back as 2010, the UK National Security Risk Assessment (NSRA) identified a major public health catastrophe as a "Tier One" threat to UK security (Chertoff et al. 2020). Yet despite this, the warning process in the lead-up to the pandemic was highly flawed. "Fundamentally," one witness told the UK Covid Inquiry panel (2023a, 21), "in relation to significant aspects of the Covid-19 pandemic, we were taken by surprise." In 2023, Boris Johnson acknowledged he "should have twigged" the seriousness of the virus sooner than he did (BBC News 2023b). This case shows how failures existed and exacerbated each other across the three dimensions.

Analytically, the trajectory of COVID-19 was—and remains—highly challenging, particularly with regard to the role of super-spreaders (Zenk et al. 2020), the containment challenges posed by asymptomatic and presymptomatic infections (Nikolai et al. 2020), and the varying infectivity of mutations (Plante et al. 2021). This produced a diagnostic challenge that was not overcome in time. Two pandemic exercises, *Exercise Alice* and *Exercise Cygnus* war-gamed the UK's pandemic preparedness in 2016. The final reports identified clear gaps: "UK's current preparedness [. . .] is currently not sufficient to cope with the extreme demands of a severe pandemic that will have a nation-wide impact across all sectors" (Public Health England 2017, 6). It was suggested there was an overreliance on the outdated 2009 response to the H1N1 virus, and that even some of that knowledge was "currently being lost" (Public Health England 2017, 7; Public Health England 2016, 16). UK assumptions about how a potential virus might spread were heavily shaped by the *UK Influenza Pandemic Preparedness Strategy* drawn up in 2011, "to the exclusion of planning for other viruses with pandemic potential," the UK COVID-19 Inquiry heard (2023a, 97). The leaked 2018 NSRA again identified a pandemic as among the top risks for the United Kingdom. Yet whilst the impact of "pandemic influenza" was rated at the highest possible level (i.e., 5/5), newly identified infectious diseases were considered of a lower risk (3/5). A flu-like pandemic was expected. A key issue with this line of reasoning is the disease patterns: influenza has shorter contagiousness windows, less asymptomatic transmission, and crucially, adaptable antiviral treatments already existed—in contrast to SARS-CoV-2. So, although some warnings proved accurate, overreliance on influenza models produced an ill-suited preparedness strategy and lead to a significant failure in this analytical dimension.

Process-wise, the inquiry found "deep flaws in decision-making," with lacking "joined-up thinking" between scientists and politicians which caused critical delays and inefficiencies in the warning process (BBC News 2023a). The preliminary 2021 inquiry had also concluded the crisis "exposed some major deficiencies in the machinery of Government" (House of Commons 2021, 6). Scientific advice was not given in a transparent or structured way and there were no protocols to share information, meaning warnings easily got lost. A culture of groupthink and complacency, additionally, created a faulty consensus that a managed spread of the virus across the United Kingdom (rather than a full containment strategy as some Asian countries had attempted) could create a herd immunity, and that this would be a better approach. Inter-agency information sharing was critically flawed. Strategic decisions were undermined by insufficient data, stemming from the ineffective circulation and utilization of core information across government bodies (House of Commons 2021, 22–3)—which had explicitly been one of the lessons of the *Cygnus* exercise (Public Health England 2017, 31). The COVID-19 inquiry was also told that there

Table 2. UK warning performance COVID-19 pandemic

Dimension	Status	
Analytical	Significant failure	Inability to accurately predict the trajectory of COVID-19, some threat awareness but overreliance on influenza models producing inadequate warnings
Process	Complete failure	Systemic failures in the decision-making process, marred by groupthink on a managed spread strategy, a lack of structured advice, inadequate inter-agency information sharing, producing critical delays and inefficiencies
Political	Significant failure	Underestimation of the pandemic severity fed by desire to protect the economy, a reluctance to implement early and decisive policy action. Despite eventually acknowledging the threat, there was a culture of ignoring scientific advice and a misalignment between short-term political goals and health objectives
Key trade-offs:	Analytical recognition of pandemic risks exacerbated by lacking political preparedness to act. Process dimension of poor decision-making structures and information sharing were compounded by political nonreceptivity	

was a “toxic culture in Downing Street and the Cabinet Office at the time,” with female experts being ignored (2023b).

The political dimension was equally strained. The severity and impact of the COVID-19 pandemic in the United Kingdom were underestimated and vulnerable groups were inadequately protected. Scientific advice was delayed due to political worries about how the wider public would perceive measures such as mask-wearing or lockdowns, producing reactive, short-term policy measures. The detrimental effects a lockdown could have on the economy were frequently prioritized over the health impact COVID could have if left unchecked, with the then chief scientific officer, Patrick Vallance, noting Prime Minister Boris Johnson had said of COVID they should “let it rip” (UK COVID-19 Inquiry 2023d). Government assumptions driven by political motives, such as the ability to suppress the virus through herd immunity, did not face sufficient challenge. A civil servant lamented in 2020 that Johnson “changed strategic direction every day [. . .] cannot lead and we cannot support him in leading with this approach. [. . .] The team captain cannot change the call on the big plays every day” (UK COVID-19 Inquiry 2023c). Even though eventually, the threat of COVID-19 did prompt policy action, faulty herd immunity assumptions, an underestimation of the virus, delayed responses, the prioritization of economic interests over public health, and inconsistent leadership produced a significant failure in the political dimension.

This case, summarized in Table 2, also demonstrates trade-offs and friction between the analytical dimension and the political dimension. The Inquiry concludes that the pandemic preparedness in the long term was “constantly prone to being sacrificed to the short-term demands that predominate in government” (House of Commons 2021). Political goals—minimizing impact on society with an overemphasis on economic concerns—were clearly misaligned with health goals aimed at minimizing infection rates. In addition, systemic decision-making issues within the United Kingdom were compounded by the political dimension in which there was a strong reluctance to acknowledge the severity of the pandemic.

Russian Election Interference in the United States

In 2016, Russia undermined Hilary Clinton's presidential election bid in favor of Donald Trump. Hackers from "Cozy Bear" and later "Fancy Bear," cyber espionage groups associated with the Russian intelligence agencies, targeted the networks of the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee, and Clinton campaign officials. Most notably, they had compromised the DNC system in the summer of 2015, and in March 2016 they compromised the email account of John Podesta, Chairman of Clinton's presidential campaign, gaining access to amongst others his emails as well as hundreds of confidential documents, after which the content was disclosed on websites such as Wikileaks. (National Security Agency 2017; The Washington Post 2017). In parallel, Russia ran an extensive disinformation campaign, stoking divisions and spreading fake news supporting amongst others Trump's claims about rigged electoral systems, untrustworthy mainstream media, and biased institutions (Senate Select Committee on Intelligence 2019a). The NSA later concluded with "high confidence" that the Kremlin ordered this campaign "to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency" (Office of the Director of National Intelligence 2017b, ii).

Analytically, US intelligence agencies achieved success. In 2014, the Joint Sigint Cyber Unit of the Netherlands intelligence services had penetrated the Cozy Bear network, gaining unique access to their computer network as well as a corridor security camera. They informed the National Security Agency (NSA) in 2015, who passed the threat onto the Federal Bureau of Investigation (FBI) in the summer of 2015.

US intelligence agencies were thus aware of Russian intrusions into the DNC systems by Cozy Bear as early as 2015 and had correctly attributed these campaigns (The Washington Post 2017; Senate Select Committee on Intelligence 2019b, 2019c). "We're aware that campaigns [and] individuals are targeted," stated the director of public affairs of the US Director of National Intelligence, "by actors with a variety of motivations [. . .] and capabilities—from defacements to intrusions" (The Washington Post 2017).

Yet despite these early warnings and a history of similar attacks (McCombie et al. 2019) it took over a year for these warnings to reach the DNC or senior White House leadership, due to a flawed process following the threat identification (The Washington Post 2017; Sanger 2018). The process dimension displays a picture of ineffective communication, bureaucratic delays, and misjudgment and inaction. After the NSA passed on the warning, in the summer of 2015 it landed on FBI agent Adrian Hawkins' desk, who was busy and could not follow-up immediately. In September, he called the DNC switchboard, hoping to brief a DNC cybersecurity team. Since no such team existed, the DNC operator transferred Hawkins to a general help desk, without further follow-up. In a later phone call, the FBI agent was able to tell a DNC employee the DNC was being hacked by a group affiliated with Russia. This employee wrote a brief but nonalarming memo, primarily because they doubted whether Hawkins was actually an FBI agent. When a second, much stronger warning came from the FBI that one of the DNC computers was sending back information to Russia, this warning was again not passed on to the DNC's top leadership (Sanger 2018). It took numerous calls from the FBI to the DNC before the DNC fully cooperated with the FBI nine months later, in June 2016 (McCombie et al. 2019). But by this time, the damage was already done. In July 2016, days before the DNC Convention, 20.000 emails were published by Wikileaks (Sanger 2018; Uhlmann and McCombie 2020).

The political dimension was strongly impacted by the flawed process preceding this stage. In August, the Central Intelligence Agency (CIA) finally briefed the White House that Putin had ordered an operation to "defeat or at least damage

Table 3. US warning performance 2016 election interference

Dimension	Status	
Analytical	Full success	US intelligence community was aware of Russian intrusions into the DNC systems early and had correctly attributed the campaigns
Process	Significant failure	Ineffective communication and significant bureaucratic delays between the discovery of the threat and the warning communication undermined early threat awareness. Critical warnings did reach DNC and Whitehouse, but not in a timely and effective manner.
Political	Moderate success/failure	A degree of success in terms of the Obama Administration's receptivity to warnings issued, yet limited comprehensive understanding due to bifurcated approach to the threat. Heavily delayed by flawed process dimension.
Key trade-off:	Between analytical accuracy and bureaucratic caution in disseminating this information to relevant parties and the public.	

Hilary Clinton and help elect her opponent, Donald Trump" (The Washington Post 2017). But by this time the United States had already been subject to the "boldest influence effort yet" in the United States (Office of the Director of National Intelligence 2017a). The Senate Select Committee later identified that the Obama administration was receptive to the warnings, as "senior administration officials told the Committee that they assessed that their warnings to Russia before the election had the desired effect" (Senate Select Committee on Intelligence 2019b, 3). The administration was, however, "frozen by 'paralysis of analysis," hamstrung by constraints both real and perceived, Obama officials debated courses of action without truly taking one' (Senate Select Committee on Intelligence 2020). The environment in which warnings were received was highly politicized, concludes the Committee. In addition, the political agenda at the time was to treat the cyber and geopolitical aspects of the Russian campaign as separate issues. "This bifurcated approach," according to the Committee, "may have prevented the Administration from understanding the full extent of the threat Russia posed" and limited its ability to respond.

Table 3 summarizes the warning performance in this case. For months, the FBI and the DNC had exchanged phone calls, with the FBI sending at least two warnings, but without any follow-up (Sanger 2018). A key-trade off emerged between analytical success and process failure: the intelligence community's desire to keep evidence of the cyberattacks classified, Sanger argues (2018), meant that none of the intelligence agencies dared to make a public call about the analytical findings concerning Russian infiltrations in the election campaigns. Therefore, in July 2016, the Director of National Intelligence James Clapper publicly continued to claim the intelligence community (IC) was uncertain about "who is behind the attacks and why" (The Washington Post 2017).

EU Warning prior to the 2014 Crimea Annexation

Since early on in his tenure as Russian president, Vladimir Putin saw the world order as one of a "competitive struggle," in which his aim was to reduce Western influence in Russia and in what he considers Russia's "near abroad" (European Parliament 2013). Over time, this discourse grew increasingly hostile and nationalist. One of the foreign policy pillars following his second election was the Eurasian Economic Union as a counter-project to the EU. Ukraine's participation in this high-profile initiative of the Eurasian Economic Union was considered imperative to its success and, as a consequence, seen as incompatible with Ukraine's closer integration with the EU (Cadier 2015). Ukraine's signing of an Association Agreement with the EU in November 2013 was deemed particularly discordant with Russian ambitions (House of Lords 2015). To dissuade Ukraine, Russia imposed trade restrictions against Ukraine over the summer 2013, geared at exploiting Ukraine's already dismal economic state (Financial Times 2013). This made Ukrainian President Viktor Yanukovych decide to forego signing the agreement with the EU, prompting protests across Ukraine (Ikani 2019). As the protests escalated into a political conflict with increasing numbers of victims, Yanukovych fled Ukraine in late February 2014. Losing a befriended regime and the prospect of another "color revolution" in the post-Soviet countries may have prompted the Kremlin to consider the extreme option of annexing the Crimea, which eventually transpired in March 2014, to the surprise of the EU and its allies (Meyer and Ikani 2022).

The analytical dimension of the EU's warning process faced significant challenges. Importantly, the event marked a substantial shift from the norms established in the status quo. Many observers contended Russia would definitely not resort to this option (Trenin 2014), whilst a mere 14 percent of the 905 worldwide IR scholars polled on the eve of the intervention considered an annexation likely (Foreign Policy 2014). The EU additionally, and unlike state actors, lacks the intelligence structures that can provide all-source intelligence, meaning it was relying on what little intelligence it was fed by European member states. This made accurate warning difficult. Yet despite these many challenges to timely and accurate analysis, we have learned that warnings were issued. A Ukraine expert working for the EU's Intelligence Analysis Centre (INTCEN, the EU's general intelligence function) drafted a report warning that Yanukovych might not sign the Association Agreement with the EU, which could lead to protests and instability (Higgins 2014). Additionally, in October 2013 the EU Delegation in Moscow had warned that the Crimea might be "used" as a Russian response should Ukraine sign the Association Agreement. The EU Consulate in Sevastopol had issued further warnings about troop movements in Crimea which would suggest Russia had specific plans in the area (Meyer et al. 2020, 247). These warnings thus highlight partial successes in this analytical dimension, even if the annexation was a surprise to the EU, as it was to the United States, the United Kingdom, and France.

In the process dimension, we see that these analytical findings were communicated and considered within the EU decision-making structures. Notably, explicit warnings about the observed troop movements were issued in January and February 2014—so with very short notice—by the EU consulate in Crimea (Meyer et al. 2020, 244). At the same time, the US intelligence community warned publicly that the Crimea could be a "flashpoint for Russian–Ukraine military conflict" (NBC News 2014). At a strategic level, unambiguous warnings were conveyed in the Foreign Affairs Council—the highest forum for EU foreign policy decisions. These warnings were issued by the foreign ministers of Poland and Sweden at the time, Radoslaw Sikorski and Carl Bildt (Meyer and Ikani 2022). Sikorski stressed in an interview that he had been repeatedly warning about the risks from Russia, for a period of months. "If you look at the resumes of European Councils from 2013, you will find that Carl Bildt and I were literally begging [. . .] warning colleagues that if we leave the Ukrainians alone on this one, the Russians will go further." (quoted in Meyer et al. 2020). Accurate though relatively late warnings were thus issued and directed to appropriate decision-making fora—indicating a near success in the process dimension.

It is the political dimension where failure is most obvious, as receptivity to the warnings was compromised by preconceptions and bias. Both Bildt and Sikorski

Table 4. EU warning performance 2014 Crimea annexation

Dimension	Status	
Analytical	Moderate Success/failure	Despite diagnostic challenges, EU INTCEN and other sources issued warnings, though limited by intelligence capabilities.
Process	Near success	Warnings were communicated within EU structures and considered in key decision-making forums.
Political	Significant failure	Warnings did reach the right fora and triggered a level of discussion and awareness, but the dismissal of warnings as “hawkish” paranoia, bias due to “cry-wolf syndrome,” and the influence of economic interests contributed to a significant underestimation of the threat and a lack of appropriate action
Key trade-off:	Political nonreceptivity to the threat undermined analytical success	

were seen in European circles as “Russia hawks.” Other EU officials dismissed their warnings, assuming they were overly paranoid, politically motivated, or had critical strategic interests involved (Meyer et al. 2020). Repeated warnings about dramatic events that turn out as false alarms are known to create a warning fatigue—what is referred to as “cry-wolf syndrome” (Wirtz 2008) which significantly decreases the political receptivity to the warnings. “The Western Europeans pooh-poohed and patronized us for these last 30 years,” Sikorski told Politico. “For years [they] were patronizing us about our attitude: ‘Oh, you know, you over-nervous, over-sensitive Central Europeans are prejudiced against Russia’” (Politico 2022). There was a pervasive sense of disbelief across the Union that Russia would try to take Crimea by force—virtually until after the fact (House of Lords 2015; Ikani and Meyer 2023). Even after the Crimea annexation, there was political disagreement regarding how to deal with Russia (European Council 2014). In 2013 and 2014, many European countries had strong ties to Russia, particularly its energy sector. Italy, Germany, Greece, and Cyprus for this reason long resisted the warnings about Russian intentions in Ukraine (European Parliament 2013).

The warning performance warning preceding the Crimea annexation is shown in Table 4. It was characterized by numerous raised alarms about possible Russian interventions in the aftermath of the Euromaidan. From multiple sources within the EU apparatus, including the EU consulate in Sevastopol, the Crimea was mentioned as the locus of potential repercussions. The most explicit warnings came from the foreign ministers of Sweden and Poland. The political nonreceptivity to these warnings was caused by the tendency to dismiss warnings coming from “Russia hawks” as these were preliminarily labeled as biased and incorrect. “Cry-wolf syndrome” exacerbated this. Political and economic interests tied with the Russian energy sector compounded this nonreceptivity, meaning that despite the warnings and the unfolding events on the ground in Ukraine, widespread disbelief persisted that Russia would resort to taking Crimea by force.

A trade-off occurred between the analytical dimension and the political one. Despite partial analytical success in recognizing the potential pattern of events, existing biases against “Russia hawks” as well as vested political interests in a stable relationship with Russia produced a lack of political receptivity to the threat.

Conclusion

History is punctuated by instances of strategic surprise. Yet despite the frequent occurrence of strategic surprises and the widely recognized need for accurate warning systems, the extant literature lacked an adequate definition of what exactly constitutes warning success or warning failure. This ambiguity has produced an overemphasis on binary classifications, questioning whether specific events—the fall of Kabul and the October 7 Hamas attack on Israel—can be labeled as warning failures. "Failure," as such, often becomes a monolithic attribute attached to events. This article argued this oversimplifies not just the complex nature of the warning process—and the many ways in which it can fall short—but also ignores the gradations in warning effectiveness that exist between full success and complete failure. It was contended that instead, we should shift our focus towards explaining warning performance, examining where and how the warning process did not achieve the desired outcomes.

To this aim, this paper introduced a multidimensional typology that allows for an evaluation of warning effectiveness on a spectrum ranging from full success to complete failure, considering the analytical, procedural, and political factors that shape the warning process. By disaggregating the various dimensions of the warning process, this typology provides a more granular understanding of warning effectiveness and how different factors contribute to or impede effective warning. This challenges the tendency within intelligence studies to approach warning success and failure in binary terms and aligns it with efforts within the fields of political science, public administration, and IR to move beyond such oppositional success–failure dichotomies when assessing instances of (foreign) policy success. By reconceptualizing how warning effectiveness and intelligence effectiveness are measured, this paper contributes to ongoing debates around the role of warning and intelligence in decision-making processes, and crisis prevention.

By breaking down the warning process into the analytical, process, and political dimensions, this paper furthermore allows for a better understanding of the factors that shape warning effectiveness. It also advances discussions on how these various dimensions interact and affect one another. It underlines that inherent trade-offs between the different dimensions exist, where success in one dimension might not compensate for failures in another—a core insight in both academic and practical terms, prompting us to also consider the limitations of warning systems. The typology's application to diverse case studies across security domains illustrates its utility for understanding of the complexities of strategic surprise, and the reasons they occur despite prior warnings. It also adds to the existing scholarship of predominantly single-case studies of warning failures, as this paper underscores how warning processes rarely constitute clear-cut successes or failures but rather exhibit varying degrees of effectiveness across the dimensions.

The "diagnostic tool" for evaluating warning effectiveness that this typology presents provides a more accurate diagnosis of past failures and serves as a lens through which future warning performance can be evaluated and enhanced. This can inform policy efforts aimed at strengthening warning systems, and allow for more targeted, adaptive, and effective security policy responses. For instance, the case studies underscore the critical nature of effective communication channels both within and between various institutions involved in the warning process. This may draw more attention to the effectiveness and impact of communication tools and channels, including Red Teaming, analytical Ombudsman roles, fusion centers, or Devil's Advocate positions. In terms of further policy implications, the typology and the case studies also suggest that warning systems need to be flexible and adaptable enough to deal with varied threat types—strategic surprises are no longer bound to the geopolitical realm. Ensuring that warning systems can adapt and upgrade their priorities, resources, methodologies, and focus as needed will make these systems more resilient.

Future research may include larger-n case studies in order to further explore the value of this approach across a wider spectrum of historical and contemporary cases. By analyzing patterns, similarities, and differences in warning processes across a larger number of cases, it will be possible to further identify how the analytical, process, and political dimensions identified in this paper interact and shape outcomes, to further refine and validate the typology proposed and to explore the various paths to warning success and warning failure across the dimensions. Whilst the case studies in this paper also drew on diverse entities—the United States, the United Kingdom, and EU—future research can further investigate how varying institutional structures and cultures impact performance across each warning dimension, with the aim of informing policy efforts to optimize warning processes. Finally, applying the typology to cases from different threat types—e.g., terrorism, economic threats, and climate change—could reveal domain-specific challenges to successful warning.

Funding

This publication is part of the WARN project (with project number VI.Veni.221R.093 of the research programme Veni which is (partly) financed by the Dutch Research Council (NWO).

References

Ackermann, Alice. 2003. “The Idea and Practice of Conflict Prevention.” *Journal of Peace Research* 40 (3): 339–47.

Adelman, Howard, and Astri Suhrke. 1996. “Early Warning and Response: Why the International Community Failed to Prevent the Genocide.” *Disasters* 20 (4): 295–304.

Allison, Graham T., and Morton H Halperin. 1972. “Bureaucratic Politics: A Paradigm and Some Policy Implications.” *World Politics* 24 (Supplement S1): 40–79.

Atkins, Sean, and Chappell Lawson. 2021. “An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure.” *Public Administration Review* 81 (5): 847–61.

Baldwin, David A. 2000. “Success and Failure in Foreign Policy.” *Annual Review of Political Science* 3 (1): 167–82.

Bar-Joseph, Uri. 2005. *The Watchman Fell Asleep: The Surprise of Yom Kippur and Its Sources*, New York: SUNY Press.

Bar-Joseph, Uri, and Rose McDermott. 2017. *Intelligence Success and Failure: The Human Factor*, in edited by, Rose McDermott and Uri Bar-Joseph. Oxford: Oxford University Press.

BBC News. 2023a. “How Inquiry Is Exposing Deep Flaws in Covid Decision-Making.” Last modified November 26, 2023. Accessed December 12, 2023, Form of Item. https://www.bbc.co.uk/news/health-67514356.

———. 2023b. “I Should Have Twigged Covid Threat Earlier, Admits Boris Johnson.” Accessed December 12, 2023, Form of Item. https://bbc.com/news/uk-politics-67639813.

Ben-Zvi, Abraham. 1976. “Hindsight and Foresight: A Conceptual Framework for the Analysis of Surprise Attacks.” *World Politics* 28 (3): 381–95.

———. 1990. “Between Warning and Response: The Case of the Yom Kippur War.” *International Journal of Intelligence and CounterIntelligence* 4 (2): 227–42.

Betts, Richard K. 1978. “Analysis, War, and Decision: Why Intelligence Failures Are Inevitable.” *World Politics* 31 (1): 61–89. Accessed December 20, 2016.

———. 1981. “Surprise Attack: Nato’s Political Vulnerability.” *International Security* 5 (4): 117–49. https://doi.org/10.2307/2538716.

———. 1982. *Surprise Attack: Lessons for Defense Planning*. Washington, DC: Brookings Institution.

———. 2010. “Intelligence for Policymaking.” *The Washington Quarterly* 3 (3): 118–29.

Boin, Arjen, Allan McConnell, and Paul. t Harteds. 2008. *Governing after Crises: The Politics of Investigation, Accountability and Learning*. Cambridge: Cambridge University Press.

Bowen, Glenn A. 2009. "Document Analysis as a Qualitative Research Method." *Qualitative Research Journal* 9 (2): 27–40.

Brändström, Annika, and Sanneke Kuipers. 2003. "From 'Normal Incidents' to Political Crises: Understanding the Selective Politicization of Policy Failures." *Government and Opposition* 38 (3): 279–305.

Byman, Daniel. 2005. "Strategic Surprise and the September 11 Attacks." *Annual Review of Political Science* 8 (1): 145–70.

Cadier, David. 2015. "Policies Towards the Post-Soviet Space: The Eurasian Economic Union as an Attempt to Develop Russia's Structural Power?" In *Russia's Foreign Policy: Ideas, Domestic Politics and External Relations*, edited by David Cadier and Margot Light, 156–74. London: Palgrave Macmillan UK.

Central Intelligence Agency. 1978. "Indications and Warning, Declassified." Accessed February 20, 2024, Form of Item. https://www.cia.gov/readingroom/docs/CIA-RDP80M00596A000300030003-8.pdf.

Chan, Steve. 1979. "The Intelligence of Stupidity: Understanding Failures in Strategic Warning." *The American Political Science Review* 73 (1): 171–80. Accessed October 3, 2023. https://dx.doi.org/10.2307/1954739.

Chertoff, Michael, Patrick Bury, and Kjetil Hatlebrekke. 2020. "National Intelligence and the Coronavirus Pandemic." Last modified March 31, 2020. Accessed October 5, 2023, Form of Item. https://rusi.org/explore-our-research/publications/commentary/national-intelligence-and-coronavirus-pandemic.

Cohen, Eliot A., and John Gooch. 1990. *Military Misfortunes : The Anatomy of Failure in War.* New York: Free Press, Collier Macmillan.

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

———. 2013b. "Why Won't They Listen? Comparing Receptivity toward Intelligence at Pearl Harbor and Midway." *Intelligence and National Security* 28 (1): 68–90.

———. 2018. "Not Your Father's Intelligence Failure: Why the Intelligence Community Failed to Anticipate the Rise of Isis." In *The Future of ISIS. Regional and International Implications*, edited by Feisal al-Istrabadi and Sumit Ganguly, 41–66. Washington, DC: Brookings Institution Press.

———. 2020. "Warnings Unheeded, Again: What the Intelligence Lessons of 9/11 Tell Us about the Coronavirus Today." *Homeland Security Affairs* 16 (7): 1–12.

———. 2023. *The COVID-19 Intelligence Failure: Why Warning Was Not Enough.* Washington, DC: Georgetown University Press.

Dahl, Robert A. 1976. *Modern Political Analysis.* 3 ed. Englewood Cliffs, NJ: Prentice-Hall.

Davies, Philip H. J. 2012. *Intelligence and Government in Britain and the United States : A Comparative Perspective*, Vol. 2. Praeger Security International. Santa Barbara, CA: Praeger.

Davis, Jack. 2003. "Strategic Warning: If Surprise Is Inevitable, What Role for Analysis?" *Kent Center Occasional Papers, Central Intelligence Agency* 2 (1): 1–17.

———. 2006. "Strategic Warning." In *Handbook of Intelligence Studies.* Johnson Loch, Chapter 13, London: Routledge.

European Council. 2014. "Council Conclusions 20/21 March 2014." Accessed May 10, 2016. https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/141749.pdf.

European Parliament. 2013. "Key Aspects of Russia's Current Foreign and Security Policy." Accessed June 6, 2024, Form of Item. https://www.europarl.europa.eu/RegData/etudes/briefing_note/join/2012/491446/EXPO-AFET_SP(2012)491446_EN.pdf.

European Union. 2022. "A Strategic Compass for Security and Defence." Accessed October 31, 2023, Form of Item. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

Financial Times. 2013. "Russia Accused of Triggering Trade War with Ukraine." Access date 12 February 2024. http://www.ft.com/cms/s/0/99068c0e-0595-11e3-8ed5-00144feab7de.html#axzz3Sg7IJrO7.

Fisher, Matthew, and Frank C. Keil. 2018. "The Binary Bias: A Systematic Distortion in the Integration of Information." *Psychological Science* 29 (11): 1846–58.

Fitzgerald, Michael, and Richard Ned Lebow. 2006. "Iraq: The Mother of All Intelligence Failures." *Intelligence and National Security* 21 (5): 884–909.

Foreign Policy, Centre. 2014. "Snap Poll: The View from the Ivory Tower." Last modified March 7, 2014. Accessed October 26, 2023, Form of Item. https://foreignpolicy.com/2014/03/07/snap-poll-the-view-from-the-ivory-tower/.

Gentry, John A. 2008. "Intelligence Failure Retrained." *Political Science Quarterly* 123 (2): 247–70.

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

George, Alexander L., and Jane E. Holl 1997. "The Warning–Response Problem and Missed Opportunities in Preventive Diplomacy." *A Report to the Carnegie Commission on Preventing Deadly Conflict.* New

York: Carnegie Corporation of New York.

Grabo, Cynthia M. 2002. *Anticipating Surprise: Analysis for Strategic Warning*, e dited by Jan Goldman. Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College.

Gray, Colin S. 2005. “"Transformation and Strategic Surprise." Strategic Studies Institute.” *US Army War College*

Handel, Michael I. 1977. “The Yom Kippur War and the Inevitability of Surprise.” *International Studies Quarterly* 21 (3): 461–502. https://doi.org/10.2307/2600234.

———. 1980. “Surprise and Change in International Politics.” *International Security* 4 (4): 57–85.

———. 1984. “Intelligence and the Problem of Strategic Surprise.” *Journal of Strategic Studies* 7 (3): 229–81.

Harris, Shane, Karen DeYoung, Isabelle Khurshudyan, Ashley Parker, and Liz Sly. 2022. “Road to War: U.S. Struggled to Convince Allies, and Zelensky, of Risk of Invasion.” *The Washington Post*, August 16. Access date 14 February 2024. https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war.

Hedley, John Hollister. 2005. “Learning from Intelligence Failures.” *International Journal of Intelligence and CounterIntelligence* 18 (3): 435–50.

Herrmann, Richard K., and Jong Kun Choi. 2007. “From Prediction to Learning: Opening Experts’ Minds to Unfolding History.” *International Security* 31 (4): 132–61.

Higgins, Andrew. 2014. “Ukraine Upheaval Highlights E.U.’S Past Miscalculations and Future Dangers (Published 2014).” Last modified March 20, 2014. Accessed October 26, 2023, Form of Item. https://www.nytimes.com/2014/03/21/world/europe/ukrainian-tumult-highlights-european-unions-errors.html.

House of, Commons, 2021. Health and Social Care, and Science and Technology Committees. *Health and Social Care, and Science and Technology Committees*: Coronavirus: Lessons Learned to Date.

House of Lords, 2015. *The EU and Russia: Before and beyond the Crisis in Ukraine*. London: House of Lords, European Union Committee.

Ikani, Nikki. 2019. “Change and Continuity in the European Neighbourhood Policy: The Ukraine Crisis as a Critical Juncture.” *Geopolitics* 24 (1): 20–50.

Ikani, Nikki, and Christoph O. Meyer 2023. “The Underlying Causes of Strategic Surprise in Eu Foreign Policy: A Post-Mortem Investigation of the Arab Uprisings and the Ukraine–Russia Crisis of 2013/14.” *European Security* 32 (2): 270–93.

Ikani, Nikki, Aviva Guttmann, and Christoph O. Meyer 2020. “An Analytical Framework for Postmortems of European Foreign Policy: Should Decision-Makers Have Been Surprised?.” *Intelligence and National Security* 35 (2): 197–215. https://doi.org/10.1080/02684527.2019.1704384.

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

Jervis, Robert. 2010a. “Response to James Lebovic’s Review of Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War.” *Perspectives on Politics* 8 (4): 1169–70.

———. 2010b. *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. Ithaca, NY: Cornell University Press.

———. 2022. “Why Postmortems Fail.” *Proceedings of the National Academy of Sciences* 119 (3): https://doi.org/10.1073/pnas.2116638118.

Johnson, Dominic D.P., and Dominic Tierney. 2006. *Failing to Win: Perceptions of Victory and Defeat in International Politics*. Cambridge: Harvard University Press.

Johnson, Loch K. 2009. “Sketches for a Theory of Strategic Intelligence.” In *Intelligence Theory: Key Questions and Debates*, edited by Peter Gill, Stephen Marrin and Mark Phythian, *Studies in Intelligence Series*, 33–53. London: Routledge.

Kam, Ephraim. 2004. *Surprise Attack: the Victim’s Perspective*. Cambridge, MA: Harvard University Press.

Kent, Sherman. 1966. *Strategic Intelligence for American World Policy*. Princeton: Princeton University Press.

Levite, Ariel. 1989. “Intelligence and Strategic Surprises Revisited: A Response to Richard K. Betts’s ’Surprise, Scholasticism, and Strategy’.” *International Studies Quarterly* 33 (3). 345–349

Levy, Marion J. 1970. “ James N. Rosenau Klaus Eugen Knorr Does It Matter If He’s Naked?” Bawled the Child.” In *Contending Approaches to International Politics*, 87–109, Princeton: Princeton University Press.

Lowenthal, Mark M. 2012. *Intelligence: From Secrets to Policy*. 5th ed. Los Angeles: SAGE/CQ Press.

Mahoney, James. 2015. “Process Tracing and Historical Explanation.” *Security Studies 24* 24 (2): 200–18.

Mandel, David R. 2015. “Accuracy of Intelligence Forecasts from the Intelligence Consumer’s Perspective.” *Policy Insights from the Behavioral and Brain Sciences* 2 (1): 111–20.

Marrin, Stephen. 2004. “Preventing Intelligence Failures by Learning from the Past.” *International Journal of Intelligence and CounterIntelligence* 17 (4): 655–72.

———. 2012. “Evaluating the Quality of Intelligence Analysis: By What (Mis) Measure?” *Intelligence and National Security* 27 (6): 896–912.

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

McCombie, Stephen, Allon J. Uhlmann, and James D. Ramsay. 2019. “The US 2016 presidential election & Russia’s troll farms.” *Intelligence and National Security* 35 (1): 95–114.

McConnell, Allan. 2010. “Policy Success, Policy Failure and Grey Areas In-Between.” *Journal of Public Policy* 30 (3): 345–62.

———. 2015. “What Is Policy Failure? A Primer to Help Navigate the Maze.” *Public Policy and Administration* 30 (3-4): 221–42.

Meyer, Christoph O., and Nikki Ikani. 2022. “The Ukraine-Russia Undeclared War 2013/2014: Lessons for the Eu’s Estimative Intelligence.” In *Estimative Intelligence in European Foreign Policymaking*, edited by Christoph O. Meyer, Eva Michaels, Nikki Ikani, Aviva Guttman and Michael S. Goodman. Edinburgh: Edinburgh University Press.

Meyer, Christoph O., Chiara De Franco, and Florian Otto. 2020. *Warning about War: Conflict, Persuasion and Foreign Policy.* Cambridge: Cambridge University Press.

Morse, Stephen S., Jonna A. K. Mazet, Mark Woolhouse, Colin R. Parrish, Dennis Carroll, William B. Karesh, Carlos Zambrana-Torrelio, W. Ian Lipkin, and Peter Daszak. 2012. “Prediction and Prevention of the Next Pandemic Zoonosis.” *The Lancet* 380 (9857): 1956–65.

National Security Agency. 2017. “Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors Target US Comapnies and US Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 Ts//Si//Oc//Rel to USA, Fvey/Fisa.” Accessed October 12, 2023, Form of Item. https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.

NATO. 2022. “Nato 2022 Strategic Concept. Adopted by Heads of State and Government at the Nato Summit in Madrid 29 June 2022.” Accessed October 31, 2023, Form of Item. https://www.nato.int/cps/en/natohq/topics_210907.htm.

NBC News. 2014. “U.S. Spy Agencies Deny Failure on Crimea Seizure.” Last modified March 6, 2014. Accessed October 26, 2023, Form of Item. https://www.nbcnews.com/storyline/ukraine-crisis/u-s-spy-agencies-deny-failure-crimea-seizure-n45581.

Nikolai, Lea A., Christian G. Meyer, Peter G. Kremsner, and Thirumalaisamy P. Velavan. 2020. “Asymptomatic Sars Coronavirus 2 Infection: Invisible yet Invincible.” *International Journal of Infectious Diseases* 100 (2020/11/01/): 112–6.

Nye, Joseph S. 1994. “Peering into the Future.” *Foreign Affairs* 73 (4): 82–93.

Office of the Director of National Intelligence. 2017a. “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution.” Last modified January 6, 2017. Accessed October 5, 2023, Form of Item. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

———. 2017b. “Intelligence Community Assessment: Background to ‘Assessing Russian Activities and Intentionsin Recent Us Elections’: The Analytic Process and Cyber Incident Attribution Ica 2017-01d.” *Form of Item* Access date 1 March 2024. https://www.scribd.com/document/335885580/Unclassified-version-of-intelligence-report-on-Russian-hacking-during-the-2016-election#fullscreen&from_embed.

Pape, Robert A. 1998. “Why Economic Sanctions Still Do Not Work.” *International Security* 23 (1): 66–77.

Parker, Charles F., and Eric K. Stern. 2002. “Blindsided? September 11 and the Origins of Strategic Surprise.” *Political Psychology* 23 (3): 601–30.

———. 2005. “Bolt from the Blue or Avoidable Failure? Revisiting September 11 and the Origins of Strategic Surprise.” *Foreign Policy Analysis* 1 (3): 301–31. Accessed May 24, 2019.

Phythian, Mark. 2006. “The Perfect Intelligence Failure? U.S. Pre-War Intelligence on Iraqi Weapons of Mass Destruction.” *Politics & Policy* 34 (2): 400–24.

Plante, Jessica A., Brooke M. Mitchell, Kenneth S. Plante, Kari Debbink, Scott C. Weaver, and Vineet D. Menachery. 2021. “The Variant Gambit: Covid-19’s Next Move.” *Cell Host & Microbe* 29 (4): 508–15.

Politico. 2022. "‘We Told You So!’ How the West Didn’t Listen to the Countries That Know Russia Best.” Last modified March 9, 2022. Accessed October 26, 2023, Form of Item. https://www.politico.eu/article/western-europe-listen-to-the-baltic-countries-that-know-russia-best-ukraine-poland/.

Public Health England. 2016. “Report: Exercise Alice Middle East Respiratory Syndrome Coronavirus (Mers-Cov) 15 February 2016.” Accessed October 5, 2023, Form of Item. https://covid19.public-inquiry.uk/wp-content/uploads/2023/06/26190532/INQ000090431_15-610-13.pdf

———. 2017. “Exercise Cygnus Report Tier One Command Post Exercise Pandemic Influenza 18-20

October 2016.” Accessed October 5, 2023, Form of Item. https://assets.publishing.service.gov.uk/media/5f8eb911d3bf7f49a1ce842c/exercise-cygnus-report.pdf.

Republique Francaise. 2023. “La Politique De Défense De La France : Les Enjeux À L’horizon 2030.” Last modified March 31, 2023. Accessed September 26, 2023, Form of Item. https://www.vie-publique.fr/dossier/270130-la-politique-de-defense-de-la-france-les-enjeux-lhorizon-2030.

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

Sanger, David E. 2018. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Penguin Random House.

Seawright, J., and J. Gerring. 2008. “Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options.” *Political Research Quarterly* 61 (2): 294–308. Accessed 2016/01/11/12:26:40. https://dx.doi.org/10.1177/1065912907313077.

Senate Select Committee on Intelligence. 2019a. “Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia’s Use of Social Media with Additional Views.” https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

———. 2019b. “Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 3: U.S. Government Response to Russian Activities.” Accessed October 31, 2023, Form of Item. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume3.pdf.

———. 2019c. “Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 4: Review of the Intelligence Community Assessment.” Accessed October 31, 2023, Form of Item. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

———. 2020. “Senate Intel Releases Bipartisan Report on Obama Admin Response to Russian Election Interference.” Last modified February 6, 2020. Accessed December 20, 2023, Form of Item. https://www.intelligence.senate.gov/press/senate-intel-releases-bipartisan-report-obama-admin-response-russian-election-interference.

Snyder, Richard C., H.W. Bruck, and Burton Sapin. 1962. *Foreign Policy Decision-Making. An Approach to the Study of International Politics*. New York: The Free Press of Glencoe.

Taleb, Nassim N., and Mark Blyth. 2011. “The Black Swan of Cairo How Suppressing Volatility Makes the World Less Predictable and More Dangerous.” *Foreign Affairs* 90 (3): 33–39.

The New York Times. 2021. “Intelligence Warned of Afghan Military Collapse, Despite Biden’s Assurances.” Last modified June 23, 2023. Accessed October 3, 2023, Form of Item. https://www.nytimes.com/2021/08/17/us/politics/afghanistan-biden-administration.html.

The Washington Post. 2017. “The Post’s New Findings in Russia’s Bold Campaign to Influence the U.S. Election.” Last modified July 11, 2017. Accessed October 12, 2023, Form of Item. https://www.washingtonpost.com/graphics/2017/world/national-security/russia-hacking-timeline/?utm_term=.5afb27cfe62c.

Trenin, Dmitri. 2014. “Why Russia Won’t Interfere.” *The New York Times*, February 23. Access date 1 March 2024. https://www.nytimes.com/2014/02/24/opinion/why-russia-wont-interfere.html.

Uhlmann, Allon J., and Stephen McCombie. 2020. “The Russian Gambit and the Us Intelligence Community: Russia’s Use of Kompromat and Implausible Deniability to Optimize Its 2016 Information Campaign against the Us Presidential Election.” *Library Trends* 68 (4): 679–96.

UK COVID-19 Inquiry. 2023a. “Transcript of Module 1 Public Hearing on 13 June 2023, Module 1.” Form of Item. https://covid19.public-inquiry.uk/documents/transcript-of-module-1-public-hearing-on-13-june-2023

———. 2023b. “Transcript of Module 2 Public Hearing on 1 November 2023.” Accessed December 12, 2023, Form of Item.

———. 2023c. “Transcript of Module 2 Public Hearing on 30 October 2023.” Accessed December 12, 2023, Form of Item.

———. 2023d. “Uk Covid-19 Inquiry: Extracts from Sir Patrick Vallance’s Notebooks.” Accessed December 12, 2023, Form of Item. https://covid19.public-inquiry.uk/wp-content/uploads/2023/12/07172506/INQ000273901_0092-0150-0230-0245-0439-0478-0608.pdf.

UK Ministry of Defence. 2023. “Joint Doctrine Publication 2-00 Intelligence, Counter-Intelligence and Security Support to Joint Operations.” Accessed February 22, 2024, Form of Item. https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf.

US Department of Defense. 2020. “The Defense Warning Network.” Last modified August 10, 2020. Accessed September 26, 2023, Form of Item. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/311516e.pdf?ver=2020-08-10-145143-097.

Wilensky, Harold L. 1967. *Organizational Intelligence; Knowledge and Policy in Government and Industry*. New York,: Basic Books.

Wirtz, James J. 1991. *The Tet Offensive*. Ithaca, NY: Cornell University Press.

———. 2003. “Theory of Surprise.” In *Paradoxes of Strategic Intelligence : Essays in Honor of Michael I. Handel*, edited by Michael I. Handel, Richard K. Betts and Thomas G. Mahnken, 101–16. Portland: Frank Cass.

———. 2008. “The Intelligence Paradigm.” *Intelligence and National Security* 4 (4): 829–37.

———. 2023. “Are Intelligence Failures Still Inevitable?” *International Journal of Intelligence and CounterIntelligence* 37 (1): 1–24. https://doi.org/10.1080/08850607.2023.2214328.

Wirtz, James J., Jeffrey E. Kline, and James A. Russell. 2023. “Indications & Warning Intelligence for the Western Pacific.” In *The U.S. Navy and the Rise of Great Power Competition*, edited by James J. Wirtz, Jeffrey E. Kline and James A. Russell. London: Routledge.

Wohlstetter, R. 1962. *Pearl Harbor: Warning and Decision*. Redwood City: Stanford University Press.

Yin, Robert K. 2017. *Case Study Research and Applications*, 6th ed. New York: SAGE.

Zegart, Amy B. 1999. *Flawed by Design: The Evolution of the Cia, Jcs, and Nsc*. Stanford: Stanford University Press.

———. 2005. “September 11 and the Adaptation Failure of U.S. Intelligence Agencies.” *International Security* 29 (4): 78–111.

———. 2007. *Spying Blind : The Cia, the Fbi, and the Origins of 9/11*. Princeton, NJ: Princeton University Press. Table of contents onlyhttp://www.loc.gov/catdir/toc/ecip077/2006103325.html

Zenk, Lukas., Gerald. Steiner, Miguel. Pina e Cunha, Manfred D. Laubichler, Martin. Bertau, Martin J. Kainz, Carlo. Jäger, and Eva S. Schernhammer. 2020. “Fast Response to Superspreading: Uncertainty and Complexity in the Context of Covid-19.” *International Journal of Environmental Research and Public Health* 17: 21.

Ikani, Nikki. (2025) Beyond the Binary: A New Typology for Evaluating Warning Success and Failure in Strategic Surprise. *International Studies Review*, https://doi.org/10.1093/isr/viaf009