Routledge
Taylor & Francis Group

Journal of Policing, Intelligence and Counter Terrorism

ISSN: 1833-5330 (Print) 2159-5364 (Online) Journal homepage: www.tandfonline.com/journals/rpic20

‘Predictive intelligence for tomorrow’s threats’: is predictive intelligence possible?

Erik J. Dahl & David Strachan-Morris

To cite this article: Erik J. Dahl & David Strachan-Morris (2024) ‘Predictive intelligence for tomorrow’s threats’: is predictive intelligence possible?, Journal of Policing, Intelligence and Counter Terrorism, 19:4, 423-435, DOI: 10.1080/18335330.2024.2404834

To link to this article: https://doi.org/10.1080/18335330.2024.2404834

Published online: 18 Sep 2024.

JOURNAL OF POLICING, INTELLIGENCE AND COUNTER TERRORISM
2024, VOL. 19, NO. 4, 423–435
https://doi.org/10.1080/18335330.2024.2404834

Routledge
Taylor & Francis Group

INTRODUCTION

‘Predictive intelligence for tomorrow’s threats’: is predictive intelligence possible?

Erik J. Dahl [a] and David Strachan-Morris[b]

[a]Department of National Security Affairs, Naval Postgraduate School, Monterey, USA; [b]History, Politics and International Relations, University of Leicester, Leicester, UK

ABSTRACT

The world is facing an ever-changing array of complex threats to international security. Yet intelligence agencies have a mixed record of anticipating these threats, while decision-makers have an equally mixed record of effectively acting on predictive intelligence when offered. Sometimes intelligence has provided a useful warning, such as Russia’s invasion of Ukraine, but at other times it has failed to anticipate critical events, such as the progress of fighting in Ukraine or the likelihood that a mob would carry out a deadly assault on the US Capitol building. And at still other times intelligence agencies appear to have provided warning, and yet policy makers failed to listen, such as before the Hamas attack on Israel on 7 October 2023. This special issue looks toward future threats and challenges and asks, how can intelligence better inform policy makers and help them anticipate and act upon future threats?

ARTICLE HISTORY
Received 12 September 2024
Accepted 12 September 2024

KEYWORDS
Intelligence; warning intelligence; predictive intelligence; national security; corporate intelligence; corporate security; intelligence failure

Introduction

It seems today that intelligence and surveillance are everywhere: government agencies monitor our social media posts, law enforcement organisations track our movements through the use of license plate readers and other tools, and corporations watch our activities and purchases online. Formerly secretive intelligence agencies appear to be more in the public eye than ever before, producing assessments and warnings about threats ranging from terrorism to nuclear weapons to unidentified flying objects (Office of the Director of National Intelligence, 2024).

And yet, despite this omnipresent surveillance, we continue to be surprised by events and threats that appear to have been unforeseen. How many of us would have taken seriously a warning in 2019 that the world would soon be engulfed in a global pandemic that would kill millions? Or in late 2020 in the United States, how many thought it possible that a violent mob could attack the US Capitol in Washington and attempt to overturn an election? Or to cite two more recent examples, how many of us only a few years ago could have foreseen that Russia would invade a European neighbour and still be fighting years later, or that Israel’s intelligence agencies could be taken surprise by a massive Hamas attack arising from its own back yard?

CONTACT Erik J. Dahl ejdahl@nps.edu

As these examples suggest, it is not at all clear whether intelligence agencies are any better today than they were in the past at warning of future threats. And when credible predictive intelligence has been offered, for instance in the case of future pandemics or the looming implications of climate change, it is often not effectively acted upon by policy makers. Is predictive intelligence possible? This paradox – of omnipresent intelligence, and yet continued surprise and intelligence failure – is at the heart of this special issue of the *Journal of Policing, Intelligence and Counter Terrorism*. The articles in this issue look toward future threats and challenges and ask, how can intelligence better inform policy makers and help them anticipate and act upon future threats? We invited contributions from both intelligence specialists and policy makers, and the five contributions included in this issue examine several issues related to this theme, including the role of warning intelligence in preventing terrorist attacks, intelligence and warning in the corporate sector, and the causes of intelligence failure in recent events such as the Russian invasion of Ukraine.

This introductory article attempts to provide context for the contributions that follow. It first examines the question of whether prediction should be considered a task for intelligence agencies and analysts in the first place. It next offers a brief overview of some of the many predictive intelligence tools and techniques available today, followed by a very tentative assessment of the state of the art of predictive intelligence. This article concludes by briefly summarising the five articles in this special issue.

Is prediction a job for intelligence?

Many episodes that have been seen as intelligence failures, such as Pearl Harbor and the 9/11 attacks, involve failures to forecast or foresee threats to come. But is it reasonable to expect intelligence agencies to anticipate future threats? Insiders often argue it is unfair to judge the US Intelligence Community (IC) on how well it can forecast or anticipate future events. Mark Jensen, for example, writes that 'Contrary to what may be desired, omniscience about the past and present and clairvoyance about the future are not legitimate expectations of the IC' (Jensen, 2012, p. 262). Although providing 'indications and warning' has long been a fundamental mission of military intelligence agencies, James Wirtz argues that it is too much to expect what he calls 'specific event predictions' (Wirtz, 2013, p. 550).

There has been a debate over whether forecasting and prediction should be considered part of the job for intelligence, or whether forecasts are useful or even desired by the recipients of intelligence (Ward, 2016). Woodrow Kuhns writes that policy makers have often been skeptical about the value of prediction and have preferred to get the facts (Kuhns, 2003). But often decision-makers are indeed looking for information about the future, such as warning of the potential for conflict between states, or about whether one policy might be more successful than another (Gleditsch, 2022; Meyer, Otto, Brante, & De Franco, 2010). As an article in the CIA's in-house journal noted with an apparent sense of resignation, 'there is no escaping the inevitable policymaker or agency-generated request to provide a predictive judgment or strategic warning on some issues of great national importance' (Batchelder, 2022, p. 17).

Perhaps in part as a response to the desire of consumers to anticipate threats to come, intelligence leaders have also been interested in the future, and in fact anticipating future

threats – prediction, if you will – has long been a goal of the intelligence community. As J. Peter Scoblic has described, Sherman Kent, often considered the father of modern American intelligence analysis, believed that the use of social science methods would enable the CIA and other agencies to help think more effectively about the future (Scoblic, 2018). Joseph Nye writes that this mission is often described as estimative intelligence, where the goal is not so much to make specific, point predictions, but to help policy makers by describing a range of possible outcomes (Nye, 1994).

A prominent example of this kind of work is what is called the *Global Trends* report series, published every four years by the National Intelligence Council to examine the state of the world in the next 15–20 years (Burrows, 2014). James Wirtz and Roger George went back recently to examine the forecasts made in the 2008 edition of *Global Trends*, and they found that, not surprisingly, the analysts got some things right – such as a warning that millions could die from a future global pandemic caused by a novel virus (Wirtz & George, 2022). But the 2008 forecast got a number of calls wrong, such as in its rosy prediction about the continuing spread of democracy around the world and failing to anticipate the rise of authoritarian governments and autocratic rulers today. The point, as Wirtz and George stress, is not to criticise the analysts of 2008 for failing to see clearly the world of the future, but simply to note that as predictions and forecasts peer farther into that future, they will inevitably suffer ever greater limitations.

The goal of estimating future threats has sometimes been described as the need to anticipate rare events, such as terrorist use of weapons of mass destruction (Ackerman et al., 2008; McMorrow, 2009). But more recently it has been seen as a need for 'anticipatory intelligence', which was described in the 2019 *National Intelligence Strategy* as intelligence that 'addresses new and emerging trends, changing conditions, and underappreciated developments' (Kerbel, 2019; Office of the Director of National Intelligence, 2019, p. 7).

Even when intelligence is accurate and a rival's options are limited, it can be virtually impossible for intelligence to predict exactly which option they will take. For example, in the US 2007 National Intelligence Estimate on Iran's nuclear capabilities and intentions, the US Intelligence Community assessed that Iran had halted its nuclear program; one of the key judgements said:

> E. We do not have sufficient intelligence to judge confidently whether Tehran is willing to maintain the halt of its nuclear weapons program indefinitely while it weighs its options, or whether it will or already has set specific deadlines or criteria that will prompt it to restart the program. (ODNI, 2007, p. 7)

The Intelligence Community was equally unsure about what might prompt Iran to halt its nuclear ambitions entirely. In a sub-paragraph to Key Judgement E, it said:

> Our assessment that Iran halted the program in 2003 primarily in response to international pressure indicates Tehran's decisions are guided by a cost-benefit approach rather than a rush to a weapon irrespective of the political, economic, and military costs. This, in turn, suggests that some combination of threats of intensified international scrutiny and pressures, along with opportunities for Iran to achieve its security, prestige, and goals for regional influence in other ways, might – if perceived by Iran's leaders as credible – prompt Tehran to extend the current halt to its nuclear weapons program. *It is difficult to specify what such a combination might be*. (ODNI, 2007, p. 7, emphasis added)

Thus, intelligence not only has to consider a rival's actions but also those of its own 'side' and those of its allies or partners. What is it that might trigger an opponent to take an assessed course of action or decide not to take that action? When exactly will that decision be made? For example, prior to the Russian invasion of Ukraine in 2022 the UK, US, France and Germany were roughly in agreement about Russia's capability, given what was known about the composition of forces near the Ukrainian border. But there was a very sharp division over intent. The US and UK were sure Putin intended to invade, whereas France and Germany were not, even though all four nations had access to much the same information (Phythian & Strachan-Morris, 2024, pp. 377–378). This allows the possibility that the differing assessments were a key factor in the decision to invade, as Putin saw an opportunity to exploit division. What might have happened (or rather not happened) if the four countries had been in agreement that an invasion was going to happen? The point here is that while intelligence may not be able to provide accurate warning or prediction, its value is in providing insight, preparing for likely scenarios, and enabling resilience to surprise.

This brief review strongly suggests that predictive intelligence is indeed a recognised and acknowledged job for intelligence agencies and analysts. But how is that job accomplished? The next section of this introductory article reviews a few of the tools and techniques that intelligence agencies use to warn of future threats.

Predictive intelligence tools and techniques

Spurred by perceived intelligence failures of the 9/11 attacks and the assessments of Iraqi weapons of mass destruction in 2003, the US intelligence community has attempted over the past two decades to improve the quality of its analytical products (Gentry, 2015). The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 called on the IC to adopt analytic tradecraft standards in order to improve the quality of intelligence – including warning intelligence – provided to decision-makers (US Congress, 2004). Much of this effort has been to train analysts in the use of what are called structured analytic techniques, or SATs, as a method of reducing analytical problems such as implicit bias; one of the goals is to help improve warning and predictive accuracy (Central Intelligence Agency, 2009).

A number of experts have recommended that the US intelligence community use tools such as the 'wisdom of the crowd' to leverage and aggregate forecasts by large numbers of analysts, potentially producing greater predictive accuracy than can be achieved by any individual intelligence officer (Ciocca et al., 2021). The British government, for example, created a forecasting tournament called the Cosmic Bazaar, in which 1300 individuals competed to offer predictions about questions such as whether China would invade Taiwan, or how widely COVID-19 infections would spread (Economist, 2021). A similar concept is the use of prediction markets, in which participants bet on the likelihood of future events (Mandel, 2019; Yeh, 2006).

Many of the efforts intended to help improve prediction use large data sets, computer algorithms, and artificial intelligence. An early example of such an effort was predictive policing: the use of data analysis to help law enforcement become more proactive than reactive. As the then-Chief of the Los Angeles Police Department put it, predictive policing promised to move law enforcement 'from focusing on what happened to

focus on what will happen and how to effectively deploy resources in front of crime, thereby changing outcomes' (Pearsall, 2010). More recently, however, critics have raised questions about the accuracy and fairness of predictive policing models, and some law enforcement agencies have found that predictive analytics provide no better intelligence and warning than traditional methods (Berk, 2021; Carleton, Cunningham, & Thorkildsen, 2020; Ibarra, 2020).

Some scholars argue that big data and artificial intelligence can only go so far in producing actionable forecasts and predictions. Lustick, for example, writes that the 'brute-force empiricism' associated with these tools is better at answering 'what, where, and when' questions, while policy makers need answers to the 'how and why' questions, which at least for now require the knowledge and expertise provided by human analysts (Lustick, 2022, p. 55). But despite these concerns, the use of artificial intelligence to predict future threats continues to be a growth business. After the 6 January 2021 attack on the US Capitol, for example, scholars and data scientists used these tools to attempt to predict future outbreaks of violence (Zeitchik, 2022).

One of the most exciting efforts to use AI to predict future threats was Raven Sentry, an AI tool used by the US military to predict insurgent attacks in Afghanistan in 2020 and 2021. The algorithm used was able to draw correlations between many different types of data, including weather, vehicle and population activity, social media posts, and commercial satellite imagery to predict when attacks would take place against district and provincial centres (Economist, 2024; Spahr, 2024). The program reportedly achieved an accuracy rate of 70% in predicting attacks before it was shut down with the US withdrawal from Afghanistan (Spahr, 2024, p. 103).

Such efforts as Raven Sentry raise many important questions about the use of AI for providing predictive intelligence, but the articles in this special issue suggest that one question is particularly important: How will decision-makers react to the predictions and warnings they receive from artificial intelligence? On the one hand, scholars have been concerned that policy makers might not – or perhaps should not – trust what they are told by an AI intelligence assistant (Lamparth & Schneider, 2024). But on the other hand, humans might come to trust AI too much. Thomas W. Spahr noted that in the case of Raven Sentry a problem arose when human analysts became accustomed to using the system, and there was a risk that they 'may stop critically examining a system's outputs and blindly trust it' (Spahr, 2024, p. 107).

Predictive intelligence for today and tomorrow

A number of scholars have argued that intelligence agencies have performed poorly in the past at anticipating and forecasting threats. Scoblic, for example, assesses that the Office of National Estimates at CIA, which Sherman Kent headed, had a 'decidedly mixed' record of anticipating and predicting threats to American national security (Scoblic, 2018, p. 99). Alexander Montgomery and Adam Mount have examined US intelligence's record in predicting the progress of foreign nuclear weapons programs and found that such predictions are often wrong (Montgomery & Mount, 2014).

Intelligence leaders such as former Director of Central Intelligence and Secretary of Defense Robert Gates have often lamented the inability of the intelligence community to predict the future actions and intentions of adversaries (Gates, 1996). Gates memorably

told cadets at West Point in 2011 that 'When it comes to predicting the nature and location of our next military engagements, since Vietnam, our record has been perfect. We have never once gotten it right' (Shaughnessy, 2011). According to Avner Barnea and Avi Meshulach, studies fail to show that the IC is getting any better today than in the past at preventing strategic surprises (Barnea & Meshulach, 2021).

Will new tools such as artificial intelligence enable intelligence agencies to make better predictions about tomorrow's threats? Not surprisingly, technology leaders and enthusiasts are optimistic. One technology company CEO said about AI-generated predictive analysis: 'This is probably going to be one of the biggest paradigm shifts in the entire national security realm – the ability to predict what your adversaries are likely to do' (Bajak, 2024). Other experts are more cautious; Zachary Tyson Brown, for example, writes that 'Looking past both the hype and the histrionics, we find that the reality of GenAI is neither quite so wondrous nor quite so bleak as either the proselytizers or the doomsayers would have us believe' (Brown, 2024, p. 2).

No matter how well new technologies and concepts are able to improve the ability of intelligence agencies to foresee future threats, a key lesson from the articles in this special issue is that while prediction and warning is clearly a job for intelligence, it is not a task that can be completed by intelligence agencies and analysts by themselves. For intelligence to have any value, it must be received and understood by a customer – a decision-maker who can act on that intelligence. One of us has written separately about the importance of policy maker receptivity toward intelligence in making intelligence actionable (Dahl, 2013), and the articles in this issue provide further evidence of the need for a strong intelligence–policy relationship if there is to be any hope that predictive intelligence can be used successfully to address tomorrow's threats.

The relationship between intelligence and policy is fraught with difficulty and opinions vary on how close this relationship should be: too close and there is the risk that intelligence could be tailored to specific policy preferences; too distant and there is a risk that intelligence lacks relevance. An ideal position is that intelligence has a 'seat at the table' or is 'in the room' where decisions and policy are discussed. In this way rather like the military extraction of orders process, in which 'mission' is derived from 'commander's intent', intelligence can determine the intent of policymakers (or at least the decisions they are trying to make) and be able to provide relevant intelligence upon which decisions can be made. Often, decisions are made without intelligence input, but intelligence still has a role in providing assessments to support the implementation of those decisions (support in the sense of enabling them to be carried out, not in the sense of providing *post hoc* justification).

As one of us has written elsewhere, this can be achieved in the corporate world where the intelligence team has intimate knowledge of the business, its aims and capabilities (if it is an internal team) or acquires this during the contracting process or during the direction phase (if it is an external vendor) and can develop a sense of what is relevant and what is not (Strachan-Morris, 2013). This, then, can provide focus for the intelligence effort because knowing the interests, intentions, capabilities and even worldview of one's own side allows for more refined use of tools to develop indicators and warnings of signs that something is going to disrupt those interests or intentions. This is obviously more difficult to achieve in the national security context, with the multiplicity of policy

areas and agencies, but is not impossible at the top level. It is, however, a model that can be transposed to military and law enforcement environments.

As we have discussed, apparent intelligence failures harm this relationship; if intelligence is unable to warn of, or predict, hazards then it can lose credibility. But intelligence has an important role to play in the post-surprise environment as a means of providing resilience and recovery. After a strategic surprise the question changes from 'What is going to happen?' to 'What is happening and what does that mean to us?' Intelligence, with its ability to contextualise and provide depth to current events, can provide on-the-spot reporting and assessment to enable decision-making about the response and recovery to take place in an informed environment. In a 'breaking news' situation, intelligence has value not only in the ability to provide subject matter expertise, but in being able to reach out to relevant assets, sources, and agencies to provide current reporting and assess how the situation may unfold (or at least develop some likely scenarios). So, what does this mean for intelligence and prediction or warning? The answer is that intelligence, if focused, can warn that 'something' is about to happen even if it can't say exactly what that is, although this in itself can provide further focus. This is where intelligence should both police the boundary between uncertainty and ignorance, and take active steps to manage that uncertainty (Canton, 2008; Phythian, 2012). When that 'something' has happened, even if by complete surprise, intelligence provides resilience by continuing to collect and analyse information, and provide assessments as events unfold.

The critical importance of the intelligence–policy relationship was dramatically reinforced on 7 October 2023, when Hamas carried out a complex, coordinated attack against Israel – an attack that has been seen as Israel's greatest intelligence failure since the Egyptian and Syrian attack on Yom Kippur almost exactly 50 years earlier. The attack came after most of the contributions for this special issue had been written, but enough information has since become available to enable us to undertake a preliminary examination of the lessons concerning predictive intelligence and the need for decision-maker receptivity.

That the Hamas attack was indeed a massive intelligence failure seems undisputed. The Israeli Defense Force intelligence chief has acknowledged it was an intelligence failure, and later said he would resign as a result of the failure (Fabian, 2023a; Gritten, 2024). The head of Shin Bet, the Israeli internal security service, also has taken responsibility for the failure (Fabian, 2023b). And an even stronger statement acknowledging intelligence failure came from a former chief of Mossad, the Israeli foreign intelligence agency, in an interview with PBS:

> It's not the first time we have had an intelligence failure. I mean, 50 years ago, we had an intelligence failure on the Yom Kippur War. That was a different story. This is a much more compelling story. The consequences are much more serious than was in the Yom Kippur War. (PBS News Hour, 2023)

Israeli intelligence agencies had received many indications and warnings prior to the attack about increased levels of activity by Hamas, but these warnings appear to have fallen on deaf ears among Israeli national security leaders. Among these warnings were reports from female soldiers assigned to border surveillance units who had observed unusual Hamas activity in the weeks before October, but these warnings were disregarded by their male superiors (Dettmer, 2023). Other warnings had come from Shin Bet, which was monitoring unusual Hamas activity in the Gaza Strip during the hours

leading up to the attack, but agency leaders concluded the activity likely meant that at most a small-scale attack was being planned (Bergman, Mazzetti, & Abi-Habib, 2023).

Even more damaging for Israeli intelligence are reports that the IDF had obtained detailed knowledge of Hamas's plans several weeks before the attack, but these warnings were disregarded because military leaders believed that new Israeli border security barriers would make such an attack unlikely to succeed ('IDF knew', 2024). These warnings may have been related to reports that Israeli officials had obtained Hamas's actual battle plan – a document known as 'Jericho Wall' – more than a year before the October 7 attack took place (Bergman & Goldman, 2023).

How could such a massive intelligence failure happen? How could one of the world's most sophisticated intelligence systems be unable to defend against a large-scale attack coming from a small strip of land that has been an intelligence focus for years – an attack that had been predicted by many different intelligence analysts and organisations? Full answers to these questions will need to wait for an official Israeli investigation, but the evidence that has been made publicly available so far suggests that the failure resulted from many of the same factors seen in previous intelligence failures including not only the 1973 Yom Kippur attack, but other disasters including the 9/11 attacks and the attack on Pearl Harbor (McLaughlin, 2023). These factors include complacency on the part of Israeli leaders, who assumed that Israel would be able to defeat any Hamas threat; an overreliance by Israel on technological surveillance tools; and a high level of operational security by Hamas, which reportedly planned the attack for more than a year under tight security, combined with an extraordinarily successful deception effort designed to convince Israeli leaders that Hamas was willing to work toward peace (Rubin & Warrick, 2023).

Ultimately, however, the Israeli intelligence failure stemmed from an unwillingness on the part of Israeli leaders to heed the warnings they received from their intelligence system. Predictive intelligence was there, but decision-makers were not willing to listen. As the articles in this special issue illustrate, such failures in the intelligence–policy relationship are all too common. It is our hope as the editors of this issue that such failures are not inevitable, and that scholarship such as is represented here will help us to understand better the limitations and capabilities of predictive intelligence, with the ultimate goal of helping protect us all from the threats and challenges of the future.

Reflections and remedies: summary of the contributions on warning and predictive intelligence

The contributions to this special issue address the core questions around prediction as a role for intelligence, techniques, and the intelligence producer-consumer interface from a range of theoretical perspectives. These contributions reflect on the nature of predictive and warning intelligence, highlighting areas of failure and discussing cases, and suggesting frameworks and approaches that will be of value to academics and practitioners alike.

Michael Ard looks at the intelligence failure(s) prior to the attack on the In Amenas gas production facility in Algeria in 2013. Using existing frameworks of analysis of intelligence failure, Ard shows how the corporate security industry suffers from additional pathologies to those seen in national security. In addition to the usual problem of lack of receptivity on

the part of the intelligence consumer and the inability of intelligence to 'join the dots' in time, the corporate security industry lacks the capability to acquire tactical-level intelligence on potential threats (particularly if these are only obtainable from secret sources) and legal complications around putting threats in writing. While this paints a somewhat gloomy picture of corporate intelligence, by exposing these hitherto unexamined issues Ard provides some avenues that corporate intelligence can seek to improve upon.

Nicole Drumhiller, Jim Burch and Casey Skvorc examine the individual level in their contribution, arguing that institutions need to look internally at individuals who work in what they term high-consequence environments. They make the important point that the actions of individuals, either deliberate or accidental, can have major consequences for security. They propose a two stage approach in which organisations first identify areas where an incident can have a major consequence (the example they give is a gas installation near a residential area) and then, in addition to identifying potential external threats, the organisation looks internally at individuals working in that area for signs that they might take action with malicious intent or where their behaviour might indicate fatigue or stress, which might lead to them causing some kind of accident. In taking this approach, Drumhiller *et al.* highlight an often-overlooked area of threat intelligence: the possibility of the 'unforced error' in which one's own actions cause a threat to manifest.

Masrur Mahmud Khan provides two new case studies on intelligence failure in the terrorist context. Taking the 2016 Holey Artisan attack in Bangladesh and the 2019 Easter attacks in Sri Lanka, Khan groups the failures within three broad themes: failure in intelligence activity itself and the inter-agency processes; political leadership and policy direction; and cognitive biases that undermined the quality of analysis and assessment. The article goes on to show how shocks like these can lead to reform – having identified problem areas, the nations in question were able to improve processes and there have been no similar attacks since.

Emmanuel Karagiannis continues the theme of cognitive biases and cultural blindspots in an analysis of the mass casualty attacks in Mumbai in 2008 and in Paris in 2015. Karagiannis argues effectively that a misunderstanding of the cost-benefit analysis from the terrorist perspective left the Indian and French intelligence agencies blind to the possibility of mass casualty attacks that might also be very costly to the attackers themselves. The article points out that terrorists are historically risk averse, in that the survival and escape of the attacking force has usually been a major planning consideration, but Islamic fundamentalist terrorism of the type seen in Mumbai and Paris views the 'martyrdom' of the attackers as an intrinsic part of the attack. The attacks were also different from previous forms of mass casualty attack in that they struck against multiple soft targets in both cities, which put the intelligence and security agencies off balance. From the religious perspective of the groups involved, there was a logic to the attacks that was not apparent to the security services of both countries, and this cultural blind spot was a significant contribution to the intelligence failure.

Mike Fowler's contribution examines the operational level intelligence in the run-up to the Russo-Ukrainian War in 2022. He examines the causes of the failure to correctly estimate the relative strengths of the Russian and Ukrainian forces, in that the former were over-estimated and the latter were under-estimated. He ascribes this to six causes:

blind spots due to focus on apparent high threats; a focus on the strategic and tactical levels led to a lack of focus on the operational level (i.e. how would both armies actualise any plans or use their power); leading on from this was a lack of discussion of logistical capabilities of both nations; deception obscured key information; and stovepiping resulted in an inability to see important operational level details; and finally, a lack of 'processing power' because there was only a finite number of analysts available. Fowler makes an important point here, that it is not enough to be able to predict what a state or organisation is going to do; there must also be a focus on how well they are likely to carry out their plans. The operational level of war is the important level at which strategy is turned into action, and intelligence must not overlook this.

While these contributions talk of intelligence failure, there is some cause for optimism. To better understand why intelligence has failed in particular cases, we can face the challenge set for intelligence by Richard Betts, who in 1978 asked whether intelligence failures may be inevitable (Betts, 1978). The articles in this issue suggest that although intelligence failures may indeed be inevitable in a general sense, each specific failure stems from particular causes and pathologies that can be addressed.

This introductory essay began by asking how intelligence can better inform policy makers and help them anticipate and act upon future threats. The answer is found by first examining and understanding the failures of the past, and then taking action to fix those problems for the future. Those fixes sometimes involve the use of new and exotic predictive tools and techniques, while at other times they require improvements to fundamental systems and processes such as the relationship between intelligence and policy. But we are confident, and we believe the authors of these contributions would agree, that fixes can be made, and improvement is possible, as intelligence professionals strive to provide predictive intelligence to help us prepare to meet the ever-increasing challenges of tomorrow.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID


Erik J. Dahl http://orcid.org/0009-0008-4484-3823

References

Ackerman, G. A., Agress, R., Ahern, B., Ambrose, F., Asal, V., & Bienenstock, E. (2008). *Anticipating rare events: Can acts of terror, use of weapons of mass destruction or other high profile acts be anticipated?*. Washington, DC: Joint Staff Strategic Multi-Layer Assessment.

Bajak, F. (2024, May 24). US intelligence agencies' embrace of generative AI is at once wary and urgent. *Associated Press*. https://apnews.com/article/us-intelligence-services-ai-models-9471e8c5703306eb29f6c971b6923187

Barnea, A., & Meshulach, A. (2021). Forecasting for intelligence analysis: Scenarios to abort strategic surprise. *International Journal of Intelligence and CounterIntelligence*, *34*(1), 106–133. doi:10.1080/08850607.2020.1793600

Batchelder, C. (2022). Introducing the kinetic predictive analytic technique. *Studies in Intelligence*, *66*(4), 17–27.

Bergman, R., & Goldman, A. (2023, November 30). Israel knew of Hamas's attack plan more than a year ago. *New York Times*. https://www.nytimes.com/2023/11/30/world/middleeast/israel-hamas-attack-intelligence.html

Bergman, R., Mazzetti, M., & Abi-Habib, M. (2023, October 29). How years of Israeli failures on Hamas led to a devastating attack. *New York Times*. https://www.nytimes.com/2023/10/29/world/middleeast/israel-intelligence-hamas-attack.html

Berk, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology*, *4*, 209–237. doi:10.1146/annurev-criminol-051520-012342

Betts, R. K. (1978). Analysis, war, and decision: Why intelligence failures are inevitable. *World Politics*, *31*(1), 61–89. doi:10.2307/2009967

Brown, Z. T. (2024). 'The incalculable element': The promise and peril of artificial intelligence. *Studies in Intelligence*, *68*(1), 1–7. https://www.cia.gov/resources/csi/studies-in-intelligence/studies-in-intelligence-68-no-1-extracts-march-2024/future-of-intelligence-the-incalculable-element-the-promise-and-peril-of-artificial-intelligence/.

Burrows, M. (2014, September 14). Predicting the future for the US government. *Slate*. https://slate.com/technology/2014/09/my-decade-writing-the-national-intelligence-councils-global-trends-report.html

Canton, B. (2008). The active management of uncertainty. *International Journal of Intelligence and CounterIntelligence*, *21*(3), 487–518. doi:10.1080/08850600802046939

Carleton, B., Cunningham, B., & Thorkildsen, Z. (2020). *The use of predictive analytics in policing* (Issue brief). Center for Naval Analyses. https://www.cna.org/reports/2020/10/use-of-predictive-analytics

Central Intelligence Agency. (2009). *A tradecraft primer: Structured analytic techniques for improving intelligence analysis*. Washington, DC: Central Intelligence Agency.

Ciocca, J., Horowitz, M. C., Kahn, L., & Ruhl, C. (2009). *How the U.S. Government Can Learn to See the Future*. Lawfare. https://www.lawfaremedia.org/article/how-us-government-can-learn-see-future.

Dahl, E. J. (2013). Why won't they listen? Comparing receptivity toward intelligence at Pearl Harbor and Midway. *Intelligence and National Security*, *28*(1), 68–90. doi:10.1080/02684527.2012.749061

Dettmer, J. (2023, November 21). Our warnings on Hamas were ignored, Israel's women border troops say. *Politico*. https://www.politico.eu/article/israel-border-troops-women-hamas-warnings-war-october-7-benjamin-netanyahu/

Economist. (2021, April 17). Welcome to the cosmic bazaar. *The Economist*. https://www.economist.com/science-and-technology/2021/04/15/how-spooks-are-turning-to-superforecasting-in-the-cosmic-bazaar

Economist. (2024, July 31). How America built an AI tool to predict Taliban attacks. *The Economist*. https://www.economist.com/science-and-technology/2024/07/31/how-america-built-an-ai-tool-to-predict-taliban-attacks

Fabian, E. (2023a, October 17). IDF Intel chief says he 'bears full responsibility' for not warning of Hamas attack. *The Times of Israel*. https://www.timesofisrael.com/idf-intel-chief-says-he-bears-full-responsibility-for-not-warning-of-hamas-attack/

Fabian, E. (2023b, October 16). Shin Bet Head says "responsibility mine" for Gaza failure. *The Times of Israel*. https://www.timesofisrael.com/shin-bet-head-says-responsibility-mine-for-gaza-failure-rockets-fired-at-tel-aviv/

Gates, R. M. (1996). *The prediction of Soviet intentions*. Studies in Intelligence. https://www.cia.gov/resources/csi/studies-in-intelligence/archives/the-prediction-of-soviet-intentions/

Gentry, J. A. (2015). Has the ODNI improved U.S. intelligence analysis? *International Journal of Intelligence and CounterIntelligence*, *28*(4), 637–661. doi:10.1080/08850607.2015.1050937

Gleditsch, K. S. (2022). One without the other? Prediction and policy in international studies. *International Studies Quarterly*, *66*(3), sqac036. doi:10.1093/isq/sqac036

Gritten, D. (2024, April 22). Israel military intelligence chief Quts over 7 October. *BBC News*. https://www.bbc.com/news/world-middle-east-68873227

Ibarra, N. (2020, June 23). Santa Cruz becomes first US city to approve ban on predictive policing. *Santa Cruz Sentinel*. https://www.santacruzsentinel.com/2020/06/23/santa-cruz-becomes-first-u-s-city-to-approve-ban-on-predictive-policing/

IDF knew of Hamas's plan to kidnap 250 before October 7 attack—Report. (2024, June 17). *The Jerusalem Post*. https://www.jpost.com/israel-hamas-war/article-806634

Jensen, M. A. (2012). Intelligence failures: What are they really and what do we do about them? *Intelligence and National Security*, *27*(2), 261–282. doi:10.1080/02684527.2012.661646

Kerbel, J. (2019, August 13). Coming to terms with anticipatory intelligence. *War on the Rocks*. https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/

Kuhns, W. J. (2003). Intelligence failures: Forecasting and the lessons of epistemology. In R. K. Betts & T. G. Mahnken (Eds.), *Paradoxes of strategic intelligence: Essays in honor of Michael I. Handel* (pp. 77–96). London: Routledge.

Lamparth, M., & Schneider, J. (2024). *Why the military can't trust AI*. Foreign Affairs. https://www.foreignaffairs.com/united-states/why-military-cant-trust-ai

Lustick, I. S. (2022). Geopolitical forecasting and actionable intelligence. *Survival*, *64*(1), 51–56. doi:10.1080/00396338.2022.2032959

Mandel, D. R. (2019). Too soon to tell if the US intelligence community prediction market is more accurate than intelligence reports: Commentary on Stastsny and Lehner (2018). *Judgment and Decision Making*, *14*(3), 288–292. doi:10.1017/S1930297500004320

McLaughlin, J. (2023, October 10). Why did Israeli intelligence fail? History suggests many causes. *The Cipher Brief*. https://www.thecipherbrief.com/why-did-israeli-intelligence-fail-history-suggests-many-causes

McMorrow, D. (2009). *Rare events* (JASON report JSR-09-108). MITRE. https://apps.dtic.mil/sti/pdfs/ADA510224.pdf

Meyer, C. O., Otto, F., Brante, J., & De Franco, C. (2010). Recasting the warning-response problem: Persuasion and preventive policy. *International Studies Review*, *12*(4), 556–578. doi:10.1111/j.1468-2486.2010.00960.x

Montgomery, A. H., & Mount, A. (2014). Misestimation: Explaining US failures to predict nuclear weapons programs. *Intelligence and National Security*, *29*(3), 357–386. doi:10.1080/02684527.2014.895593

Nye, J. S. (1994). Peering into the future. *Foreign Affairs*, *73*(4), 82–93. doi:10.2307/20046745

Office of the Director of National Intelligence. (2007). *Iran: Nuclear capabilities and intentions*. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20071203_release.pdf

Office of the Director of National Intelligence. (2019). *National intelligence strategy of the United States of America*. https://www.dni.gov/index.php/newsroom/reports-publications/item/1943-2019-national-intelligence-strategy

Office of the Director of National Intelligence. (2024). *Reports and publications 2024*. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024

PBS News Hour. (2023, November 1). *Some civilians trapped in Gaza allowed to cross into Egypt as Israeli airstrikes continue*. https://www.pbs.org/newshour/show/some-civilians-trapped-in-gaza-allowed-to-cross-into-egypt-as-israeli-airstrikes-continue

Pearsall, B. (2010). *Predictive policing: The future of law enforcement?* National Institute of Justice Journal. https://nij.ojp.gov/topics/articles/predictive-policing-future-law-enforcement

Phythian, M. (2012). Policing uncertainty: Intelligence, security and risk. *Intelligence and National Security*, *27*(2), 187–205. doi:10.1080/02684527.2012.661642

Phythian, M., & Strachan-Morris, D. (2024). Intelligence & the Russo-Ukrainian war: Introduction to the special issue. *Intelligence and National Security*, *39*(3), 377–385. doi:10.1080/02684527.2024.2330132

Rubin, S., & Warrick, J. (2023, November 13). Hamas envisioned deeper attacks, aiming to provoke an Israeli war. *Washington Post*. https://www.washingtonpost.com/national-security/2023/11/12/hamas-planning-terror-gaza-israel/

Scoblic, J. P. (2018). Beacon and warning: Sherman Kent, Scientific Hubris, and the CIA's Office of National Estimates. *Texas National Security Review*, *1*(4), 98–117. doi:10.15781/T2J38M448

Shaughnessy, L. (2011, February 26). Defense secretary warns against fighting more ground wars. *CNN.com*. http://www.cnn.com/2011/US/02/25/gates.west.point/index.html

Spahr, T. W. (2024). Raven Sentry: Employing AI for indications and warnings in Afghanistan. *Parameters*, *54*(2), 95–109.

Strachan-Morris, D. (2013). The intelligence cycle in the corporate world: Bespoke or off-the-shelf? In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 119–133). Oxford: Taylor & Francis.

US Congress. (2004, December 17). *Intelligence reform and terrorism prevention act of 2004, public law 108-458*. https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf

Ward, M. D. (2016). Can we predict politics? Toward what end? *Journal of Global Security Studies*, *1*(1), 80–91. doi:10.1093/jogss/ogv002

Wirtz, J. J. (2013). Indications and warning in an age of uncertainty. *International Journal of Intelligence and CounterIntelligence*, *26*(3), 550–562. doi:10.1080/08850607.2013.780558

Wirtz, J. J., & George, R. Z. (2022). Assessing futures intelligence: Looking back on global trends 2025. *Political Science Quarterly*, *137*(3), 481–510. doi:10.1002/polq.13354

Yeh, P. F. (2006). Using prediction markets to enhance US intelligence capabilities. *Studies in Intelligence*, *50*(4), 1–24. https://www.cia.gov/resources/csi/static/Prediction-Markets-Enhance-Intel.pdf.

Zeitchik, S. (2022, January 6). The battle to prevent another Jan. 6 features a new weapon: The algorithm. *The Washington Post*. https://www.washingtonpost.com/technology/2022/01/06/jan6-algorithms-prediction-violence/