# DOES CANADA HAVE ANYTHING IN THE WAY OF A STRATEGIC WARNING INTELLIGENCE CULTURE (AND DOES IT NEED ONE)?

*Dr. John Gilmour, Professional Development Institute – Ottawa University, Canada*

## Abstract

During the Cold War, Strategic Warning Intelligence (SWI) was a necessary and recognized function within the intelligence community given the threats posed by conventional Warsaw Pact forces in Western Europe and Soviet ballistic missiles. With the end of the Cold War, the focus of intelligence shifted to tactical or operational issues against known threats, and the SWI function and expertise atrophied as a result. With today's expanding and more complex threat environment, this article examines whether SWI capacities should be reintroduced in order to apprise decision makers of trending threats to national security, albeit based on faint signals, so the necessary policy decisions can be made and prioritized to mitigate said threats in a timely manner.

"It's tough to make predictions, especially about the future."
– Yogi Berra

Though perhaps not facing the same degree of definitional challenges the term 'terrorism' has given rise to over the decades, 'intelligence' has also come to mean something different to different communities. This is likely reflective of the fact that 1) it can apply to strategic, operational, and tactical levels; 2) be considered a product, a process, a mission, and an organization; and 3) it has application and a role in military, national security, law enforcement, and political, economic, and commercial mandates. It may focus on the collection of information others may not want you to know or, conversely, the protection of information you may have from getting into the hands of others. The resulting knowledge derived from intelligence ideally serves to better manage ones operating environment, so in "its simplest terms, intelligence is knowledge and foreknowledge of the world around us" (Central Intelligence Agency [CIA], 1991, p. vii).

For the purposes of this article, as distinct from strategic intelligence, current intelligence, estimative intelligence or tactical intelligence, strategic warning intelligence (SWI) is defined as "communication to senior national decision makers of the potential for, or actually impending, events of major significance to national interests, and recommendations that leaders consider making policy

decisions and/or taking action to address the situation" (Gentry & Gordon, 2019, p. 12). As such, it is considered *the* premier task of intelligence (Gentry & Gordon, 2019, p. 11), as it is presumed policy or decision makers would prefer to implement a response to an emerging issue or threat before being forced to do so under less than ideal circumstances. As noted by Lowenthal (2015), the key word is 'strategic,' suggesting there is something involved of sufficient gravity or importance as to put the nation at risk.

A review of various sources related to the conduct of SWI-type activity suggests that terminology associated with its processes and functions has yet to be standardized. In some cases, for example, a structured process to predict the future is referred to as 'horizon scanning' while in others it is termed 'foresight,' 'future(s) thinking,' or 'indications intelligence.' That said, foresight analysis is typically regarded as a process-based approach for examining and narrowing down possible outcomes in a future scenario by applying traditional research or analysis that results in estimates based on probability. Horizon scanning focuses more on the identification of emerging 'signals' or indicators. Both sub-disciplines and processes can be applied for the purposes of SWI.

Given SWI is considered the key outcome of the intelligence process as it relates to the setting of national security policy, one would assume Canada's national security agencies and military would both embrace the need for, and have the necessary capacities to undertake, strategic warning analysis.

But is this the case?

In an attempt to answer this question, this article will look at the nature of strategic warning intelligence, why it requires expert analytical capacity as opposed to 'line' analysis, the challenges in delivering warning messages to decision or policy makers, and what could be done to address current challenges associated with strategic warning capacities in Canada.

## The Nature of Strategic Warning Intelligence

In a historical context, the glory days of SWI occurred in the midst of the Cold War. With the memories of Pearl Harbour and the invasion of South Korea still fresh in western military and political mindsets, there was a demonstrated need on the part of western allies to mitigate the possibility of a surprise attack by the Soviet Union or Warsaw Pact countries in either a conventional military sense against Western Europe, or ballistic missile attacks against the North American continent or Western Europe. Key indicators related to changes in force strength

(capacity) and unit mobility were monitored on a regular basis. The *intent* of Soviet leadership at any given time was much harder to ascertain (placement of missiles in Cuba, the decision to invade Afghanistan or possibly Poland). Nevertheless, it is somewhat ironic that the golden age of SWI took place when the strategic level threats during the Cold War period were clearly well identified. However, with the fall of the Soviet Union and a reduced risk of state-on-state conflict, and during the 1990s when the threat posed by jihadist-based terrorism became something more than just faint signals, it is suggested a demand for SWI declined significantly.[1] There are a number of key reasons for this. First, although the threat spectrum became more complex in the post-Cold War environment (as noted by former CIA Director James Woolsey in 1993, there were now a greater number of 'snakes' as opposed to one 'dragon'), and while there were exceptions such as the rapid emergence and success of the Islamic State of Iraq and the Levant (ISIL), the threat spectrum for the next thirty years was reasonably consistent — espionage and influence activities, terrorism and insurgency in its various guises, concerns related to the proliferation of weapons of mass destruction (WMD), and, on the periphery, threats posed by extreme right-wing or left-wing communities. Intelligence efforts were inclined to focus on specific groups, individuals or ideologies that were more or less 'known' in the verbiage of Donald Rumsfeld, albeit in support of broader preventative strategies. Second, with reference to Lowenthal's previously noted observation, the threat posed by transnational terrorism that has consumed the lion's share of the intelligence bandwidth in the post 9/11 environment did not represent an existential threat to western countries as did a Soviet ballistic missile strike. Third, the intent of transnational terrorist groups has been clearly articulated through videos, fatwahs, speeches, etc. The capacity to engage in individual attacks is perhaps less clear, but, other than the use of aircraft as weapons on 9/11, terrorist attacks continue to use easy-to-obtain weapons that result in relatively low levels of lethality. The possible use of WMD by such groups has not been totally discounted but is seen as increasingly unlikely.

[1] Gentry and Gordon (2019) suggest that 9/11 was not a strategic intelligence warning failure. Rather, the US intelligence community repeatedly warned that an Al-Qaeda attack on the US was imminent but did not identify specific attack-related activities or planning. So, while SWI got it right in terms of the possibility of an attack on the US homeland, tactical intelligence was not able to determine date, time, or place. Furthermore, the 1993 attack on the World Trade Centre had already demonstrated jihadist terrorists had the capacity and intent to attack the US homeland. (p. 12)

Consequently, SWI capacities in western countries, both organizationally and cognitively, and the associated training that went along with it, appear to have atrophied as a result.

Today, however, the threat spectrum is expanding in ways that fall outside the norms of the past few decades. In the geopolitical realm, there is an undeniable increase in more traditional state-on-state competition, possibly elevating to conflict, including the associated and ongoing application of soft-war elements of hybrid warfare directed towards western countries. Threats to economic security, the impact of climate change on national security and geopolitical interests (e.g., the Arctic), and the call for enhanced health or 'bio' security in a post-COVID environment have collectively resulted in a significantly more complex and complicated security environment. The scope of these threats requires both whole-of-government and indeed whole-of-society based strategies and policies to mitigate them (Gilmour, 2021). Given the policy and security risks and impacts of second, third, and fourth-degree effects — political, economic, environmental, social, and the personal intangibles associated with the agendas and intentions of individual leaders within this new security environment — and how these threats and risks are to be prioritized, it is presumed policy, and decision makers expect to be apprised of emerging threats before they are forced to do so under less than optimal circumstances.

Does this suggest the need for a re-birth of SWI capacity within Canada once again? If so, how could this be shaped? Before this is examined, however, it is important to consider a number of key elements associated with SWI.

First, any intelligence officer will tell you that an attempt to provide intelligence clients with anything in the way of 'prediction' is heading down a slippery slope. Instead, the purpose of SWI is to identify trends of growing importance, often based on the faintest of signals, so that senior decision makers can make informed decisions as far in advance as possible to mitigate a trending threat. Rather than typical line or day-to-day analysis required to examine the specifics associated with a current crisis, SWI helps decision makers rationalize the need for resources and strategic policy decisions necessary to position a government in as advantageous position as possible relative to an emerging or trending threat. In this sense, SWI is not about prediction but more about enhancing a decision-maker's ability to diagnose trending threats and reduce uncertainties about potentially unfolding events (Gentry & Gordon, 2019, p. 114). SWI assessments can be grounded in the language of probabilities and risk assessment supported by rigorous and expert-based analysis. It can determine whether emerging issues

lend themselves to a policy response or if they are beyond the scope of any sort of management control and what the potential costs may be of not responding to an emerging threat at all. What sort of policy response may be most appropriate: diplomatic, military, technological, aid? Can the threat be managed unilaterally or is a multilateral effort required? Rather than prediction, even if decision makers are not willing to take any concrete action at the time, a recognition of the need to continue to monitor a situation can be considered something of a win.

Another key question for SWI practitioners is: what is the optimum temporal horizon for SWI analysis? In the simplest terms, it is suggested the temporal optimum is between 'not too early' and 'not too late.' There is a balance that recognizes the need to provide decision makers with adequate time to develop mitigation strategies with all that that entails, and the reality that decision makers are largely focused on agendas that are centred in the here and now. Issues that are expected to become a problem fifteen years hence are not likely to get much traction to undertake mitigation efforts unless one's client is an exceptionally enlightened individual (and even if they are, it is likely their political colleagues who are required to endorse mitigation plans are not). The analytical horizon should not extend so long that the first impulse of decision makers is to put things on the shelf. In practice, it appears that anything between a six-to-twenty-four-month analytical horizon best serves both the analytical/intelligence and decision-making communities.

Next, at what point is it appropriate to transfer an emerging threat from SWI analytical desks to what can be considered day-to-day, line analytical desks, assuming the SWI function is conducted by a distinct SWI unit? This is to avoid SWI desks gradually evolving into line analytical desks or assuming line analytical functions, as opposed to remaining dedicated to a SWI mandate.

SWI can also point to where support functions within the intelligence structure (IT and data assets, linguistic capacities, training, siting of forward deployed resources) need to be positioned in support of responding to emerging threats and as part of the policy response process.

Finally, and as is commonly stated, 'your opponent gets a vote.' SWI analysts must remain cognizant that an adversary could be actively engaged in relatively sophisticated denial and deception efforts to hide broader strategies. Adversaries are most likely aware of a target government's weaknesses and vulnerabilities and how individual decision makers may act in a given situation. Ideally, rigorous analysis will serve to uncover true intentions, despite attempts at deception.

In summary, the objective of SWI efforts is to avoid the situation where slow, evolutionary movements of small individual events that escape the view of day-to-day line analysts and that on their own do not signal ‘crisis’, ultimately come together at some point to result in just that.

## The Need for Analytical Expertise

This gets to the ongoing debate of whether it is better to have analysts that are ‘generalists’ or ‘experts.’ In the opinion of academics and practitioners associated with the SWI function, there is no question (Gentry & Gordon, 2019, p. 217–224; Grabo & Goldman, 2015, p. 102–112; McCarthy, 1998). “Substantive expertise is critical to strategic warning analysis. Analysts need expertise to adequately monitor enduring warning problems for important changes… and assess anomalies that may become warning issues of the future” (Gentry & Gordon, 2019, p. 223). Expertise and experience on the part of individual analysts is key in the application of the different types of SWI structured analytical methodologies. These can include, by way of example, alternative futures analysis, the cone of plausibility, high impact/low probability analysis, indicators analysis, What-If analysis, and key assumptions checks. There is a need to understand political cultures and the perceptions of individual leaders, underlying political motivations and incentives, military doctrines, technical development, and the role of opposition groups and internal threats facing governing bodies. Mary McCarthy (1998) adds that warning intelligence “requires laborious, methodological, rigorous analytical work; it requires imagination; and it requires a diversity of outlooks” (para, 9). And while it is desirable to have SWI analysts that are considered subject-matter experts that are comparable to those in academia, their efforts are not simply an academic exercise. Rather, analysts in the intelligence community are also obliged to translate their assessments into actionable intelligence products, requiring a good understanding of the decision making and policy communities that ultimately serve as the analyst’s clients. That said, academic sources should also be engaged where possible as a ‘systems check’ on hypothesis or theories that are developing within the intelligence community.

But the completion of analysis is only half the battle. As reflected in the next section, demonstrating the relevance of a warning assessment to decision makers is perhaps the most challenging part of the process. While adequate collection and analysis are core functions, persuasive communication of concerns to decision makers is the point where strategic warning intelligence most often falters.

Unless it can be convincingly communicated why and how an emerging trend is important and requires some form of action on the part of decision makers, an assessment is of little use. Expertise and analytic due diligence are essential to sell the product. Assessments need to adequately address the 'So what?' question posed by decision makers, so they can, in turn, consider the degree they need to formulate a 'Now what?' response. As summarized by McCarthy (1998), "[n]either the identification nor the communication of the threat, which are two distinct phases of the warning process, can be done in a haphazard way. Each step must be deliberate, carefully constructed and planned" (para, 1).

## Client Receptiveness

Various sorts of cognitive challenges on the part of both analysts and intelligence consumers in the application of any sort of intelligence program have been identified in numerous sources over the years, and it is appreciated they must be recognized and acknowledged as a feature of the SWI processes as well. Those faced with an SWI mandate, however, face a number of daunting hurdles when trying to get some traction with decision makers on issues that are the result of faint signals.

First, as noted by Grabo (2004), "[w]arning is an intangible, an abstraction, a theory, a deduction, a perception, and a belief …. it is not based on facts" (p. 4). An assessment based on probabilities is a creature with the need to consider a broad range of variables and factors and how they may roll out over time — political, economic, social, military, and especially the foibles of individual leaders. This analytical complexity is compounded when, as noted, the possible impacts of second, third, and fourth effects of possible future events need to be considered in the course of an analysis. Decision makers are obviously not in a position to craft actionable and tangible policy responses to a trending threat concern if advised events could go this way or that way in terms of a possible outcome. In order for SWI analysis to result in something that leads to an assessment that is actionable, decision makers must be presented with something that resembles at least a best guess. This is where the intangibles of analytical rigour, expertise, experience, credibility (based on past performance), and communication skills are called upon from the SWI analytical community. The irony, as noted by Dahl (2013), is that decision makers are more often prone to act on specific tactical-level type information, something that SWI is not in a position to provide. This leads us to the next challenge.

Decision makers are almost exclusively focused on the here and now. During my tenure in Canada's national security community, requests for information from 'the centre' pertained either to 'What's happening?' or 'What just happened?', and rarely, if ever, 'What could happen?', at least at the strategic level. This is not a problem limited to Canada. As far back as 1981, the Deputy Director of the CIA, Bobby Inman, observed when trying to develop a five-year plan for the Agency that "no administration would likely care much about that far in the future. Immediate problems received 99 percent of the available attention" (Woodward, 1987, p. 159). And where it is understandable that decision makers prefer not to be forced into crisis management based on intelligence for something that was unanticipated but imminent, they would be especially reluctant to do so on something that could be an issue two-years hence. This is especially challenging in Canada where the vast majority of elected decision makers have neither any actual familiarity with how intelligence functions nor military experience, and in some cases actually look at the national security community with some suspicion.

The main problem is that decision makers are focused on issues that concern them now, while the *raison d'etre* of strategic warning intelligence is to identify issues they do not know about yet, but which should concern them greatly. Gentry and Gordon (2019) refer to this as "the tyranny of current intelligence" (p. 225). For the most part, elected decision makers strive to deliver something tangible within short-term agendas. Taken collectively, they tend not to focus on national security or intelligence-related issues until it becomes important to them. Intuitively, they are not looking for issues coming out of left field that may require them to make some unanticipated hard decisions or skew existing or planned policies and programs that were the outcome of some comprehensive and time-consuming up-front efforts. Furthermore, decision makers likely feel awkward when faced with the various degrees of ambiguity that are characteristic of early-warning assessments. It is a function of the SWI community, who deals with said ambiguities on a daily basis, to provide decision makers with best judgements in terms of the who, when, where, and what, in order to enable decision makers to make informed decisions on what to do next.

The relationship is captured succinctly by Jack Davis (2007), a recognized SWI expert, when he states

> Strategic warning, to be effective, has to be credible in assessing contingent dangers … Intelligence analysts must issue a strategic warning far enough in advance of a feared event for officials to take protective

> action, yet with credibility to motivate them to do so. No mean feat. (p. 174)

The SWI analyst has quite the tightrope act to follow. They need to be listened to in terms of conveying the seriousness of the threat, without relying on hyperbolic language that may seem either excessive or irritating to a decision maker.

## Other Key Challenges

The identification of indicators to be monitored or the incorporation of different economic or societal factors in more process-based SWI analysis is based on a number of key assumptions. Consequently, one of the initial challenges associated with the SWI process is to determine whether current assumptions will remain valid for the temporal horizon or purposes of the analysis. Are the assumptions about the intentions or objectives of an adversary, correct? Pearl Harbour and the 1973 Yom Kippur war are examples of where they were not. Is the analysis based on the assumption an adversary is a rational actor (Kim Jong-un)? A lack of solid confidence in the assumptions can fundamentally skew the rest of an analysis going forward and raise questions on the part of decision makers.

Of course, intelligence functions, including SWI, cannot always predict the ‘bolt out of the blue’ or ‘black-swan’ events. The spark and extent of the Arab Spring, and the surprising initial success of ISIL that brought it to the gates of Baghdad are but two recent examples. Given their nature and possible sources, cyber attacks represent the greatest challenge in this regard. They do not allow for the traditional sort of preventative analysis associated with SWI, as they do not give off any signals, feint or otherwise, of an impending attack. They have no barrier to their implementation and represent a threat that can do significant damage with little effort or planning. Cyber attacks provide for anonymity, deniability, can target both government and private sectors, and seek a number of potential outcomes — ransom and infrastructure damage to support broader hybrid warfare strategies, to name a few.

## What Can Be Done to Increase Canada’s SWI Capacity?

Assuming there is a demonstrated need and a willingness to improve Canada’s SWI capacity, what could that look like?

It is generally recognized that an SWI function, whether centrally located or embedded in individual agencies, needs to be separated organizationally from what is considered line or day-to-day analysis. This is to mitigate against the SWI function gradually morphing into just another line analysis unit through task-related osmosis if SWI resources are frequently used to support line analysis capacity in response to the tight reporting deadlines they typically face. Ideally, SWI analysts would be able to devote their full time to the SWI function and be functionally independent and flexible from the processes and potentially limiting organizational structures or processes of traditional intelligence agencies. The application of the 'intelligence cycle' need not be strictly adhered to, and consultation with various external groups (academia, NGOs, the private sector) would be encouraged. One good outcome of the current lack of SWI capacity within Canada is that there is no risk of a dedicated SWI unit duplicating or poaching the turf of other SWI units.

SWI is best developed adopting a 'whole-of-government' approach. If the function is centred in individual agencies, the SWI function may only focus on issues covered by the mandate of that agency. In the interest of adopting such an 'all-source' intelligence approach, it would be beneficial to have a centralized SWI unit with representation from a number of different agencies, akin to the structure of Canada's Integrated Terrorism Assessment Centre (ITAC). Such a fusion-centre approach would provide for a structure that enables a rapid exchange of information amongst subject matter experts, hopefully without a strict adherence to the individual agendas of the agencies represented. It would also make sense to have it structured or sub-divided organizationally along geographic lines as opposed to subject matter (political, economic, military). As the intent of SWI is to direct the attention of high-level decision makers to a variety of potential emerging issues, perhaps such a unit would be best located in the Privy Council's Security and Intelligence or Intelligence Assessment Secretariat (IAS) branches. Locating the SWI function in PCO would also give the unit an element of instant status and credibility and would help mitigate against the possibility the unit would become an analytical backwater. It would also give the unit some bureaucratic clout in ensuring all necessary information was made available to it by other agencies.

Another possible model to follow is Singapore's (like Canada, also considered a mid-level power) successful Risk Assessment and Horizon Scanning Program (RAHS).

The objective of the RAHS program is to enable the government to detect weak signals and indications of impending 'shocks' through collaboration between a number of different communities in the interest of informed analysis (Quiggin, 2007). Instead of being located within a specific department, RAHS is a technologically networked approach with a number of government agencies being interconnected through a common IT system, with the parallel capacity to reach out to both the private and academic sectors. Each user feeds the system with information from its own sources, allowing access by others. It enables users to process large amounts of information and perform a variety of analysis by providing quick access to required information. The process leads to the identification of a number of high risk/ low-probability events or 'wild cards' that are ultimately filtered down to a limited number of issues by a secretariat, then presented to decision makers for further consideration. This is a function that would be necessary in the construct of any SWI unit.

During the Cold War, the identification and application of key indicators (or red flags, or trip wires) to a specific geographic or subject matter area formed the core of SWI analysis and resulting assessments. This approach was assessed as being generally successful and manageable (Grabo & Goldman, 2015), and although the focus was admittedly narrower relative to today's threat environment, such an approach likely still has application augmented by other analytical techniques in the interest of analytical due diligence. Training in the use of strategic indicators or strategic warning should also be introduced as separate courses into intelligence and military analyst training programs in order to emphasize it is a distinct function from day-to-day 'line' intelligence.

The actual construct of individual SWI assessments also needs to be considered. The record will show that a consensus-based approach to assessments has the potential to result in watered-down narratives or 'group-think based analysis, potentially undermining the urgency of the message. An institutional acceptance that dissenting views can and should be reflected in SWI assessments is likely a more constructive approach although it may serve to add to a decision maker's angst regarding the ambiguity of the issue depending on the degree the dissenting opinion diverts from an assessment's main message.

## Conclusion: Does Canada Need a Dedicated SWI Capacity?

U.S. and U.K. administrations that have a greater interest in preserving and protecting their more comprehensive global interests have a spotty record when it comes to the contribution and sustainability of post-Cold War dedicated SWI

programs and organizations within their respective intelligence communities. Often, they are constituted in the aftermath of an issue that is perceived as an intelligence failure (an organizational response to the issue that is so often seen as the solution), only to peter out for a number of reasons after a time — strategic surprises continue regardless, lack of executive support for the program, subject matter experts prefer to remain in established line analytical units, etc. Presumably, Canada, with its comparatively limited global interests (and quite frankly a more-than-modest reliance on shared reporting from partner agencies), can, and has, serve(d) its national security obligations over the past three decades without the need for some formal, dedicated SWI capacity.

But as noted, the threat spectrum is expanding into non-traditional areas such as economic, environmental, and health-related security, and the potential for state-on-state conflict is increasing. Emerging strategic threats are often transnational in nature and involve a number of different communities and players, often blurring the distinction between external and domestic environments. The impact of social media has demonstrated that simmering local or regional issues can quickly explode into a crisis situation, and policy makers are pressured to 'do something!' in increasingly shorter periods of time and under less-than-ideal conditions. There is no question that Canada will become engaged in at least some of these issues. This raises some key questions. Given the presumed nexus of SWI to a country's strategic interests, have Canada's key strategic interests been clearly articulated within the context of the current global environment to decision makers, other levels of government, and the general public? Do existing intelligence agencies have adequate resources and cognitive capacities to bring to bear on the faint signals associated with emerging threats, whether conventional or non-traditional, when faced with day-to-day analytical demands for current issues? Does the overarching obligation to provide decision makers with as much warning as possible on developing issues within this growing threat spectrum suggest there is, indeed, a need for an enhanced SWI within Canada's intelligence community? Is there enough SWI-related work to support the establishment of a dedicated-full time unit?

In the immediate post-COVID environment, western governments, including Canada, will be preoccupied with socio-economic issues. In parallel, however, ambiguous and seemingly innocent events will be taking place at some point on the globe that may ultimately coalesce into something that amounts to a threat of strategic proportions to Canadian interests. If over the course of the next few years there are clusters of intelligence 'surprises' or 'failures' (arguably COVID-19 being the most recent example), then decision makers, the media, and even

the general public — which in the case of Canada is typically not engaged much on issues of national security — may start to question the value or relevancy of Canada's intelligence agencies or seek to employ radical organizational remedies to fix the situation. Canada's SWI capacity is negligible at the present time, and arguably non-existent. At the very least, some thought by Canada's intelligence community and national security decision makers needs to be applied to addressing this situation. If not to demonstrate the ongoing credibility and relevancy of the intelligence community, then to at least ensure the government is proactively positioned in advance to mitigate against faint, but nevertheless, emerging threats to Canadians and Canadian interests.

## References

Central Intelligence Agency. (1999). *A consumer's guide to intelligence.* Office of Public Affairs.

Dahl, E. J. (2013). Why wont they listen? Comparing receptivity towards intelligence at Pearl Harbor and Midway. *Intelligence and National Security*, *28*(1), 68–90.

Davis, J. (2007). Strategic warning: Intelligence support in a world of uncertainty and surprise. In L. K. Johnson (Ed.), *Handbook of intelligence studies* (pp. 173–188). Routledge.

Gentry, J. A., & Gordon, J. S. (2019). *Strategic warning intelligence: History, challenges, and prospects.* Georgetown Press.

Gilmour, J. (2021, July). *Does Canada need a new national security policy?* Canadian Global Affairs Institute. https://www.cgai.ca/does_canada_need_a_new_national_security_policy

Grabo, C. (2004). *Anticipating surprise: Analysis for strategic warning.* University Press of America.

Grabo, C., & Goldman, J. (2015). *Handbook of warning intelligence.* Rowman & Littlefield.

Lowenthal, M. (2015). Strategic early warning: Where are we now? *Journal of Intelligence & Analysis*, *22*(2), 1–10.

McCarthy, M. O. (1998). *The mission to warn: Disaster looms, 7*(2), 17–31. http://cryptome.info/0001/mccarthy-mtw.htm

Quiggin, T. (2007). *Seeing the invisible: National security intelligence in an uncertain age.* World Scientific Publishing Co.

Woodward, B. (1987). *Veil: The secret wars of the CIA, 1981 – 1987.* Simon & Schuster.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/