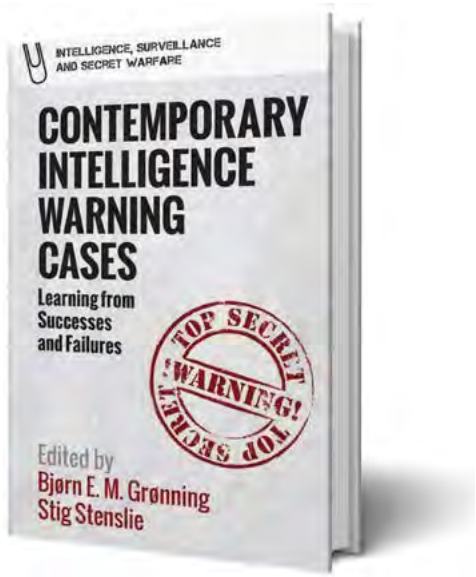
intelligence in public media

Contemporary Intelligence Warning Cases: Learning from Successes and Failures

Reviewed by Johnathan Proctor



Author:	*Bjørn E. M. Grønning and Stig Stenslie (eds.)*
Published By:	Edinburgh University Press, 2024
Print Pages	376, references and index
Reviewer:	Johnathan Proctor is a member of the J2's Defense Warning Staff.

Case studies have been a mainstay of intelligence education and research for decades, starting with and exemplified by Rebecca Wohlstetter's *Pearl Harbor: Warning and Decision*, published in 1962. However, in their 2017 series of case studies, *Intelligence Success and Failure: The Human Factor*, Rose McDermott and Uri Bar-Joseph pointed out what they perceived to be gaps in the literature of intelligence case studies. First, they argued these case studies, focusing primarily on failures, do not pay enough attention to successes. Second, they said that most studies focus on the US experience, specifically on Pearl Harbor and 9/11.[a] *Contemporary Intelligence Warning Cases* fills both of these gaps in the literature, while simultaneously providing a series of case studies recent enough to resonate with the current and next generations of intelligence professionals, many of whom served, or were at least alive, during the events explored.

Contemporary Intelligence Warning Cases is a compilation of 16 short studies written by a diverse group of scholars and edited by Bjørn Grønning and Stig Stenslie, the deputy research director and head of The Center for Intelligence Studies at the Norwegian Intelligence School, respectively.

While the full list of authors represents several nationalities, most are connected through King's College London—specifically the Department of War Studies or Center for the Study of Intelligence—or the Norwegian Intelligence School, where many authors are full-time or visiting faculty. Chapters written by three American

a. Rose McDermott and Uri Bar-Joseph, *Intelligence Success and Failure: The Human Factor* (Oxford University Press, 2027), 2–4.

All statements of fact, opinion,or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

authors provide the exceptions to this rule, including two biographies that cite US Intelligence Community experience within CIA: John Gentry and Soo Kim.

While the roster of authors slants more toward academic experience over current or former practitioners, each author is well established through career experience or publication history. The variety of intellectual backgrounds is a strength of the book, with authors focused on events well within their specific fields of expertise. For example, Aaron Brantley, who explores the 2015 Russian cyber attack on Ukraine's power grid, has published four books on cybersecurity, intelligence, decisionmaking, and cyber deterrence.

Contemporary Intelligence Warning Cases explores warning failures and successes, but it does not concur with the idea that only intelligence failures and policy successes exist. A central premise of the book, clearly articulated by the editors in the introductory chapter, is that warning is a "joint venture in the intelligence-policy nexus" with two elements: the intelligence services' responsibility to "detect, discern, and alert decisionmakers" and the "decisionmaker's preventative response" to the threat warning. (1–5) The idea of warning as persuasive communication is acknowledged by other authors from the King's College school,[a] but Bronning and Stenslie imply that there are limits to the responsibility of intelligence services to persuade, challenging the idea expressed in Henry Kissinger's reported statement, "You warned me, but you did not convince me."[b] They divide warning failures into two types: *Type A* failures are those in which an intelligence service does not detect and communicate a threat warning; *Type B* failures occur when policymakers do not act on the threat warnings.

In addition to Type A and Type B successes and failures, the authors include two other critical distinctions in their case studies. First, they look at both traditional and nontraditional warnings. Traditional cases focus, as expected, on military attacks, terrorism, and cyber-attacks. Nontraditional cases examine such events as the 2008 financial collapse, ISIS's destruction of world heritage sites in Palmyra in 2015, the COVID-19 pandemic, extreme flooding in Pakistan in 2022, and a national intervention in the sale of a private company to a Russia-connected firm in 2022.

Second, the authors distinguish between strategic and tactical failures, defining each primarily by time frame and the ability to act on warning. They characterize strategic warning as longer-term, broader, and often less actionable. Tactical warning, by contrast, is more specific, in timing and scope, and is thus generally more actionable. The authors cite Gordon and Gentry's *Strategic Warning Intelligence* and Erik Dahl's *Intelligence and Surprise Attack* in their definitions.[c] However, the picture of strategic and tactical warning emerging from the 16 individual case studies most closely aligns with the late CIA analyst Jack Davis' strategic and "incident" warning framework.[d]

The editors establish the overall framework and relevant definitions in the opening chapter, and the case studies that follow use them consistently. Each chapter provides background information and a narrative of the event, discusses the type of success or failure, and closes with a series of lessons and recommendations for intelligence practitioners. Four major themes emerge from the case studies:

- the importance of the intelligence-policy nexus and the relationship between the two elements;
- the critical role that bias and politicization play in both intelligence and policy circles;
- an emphasis on cooperation, both inter- and intra-governmental; and
- the importance of expressing warnings directly and clearly, often recommending dedicated warning products over the practice of embedding warnings in standard production.

While one of the book's core strengths is its exploration of a wide variety of cases, the inevitable

a. Christoph Meyer et al., *Warning About War: Conflict, Persuasion, and Foreign Policy* (Cambridge University Press, 2020), 6.
b. Roger George and James Bruce, *Analyzing Intelligence: National Security Practitioners' Perspectives*, 2nd ed. (Georgetown University Press, 2014), 366, accessed March 20, 2023. ProQuest Ebook Central.
c. John Gentry and Joseph Gordon, *Strategic Warning Intelligence* (Georgetown University Press, 2019), 11–17; Erik Dahl, *Intelligence and Surprise Attack: Failure and Success From Pearl Harbor to 9/11 and Beyond* (Georgetown University Press, 2013), 2–4.
d. Jack Davis, *Improving CIA Analytic Performance: Strategic Warning* (CIA, Sherman Kent Center for Analysis, 2002), 2–4.

trade-off is that no chapter goes into significant detail on any one, particularly when they are compared to case studies from World War II, the Korean War, the first Yom Kippur War, or 9/11. The average chapter runs approximately 14 pages, with an additional two to three pages of citations and endnotes. Another strength is each event's contemporary nature. However, the resulting trade-off in this event is a lack of detailed information on intelligence collection and production, much of which has yet to be declassified and made public. Several authors acknowledge their reliance on publicly available information and its effect on their chapters.

Chapters are standardized with lessons and recommendations at the end of each, but not all chapters clearly state the type of problem (i.e., traditional or nontraditional) or the specific nature of each failure (i.e., strategic or tactical, Type A or Type B). While some cases are very clearly one type or another—tactical or strategic, or traditional or nontraditional—there are cases in which the types of failure are more difficult to discern or more debatable. In such instances, clear articulation of the authors' overall assessments and reasoning might help individual readers, especially those with less knowledge or experience in intelligence. However, for academics or instructors in a classroom environment, this creates an opportunity for classroom discussion and debate on the categorizations that might be appropriate in each case.

None of these issues detracts from the book's quality and relevance for intelligence practitioners or scholars. It is also an excellent read for decisionmakers looking to understand their roles in the warning equation and the challenges intelligence faces in working to provide warning. The length of each case study does not detract from their overall accuracy or the relevance of the lessons and recommendations. Their conciseness does, however, make the chapters more digestible, indeed optimal for use in undergraduate, graduate, or professional training environments.

Likewise, a reliance on OSINT does not allow for information on what intelligence services knew, when they knew it, and the form of collection that provided, or failed to provide, that information. While some might argue that these are necessary elements of any complete case study, their absence does not affect the value and applicability of each chapter's conclusions and recommendations.

Finally, one of the book's most important contributions to intelligence studies is its consideration of strategic warning. Several authors cite Dahl's work and his theory of preventative action, which emphasizes the importance of detailed tactical warning in preventing threats, despite the usual calls from decisionmakers for more and better strategic warning.[a] None of the cases presented contradict Dahl's findings and generally support his emphasis on tactical warning and receptivity from decisionmakers. However, the Bergen AS case study (Russian acquisition of critical technology through a business transaction) demonstrates that strategic warning can also be highly effective. In the Bergen AS case, strategic warning on the threats posed by business acquisitions enabled the establishment of the legal framework eventually used to act on tactical warnings. As the editors state, "strategic warning requires strategic response."[b]

Overall, *Contemporary Intelligence Warning Cases* is an excellent addition to the scholarly literature on warning and deserves a place in organizational and personal libraries. It performs an essential service, filling gaps in the case study literature by adding a series of contemporary cases explored from various intellectual and national perspectives and touching on topics not commonly associated with intelligence warning. Furthermore, it adds distinct value to the field through its framework of intelligence success and failure, its discussion of strategic warning's importance, and its emphasis on the importance of the intelligence-policy relationship. Intelligence officers would do well to understand the policy space in which decisionmakers operate, and those decisionmakers need to form realistic expectations of what intelligence can provide with high levels of confidence, particularly against lingering and complex issues. ■

a. Dahl, *Intelligence and Surprise Attack*, 23–24.
b. Bronning and Stenslie, *Contemporary Intelligence Warning Cases,* 298.